PlateSpin® Protect 11.0.1

Guide de l'utilisateur

2 septembre 2014

www.netiq.com/documentation

Mentions légales

Octroi de licence

Les licences de PlateSpin Protect 10.4 ne peuvent pas être utilisées avec les versions antérieures de PlateSpin Protect.

Logiciels tiers

Consultez la page intitulée *PlateSpin Third-Party License Usage and Copyright (https://www.netiq.com/documentation/platespin_licensing/platespin_licensing_qs/data/platespin_licensing_qs.html)* pour plus d'informations sur les logiciels tiers utilisés dans PlateSpin Protect.

Table des matières

À propos de NetIQ Corporation

NetIQ, société Attachmate, est un leader mondial en systèmes et gestion de la sécurité. Avec plus de 12 000 clients dans plus de 60 pays, les solutions NetIQ permettent de tirer le meilleur parti des investissements en technologie et d'optimiser les processus IT afin de réaliser des économies significatives. Le portefeuille de l'entreprise comprend des produits de gestion reconnus pour l'automatisation des processus IT, la gestion système, la gestion de la sécurité, l'audit et le contrôle de configuration, l'administration d'entreprise et la gestion unifiée des communications. Pour plus d'informations, consultez le site www.netiq.com.

Contacter le support

Pour toute question concernant les produits, tarifs et fonctionnalités, contactez votre partenaire local. Si vous ne pouvez pas contacter votre partenaire, contactez notre équipe de support ventes.

Monde :	www.netiq.com/about_netiq/officelocations.asp
États-Unis et Canada :	888-323-6768
Courrier électronique :	info@netiq.com
Site Web :	www.netiq.com

Contacter le support technique

Pour tout problème spécifique au produit, contactez notre équipe du support technique.

Monde :	www.netiq.com/Support/contactinfo.asp
Amérique du Nord et du Sud :	1-713-418-5555
Europe, Moyen-Orient et Afrique:	+353 (0) 91-782 677
Courrier électronique :	support@netiq.com
Site Web :	www.netiq.com/support

Contacter le support en charge de la documentation

Notre objectif est de vous proposer une documentation qui réponde à vos besoins. Si vous avez des suggestions d'améliorations, cliquez sur le bouton **Add Comment** (Ajouter un commentaire) au bas de chaque page dans les versions HTML de la documentation publiée à l'adresse www.netiq.com/documentation. Vous pouvez également envoyer un message électronique à l'adresse Documentation-Feedback@netiq.com. Nous accordons une grande importance à vos commentaires et sommes impatients de connaître vos impressions.

Contacter la communauté d'utilisateurs en ligne

La communauté en ligne de NetIQ, Qmunity, est un réseau collaboratif vous mettant en relation avec vos homologues et des spécialistes de NetIQ. En proposant des informations immédiates, des liens utiles vers des ressources et un accès aux experts NetIQ, Qmunity vous aide à maîtriser les connaissances nécessaires pour tirer pleinement parti du potentiel de vos investissements informatiques. Pour plus d'informations, consultez le site http://community.netiq.com.

À propos de ce guide

Ce guide fournit des informations sur l'utilisation de PlateSpin Protect.

Public

Ce guide s'adresse au personnel informatique, notamment les opérateurs et administrateurs de centres de données qui utilisent PlateSpin Protect dans le cadre de leurs projets de protection de workload quotidiens.

Commentaires

Nous souhaiterions connaître vos commentaires et suggestions sur ce guide et les autres documentations fournies avec ce produit. Utilisez la fonctionnalité *Commentaires de l'utilisateur*, disponible en haut et en bas de chaque page de la documentation en ligne.

Documentation supplémentaire

Le présent guide fait partie de la documentation de PlateSpin Protect. Pour obtenir une liste complète des publications relatives à cette version logicielle, visitez le site Web de documentation en ligne du produit.

Documentation en ligne de PlateSpin Protect 11 (https://www.netiq.com/documentation/platespin_protect_11/)

Mises à jour de la documentation

La version la plus récente de ce guide est disponible sur le site Web de documentation en ligne de PlateSpin Protect 11 (https://www.netiq.com/documentation/platespin_protect_11/) :

Ressources supplémentaires

Nous vous recommandons d'utiliser les ressources supplémentaires suivantes disponibles sur Internet :

- Communauté des utilisateurs de NetIQ (https://www.netiq.com/communities/) : communauté Web traitant de divers sujets de discussion.
- Base de connaissances du support technique de NetIQ (https://www.netiq.com/support/kb/) : ensemble d'articles techniques détaillés.
- Forums d'assistance NetIQ (https://forums.netiq.com/forum.php) : sections du site Web dans lesquelles les utilisateurs peuvent discuter des fonctionnalités des produits NetIQ et partager des conseils.
- MyNetIQ (https://www.netiq.com/f/mynetiq/) : ce site Web propose des services et des informations sur PlateSpin. Vous pouvez ainsi disposer d'un accès à des livres blancs de grande qualité, vous inscrire à des émissions Web (webcasts) ou encore télécharger des évaluations de produit.

Support technique

Vous pouvez accéder au Guide de l'assistance technique (https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and) pour en savoir plus sur les règles et les procédures du support technique de NetIQ.

Utilisez ces ressources pour obtenir une assistance spécifique à PlateSpin Protect :

- Numéro de téléphone au Canada et aux États-Unis : 1-800-858-4000
- Numéro de téléphone en dehors des États-Unis : 1-801-861-4000
- Adresse électronique : support@platespin.com
- Informations spécifiques au produit : PlateSpin Protect Support (https://www.netiq.com/support/kb/product.php?id=SG_XPLATESPINPROTECT_1_2)

1 Présentation du produit

Cette section présente les informations suivantes :

1.1 À propos de PlateSpin Protect

PlateSpin Protect est un logiciel assurant la continuité des opérations et la reprise après sinistre qui protège les workloads physiques et virtuels (systèmes d'exploitation, intergiciels et données) à l'aide de la technologie de virtualisation. En cas de panne de serveur de production ou de sinistre, une réplique virtuelle d'un workload peut être rapidement mise en oeuvre au sein du *conteneur* cible (hôte de VM) et continuer à fonctionner normalement jusqu'à la restauration de l'environnement de production.

PlateSpin Protect vous offre les possibilités suivantes :

- récupérer rapidement les workloads en cas de problème ;
- protéger simultanément plusieurs workloads ;
- tester le workload de basculement sans perturber l'environnement de production ;
- rétablir les workloads de basculement dans leur infrastructure originale ou dans une infrastructure totalement nouvelle, physique ou virtuelle ;
- profiter des solutions de stockage externe existantes, telles que les SAN (sous-réseaux de stockage).

1.2 Configurations prises en charge

1.2.1 Charges de travail Windows prises en charge

PlateSpin Protect prend en charge la plupart des workloads Windows.

Les réplications par fichier et par bloc sont prises en charge, moyennant certaines restrictions. Reportez-vous à la Section 5.4, « Transfert de données », page 74.

Tableau 1-1 *Charges de travail Windows prises en charge*

Système d'exploitation	Remarques
Workloads de catégorie serveur	
Windows Server 2012 R2 Windows Server 2012	
Windows Server 2008 R2 (64 bits) Windows Server 2008 (64 bits)	Y compris les contrôleurs de domaine (DC) et les éditions SBS (Small Business Server)
Windows Server 2003 R2 (64 bits) Windows Server 2003 R2 (32 bits) Windows Server 2003, SP le plus récent (64 bits) Windows Server 2003, SP le plus récent (32 bits)	Windows 2003 nécessite le Service Pack 1 ou une version ultérieure pour la réplication par bloc.
Grappes (clusters) Windows	Reportez-vous à la section « Protection des grappes Windows » page 85 pour connaître les configurations de grappes spécifiques prises en charge.
Workloads de catégorie Poste de travail	
Windows 8.1 Windows 8	**AVERTISSEMENT :** vous devez sélectionner le mode de gestion de l'alimentation *Performances élevées* sur la source Windows 8 afin que le basculement et le rétablissement du workload fonctionnent correctement. Pour configurer le mode de gestion de l'alimentation à partir du Panneau de configuration Windows : 1. Sélectionnez *Tous les Panneaux de configuration* > *Options d'alimentation*. 2. Dans la boîte de dialogue permettant de *choisir ou personnaliser le mode de gestion de l'alimentation*, sélectionnez *Afficher les modes supplémentaires* > *Performances élevées*. 3. Fermez le panneau de configuration.

Versions internationales prises en charge : français, allemand, japonais, chinois traditionnel et chinois simplifié.

Prise en charge du microprogramme de workload (UEFI et BIOS) : PlateSpin Protect met en miroir la prise en charge Microsoft des workloads Windows basés sur UEFI ou BIOS. Il transfère les workloads (par bloc et par fichier) de la source à la cible tout en appliquant le microprogramme pris en charge pour les systèmes d'exploitation source et cible respectifs. Il procède de la même manière pour un rétablissement vers une machine physique. Lorsqu'une transition (basculement ou rétablissement) a été lancée entre des systèmes UEFI et BIOS, PlateSpin Protect l'analyse et vous informe sur sa validité.

REMARQUE : si vous protégez un workload UEFI et souhaitez continuer à utiliser le même mode de démarrage du microprogramme pendant tout son cycle de vie, vous devez cibler un conteneur vSphere 5.0 ou version ultérieure.

Vous trouverez, ci-dessous, des exemples du comportement de PlateSpin Protect lors de la protection et du rétablissement de systèmes UEFI et BIOS :

- Lors du transfert d'un workload UEFI vers un conteneur VMware vSphere 4.*x* (qui ne prend pas en charge UEFI), PlateSpin Protect fait migrer le microprogramme UEFI du workload vers BIOS au moment du basculement. Ensuite, lorsqu'un rétablissement est sélectionné sur une machine physique UEFI, PlateSpin Protect inverse la transition du microprogramme de BIOS vers UEFI.
- Si vous essayez de rétablir un workload Windows 2003 protégé vers une machine physique UEFI, PlateSpin Protect analyse cette possibilité et vous informe qu'elle n'est pas valide (en d'autres termes, la transition d'un microprogramme BIOS vers UEFI n'est pas prise en charge ; Windows 2003 ne prend pas en charge le mode de démarrage UEFI).
- Lors de la protection d'une source UEFI sur une cible BIOS, Protect fait migrer les disques de démarrage du système UEFI, qui étaient de type GPT, vers MBR. Le rétablissement de ce workload BIOS vers une machine physique UEFI a pour effet de reconvertir les disques de démarrage au format GPT.

1.2.2 Workloads Linux pris en charge

PlateSpin Protect prend en charge plusieurs distributions Linux.

La réplication s'effectue au niveau du bloc et pour ce faire, votre logiciel PlateSpin requiert un module `blkwatch` compilé pour assurer la protection d'une distribution Linux spécifique.

Certaines des versions de Linux prises en charge requièrent la compilation du module `blkwatch` PlateSpin pour votre kernel spécifique. Ces workloads sont appelés explicitement.

Tableau 1-2 *Workloads Linux pris en charge*

Système d'exploitation	Remarques
Workloads de catégorie Serveur Linux	
Red Hat Enterprise Linux (RHEL) 6.2	Transfert par bloc uniquement.
Red Hat Enterprise Linux (RHEL) 4 (32 bits)	Transfert par bloc uniquement.
Novell Open Enterprise Server (OES) 11, SP1 et SP2	**REMARQUE :** la version de kernel par défaut 3.0.13 d'OES 11 SP2 n'est pas prise en charge. Avant d'inventorier le workload, effectuez une mise à niveau vers la version 3.0.27 ou ultérieure du kernel. Transfert par bloc uniquement.

Systèmes de fichiers Linux pris en charge

Les systèmes de fichiers EXT2, EXT3, EXT4, REISERFS et NSS (workloads OES 2) sont pris en charge (transfert par bloc uniquement).

REMARQUE : les volumes codés de workloads sur la source sont décodés dans la machine virtuelle de basculement.

1.2.3 Conteneurs de VM pris en charge

Tableau 1-3 *Plates-formes prises en charge en tant que conteneurs VM*

Conteneur	Remarques
Grappe VMware DRS dans vSphere 5.5	◆ La configuration DRS doit être **Partiellement automatisé** ou **Entièrement automatisé** (mais ne peut pas être réglée sur **Manuel**). ◆ En tant que conteneur VM, la grappe DRS doit être constituée uniquement de serveurs ESXi 5.5 et peut uniquement être gérée par vCenter 5.5.
Grappe VMware DRS dans vSphere 5.1	◆ La configuration DRS doit être **Partiellement automatisé** ou **Entièrement automatisé** (mais ne peut pas être réglée sur **Manuel**). ◆ En tant que conteneur VM, la grappe DRS doit être uniquement constituée de serveurs ESXi 5.1 et peut uniquement être gérée par vCenter 5.1.
Grappe VMware DRS dans vSphere 4.1	◆ La configuration DRS doit être **Partiellement automatisé** ou **Entièrement automatisé** (mais ne peut pas être réglée sur **Manuel**). ◆ En tant que conteneur VM, la grappe peut utiliser une combinaison de serveurs ESX 4.1 et ESX**i** 4.1 et peut uniquement être gérée par vCenter 4.1.

1.2.4 Microprogrammes système pris en charge

PlateSpin Protect met en miroir la prise en charge Microsoft de l'interface UEFI. . Pour plus d'informations, reportez-vous à la Section 1.2.1, « Charges de travail Windows prises en charge », page 11.

1.3 Sécurité et confidentialité

PlateSpin Protect propose différentes fonctions qui vous aident à sauvegarder vos données et à accroître la sécurité.

1.3.1 Sécurité des données de workload lors d'une transmission

Pour sécuriser davantage vos données de workload, vous pouvez configurer la protection de workload afin de coder les données. Lorsque le codage est activé, les données répliquées sur le réseau sont codées avec l'algorithme AES (Advanced Encryption Standard).

Si nécessaire, vous pouvez configurer votre serveur PlateSpin pour qu'il utilise un algorithme de codage des données conforme à la norme FIPS (Federal Information Processing Standards) 140-2. Reportez-vous à la section « Activation de la prise en charge des algorithmes de codage de données conformes à la norme FIPS (facultatif) » du *Guide d'installation*.

Vous pouvez activer ou désactiver le chiffrement individuellement pour chaque workload. Reportez-vous à la section « Détails de protection de workload » page 54.

1.3.2 Sécurité des communications client/serveur

Étant donné que l'installation du serveur PlateSpin active le protocole SSL sur l'hôte du serveur PlateSpin, une transmission sécurisée des données entre votre navigateur Web et le serveur PlateSpin est déjà configurée sur HTTPS (Hypertext Transfer Protocol Secure). L'installation ajoute également un certificat auto-signé si aucun certificat valide n'est trouvé.

1.3.3 Sécurité des références

Les références que vous utilisez pour accéder à divers systèmes (tels que les workloads et les cibles de rétablissement) sont stockées dans la base de données PlateSpin . Elles sont donc protégées par les mêmes dispositifs de sécurité que ceux mis en place pour l'hôte du serveur PlateSpin Protect.

En outre, les références sont incluses dans les diagnostics, qui sont accessibles aux utilisateurs autorisés. Vous devez vous assurer que les projets de protection de workload sont traités par du personnel habilité.

1.3.4 Authentification et autorisation utilisateur

PlateSpin Protect propose un mécanisme complet et sécurisé d'autorisation et d'authentification utilisateur basé sur des rôles utilisateur et surveille l'accès aux applications ainsi que les opérations que les utilisateurs peuvent effectuer. Reportez-vous à la Section 2.2, « Configuration de l'authentification et de l'autorisation utilisateur », page 21.

1.4 Performances

1.4.1 À propos des caractéristiques de performances du produit

Les performances de votre produit PlateSpin Protect dépendent de multiples facteurs, dont :

- les profils logiciels et matériels de vos workloads sources ;
- les profils logiciels et matériels de vos conteneurs cibles ;
- les profils logiciels et matériels de l'hôte du serveur PlateSpin ;
- les particularités de la bande passante, de la configuration et des conditions de votre réseau ;
- le nombre de workloads protégés ;
- le nombre de volumes sous protection ;
- la taille des volumes sous protection ;
- la densité de fichiers (nombre de fichiers par unité de capacité) dans vos volumes du workload source ;

- les niveaux E/S sources (taux d'occupation de votre workload) ;
- le nombre de réplications simultanées ;
- l'activation/la désactivation du chiffrement des données ;
- activation/désactivation de la compression des données.

Pour planifier des plans de protection de workload à grande échelle, il est recommandé de procéder à un test de protection d'un workload typique et d'utiliser les résultats comme référence, en optimisant vos mesures régulièrement tout au long du projet.

1.4.2 Compression des données

Si nécessaire, PlateSpin Protect peut compresser les données de workload avant de les transférer sur le réseau. Cela permet de réduire le volume global de données transférées durant les réplications.

Les taux de compression dépendent des types de fichiers dans les volumes du workload source et peuvent varier d'environ 0,9 (100 Mo de données compressées à 90 Mo) à environ 0,5 (100 Mo de données compressées à 50 Mo).

REMARQUE : la compression des données utilise la puissance du processeur du workload source.

La compression de données peut être configurée individuellement pour chaque workload ou par niveau de protection. Reportez-vous à la section « Niveaux de protection » page 76.

1.4.3 Limitation de la bande passante

PlateSpin Protect permet de contrôler la quantité de bande passante consommée par une communication source-cible directe lors d'une protection de workload ; vous pouvez définir un débit pour chaque contrat de protection. Cette méthode permet d'éviter la congestion de votre réseau de production à cause du trafic de réplication, ainsi que de réduire la charge globale de votre serveur PlateSpin.

La limitation de bande passante peut être configurée pour chaque workload ou par niveau de protection. Reportez-vous à la section « Niveaux de protection » page 76.

1.4.4 Spécifications RPO, RTO et TTO

- **Perte de données maximale admissible (PDMA ou RPO – Recovery Point Objective) :** décrit la quantité acceptable de perte de données, mesurée dans le temps. La perte de données maximale admissible est déterminée en fonction du temps écoulé entre les réplications incrémentielles d'un workload protégé et est affectée par les niveaux d'utilisation actuels de PlateSpin Protect, la fréquence et l'étendue des changements au niveau du workload, la vitesse de votre réseau et la planification de réplication choisie.
- **Délai maximal d'interruption admissible (DMIA ou RTO – Recovery Time Objective) :** décrit le temps nécessaire à une opération de basculement (mise en ligne d'un workload de basculement pour remplacer temporairement un workload de production protégé).

  Le DMIA pour le basculement d'un workload sur sa réplique virtuelle dépend du temps nécessaire à la configuration et à l'exécution de l'opération de basculement (10 à 45 minutes). Reportez-vous à la section « Basculement » page 58.

- **Délai maximal de test admissible (DMTA ou TTO – Test Time Objective) :** décrit le temps nécessaire au test de la reprise après sinistre avec un niveau de confiance pour la restauration du service.

  Utilisez la fonction *Test de basculement* pour passer en revue les différents scénarios et générer des données d'évaluation des performances. Reportez-vous à la section « Utilisation de la fonction Tester le basculement » page 59.

Parmi les facteurs influant sur la PDMA, le DMIA et le DMTA figure le nombre d'opérations de basculement simultanées requises. En effet, un workload de basculement unique dispose de davantage de mémoire et de ressources d'UC que plusieurs workloads de basculement, lesquels partagent les ressources de leur infrastructure sous-jacente.

Vous devez déterminer le nombre moyen de basculements pour les workloads dans votre environnement en effectuant des tests de basculement à des heures différentes, puis les utiliser comme données de référence dans le cadre de vos plans généraux de récupération de données. Reportez-vous à la section « Génération de rapports sur les workloads et leur protection » page 47.

1.4.5 Évolutivité

L'évolutivité comprend (et repose sur) les caractéristiques majeures suivantes de votre produit PlateSpin Protect :

- **Workloads par serveur :** le nombre de workloads par serveur PlateSpin peut varier de 10 à 50, en fonction de divers facteurs, dont vos besoins PDMA et les caractéristiques matérielles de l'hôte du serveur.
- **Protections par conteneur :** le nombre maximal de protections par conteneur est lié (mais pas identique) aux spécifications de VMware se rapportant au nombre maximal de machines virtuelles prises en charge par l'hôte ESXi. D'autres facteurs comprennent les statistiques de récupération (dont les réplications et les basculements simultanés) et les spécifications du fournisseur de matériel.

Il est recommandé d'effectuer des tests, d'ajuster vos chiffres de capacité de façon incrémentielle et de les utiliser pour déterminer votre plafond d'évolutivité.

2 Configuration de l'application PlateSpin Protect

Cette section contient des informations sur les sujets suivants :

2.1 Activation de la licence du produit

Cette section fournit des informations sur l'activation de votre logiciel PlateSpin Protect.

2.1.1 Obtention d'un code d'activation de licence

Pour activer la licence de votre produit, vous devez disposer d'un code d'activation. Si ce n'est pas le cas, demandez-en un via le site Web Customer Center (http://www.netiq.com/center/). Un code d'activation de licence vous sera envoyé par message électronique.

La première fois que vous vous connectez à PlateSpin Protect, le navigateur est automatiquement redirigé vers la page d'activation de la licence. Vous pouvez activer la licence de votre produit de deux façons, à l'aide de l'Activation en ligne de la licence ou de l'Activation hors ligne de la licence.

2.1.2 Activation en ligne de la licence

Pour l'activation en ligne, PlateSpin Protect nécessite un accès Internet.

REMARQUE : les proxys HTTP peuvent être à l'origine d'échecs au cours de l'activation en ligne. L'activation hors ligne est recommandée pour les utilisateurs d'environnements employant un proxy HTTP.

---

1. Dans l'interface Web PlateSpin Protect, cliquez sur *Paramètres* > *Licences* > *Ajouter une licence*. La page License Activation (Activation de la licence) s'affiche.

2 Sélectionnez *Activation en ligne*, saisissez l'adresse électronique que vous avez spécifiée lorsque vous avez passé votre commande ainsi que le code d'activation que vous avez reçu, puis cliquez sur *Activer*.

   Le système obtient la licence requise via Internet et active le produit.

2.1.3 Activation hors ligne de la licence

Pour une activation hors ligne, vous obtenez une clé de licence via Internet à l'aide d'une machine disposant d'un accès Internet.

REMARQUE : pour pouvoir obtenir une clé de licence, vous devez posséder un compte Novell. Si vous êtes déjà un client PlateSpin mais ne disposez pas encore d'un compte Novell Customer Center, commencez par en créer un. Utilisez votre nom d'utilisateur PlateSpin existant (adresse électronique valide enregistrée auprès de PlateSpin) comme nom d'utilisateur pour votre compte Novell Customer Center.

---

1 Cliquez sur *Paramètres* > *Licence*, puis sur *Ajouter une licence*. La page d'activation de la licence s'affiche.

2 Sélectionnez *Activation hors ligne* et copiez l'ID du matériel affiché.

3 Utilisez un navigateur Web sur un ordinateur disposant d'un accès Internet pour accéder au site Web d'activation des produits PlateSpin (http://www.platespin.com/productactivation/ActivateOrder.aspx). Loguez-vous avec votre nom d'utilisateur Novell.

4 Entrez dans les champs appropriés :

   - le code d'activation reçu ;
   - l'adresse électronique renseignée lors de votre commande ;
   - l'ID matériel copié à l'Étape 2.

5 Cliquez sur *Activer*.

   Le système génère un fichier de clé de licence qu'il vous invite à enregistrer.

6 Enregistrez le fichier de clé de licence, transférez-le sur l'hôte du produit qui ne dispose pas d'une connexion Internet et utilisez-le pour activer le produit.

2.2 Configuration de l'authentification et de l'autorisation utilisateur

Cette section comprend les informations suivantes :

2.2.1 À propos de l'autorisation et de l'authentification des utilisateurs de PlateSpin Protect

Le mécanisme d'authentification et d'autorisation des utilisateurs de PlateSpin Protect est basé sur les rôles des utilisateurs et contrôle l'accès aux applications ainsi que les opérations pouvant être exécutées par ces derniers. Ce mécanisme est basé sur l'authentification Windows intégrée (IWA) et son interaction avec les services IIS (Internet Information Services).

Le système d'accès basé sur les rôles vous permet d'implémenter l'authentification et l'autorisation utilisateur de différentes manières :

- limiter l'accès aux applications à certains utilisateurs ;
- autoriser uniquement certains utilisateurs à exécuter des opérations spécifiques ;
- octroyer à chaque utilisateur un accès à des workloads spécifiques pour exécuter des opérations définies par le rôle qui lui a été assigné.

Chaque instance PlateSpin Protect comporte l'ensemble suivant de groupes d'utilisateurs de niveau système d'exploitation qui définissent les rôles fonctionnels associés :

- **Les administrateurs chargés de la protection des workloads :** ces utilisateurs bénéficient d'un accès illimité à toutes les fonctions de l'application. Un administrateur local appartient implicitement à ce groupe.
- **Les utilisateurs avec pouvoir chargés de la protection des workloads :** ces utilisateurs bénéficient d'un accès à la plupart des fonctions de l'application avec quelques restrictions, notamment en ce qui concerne la modification des paramètres système liés à l'octroi des licences et à la sécurité.
- **Les opérateurs chargés de la protection des workloads :** ces utilisateurs bénéficient d'un accès à un sous-ensemble limité de fonctions système, suffisant pour assurer un fonctionnement au quotidien.

Lorsqu'un utilisateur tente de se connecter à PlateSpin Protect, les références spécifiées via le navigateur sont validées par les services IIS. Si l'utilisateur n'est pas membre de l'un des rôles de protection de workload, la connexion est refusée.

Tableau 2-1 *Détails des rôles de protection de workload et des autorisations*

Détails des rôles de protection de workload	Administrateurs	Utilisateurs avec pouvoir	Opérateurs
Ajouter un workload	Autorisé	Autorisé	Refusé

Détails des rôles de protection de workload	Administrateurs	Utilisateurs avec pouvoir	Opérateurs
Supprimer le workload	Autorisé	Autorisé	Refusé
Configurer la protection	Autorisé	Autorisé	Refusé
Préparer la réplication	Autorisé	Autorisé	Refusé
Exécuter la réplication (complète)	Autorisé	Autorisé	Autorisé
Exécuter le transfert incrémentiel	Autorisé	Autorisé	Autorisé
Suspendre/reprendre la planification	Autorisé	Autorisé	Autorisé
Test de basculement	Autorisé	Autorisé	Autorisé
Basculement	Autorisé	Autorisé	Autorisé
Annuler le basculement	Autorisé	Autorisé	Autorisé
Abandonner	Autorisé	Autorisé	Autorisé
Fermer (la tâche)	Autorisé	Autorisé	Autorisé
Paramètres (tous)	Autorisé	Refusé	Refusé
Exécuter des rapports/diagnostics	Autorisé	Autorisé	Autorisé
Rétablissement	Autorisé	Refusé	Refusé
Reprotéger	Autorisé	Autorisé	Refusé

En outre, le logiciel PlateSpin Protect fournit un mécanisme basé sur les *groupes de sécurité* qui définissent quels utilisateurs ont accès à quels workloads dans l'inventaire de workloads de PlateSpin Protect.

La configuration d'un accès basé sur les rôles à PlateSpin Protect englobe deux tâches :

1. L'ajout d'utilisateurs aux groupes d'utilisateurs requis détaillés dans le Tableau 2-1 (reportez-vous à votre documentation Windows).
2. La création de groupes de sécurité de niveau application qui associent ces utilisateurs à des workloads spécifiques (reportez-vous à la section « Gestion des groupes de sécurité et des autorisations de workload de PlateSpin Protect » page 24).

2.2.2 Gestion de l'accès et des autorisations de PlateSpin Protect

Pour plus d'informations, reportez-vous aux sections suivantes :

- « Ajout d'utilisateurs PlateSpin Protect » page 23
- « Assignation d'un rôle de protection de workload à un utilisateur PlateSpin Protect » page 23

Ajout d'utilisateurs PlateSpin Protect

Utilisez la procédure décrite dans cette section pour ajouter un nouvel utilisateur PlateSpin Protect.

Si vous souhaitez octroyer des autorisations de rôle spécifiques à un utilisateur existant sur l'hôte du serveur PlateSpin , reportez-vous à la section « Assignation d'un rôle de protection de workload à un utilisateur PlateSpin Protect » page 23.

1. Sur l'hôte de votre serveur PlateSpin , accédez à la console des utilisateurs et groupes locaux du système (*Démarrer* > *Exécuter* > `lusrmgr.msc` > *Entrée*).
2. Cliquez avec le bouton droit sur le noeud *Utilisateurs*, sélectionnez *Nouvel utilisateur*, spécifiez les informations requises et cliquez sur *Créer*.

Vous pouvez maintenant assigner un rôle de protection de workload à l'utilisateur que vous venez de créer. Reportez-vous à la section « Assignation d'un rôle de protection de workload à un utilisateur PlateSpin Protect » page 23.

Assignation d'un rôle de protection de workload à un utilisateur PlateSpin Protect

Avant d'assigner un rôle à un utilisateur, déterminez l'ensemble d'autorisations qui lui convient le mieux. Reportez-vous au Tableau 2-1, « Détails des rôles de protection de workload et des autorisations », page 21.

1. Sur l'hôte de votre serveur PlateSpin , accédez à la console des utilisateurs et groupes locaux du système (*Démarrer* > *Exécuter* > `lusrmgr.msc` > *Entrée*).
2. Cliquez sur le noeud *Utilisateurs*, puis double-cliquez sur l'utilisateur souhaité dans le volet de droite.
3. Dans l'onglet *Membre de*, cliquez sur *Ajouter*, recherchez le groupe de protection de workload souhaité et assignez-le à l'utilisateur.

Plusieurs minutes peuvent être nécessaires pour que le changement soit pris en compte. Pour essayer d'appliquer manuellement les modifications, redémarrez votre serveur en procédant comme suit :

1. Accédez au sous-répertoire `bin\RestartPlateSpinServer` du serveur PlateSpin.
2. Double-cliquez sur l'exécutable `RestartPlateSpinServer.exe`.

   Une fenêtre d'invite de commande s'ouvre et vous demande confirmation.
3. Confirmez en saisissant `Y` et en appuyant sur `Entrée`.

Vous pouvez maintenant ajouter cet utilisateur à un groupe de sécurité PlateSpin Protect et lui associer un groupe spécifique de workloads. Reportez-vous à la section « Gestion des groupes de sécurité et des autorisations de workload de PlateSpin Protect » page 24.

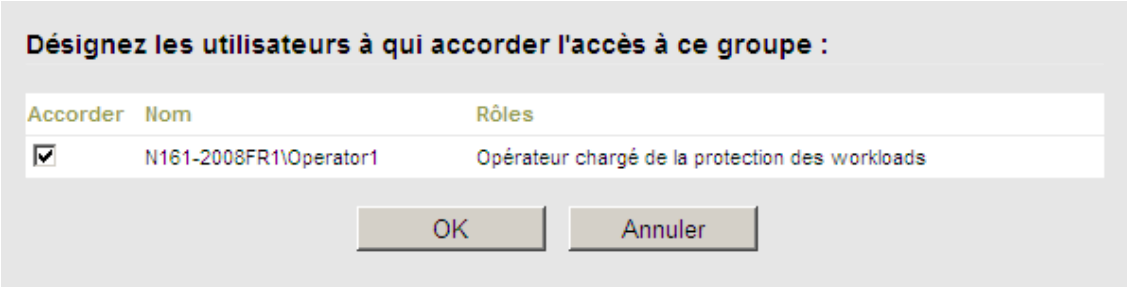
2.2.3 Gestion des groupes de sécurité et des autorisations de workload de PlateSpin Protect

PlateSpin Protect intègre un mécanisme d'accès de niveau application granulaire qui permet à certains utilisateurs d'exécuter des tâches de protection de workload spécifiques sur des workloads donnés. Pour ce faire, vous devez configurer des *groupes de sécurité*.

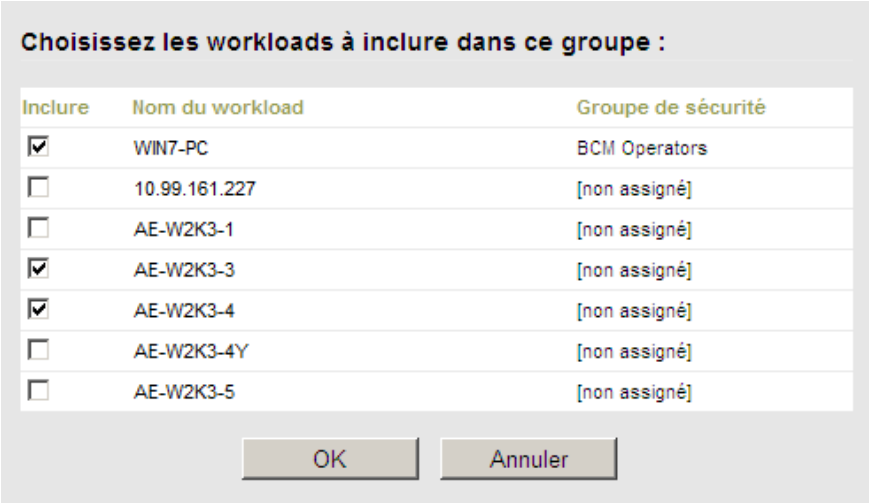
1. Assignez à un utilisateur PlateSpin Protect un rôle de protection de workload dont les autorisations sont les plus adaptées à ce rôle dans votre organisation. Reportez-vous à la section « Assignation d'un rôle de protection de workload à un utilisateur PlateSpin Protect » page 23.
2. Accédez à PlateSpin Protect en tant qu'administrateur à l'aide de l'interface Web de PlateSpin Protect, puis cliquez sur *Paramètres* > *Autorisations*.

   La page Groupes de sécurité s'ouvre.
3. Cliquez sur *Créer un groupe de sécurité*.
4. Dans le champ *Nom du groupe de sécurité*, saisissez un nom pour votre groupe de sécurité.
5. Cliquez sur *Ajouter des utilisateurs* et sélectionnez les utilisateurs que vous souhaitez ajouter à ce groupe de sécurité.

   Si vous souhaitez ajouter un utilisateur PlateSpin récemment ajouté à l'hôte du serveur PlateSpin Protect, celui-ci risque de ne pas être disponible immédiatement dans l'interface utilisateur. Dans ce cas, cliquez d'abord sur *Rafraîchir les comptes utilisateur*.



6. Cliquez sur *Ajouter des workloads* et sélectionnez les workloads souhaités :



   Seuls les utilisateurs faisant partie de ce groupe de sécurité auront accès aux workloads sélectionnés.

7 Cliquez sur *Créer*.

La page se recharge et affiche votre nouveau groupe dans la liste des groupes de sécurité.

Pour éditer un groupe de sécurité, cliquez sur son nom dans la liste des groupes de sécurité.

2.3 Conditions d'accès et de communication requises sur votre réseau de protection

Cette section présente les informations suivantes :

2.3.1 Conditions d'accès et de communication requises pour les workloads

Le tableau ci-dessous liste les configurations logicielle, réseau et pare-feu requises pour les workloads que vous souhaitez protéger à l'aide de PlateSpin Protect.

Tableau 2-2 *Conditions d'accès et de communication requises pour les workloads*

Type de workload	Conditions préalables	Ports requis (valeurs par défaut)
Tous les workloads	Prise en charge de la fonctionnalité ping (demande et réponse d'écho ICMP)	
Tous les workloads Windows	Microsoft .NET Framework version 2.0 ou 3.5 SP1	

Type de workload	Conditions préalables	Ports requis (valeurs par défaut)
Windows 7 ; Windows Server 2008 ; Windows Vista	◆ Références de compte `Administrateur` ou d'administrateur de domaine (l'appartenance au groupe Administrateurs local uniquement est insuffisante). Sous Vista, le compte doit être activé (il est désactivé par défaut). ◆ Le pare-feu Windows doit être configuré pour autoriser le *partage de fichiers et d'imprimantes*. Utilisez l'une des options suivantes : ◆ **Option 1, à l'aide du pare-feu Windows :** utilisez l'élément de base du Panneau de configuration *Pare-feu Windows* (`firewall.cpl`) et sélectionnez *Partage de fichiers et d'imprimantes* dans la liste d'exceptions. - OU - ◆ **Option 2, à l'aide de l'utilitaire Pare-feu Windows avec fonctions avancées de sécurité :** employez l'utilitaire *Pare-feu Windows avec fonctions avancées de sécurité* (`wf.msc`) avec les *règles de trafic entrant* activées et définies sur `Autoriser` : ◆ *Partage de fichiers et d'imprimantes (demande d'écho - ICMPv4In)* ◆ *Partage de fichiers et d'imprimantes (demande d'écho - ICMPv6In)* ◆ *Partage de fichiers et d'imprimantes (NB-Datagramme-Entrée)* ◆ *Partage de fichiers et d'imprimantes (NB-Nom-Entrée)* ◆ *Partage de fichiers et d'imprimantes (NB-Session-Entrée)* ◆ *Partage de fichiers et d'imprimantes (SMB-Entrée)* ◆ *Partage de fichiers et d'imprimantes (Service de spouleur - RPC)* ◆ *Partage de fichiers et d'imprimantes (Service de spouleur - RPC-EPMAP)*	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 et UDP 137, 138) TCP 135/445
Windows Server 2003 (y compris SP1 Standard, SP2 Enterprise et R2 SP2 Enterprise)	**REMARQUE :** après avoir activé les ports requis, exécutez la commande suivante au niveau de l'invite serveur afin d'autoriser l'administration à distance de PlateSpin : `netsh firewall set service RemoteAdmin enable` Pour plus d'informations sur netsh, consultez l'article Microsoft TechNet suivant : http://technet.microsoft.com/fr-fr/library/cc785383%28v=ws.10%29.aspx (http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx).	◆ **TCP :** 3725, 135, 139, 445 ◆ **UDP :** 137, 138, 139

Type de workload	Conditions préalables	Ports requis (valeurs par défaut)
Windows Server 2000 ; Windows XP	◆ Windows Management Instrumentation (WMI) installé WMI (RPC/DCOM) peut utiliser les ports TCP 135 et 445 ainsi que les ports aléatoires ou assignés dynamiquement supérieurs à 1024. Si des problèmes se produisent lors de l'ajout du workload, envisagez de le placer provisoirement dans une zone démilitarisée ou d'ouvrir temporairement les ports protégés par le pare-feu le temps d'ajouter le workload à PlateSpin Protect. Pour plus d'informations, telles que des conseils pour la limitation de la plage de ports pour DCOM et RPC, reportez-vous aux articles techniques Microsoft suivants. ◆ Utilisation de DCOM avec des pare-feux (http://msdn.microsoft.com/en-us/library/ms809327.aspx) ◆ Configuration de l'allocation dynamique de port RPC en vue de son fonctionnement avec des pare-feux (http://support.microsoft.com/default.aspx?scid=kb;en-us;154596) ◆ Configuration de DCOM pour fonctionner sur un pare-feu NAT (http://support.microsoft.com/kb/248809)	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 et UDP 137, 138) RPC (TCP 135)
Tous les workloads Linux	Serveur Secure Shell (SSH)	TCP 22, 3725

2.3.2 Conditions d'accès et de communication requises pour les conteneurs

Le tableau ci-dessous liste les configurations logicielle, réseau et pare-feu requises pour les conteneurs de workloads pris en charge.

Tableau 2-3 *Conditions d'accès et de communication requises pour les conteneurs*

Système	Conditions préalables	Ports requis (valeurs par défaut)
Tous les conteneurs	Fonctionnalité ping (demande et réponse d'écho ICMP).	
VMware ESX/ESXi 4.1 VMware ESXi 5.0	◆ Compte VMware avec rôle d'administrateur ◆ API de gestion de fichiers et API de services Web VMware	HTTPS (TCP 443)
vCenter Server	L'utilisateur disposant de l'accès doit se voir accorder les autorisations et rôle appropriés. Pour plus d'informations à ce sujet, consultez la version correspondante de la documentation VMware.	HTTPS (TCP 443)

2.3.3 Exigences de port ouvert pour les hôtes du serveur PlateSpin

Voici les exigences de port ouvert auxquelles doivent répondre les hôtes du serveur PlateSpin

Tableau 2-4 Exigences de port ouvert pour les hôtes du serveur PlateSpin

Port (par défaut)	Remarques
TCP 80	Pour la communication HTTP
TCP 443	Pour la communication HTTPS (si SSL est activé)

2.3.4 Protection sur des réseaux publics et privés via NAT

Dans certains cas, une source, une cible ou PlateSpin Protect peut se trouver sur un réseau (privé) interne derrière un périphérique NAT (Network Address Translator) et être incapable de communiquer avec l'autre partie durant la protection.

PlateSpin Protect vous permet de résoudre ce problème, en fonction de l'hôte qui se trouve derrière le périphérique NAT :

- **Serveur PlateSpin :** dans l'outil de *configuration de votre serveur PlateSpin*, indiquez les adresses IP supplémentaires assignées à cet hôte. Reportez-vous à la section « Configuration de l'application en vue de son fonctionnement dans des environnements NAT » page 28.
- **Conteneur cible :** lorsque vous essayez de découvrir un conteneur (tel que VMware ESX), spécifiez l'adresse IP publique (ou externe) de cet hôte dans les paramètres de découverte.
- **Workload :** lorsque vous essayez d'ajouter un workload, spécifiez l'adresse IP publique (externe) de ce workload dans les paramètres de découverte.
- **VM de basculement :** au cours du rétablissement, vous pouvez spécifier une adresse IP alternative pour le workload de basculement à la section Détails du rétablissement (Workload sur VM) (page 62).
- **Cible de rétablissement :** au cours d'une tentative d'enregistrement d'une cible de rétablissement, lorsque vous êtes invité à fournir l'adresse IP du serveur PlateSpin, renseignez soit l'adresse locale de l'hôte du serveur Protect, soit l'une de ses adresses (externes) publiques enregistrées dans l'outil *de configuration du serveur PlateSpin* (reportez-vous à la section *Serveur PlateSpin* ci-dessus).

Configuration de l'application en vue de son fonctionnement dans des environnements NAT

Pour permettre au serveur PlateSpin de fonctionner dans des environnements NAT, vous devez enregistrer ses adresses IP supplémentaires dans la base de données de l'outil de *configuration du serveur PlateSpin* lue au démarrage.

Pour plus d'informations sur la procédure de mise à jour, reportez-vous à la section « Configuration du comportement du serveur PlateSpin via les paramètres de configuration XML » page 33.

2.3.5 Remplacement du shell bash par défaut pour l'exécution de commandes sur les workloads Linux

Par défaut, le serveur PlateSpin utilise le shell `/bin/bash` pour l'exécution de commandes sur un workload source Linux.

Si nécessaire, vous pouvez remplacer le shell par défaut en modifiant la clé de registre correspondante sur le serveur PlateSpin

Reportez-vous à l'article de la base de connaissances n° 7010676 (https://www.netiq.com/support/kb/doc.php?id=7010676).

2.3.6 Conditions requises pour les grappes VMware DRS en tant que conteneurs

Pour être une cible de protection valide, vous devez ajouter votre grappe VMware DRS à l'ensemble de conteneurs (inventoriés) en tant que grappe VMware. ne tentez pas d'ajouter une grappe DRS en tant qu'ensemble de serveurs ESX distincts. Reportez-vous à la section « Ajout de conteneurs (cibles de protection) » page 51.

En outre, votre grappe VMware DRS doit respecter la configuration requise suivante :

- DRS est activé et défini sur `Partiellement automatisé` ou `Entièrement automatisé`.
- Les serveurs ESX de la grappe VMware partagent au moins une banque de données.
- Au moins un vSwitch et un groupe de ports virtuel ou un commutateur distribué vNetwork sont communs à tous les serveurs ESX de la grappe VMware.
- Les workloads de basculement (VM) pour chaque contrat de protection sont placés exclusivement sur les banques de données, les vSwitch et les groupes de ports virtuels partagés par tous les serveurs ESX de la grappe VMware.

2.4 Configuration des options par défaut de PlateSpin Protect

Cette section présente les informations suivantes :

2.4.1 Configuration des notifications automatiques des événements et rapports par message électronique

Vous pouvez configurer PlateSpin Protect pour envoyer automatiquement des notifications des événements et rapports de réplication aux adresses électroniques spécifiées. Pour cette fonctionnalité, vous devez d'abord spécifier un serveur SMTP valide que PlateSpin Protect doit utiliser.

- « Configuration SMTP » page 30
- « Configuration des notifications automatiques des événements par message électronique » page 30
- « Configuration des rapports de réplication automatiques par message électronique » page 32

Configuration SMTP

Utilisez l'interface Web de PlateSpin Protect afin de configurer les paramètres SMTP (Simple Mail Transfer Protocol) pour le serveur qui envoie des notifications par courrier électronique des événements et des rapports de réplication.

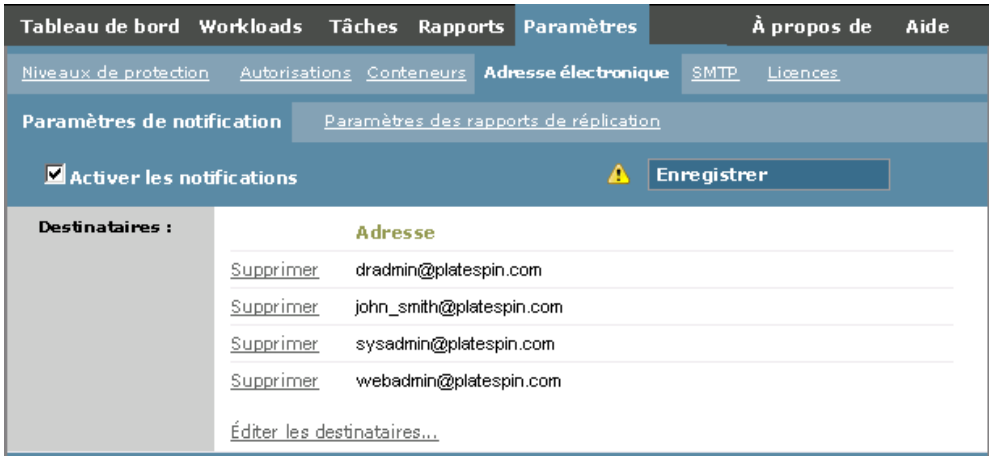
Figure 2-1 *Paramètres SMTP (Simple Mail Transfer Protocol)*

Pour configurer les paramètres SMTP :

1. Dans votre interface Web PlateSpin Protect, cliquez sur *Paramètres* > *SMTP*.
2. Spécifiez une *adresse* de serveur SMTP, un *port* (le port par défaut porte le numéro 25) et une *adresse de réponse* pour la réception des notifications d'événements et de progression par message électronique.
3. Saisissez un *nom d'utilisateur* et un *mot de passe*, puis confirmez le mot de passe.
4. Cliquez sur *Enregistrer*.

Configuration des notifications automatiques des événements par message électronique

1. Configurez le serveur SMTP que PlateSpin Protect doit utiliser. Reportez-vous à la section « Configuration SMTP » page 30.
2. Dans votre interface Web PlateSpin Protect, cliquez sur *Paramètres* > *Adresse électronique* > *Paramètres de notification*.
3. Sélectionnez l'option *Activer les notifications*.
4. Cliquez sur *Éditer les destinataires*, entrez les adresses électroniques souhaitées en les séparant par des virgules, puis cliquez sur *OK*.



5 Cliquez sur *Enregistrer*.

Pour supprimer des adresses électroniques, cliquez sur *Supprimer* en regard des adresses à supprimer.

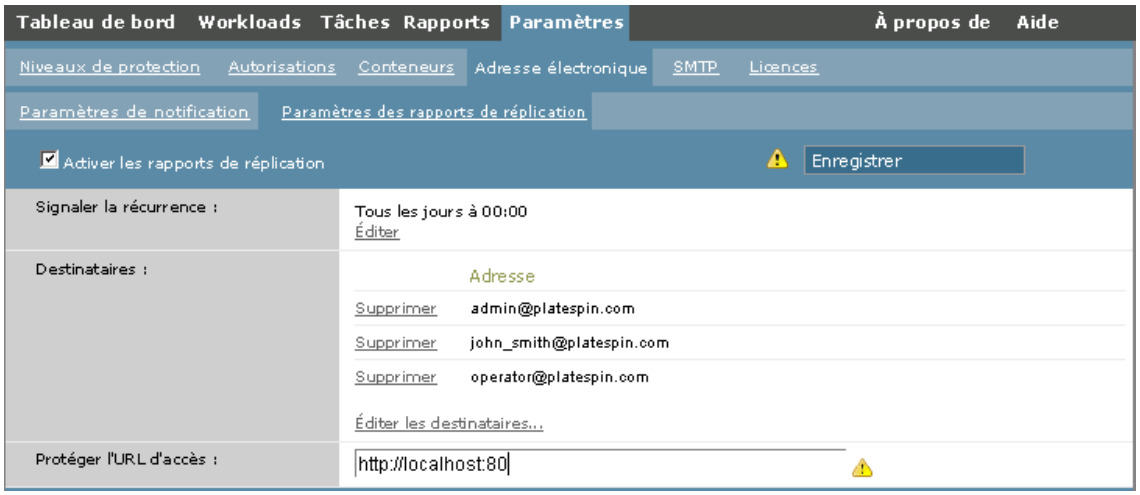
Les événements suivants déclenchent des notifications par message électronique :

Événement	Remarques
`Détection de workload en ligne`	Généré lorsque le système détecte qu'un workload précédemment hors ligne est désormais en ligne. S'applique aux workloads dont l'état du contrat de protection n'est pas *Suspendu*.
`Détection de workload hors ligne`	Généré lorsque le système détecte qu'un workload précédemment en ligne est désormais hors ligne. S'applique aux workloads dont l'état du contrat de protection n'est pas *Suspendu*.
`Réplication complète terminée`	
`Échec de la réplication complète`	
`Réplication complète manquée`	Similaire à l'événement `Réplication incrémentielle manquée`.
`Réplication incrémentielle terminée`	
`Échec de la réplication incrémentielle`	
`Réplication incrémentielle manquée`	Se produit dans les cas suivants : ◆ Une réplication est suspendue manuellement alors qu'une réplication incrémentielle planifiée doit être effectuée. ◆ Le système tente d'exécuter une réplication incrémentielle planifiée alors qu'une réplication déclenchée manuellement est en cours. ◆ Le système détecte que l'espace disque libre sur la cible est insuffisant.
`Test de basculement effectué`	Généré lors du marquage manuel d'une opération de test de basculement comme réussie ou échouée.
`Préparation du basculement effectuée`	
`Échec de la préparation du basculement`	
`Basculement effectué`	
`Échec du basculement`	

Configuration des rapports de réplication automatiques par message électronique

Pour que PlateSpin Protect envoie automatiquement des rapports de réplication par message électronique, procédez comme suit :

1. Configurez le serveur SMTP que PlateSpin Protect doit utiliser. Reportez-vous à la section Configuration SMTP (page 30).
2. Dans l'interface Web PlateSpin Protect, cliquez sur *Paramètres* > *Adresse électronique* > *Paramètres des rapports de réplication*.
3. Sélectionnez l'option *Activer les rapports de réplication*.
4. Dans la section *Signaler la récurrence*, cliquez sur *Configurer* et spécifiez le schéma de récurrence souhaité pour les rapports.
5. Dans la section *Destinataires*, cliquez sur *Éditer les destinataires*, entrez les adresses électroniques souhaitées en les séparant par des virgules, puis cliquez sur *OK*.



6. (Facultatif) Dans la section *Protéger l'URL d'accès*, spécifiez une URL autre que celle par défaut pour votre serveur PlateSpin (par exemple, quand l'hôte du serveur PlateSpin possède plusieurs cartes réseau ou s'il se trouve derrière un serveur NAT). Cette URL influe sur le titre du rapport et la fonctionnalité d'accès à du contenu approprié sur le serveur via des liens hypertexte dans des rapports envoyés par message électronique.
7. Cliquez sur *Enregistrer*.

Pour plus d'informations sur les autres types de rapports que vous pouvez générer et consulter à la demande, reportez-vous à la section « Génération de rapports sur les workloads et leur protection » page 47.

2.4.2 Configuration de la langue pour les versions internationales de PlateSpin Protect

PlateSpin Protect assure la prise en charge des langues nationales (fonction NLS, National Language Support) suivantes : allemand, chinois simplifié, chinois traditionnel, français et japonais.

Pour utiliser l'interface Web PlateSpin Protect et l'aide intégrée dans l'une de ces langues, vous devez ajouter cette dernière dans votre navigateur Web et la déplacer vers le haut de la liste de préférence :

1. Accédez à la configuration des langues dans votre navigateur Web :
   - **Internet Explorer :** cliquez sur *Outils* > *Options Internet* > *onglet Général* > *Langues*.
   - **Firefox :** cliquez sur *Outils* > *Options* > *onglet Contenu* > *Langues*.
2. Ajoutez la langue souhaitée et déplacez-la vers le haut de la liste.
3. Enregistrez les paramètres, puis démarrez l'application client en vous connectant à votre serveur PlateSpin . Reportez-vous à la section « Lancement de l'interface Web PlateSpin Protect » page 39.

REMARQUE : (pour les utilisateurs des versions en chinois traditionnel et simplifié) les tentatives de connexion au serveur PlateSpin avec un navigateur n'intégrant pas une version spécifique du chinois ajouté peuvent entraîner l'affichage de messages d'erreur du serveur Web. Afin d'obtenir un fonctionnement correct, ajoutez, par l'intermédiaire des paramètres de configuration du navigateur, une langue chinoise spécifique (par exemple, `Chinois/Chine [zh-cn]` ou `Chinois/Taïwan [zh-tw]`). N'utilisez pas la langue culturellement neutre `Chinois [zh]`.

La langue de certains messages système générés par le serveur PlateSpin dépend de la langue d'interface du système d'exploitation sélectionnée sur votre VM de gestion PlateSpin :

1. Accédez à l'hôte du serveur PlateSpin .
2. Lancez l'applet Options régionales et linguistiques (cliquez sur *Démarrer* > *Exécuter*, saisissez `intl.cpl` et appuyez sur Entrée), puis cliquez sur l'onglet *Langues* (Windows Server 2003) ou *Claviers et langues* (Windows Server 2008).
3. S'il n'est pas encore installé, installez le module linguistique requis. Vous devrez peut-être accéder au support d'installation du système d'exploitation.
4. Sélectionnez la langue souhaitée comme langue d'interface du système d'exploitation. Lorsque vous y être invité, déconnectez-vous et redémarrez le système.

2.4.3 Configuration du comportement du serveur PlateSpin via les paramètres de configuration XML

Certains aspects du comportement de votre serveur PlateSpin sont déterminés par les paramètres de configuration définis sur une page Web de configuration résidant sur l'hôte de votre serveur PlateSpin (`https://`*`Votre_serveur_PlateSpin`*`/platespinconfiguration/`).

Dans des circonstances normales, vous n'avez pas besoin de modifier ces paramètres, sauf si le support PlateSpin vous le recommande. Cette section présente des cas d'emploi courants ainsi que des informations sur la procédure à suivre.

Procédez comme suit pour modifier et appliquer des paramètres de configuration :

1. Ouvrez `https://Votre_serveur_PlateSpin/platespinconfiguration/` dans le navigateur Web de votre choix.
2. Recherchez le paramètre de serveur requis et modifiez sa valeur.
3. Enregistrez vos paramètres et quittez la page.

Aucun redémarrage des services n'est nécessaire après avoir modifié l'outil de configuration.

Les rubriques suivantes contiennent des informations concernant des situations spécifiques au cours desquelles le comportement du produit devra éventuellement être modifié à l'aide d'une valeur de configuration XML.

- « Optimisation du transfert de données sur les connexions WAN » page 34
- « Configuration de la prise en charge de SRM » page 35

Optimisation du transfert de données sur les connexions WAN

Vous pouvez optimiser les performances de transfert de données et les ajuster pour les connexions WAN. Pour ce faire, modifiez les paramètres de configuration lus par le système à partir des réglages effectués dans un outil de configuration résidant sur l'hôte de votre serveur PlateSpin. Pour la procédure générique, reportez-vous à la section « Configuration du comportement du serveur PlateSpin via les paramètres de configuration XML » page 33.

Ces paramètres permettent d'optimiser les transferts de données dans un environnement WAN. Ces paramètres sont globaux et affectent l'ensemble des réplications basées sur les fichiers et VSS.

REMARQUE : si ces valeurs sont modifiées, le temps de réplication sur les réseaux à haute vitesse, comme Gigabit Ethernet, risque d'être allongé. Avant de modifier l'un de ces paramètres, demandez d'abord conseil au support PlateSpin.

Le Tableau 2-5 liste les paramètres de configuration avec les valeurs par défaut et les valeurs recommandées pour un fonctionnement optimal dans un environnement WAN à latence élevée.

Tableau 2-5 *Paramètres de configuration par défaut et optimisés dans* `https://Votre_serveur_PlateSpin/platespinconfiguration/`

Paramètre	Valeur par défaut	Valeur optimale
`fileTransferMinCompressionLimit` Spécifie en octets le seuil de compression au niveau des paquets.	0 (désactivé)	65 536 max (64 Ko)
`fileTransferCompressionThreadsCount` Contrôle le nombre de threads utilisés pour la compression des données au niveau des paquets. Ce paramètre est ignoré si la compression est désactivée. Étant donné que la compression fait appel à l'UC, ce paramètre peut avoir un impact sur les performances.	2	S/O

Paramètre	Valeur par défaut	Valeur optimale

`fileTransferSendReceiveBufferSize`
 	
Paramètre de taille de la fenêtre TCP/IP pour les connexions de transfert de fichiers. Contrôle le nombre d'octets envoyés sans accusé de réception TCP, en octets.
 	
Lorsque la valeur est définie sur 0, la taille par défaut de la fenêtre TCP est utilisée (8 Ko). Pour personnaliser les tailles, spécifiez-les en octets. Utilisez la formule suivante pour déterminer la valeur appropriée :
 	
((VITESSE_LIAISON (Mbits/s)/8)*DURÉE (s))*1000*1000
 	
Par exemple, pour une liaison de 100 Mbits/s et une latence de 10 ms, la taille de tampon appropriée est de :
 	
`(100/8)*0,01*1000*1000 = 125 000 octets`
	0 (8 192 octets)	5 242 880 max (5 Mo)

Configuration de la prise en charge de SRM

Les workloads répliqués par PlateSpin Protect et gérés sur le gestionnaire de récupération VMware vCenter Site Recovery Manager (SRM) peuvent fonctionner de manière transparente si le produit est configuré pour prendre en charge SRM. Dans le cadre de la configuration, certains paramètres de configuration XML du serveur PlateSpin doivent être modifiés. Pour les informations concernant ces modifications de configuration, reportez-vous à la Section 2.4.4, « Configuration de la prise en charge de VMware vCenter Site Recovery Manager », page 35.

2.4.4 Configuration de la prise en charge de VMware vCenter Site Recovery Manager

Vous pouvez utiliser PlateSpin Protect pour protéger vos workloads localement et ensuite recourir à une autre méthode pour répliquer ces workloads à un emplacement distant, tel qu'un SAN (sous-réseau de stockage). Par exemple, vous avez la possibilité d'utiliser VMware vCenter Site Recovery Manager (SRM) pour répliquer sur un site distant l'intégralité d'une banque de données de machines virtuelles cibles répliquées. Dans ce cas, des étapes de configuration spécifiques sont nécessaires afin d'assurer que les machines virtuelles cibles peuvent être répliquées et fonctionnent normalement lorsqu'elles sont mises en service sur le site distant.

La configuration de Protect pour la prise en charge de SRM consiste à réaliser les ajustements suivants :

- Configurez un paramètre pour conserver les images ISO et les unités de disquette de PlateSpin Protect dans la même banque de données que les fichiers VMware `.vmx` et `vmdk`.
- Préparez l'environnement PlateSpin Protect en vue de la copie des outils VMware vers la cible de basculement. Cela implique la création et la copie manuelles de fichiers en plus de certains réglages de configuration permettant d'accélérer le processus d'installation des outils VMware.

Procédez comme suit pour être certain que les fichiers de workload soient conservés dans la même banque de données :

1. Depuis un navigateur Web, ouvrez `https://votre_serveur_PlateSpin/platespinconfiguration/` pour afficher la page Web de configuration.
2. Dans la page Web de configuration, trouvez le paramètre de serveur `CreatePSFilesInVmDatastore` et remplacez sa valeur par `true`.

   REMARQUE : il incombe à la personne qui configure le contrat de réplication de vérifier que la banque de données spécifiée est la même pour tous les fichiers de disque de la machine virtuelle cible.

3. Enregistrez vos paramètres et quittez la page.

Il est possible de copier les paquetages d'installation des outils VMware sur la cible de basculement lors de la réplication afin que le service de configuration puisse les installer lorsque la machine virtuelle est démarrée. Cette opération est effectuée automatiquement lorsque la cible de basculement est en mesure de contacter le serveur PlateSpin Protect. À défaut, vous devez préparer votre environnement avant la réplication en procédant comme suit :

1. Récupérez les paquetages des outils VMware à partir d'un hôte ESX :
   - **1a** Effectuez une copie sécurisée (`scp`) de l'image `windows.iso` à partir du répertoire `/usr/lib/vmware/isoimages` d'un hôte VMware accessible vers un dossier temporaire local.
   - **1b** Ouvrez l'image ISO, extrayez ses paquetages d'installation et enregistrez-les à un emplacement auquel vous avez accès :
     - **VMware 5.0 et 5.1 :** les paquetages d'installation sont `setup.exe` et `setup64.exe`.
     - **VMware 4.0 et 4.1 :** les paquetages d'installation sont `VMware Tools.msi` et `VMware Tools64.msi`.
2. Créez des paquetages OFX à partir des paquetages d'installation que vous avez extraits depuis le serveur VMware :
   - **2a** Zippez le paquetage souhaité en vous assurant que le fichier du programme d'installation se trouve à la racine de l'archive `.zip`.
   - **2b** Renommez l'archive `.zip` en `1.package` afin de pouvoir l'utiliser comme paquetage OFX.

     REMARQUE : si vous souhaitez créer un paquetage OFX pour plusieurs paquetages d'installation, n'oubliez pas que chaque paquetage d'installation doit avoir sa propre archive `.zip` unique.

     Étant donné que chaque paquetage doit avoir le même nom (`1.package`), si vous souhaitez enregistrer plusieurs archives `.zip` en tant que paquetages OFX, vous devez enregistrer chacune d'entre elles dans son propre sous-répertoire unique.
3. Copiez le paquetage OFX (`1.package`) voulu sous `%ProgramFiles(x86)%\PlateSpin\Packages\%GUID%` sur le serveur PlateSpin. La valeur de `%GUID%` dépend de la version de votre serveur VMware et de son architecture des outils VMware.

Le tableau suivant répertorie les versions de serveur, l'architecture des outils VMware et l'identifiant GUID dont vous avez besoin pour copier le paquetage dans le répertoire correct :

Version du serveur VMware	Architecture des outils VMware	GUID
4.0	x86	D052CBAC-0A98-4880-8BCC-FE0608F0930F
4.0	x64	80B50267-B30C-4001-ABDF-EA288D1FD09C
4.1	x86	F2957064-65D7-4bda-A52B-3F5859624602
4.1	x64	80B1C53C-6B43-4843-9D63-E9911E9A15D5
5	x86	AD4FDE1D-DE86-4d05-B147-071F4E1D0326
5	x64	F7C9BC91-7733-4790-B7AF-62E074B73882
5.1	x86	34DD2CBE-183E-492f-9B36-7A8326080755
5.1	x64	AD4FDE1D-DE86-4d05-B147-071F4E1D0326

Accélération du processus de configuration

Une fois que la cible de basculement a démarré, le service de configuration est lancé afin de préparer la machine virtuelle en vue de son utilisation, mais reste inactif pendant quelques minutes, le temps de recevoir les données en provenance du serveur PlateSpin ou de rechercher les outils VMware sur le CD-ROM. Pour écourter ce temps d'attente :

1. Sur la page Web de configuration, trouvez le paramètre de configuration `ConfigurationServiceValues` et remplacez la valeur de son sous-paramètre `WaitForFloppyTimeoutInSecs` par zéro (0).
2. Dans la page Web de configuration, trouvez le paramètre `ForceInstallVMToolsCustomPackage` et remplacez sa valeur par `true`.

Avec ces paramètres, le processus de configuration prend moins de 15 minutes : la machine cible redémarre (jusqu'à deux fois), les outils VMware sont installés et le gestionnaire SRM accède aux outils dont il a besoin pour configurer la mise en réseau sur le site distant.

3 Fonctionnement

Cette section fournit des informations sur les fonctions essentielles de PlateSpin Protect et son interface.

3.1 Lancement de l'interface Web PlateSpin Protect

La plupart de vos interactions avec l'applicatif s'effectuent via le client Web PlateSpin Protect basé sur un navigateur.

Les navigateurs pris en charge sont les suivants :

- *Google Chrome* 34.0 et versions ultérieures
- *Microsoft Internet Explorer* 11.0 et versions ultérieures
- *Mozilla Firefox* 29.0 et versions ultérieures

REMARQUE : JavaScript (Active Scripting) doit être activé dans votre navigateur :

- **Chrome :** dans le menu Chrome, sélectionnez **Paramètres**, faites défiler les options pour sélectionner **Afficher les paramètres avancés...**, puis sélectionnez **Paramètres de contenu** > **Autoriser tous les sites à exécuter JavaScript**.
- **IE :** dans le menu Outils, sélectionnez **Options Internet** > **Sécurité**, puis cliquez sur **Personnaliser le niveau...**. Faites défiler les options pour sélectionner **Active Scripting**, puis cliquez sur **Activer**, puis sur **Oui** lorsque la boîte de dialogue d'avertissement s'affiche. Cliquez sur **OK**, puis sur **Appliquer** > **OK**.
- **Firefox :** cliquez sur **Outils** > **Options** > **Contenu**, puis sélectionnez l'option **Activer JavaScript**.

Pour utiliser l'interface Web PlateSpin Protect et l'aide intégrée dans une des langues prises en charge, reportez-vous à la Section 2.4.2, « Configuration de la langue pour les versions internationales de PlateSpin Protect », page 33.

Pour lancer l'interface Web PlateSpin Protect :

1. Ouvrez un navigateur Web et accédez à l'adresse :

   `https://`*<nom_hôte | adresse_IP>*`/Protect`

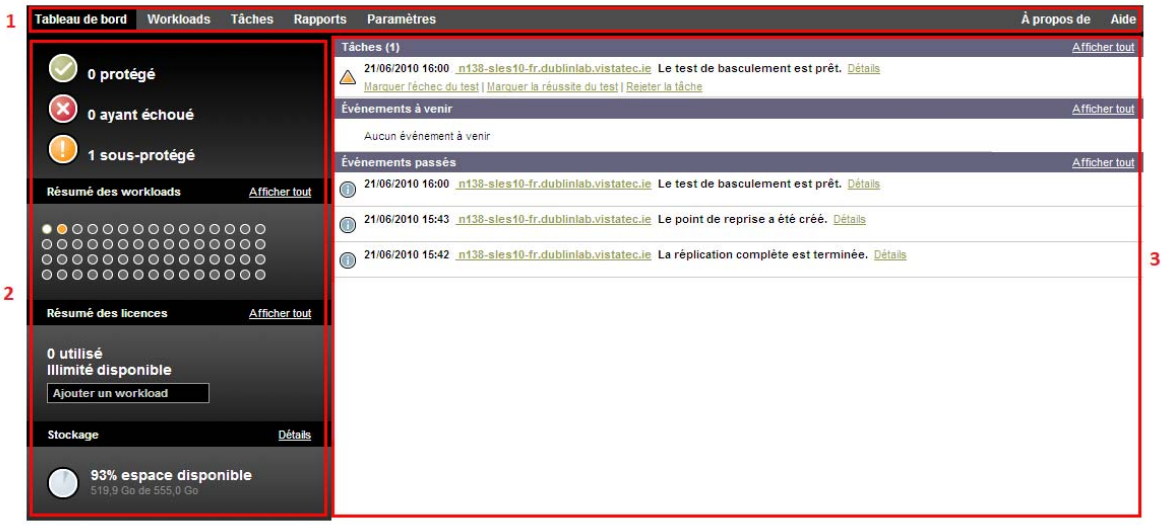
Remplacez <*nom_hôte* | *adresse_IP*> par le nom d'hôte et l'adresse IP de l'hôte du serveur PlateSpin.

Si SSL n'est pas activé, utilisez le protocole `http` dans l'URL.

3.2 Éléments de l'interface Web de PlateSpin Protect

L'interface par défaut de l'interface Web PlateSpin Protect est la page Tableau de bord, qui contient des éléments permettant d'accéder à différentes zones fonctionnelles de l'interface et d'exécuter des opérations de protection et de récupération de workload.

Figure 3-1 *Page Tableau de bord par défaut de l'interface Web PlateSpin Protect*



La page Tableau de bord comprend les éléments suivants :

1. **Barre de navigation :** figure sur la plupart des pages de l'interface Web PlateSpin Protect.
2. **Panneau de résumé visuel :** fournit une vue d'ensemble de l'état global de l'inventaire des workloads de PlateSpin Protect.
3. **Panneau des tâches et événements :** fournit des informations sur les événements et les tâches nécessitant l'attention de l'utilisateur.

Pour plus d'informations, reportez-vous aux rubriques suivantes :

- Section 3.2.1, « Barre de navigation », page 41
- Section 3.2.2, « Panneau de résumé visuel », page 41
- Section 3.2.3, « Panneau Tâches et événements », page 42

3.2.1 Barre de navigation

La barre de navigation fournit les liens suivants :

- **Tableau de bord :** affiche la page Tableau de bord par défaut.
- **Workloads :** affiche la page Workloads. Reportez-vous à la section « Workloads et commandes de workload » page 42.
- **Tâches :** affiche la page Tâches, qui liste les éléments nécessitant une intervention de l'utilisateur.
- **Rapports :** affiche la page Rapports. Reportez-vous à la section « Génération de rapports sur les workloads et leur protection » page 47.
- **Paramètres :** affiche la page Paramètres, qui permet d'accéder aux options de configuration suivantes :
  - **Niveaux de protection :** reportez-vous à la section « Niveaux de protection » page 76.
  - **Autorisations :** reportez-vous à la section « Configuration de l'authentification et de l'autorisation utilisateur » page 21.
  - **Conteneurs :** reportez-vous à la section « Ajout de conteneurs (cibles de protection) » page 51.
  - **Adresse électronique/SMTP :** reportez-vous à la section « Configuration des notifications automatiques des événements et rapports par message électronique » page 29.
  - **Licences/Désignations des licences :** reportez-vous à la section « Activation de la licence du produit » page 19.

3.2.2 Panneau de résumé visuel

Le panneau de résumé visuel fournit une vue d'ensemble de tous les workloads sous licence et de la capacité de stockage disponible.

Les workloads inventoriés sont classés en trois catégories :

- **Protégé :** indique le nombre de workloads sous protection active.
- **Ayant échoué :** indique le nombre de workloads protégés que le système a renseignés comme ayant échoué, en fonction du niveau de protection de ces derniers.
- **Sous-protégé :** indique le nombre de workloads protégés nécessitant l'attention de l'utilisateur.

La zone au centre du panneau de gauche représente un résumé graphique de la page Workloads. Les icônes en forme de point suivantes indiquent les différents états possibles des workloads :

Tableau 3-1 *Icônes en forme de point indiquant l'état des workloads*

● Non protégé	● *Sous-protégé*
○ *Non protégé - Erreur*	● *Ayant échoué*
● *Protégé*	● *Expiré*
● *Inutilisé*	

Les icônes s'affichent par ordre alphabétique selon le nom du workload. Passez la souris sur une icône en forme de point pour afficher le nom du workload ou cliquez dessus pour consulter la page de détails correspondante.

Stockage fournit des informations sur l'espace de stockage disponible dans le conteneur pour PlateSpin Protect.

3.2.3 Panneau Tâches et événements

Le panneau Tâches et événements affiche les tâches et les événements passés les plus récents, ainsi que les prochains événements à venir.

Des événements sont consignés à chaque fois que quelque chose de particulier en rapport avec le système ou le workload se produit. Par exemple, l'ajout d'un nouveau workload protégé, la réplication d'un workload en cours de démarrage ou en état d'échec, ou encore la détection d'un échec de workload protégé constituent des événements. Certains événements génèrent des notifications automatiques par message électronique si SMTP est configuré. Reportez-vous à la section « Configuration des notifications automatiques des événements et rapports par message électronique » page 29.

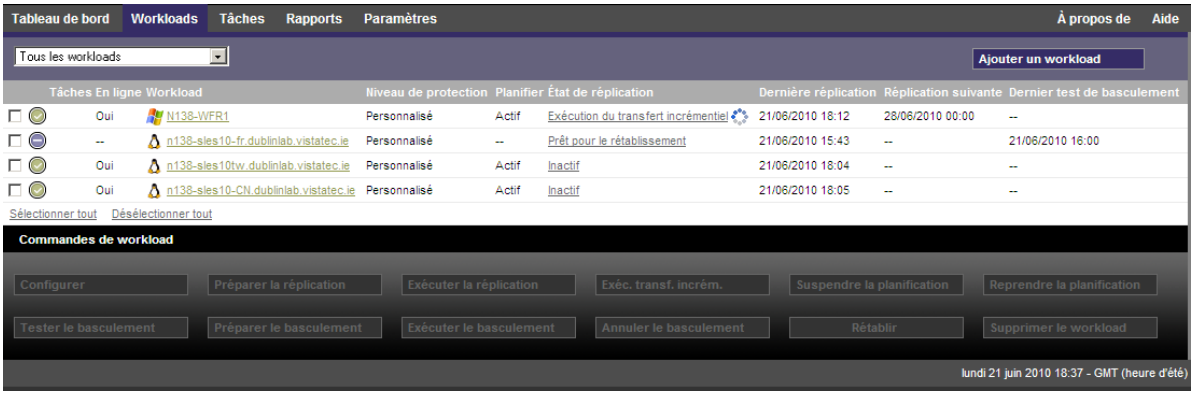
Les tâches sont des commandes spéciales qui sont liées à des événements exigeant l'intervention de l'utilisateur. Par exemple, à la fin de l'exécution d'une commande Tester le basculement, le système génère un événement associé à deux tâches : `Marquer le test comme réussi` et `Marquer le test comme échoué`. Un clic sur une de ces tâches entraîne l'annulation de l'opération Tester le basculement et l'enregistrement d'un événement dans l'historique. Autre exemple, l'événement `FullReplicationFailed`, qui est illustré en liaison avec une tâche `StartFull`. Vous trouverez la liste complète des tâches actuelles sous l'onglet *Tâches*.

Dans le panneau Tâches et événements du tableau de bord, chaque catégorie présente au maximum trois entrées. Pour voir toutes les tâches ou tous les événements passés et à venir, cliquez sur *Afficher tout* dans la section appropriée.

3.3 Workloads et commandes de workload

La page Workloads affiche un tableau dans lequel chaque ligne correspond à un workload inventorié. Cliquez sur le nom d'un workload pour afficher sa page de détails, qui permet de consulter ou d'éditer les configurations relatives au workload et à son état.

Figure 3-2 *Page Workloads*

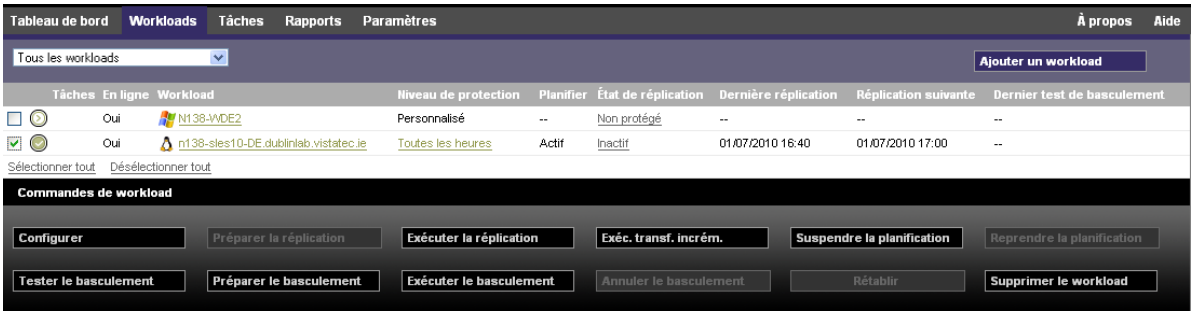


REMARQUE : tous les tampons horaire reflètent le fuseau horaire de l'hôte du serveur PlateSpin , lequel peut être différent du fuseau horaire du workload protégé ou de celui de l'hôte sur lequel vous exécutez l'interface Web PlateSpin Protect. La date et l'heure du serveur s'affichent en bas en droite de la fenêtre du client.

3.3.1 Commandes de protection et de récupération de workload

Les commandes représentent le workflow de protection et de récupération de workload. Pour exécuter une commande sur un workload, sélectionnez la case à gauche du workload correspondant. Les commandes applicables dépendent de l'état actuel du workload.

Figure 3-3 *Commandes de workload*



Le tableau suivant présente les commandes de workload et leur description fonctionnelle.

Tableau 3-2 *Commandes de protection et de récupération de workload*

Commande de workload	Description
Configurer	Démarre la configuration de protection de workload à l'aide des paramètres applicables à un workload inventorié.
Préparer la réplication	Installe le logiciel de transfert des données requis sur la source et crée un workload de basculement (une machine virtuelle) sur le conteneur cible en vue de la réplication du workload.
Exécuter la réplication	Commence à répliquer le workload en fonction des paramètres spécifiés (réplication complète).
Exécuter le transfert incrémentiel	Effectue un transfert incrémentiel des données modifiées de la source vers la cible, hors du contrat de protection des workloads.
Suspendre la planification	Suspend la protection ; toutes les réplications planifiées sont ignorées jusqu'à la reprise de la planification.
Reprendre la planification	Reprend la protection en fonction des paramètres de protection enregistrés.
Tester le basculement	Démarre et configure le workload de basculement dans un environnement isolé du conteneur à des fins de test.
Préparer le basculement	Démarre le workload de basculement en vue d'une opération de basculement.
Exécuter le basculement	Démarre et configure le workload de basculement qui reprend les services métier d'un workload ayant échoué.
Annuler le basculement	Abandonne le processus de basculement.
Rétablissement	À la suite d'une opération de basculement, rétablit le workload de basculement dans son infrastructure initiale ou dans une nouvelle infrastructure (virtuelle ou physique).

Commande de workload	Description
Supprimer le workload	Supprime un workload de l'inventaire.

3.4 Gestion de plusieurs instances de PlateSpin Protect et PlateSpin Forge

PlateSpin Protect inclut une application client basée sur le Web, la console de gestion PlateSpin Protect, qui fournit un accès centralisé à plusieurs instances de PlateSpin Protect et PlateSpin Forge.

Dans un centre de données comportant plusieurs instances de PlateSpin Protect, vous pouvez désigner l'une d'elles en tant que gestionnaire et exécuter la console de gestion à partir de cette dernière. Les autres instances sont ajoutées sous le gestionnaire, qui constitue un point de contrôle et d'interaction unique.

- Section 3.4.1, « Utilisation de la console de gestion de PlateSpin Protect », page 44
- Section 3.4.2, « À propos des cartes de la console de gestion de PlateSpin Protect », page 45
- Section 3.4.3, « Ajout d'instances de PlateSpin Protect et PlateSpin Forge à la console de gestion », page 46
- Section 3.4.4, « Gestion des cartes sur la console de gestion », page 46

3.4.1 Utilisation de la console de gestion de PlateSpin Protect

1. Ouvrez un navigateur Web sur une machine qui a accès aux instances de PlateSpin Protect et accédez à :

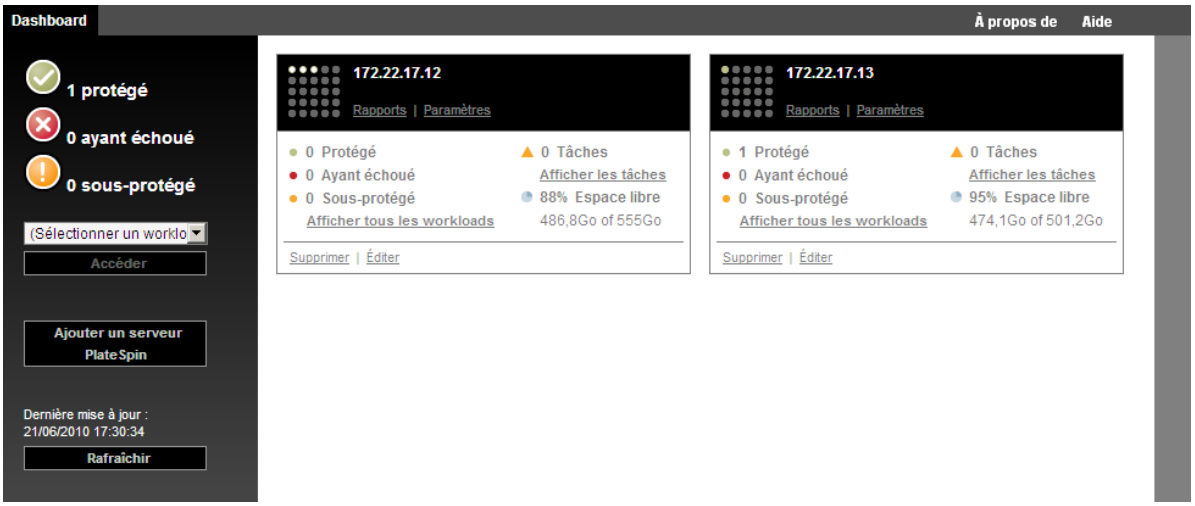
   `https://`*<adresse_IP | nom_hôte>*`/console`

   Remplacez *<adresse_IP | nom_hôte>* par l'adresse IP ou le nom de l'hôte du serveur PlateSpin désigné comme gestionnaire.

2. Loguez-vous à l'aide de votre nom d'utilisateur et votre mot de passe.

   La page Tableau de bord par défaut de la console s'affiche.

Figure 3-4 *Page Tableau de bord par défaut de la console de gestion*



3.4.2 À propos des cartes de la console de gestion de PlateSpin Protect

Lorsqu'une instance individuelle de PlateSpin Protect ou de PlateSpin Forge est ajoutée à la console de gestion, elle est représentée sous la forme d'une carte.

Figure 3-5 *Carte de l'instance PlateSpin Protect*

La carte affiche les informations de base relatives à l'instance correspondante de PlateSpin Protect ou de PlateSpin Forge, telles que :

- l'adresse IP/le nom d'hôte ;
- l'emplacement ;
- le numéro de version ;
- le nombre de workloads ;
- l'état des workloads ;
- la capacité de stockage ;
- l'espace libre disponible.

Chaque carte comporte des liens hypertexte qui permettent d'accéder aux pages Workloads, Rapports, Paramètres et Tâches de l'instance. D'autres liens hypertexte permettent d'éditer la configuration d'une carte ou de supprimer une carte de l'affichage.

3.4.3 Ajout d'instances de PlateSpin Protect et PlateSpin Forge à la console de gestion

L'ajout d'une instance de PlateSpin Protect ou de PlateSpin Forge à la console de gestion génère une nouvelle carte dans le tableau de bord de celle-ci.

REMARQUE : lorsque vous vous connectez à la console de gestion exécutée sur une instance de PlateSpin Protect et PlateSpin Forge, cette instance n'est pas automatiquement ajoutée à la console. L'ajout doit se faire manuellement.

Pour ajouter une instance de PlateSpin Protect ou PlateSpin Forge à la console :

1. Sur le tableau de bord principal de la console, cliquez sur *Ajouter un serveur PlateSpin*.

   La page *Ajouter/éditer* s'affiche.
2. Spécifiez l'URL de l'hôte du serveur PlateSpin ou de la machine virtuelle Forge. Utilisez HTTPS si SSL est activé.
3. (Facultatif) Cochez la case *Utiliser les références de la console de gestion* pour utiliser les mêmes références que celles employées par la console. Si vous cochez cette case, la console remplit automatiquement le champ *Domaine\nom d'utilisateur*.
4. Dans le champ *Domaine\nom d'utilisateur*, saisissez un nom de domaine et un nom d'utilisateur valides pour l'instance de PlateSpin Protect ou PlateSpin Forge que vous ajoutez. Dans le champ *Mot de passe*, saisissez le mot de passe adéquat.
5. (Facultatif) Spécifiez un *nom d'affichage* identifiant ou descriptif (maximum 15 caractères), un *emplacement* (maximum 20 caractères) et les éventuelles *remarques* que vous souhaitez ajouter (maximum 400 caractères).
6. Cliquez sur *Ajouter/enregistrer*.

   Une nouvelle carte est ajoutée au tableau de bord.

3.4.4 Gestion des cartes sur la console de gestion

Vous pouvez modifier les détails d'une carte sur la console de gestion.

1. Cliquez sur le lien hypertexte *Éditer* de la carte que vous souhaitez modifier.

   La page *Ajouter/éditer* de la console s'affiche.
2. Apportez les modifications souhaitées, puis cliquez sur *Ajouter/enregistrer*.

   Le tableau de bord de la console s'affiche en intégrant les modifications que vous venez d'effectuer.

Pour supprimer une carte de la console de gestion :

1. Cliquez sur le lien hypertexte *Supprimer* de la carte que vous souhaitez supprimer.

   Une invite de confirmation s'affiche.
2. Cliquez sur *OK*.

   Cette carte est supprimée du tableau de bord.

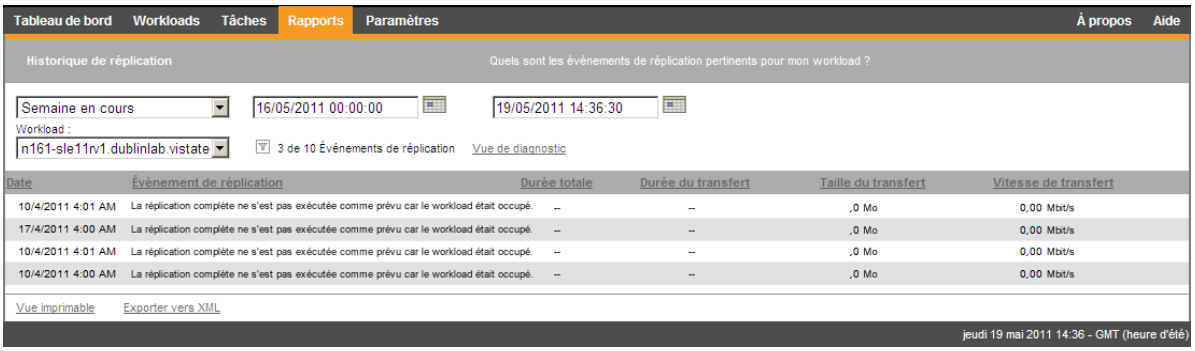
3.5 Génération de rapports sur les workloads et leur protection

PlateSpin Protect vous permet de générer des rapports fournissant un aperçu analytique de vos contrats de protection de workload dans le temps.

Les types de rapport suivants sont pris en charge :

- **Protection de workload :** reprend les événements de réplication pour tous les workloads, dans une plage de temps sélectionnable.
- **Historique de réplication :** reprend le type, la taille et l'heure de réplication ainsi que la vitesse de transfert pour chaque workload, dans une plage de temps sélectionnable.
- **Fenêtre de réplication :** reprend la dynamique des réplications complètes et incrémentielles, lesquelles peuvent être résumées selon les critères *Moyenne*, *Dernier/dernière*, *Somme* et *Pointe*.
- **État de protection actuel :** reprend les données *RPO cible*, *RPO réel*, *TTO réel*, *RTO réel*, *Dernier test de basculement*, *Dernière réplication* et les statistiques *Âge du test*.
- **Événements :** reprend les événements système pour tous les workloads, dans une plage de temps sélectionnable.
- **Événements planifiés :** reprend uniquement les événements de protection de workload à venir.

Figure 3-6 *Options d'un rapport de type Historique de réplication*



Pour générer un rapport :

1. Dans votre interface Web PlateSpin Protect, cliquez sur *Rapports*.

   Une liste des types de rapport s'affiche.
2. Cliquez sur le nom du type de rapport souhaité.

4 Protection de workload

PlateSpin Protect crée une réplique de votre workload de production et la met régulièrement à jour selon la planification que vous définissez.

La réplique, ou *workload de basculement*, est une machine virtuelle figurant dans le conteneur de VM de PlateSpin Protect qui reprend la fonction métier de votre workload de production en cas de perturbation au niveau du site de production.

4.1 Workflow de base pour la protection et la récupération de workload

PlateSpin Protect définit le workflow suivant pour la protection et la récupération de workload :

1 **Préparation :** il s'agit d'étapes préparatoires en vue de permettre à vos workloads, vos conteneurs et votre environnement de répondre aux critères requis.

   1a Vérifiez que PlateSpin Protect prend en charge votre workload.

   Reportez-vous à la section « Configurations prises en charge » page 11.

   1b Assurez-vous que vos workloads et conteneurs remplissent les critères réseau et d'accès.

   Reportez-vous à la section « Conditions d'accès et de communication requises sur votre réseau de protection » page 25.

   1c (Linux uniquement)

   - (Facultatif) Si vous envisagez de protéger un workload Linux pris en charge qui comporte un kernel non standard, personnalisé ou plus récent, reconstruisez le module PlateSpin `blkwatch` nécessaire à la réplication de données par bloc.

     Reportez-vous à l'article de la base de connaissances n° 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873).

- (Recommandé) Préparez des instantanés du gestionnaire de volumes logiques (LVM) pour le transfert de données par bloc. Assurez-vous que chaque groupe de volumes dispose de suffisamment d'espace libre pour accueillir les instantanés LVM (au moins 10 % de la somme de toutes les partitions).

  Reportez-vous à l'article de la base de connaissances n° 7005872 (https://www.netiq.com/support/kb/doc.php?id=7005872).

- (Facultatif) Préparez vos scripts `freeze` et `thaw` pour qu'ils s'exécutent sur votre workload source lors de chaque réplication.

  Reportez-vous à la « Utilisation des scripts freeze et thaw pour chaque réplication (Linux) » page 79.

2 **Inventaire :** cette étape comprend l'ajout de workloads et de conteneurs à la base de données du serveur PlateSpin.

  Les workloads que vous souhaitez protéger et les conteneurs qui hébergent des workloads de basculement doivent être correctement inventoriés. Vous pouvez ajouter des workloads et des conteneurs dans n'importe quel ordre ; cependant, chaque contrat de protection nécessite un workload et un conteneur définis qui ont été inventoriés par le serveur PlateSpin. Reportez-vous aux sections « Ajout de conteneurs (cibles de protection) » page 51 et « Ajout de workloads à protéger » page 52.

3 **Définition du contrat de protection :** cette étape consiste à définir les détails et les spécifications d'un contrat de protection, puis à préparer la réplication.

  Reportez-vous à la section « Configuration des détails de protection et préparation de la réplication » page 53.

4 **Lancement de la protection :** cette étape lance le contrat de protection conformément à vos exigences.

  Reportez-vous à la section « Démarrage de la protection du workload » page 56.

5 **Étapes facultatives dans le cycle de vie de protection :** ces étapes sortent du cadre de la planification de réplication automatisée. Cependant, elles peuvent généralement s'avérer utiles dans diverses situations ou être dictées par votre stratégie de continuité des opérations.

  - *Réplication incrémentielle manuelle*. Vous pouvez exécuter une réplication incrémentielle manuellement, en dehors du contrat de protection des workloads, en cliquant sur *Exécuter le transfert incrémentiel*.
  - *Test*. Vous pouvez tester la fonctionnalité de basculement dans un environnement et une procédure contrôlés. Reportez-vous à la section Utilisation de la fonction Tester le basculement.

6 **Basculement :** au cours de cette étape, un basculement de votre workload protégé est effectué vers sa réplique qui s'exécute dans votre conteneur de machines virtuelles. Reportez-vous à la section « Basculement » page 58.

7 **Rétablissement :** cette étape correspond à la phase de reprise des activités, après la résolution des problèmes liés à votre workload de production. Reportez-vous à la section « Rétablissement » page 60.

8 **Reprotection :** cette étape vous permet de redéfinir le contrat de protection d'origine pour votre workload. Reportez-vous à la section « Reprotection d'un workload » page 65.

La plupart de ces étapes sont représentées par des commandes de workload sur la page Workloads. Reportez-vous à la section « Workloads et commandes de workload » page 42.

La commande *Reprotéger* devient disponible après une opération de rétablissement réussie.

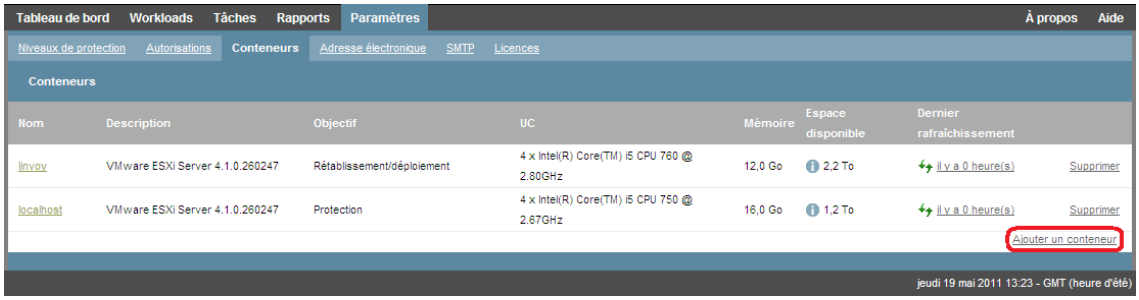
4.2 Ajout de conteneurs (cibles de protection)

Un conteneur est une infrastructure de protection opérant en tant qu'hôte d'une réplique régulièrement mise à jour d'un workload protégé. Cette infrastructure peut être un serveur VMware ESX ou une grappe VMware DRS.

Pour qu'il soit possible de protéger un workload, un workload et un conteneur doivent être inventoriés par le serveur PlateSpin (ou y être *ajoutés*).

Pour ajouter un conteneur :

1 Dans l'interface Web PlateSpin Protect, cliquez sur *Paramètres* > *Conteneurs* > *Ajouter un conteneur*.



2 Spécifiez les paramètres suivants :

- **Type :** sélectionnez le type de conteneur (*Serveur VMware ESX* ou *Grappe VMware DRS*). Assurez-vous que le conteneur sélectionné est pris en charge.

  Pour plus d'informations, reportez-vous à la section « Conteneurs de VM pris en charge » page 14.

- **Nom d'hôte ou adresse IP :** saisissez le nom d'hôte ou l'adresse IP du conteneur.
- **Nom d'hôte vCenter ou adresse IP :** (grappes DRS uniquement) entrez le nom d'hôte ou l'adresse IP du serveur vCenter.
- **Nom de la grappe :** (grappes DRS uniquement) entrez le nom de la grappe DRS souhaitée.

  Lorsque vous essayez d'ajouter ou de rafraîchir une grappe DRS, l'opération de découverte sous-jacente peut échouer si :

  - une grappe ne contient pas d'hôtes ESX ;
  - un nom de grappe n'est pas unique sur un serveur vCEnter (même si son chemin d'inventaire est unique) ;
  - aucun membre de la grappe n'est accessible (par exemple, parce que le serveur vCenter est en mode de maintenance).

- **Nom d'utilisateur/mot de passe :** indiquez des références d'administrateur pour accéder à l'hôte requis. Reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 68.
- **Objectif :** (conteneurs de VM uniquement) sélectionnez l'élément requis (*Protection*, *Rétablissement/déploiement* ou les deux). Si vous sélectionnez les deux éléments (*Protection* et *Rétablissement/déploiement*, le conteneur peut être sélectionné en tant que cible pour les opérations de protection et de rétablissement/déploiement.

3 Cliquez sur *Ajouter*.

PlateSpin Protect recharge la page Conteneurs et affiche un indicateur de processus pour le conteneur en cours d'ajout. Une fois le processus terminé, cet indicateur se transforme en icône *Rafraîchir*.

Pour rafraîchir un conteneur, cliquez sur l'icône *Rafraîchir* en regard de ce conteneur. Cela exécute un nouvel inventaire du conteneur.

Pour supprimer un conteneur, cliquez sur *Supprimer* en regard de ce conteneur.

4.3 Ajout de workloads à protéger

Un workload, l'objet de protection de base d'une banque de données, est un système d'exploitation comprenant des intergiciels et des données, dissocié de l'infrastructure virtuelle ou physique sous-jacente.

Pour protéger un workload, un workload et un conteneur doivent être inventoriés par le serveur PlateSpin (ou y être *ajoutés*).

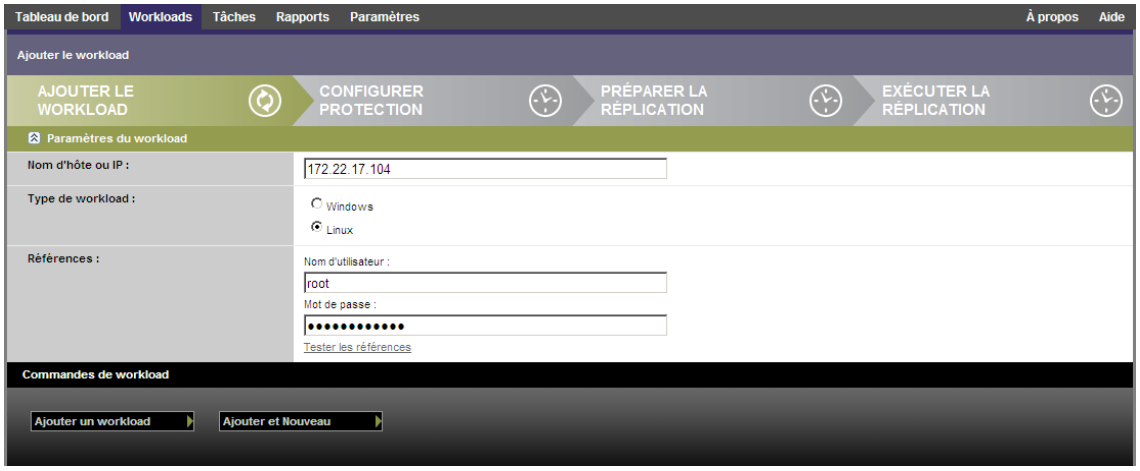
Pour ajouter un workload :

1. Suivez les étapes préparatoires requises.

   Reportez-vous à l'Étape 1 de la section « Workflow de base pour la protection et la récupération de workload » page 49.

2. Sur la page Tableau de bord ou Workloads, cliquez sur *Ajouter un workload*.

   L'interface Web PlateSpin Protect affiche la page Ajouter un workload.



3. Spécifiez les détails de workload requis.

   - **Paramètres du workload :** spécifiez le nom d'hôte et l'adresse IP de votre workload, le système d'exploitation, ainsi que les références de niveau administrateur.

     Utilisez le format requis pour les références. Reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 68.

     Pour vérifier que PlateSpin Protect peut accéder au workload, cliquez sur *Tester les références*.

4. Cliquez sur *Ajouter un workload*.

   PlateSpin Protect recharge la page Workloads et affiche un indicateur de processus pour le workload en cours d'ajout . Attendez que le processus se termine. Une fois l'opération terminée, un événement *Workload ajouté* est affiché dans le tableau de bord et le nouveau workload est disponible dans la page Workloads.

Si vous n'avez pas encore ajouté de conteneur, faites-le afin de préparer la protection du workload. Dans le cas contraire, passez à la section « Configuration des détails de protection et préparation de la réplication » page 53.

4.4 Configuration des détails de protection et préparation de la réplication

Les détails de protection contrôlent les paramètres de protection et de récupération de workload, ainsi que le comportement d'un workload protégé durant tout son cycle de vie. À chaque phase du workflow de protection et de récupération (voir section « Workflow de base pour la protection et la récupération de workload » page 49), les paramètres pertinents sont lus à partir des détails de protection.

Pour configurer les détails de protection de votre workload :

1. Ajoutez un workload. Reportez-vous à la section « Ajout de workloads à protéger » page 52.
2. Ajoutez un conteneur. Reportez-vous à la section « Ajout de conteneurs (cibles de protection) » page 51.
3. Sur la page Workloads, sélectionnez le workload souhaité, puis cliquez sur *Configurer*.

   Vous pouvez également cliquer sur le nom du workload.

   REMARQUE : si l'inventaire PlateSpin Protect ne contient pas encore de conteneur, le système vous invite à en ajouter un. Pour ce faire, cliquez sur *Ajouter un conteneur* au bas de l'écran.

4. Sélectionnez une *méthode de réplication initiale*. Celle-ci indique si les données de volume doivent être transférées entièrement de votre workload vers la machine virtuelle de basculement ou être synchronisées avec des volumes sur une machine virtuelle existante. Reportez-vous à la section « Méthode de réplication initiale (totale et incrémentielle) » page 77.
5. Assignez une cible de protection. Il peut s'agir d'un conteneur ou, si vous avez sélectionné *Réplication incrémentielle* comme méthode de réplication initiale, d'un workload *préparé*. Reportez-vous à la section « Méthode de réplication initiale (totale et incrémentielle) » page 77.

   REMARQUE : si votre inventaire ne comporte qu'un seul conteneur, votre workload est automatiquement assigné à ce dernier.

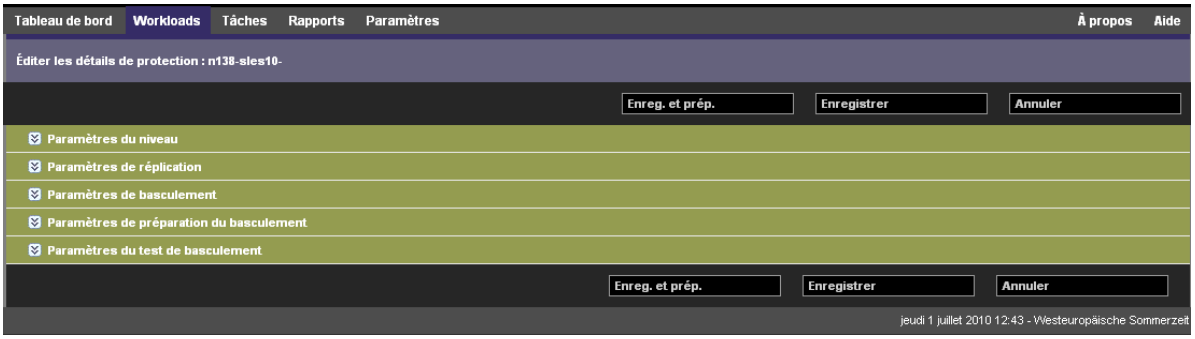
6. Configurez les détails de la protection dans chaque ensemble de paramètres en fonction de vos besoins en matière de continuité des opérations. Reportez-vous à la section « Détails de protection de workload » page 54.
7. Corrigez les erreurs de validation qu'affiche éventuellement l'interface Web PlateSpin Protect.
8. Cliquez sur *Enregistrer*.

   Vous pouvez également cliquer sur *Enregistrer et préparer*. Cette opération enregistre les paramètres et exécute simultanément la commande *Préparer la réplication* (en installant, si nécessaire, des pilotes de transfert de données sur le workload source et en créant une réplique de VM initiale de votre workload).

   Attendez que le processus se termine. Une fois terminé, un événement *La configuration du workload est terminée* s'affiche dans le tableau de bord.

4.4.1 Détails de protection de workload

Les détails de protection de workload sont représentés par cinq ensembles de paramètres :



Vous pouvez développer ou réduire chaque ensemble de paramètres en cliquant sur l'icône à gauche.

Le tableau suivant reprend les détails des cinq ensembles de paramètres :

Tableau 4-1 *Détails de protection du workload*

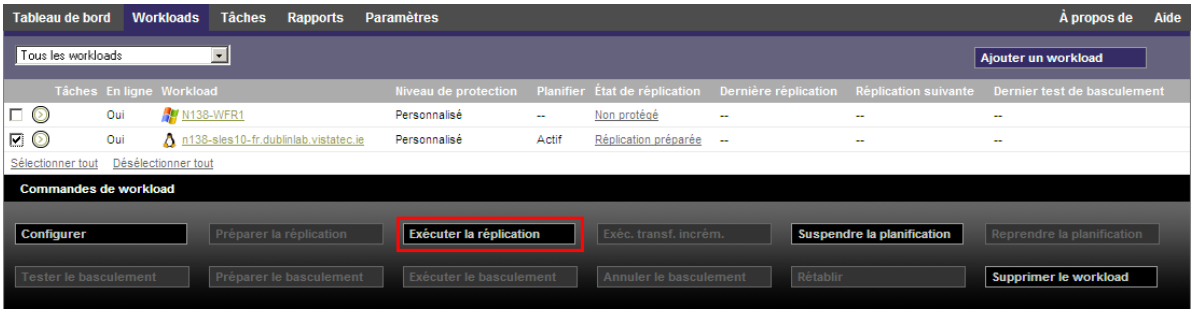
Ensemble de paramètres (paramètres)	Détails
Niveau	Indique le niveau de protection assuré par la protection actuelle. Reportez-vous à la section « Niveaux de protection » page 76.

Ensemble de paramètres (paramètres)	Détails
Réplication	**Méthode de transfert :** (Windows) permet de sélectionner un mécanisme de transfert des données ainsi qu'une sécurité par le biais du codage. Reportez-vous à la section « Transfert de données » page 74. **Chiffrement du transfert :** pour activer le codage, sélectionnez l'option *Coder le transfert des données*. Reportez-vous à la section « Sécurité et confidentialité » page 14. **Références sources :** requises pour accéder au workload. Reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 68. **Nombre d'UC :** permet de spécifier le nombre requis d'UC virtuelles assignées au workload de basculement (s'applique uniquement lorsque la méthode de réplication initiale sélectionnée est *Complète*). **Réseau de réplication :** permet de scinder le trafic de réplication en fonction des réseaux virtuels définis sur votre conteneur de VM. Reportez-vous à la section « Réseautique » page 82. **Banque de données des fichiers de configuration :** permet de sélectionner une banque de données associée au conteneur de votre machine virtuelle pour stocker les fichiers de configuration de la machine virtuelle. Reportez-vous à la section « Points de reprise » page 77. **Volumes protégés :** ces options permettent de sélectionner des volumes à protéger et d'assigner leurs répliques à des banques de données spécifiques de votre conteneur de VM. **Option de disque léger :** active la fonction de disque virtuel alloué dynamiquement, un disque virtuel qui se présente à la machine virtuelle avec une taille définie, mais qui ne consomme que l'espace disque effectivement requis par les données sur ce disque. **Services/daemons à arrêter pendant la réplication :** permet de sélectionner les services Windows ou les daemons Linux à arrêter automatiquement pendant la réplication. Reportez-vous à la section « Contrôle des services et des daemons » page 79.
Basculement	**Mémoire de la machine virtuelle :** permet de spécifier la quantité de mémoire allouée au workload de basculement. **Nom d'hôte et affiliation au domaine/groupe de travail :** ces options permettent de contrôler l'identité et l'affiliation à un domaine/groupe de travail du workload de basculement lorsqu'il est actif. Pour l'affiliation au domaine, les références de l'administrateur du domaine sont requises. **Connexions réseau :** ces options permettent de contrôler les paramètres LAN du workload de basculement. Reportez-vous à la section « Réseautique » page 82. **États des services/daemons à modifier :** permet de contrôler l'état de démarrage de services d'application (Windows) ou de daemons (Linux) spécifiques. Reportez-vous à la section « Contrôle des services et des daemons » page 79.
Préparer le basculement	Permet de contrôler les paramètres réseau temporaires du workload de basculement pendant l'opération facultative Préparer le basculement. Reportez-vous à la section « Réseautique » page 82.

Ensemble de paramètres (paramètres)	Détails
Test de basculement	**Mémoire de la machine virtuelle :** permet d'assigner la quantité de mémoire virtuelle requise au workload temporaire. **Nom d'hôte :** permet d'assigner un nom d'hôte au workload temporaire. **Domaine/groupe de travail :** permet d'affilier le workload temporaire à un domaine ou groupe de travail. Pour l'affiliation au domaine, les références de l'administrateur du domaine sont requises. **Connexions réseau :** contrôle les paramètres LAN du workload temporaire. Reportez-vous à la section « Réseautique » page 82. **États des services/daemons à modifier :** permet de contrôler l'état de démarrage de services d'application (Windows) ou de daemons (Linux) spécifiques. Reportez-vous à la section « Contrôle des services et des daemons » page 79.

4.5 Démarrage de la protection du workload

La protection du workload démarre avec la commande *Exécuter la réplication* :



Vous pouvez exécuter la commande Exécuter la réplication après avoir effectué les opérations suivantes :

- Ajout d'un workload.
- Configuration des détails de protection du workload.
- Préparation de la réplication initiale.

Lorsque vous êtes prêt à poursuivre :

1. Sur la page Workloads, sélectionnez le workload requis, puis cliquez sur *Exécuter la réplication*.
2. Cliquez sur *Exécuter*.

   PlateSpin Protect démarre l'exécution et affiche un indicateur de processus pour l'étape *Copier les données* .

REMARQUE : après la protection du workload :

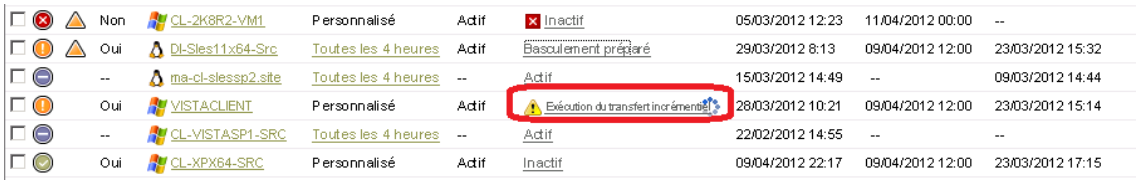
- Le changement de la taille d'un volume sous protection par bloc invalide la protection. La procédure appropriée consiste à 1. supprimer le workload de la protection, 2. redimensionner les volumes tel que requis ; 3. rétablir la protection en rajoutant le workload, en configurant ses détails de protection et en démarrant les réplications.
- Toute modification significative du workload protégé requiert le rétablissement de la protection. Exemples : l'ajout de volumes ou de cartes réseau au workload sous protection.

4.6 Abandon des commandes

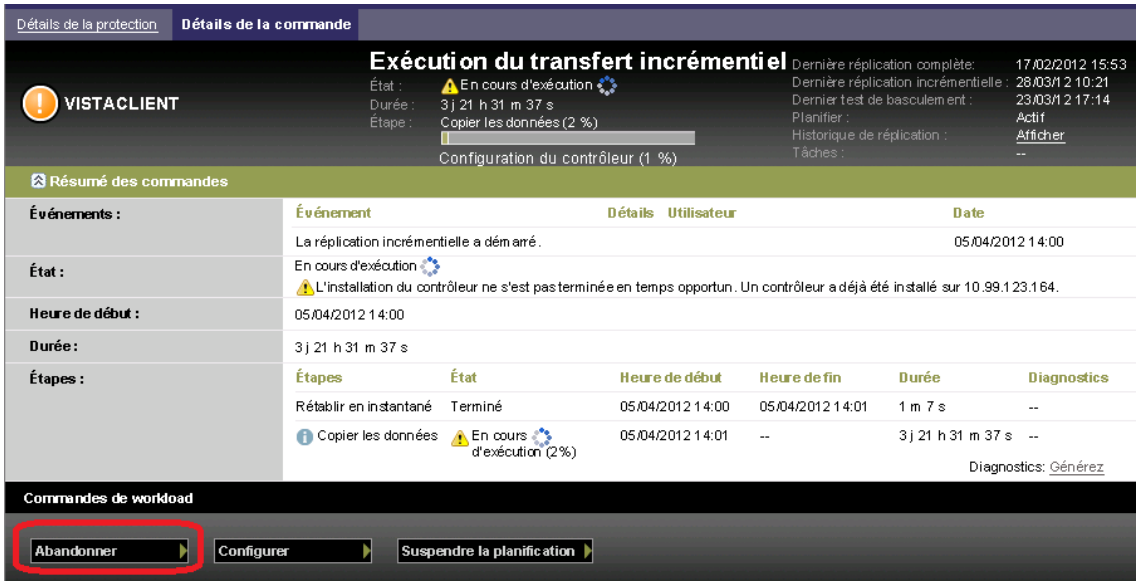
Vous pouvez abandonner une commande après ou pendant son exécution, sur la page Détails de la commande.

Pour accéder à la page Détails de la commande en cours d'exécution :

1. Accédez à la page Workloads.
2. Localisez le workload souhaité, puis cliquez sur le lien représentant la commande actuellement en cours d'exécution sur le workload.



L'interface Web PlateSpin Protect affiche la page Détails de la commande correspondante.



3. Cliquez sur *Abandonner*.

4.7 Basculement

Un *basculement* se produit lorsque la fonction métier d'un workload qui a échoué est reprise par un workload de basculement figurant dans un conteneur de machine virtuelle PlateSpin Protect.

- Section 4.7.1, « Détection des workloads hors ligne », page 58
- Section 4.7.2, « Exécution d'un basculement », page 59
- Section 4.7.3, « Utilisation de la fonction Tester le basculement », page 59

4.7.1 Détection des workloads hors ligne

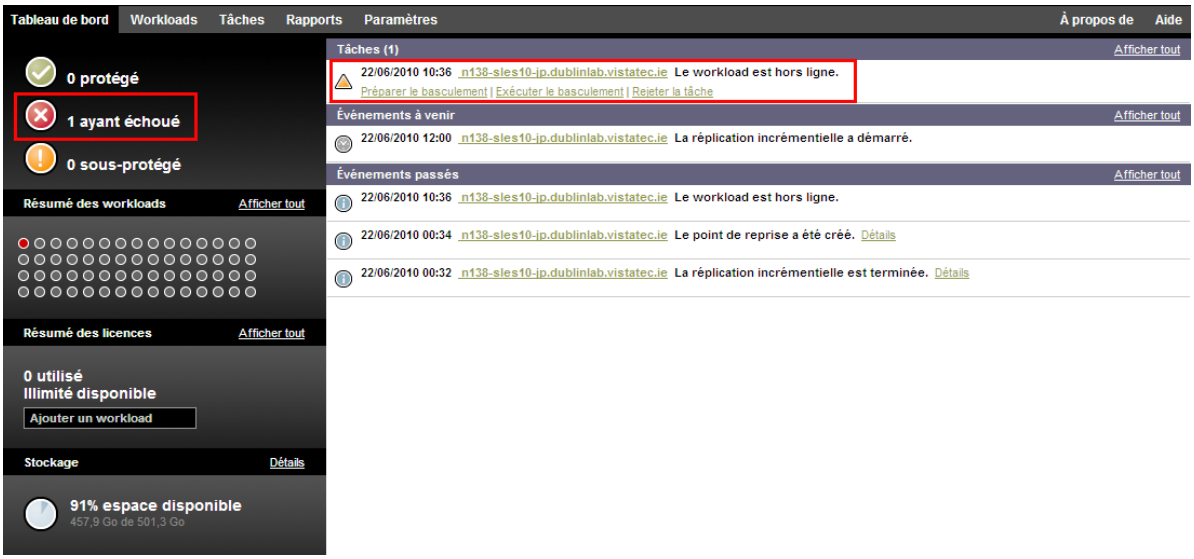
PlateSpin Protect surveille en permanence vos workloads protégés. Si une tentative de surveillance d'un workload échoue un certain nombre de fois, PlateSpin Protect génère un événement *Le workload est hors ligne*. Les critères qui déterminent et consignent les échecs de workload font partie des paramètres de niveau de protection de workload (reportez-vous à la ligne Niveau dans la section « Détails de protection de workload » page 54).

Si des notifications sont configurées avec des paramètres SMTP, PlateSpin Protect envoie simultanément une notification par message électronique aux destinataires spécifiés. Reportez-vous à la section « Configuration des notifications automatiques des événements et rapports par message électronique » page 29.

Si un échec de workload est détecté alors que l'état de la réplication est *Inactif*, vous pouvez exécuter la commande *Exécuter le basculement*. En cas d'échec d'un workload pendant un transfert incrémentiel, la tâche est interrompue. Dans ce cas, abandonnez la commande (reportez-vous à la section « Abandon des commandes » page 57), puis appliquez la commande *Exécuter le basculement*. Reportez-vous à la section « Exécution d'un basculement » page 59.

La figure ci-dessous représente la page Tableau de bord de l'interface Web PlateSpin Protect lorsqu'un échec de workload est détecté. Les tâches applicables s'affichent dans le volet des tâches et des événements.

Figure 4-1 *Page Tableau de bord en cas de détection d'un échec de workload (Workload hors ligne)*



4.7.2 Exécution d'un basculement

Les paramètres de basculement, dont les paramètres LAN et d'identité réseau du workload de basculement, sont enregistrés avec les détails de protection du workload au moment de la configuration. Reportez à la ligne Basculement dans la section « Détails de protection de workload » page 54.

Pour exécuter un basculement, vous pouvez utiliser les méthodes suivantes :

- Sélectionnez le workload souhaité sur la page Workloads et cliquez sur *Exécuter le basculement*.
- Cliquez sur le lien hypertexte de commande correspondant à l'événement *Le workload est hors ligne* dans le volet des tâches et des événements. Reportez-vous à la Figure 4-1.
- Exécutez une commande *Préparer le basculement* pour démarrer la machine virtuelle de basculement à temps. Vous pouvez toujours annuler le basculement (utile lors de basculement échelonnés).

Utilisez l'une de ces méthodes pour démarrer le processus de basculement et sélectionnez un point de reprise à appliquer au workload de basculement (reportez-vous à la section « Points de reprise » page 77). Cliquez sur *Exécuter* et surveillez la progression. Une fois le processus terminé, l'état de réplication du workload devrait être *Actif*.

Pour tester le workload ou le processus de basculement dans le cadre d'un exercice planifié de reprise après sinistre, reportez-vous à la section « Utilisation de la fonction Tester le basculement » page 59.

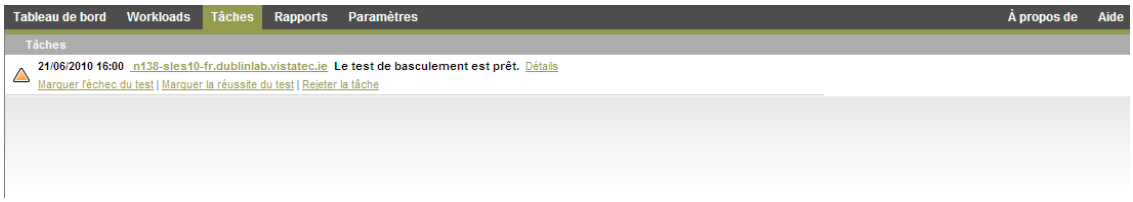
4.7.3 Utilisation de la fonction Tester le basculement

PlateSpin Protect permet de tester la fonctionnalité de basculement et l'intégrité du workload de basculement. Cette opération est effectuée à l'aide de la commande *Tester le basculement* qui démarre le workload de basculement dans un environnement réseau réservé au test.

Lorsque vous exécutez la commande, PlateSpin Protect applique au workload de basculement les paramètres du test de basculement tels qu'enregistrés dans les détails de protection de workload (reportez-vous à la ligne Test de basculement dans la section « Détails de protection de workload » page 54).

1. Définissez une fenêtre de temps appropriée pour les tests et vérifiez qu'aucune réplication n'est en cours. L'état de réplication du workload doit être *Inactif*.
2. Sur la page Workloads, sélectionnez le workload requis, cliquez sur *Tester le basculement*, sélectionnez un point de reprise (voir section « Points de reprise » page 77), puis cliquez sur *Exécuter*.

   Une fois l'opération terminée, PlateSpin Protect génère une tâche et un événement correspondants avec un ensemble de commandes applicables :



3. Vérifiez l'intégrité et la fonctionnalité métier du workload de basculement. Utilisez le client VMware vSphere pour accéder au workload de basculement dans le conteneur de VM.

4 Indiquez si le test a *échoué* ou *réussi*. Utilisez les commandes correspondantes dans la tâche (*Marquer l'échec du test*, *Marquer la réussite du test*). L'opération sélectionnée est enregistrée dans l'historique des événements associés au workload et peut être récupérée via les rapports. L'option *Fermer la tâche* rejette la tâche et l'événement.

   Lorsque la tâche *Marquer l'échec du test* ou *Marquer la réussite du test* est terminée, PlateSpin Protect rejette les paramètres temporaires appliqués au workload de basculement et la protection reprend son état d'avant le test.

4.8 Rétablissement

Une opération de rétablissement constitue l'étape logique à la suite d'un basculement. Elle transfère le workload de basculement vers son infrastructure d'origine ou, si nécessaire, vers une nouvelle infrastructure.

Les méthodes de rétablissement prises en charge dépendent du type de l'infrastructure cible et du degré d'automatisation du processus de rétablissement :

- **Rétablissement automatisé sur une machine virtuelle :** pris en charge pour les plates-formes VMware ESX et les grappes VMware DRS.
- **Rétablissement semi-automatisé sur une machine physique :** pris en charge pour toutes les machines physiques.
- **Rétablissement semi-automatisé sur une machine virtuelle :** pris en charge pour les plates-formes Xen sous SLES et Microsoft Hyper-V.

Pour un complément d'informations, reportez-vous aux sections suivantes :

- Section 4.8.1, « Rétablissement automatisé sur une plate-forme VM », page 60
- Section 4.8.2, « Rétablissement semi-automatisé sur une machine physique », page 63
- Section 4.8.3, « Rétablissement semi-automatisé sur une machine virtuelle », page 64

4.8.1 Rétablissement automatisé sur une plate-forme VM

Les conteneurs suivants sont pris en charge en tant que cibles de basculement automatisées :

Cible	Remarques
Grappe VMware DRS dans vSphere 5.15	◆ La configuration DRS doit être **Partiellement automatisé** ou **Entièrement automatisé** (mais ne peut pas être réglée sur **Manuel**). ◆ En tant que conteneur VM, la grappe DRS doit être constituée uniquement de serveurs ESXi 5.5 et peut uniquement être gérée par vCenter 5.5.
Grappe VMware DRS dans vSphere 5.1	◆ La configuration DRS doit être **Partiellement automatisé** ou **Entièrement automatisé** (mais ne peut pas être réglée sur **Manuel**). ◆ En tant que conteneur VM, la grappe DRS doit être uniquement constituée de serveurs ESXi 5.1 et peut uniquement être gérée par vCenter 5.1.
Grappe VMware DRS dans vSphere 5.0	◆ La configuration DRS doit être **Partiellement automatisé** ou **Entièrement automatisé** (mais ne peut pas être réglée sur **Manuel**). ◆ En tant que conteneur VM, la grappe DRS doit être constituée uniquement de serveurs ESXi 5.0 et peut uniquement être gérée par vCenter 5.0.

Cible	Remarques
Grappe VMware DRS dans vSphere 4.1	◆ La configuration DRS doit être **Partiellement automatisé** ou **Entièrement automatisé** (mais ne peut pas être réglée sur **Manuel**). ◆ En tant que conteneur VM, la grappe peut utiliser une combinaison de serveurs ESX 4.1 et ESX**i** 4.1 et peut uniquement être gérée par vCenter 4.1.
VMware ESX**i** 4.1, 5.0, 5.1	Les versions ESX**i** doivent disposer d'une licence payante ; la protection n'est pas prise en charge sur ces systèmes s'ils fonctionnent avec une licence gratuite.
VMware ESX 4.1	

Appliquez cette procédure pour effectuer un rétablissement automatisé d'un workload de récupération sur un conteneur VMware cible.

1. Après un basculement, sélectionnez le workload sur la page Workloads, puis cliquez sur *Rétablir*.

   Le système vous invite à effectuer les sélections suivantes :

2. Spécifiez les ensembles de paramètres suivants :
   - **Paramètres du workload :** spécifiez le nom d'hôte ou l'adresse IP du workload de basculement et entrez les références d'un administrateur. Utilisez le format requis pour les références (reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 68).
   - **Paramètres cibles du rétablissement :** spécifiez les paramètres suivants.
     - **Méthode de réplication :** sélectionnez l'étendue de la réplication des données. Si vous sélectionnez *Incrémentielle*, vous devez *préparer*. Reportez-vous à la section « Méthode de réplication initiale (totale et incrémentielle) » page 77.
     - **Type de cible :** sélectionnez *Cibles virtuelles*. Si vous ne disposez pas encore d'un conteneur de rétablissement, cliquez sur *Ajouter un conteneur* et inventoriez un conteneur pris en charge.

3. Cliquez sur *Enregistrer et préparer* et surveillez la progression sur l'écran Détails de la commande.

   Une fois cette opération terminée, PlateSpin Protect charge l'écran Prêt pour le rétablissement et vous invite à spécifier les détails de l'opération de rétablissement.

4. Configurez les détails du rétablissement. Reportez-vous à la section « Détails du rétablissement (Workload sur VM) » page 62.

5. Cliquez sur *Enregistrer et rétablir* et surveillez la progression sur la page Détails de la commande. Reportez-vous à la Figure 4-2.

   PlateSpin Protect exécute la commande. Si vous avez sélectionné l'option *Reprotection après rétablissement* dans l'ensemble *Paramètres de post-rétablissement*, une commande Reprotéger s'affiche dans l'interface Web PlateSpin Protect.

Figure 4-2 *Détails de la commande Rétablissement*

Détails du rétablissement (Workload sur VM)

Les détails du rétablissement sont représentés par trois ensembles de paramètres que vous configurez lorsque vous effectuez une opération de rétablissement de workload sur une machine virtuelle.

Tableau 4-2 *Détails du rétablissement (VM)*

Ensemble de paramètres (paramètres)	Détails
Rétablissement	**Méthode de transfert :** permet de sélectionner un mécanisme de transfert des données ainsi qu'une sécurité par le biais du codage. Reportez-vous à la section « Transfert de données » page 74. **Réseau de rétablissement :** permet de diriger le trafic de rétablissement sur un réseau dédié, sur la base des réseaux virtuels définis sur votre conteneur de VM. Reportez-vous à la section « Réseautique » page 82. **Banque de données de VM :** permet de sélectionner une banque de données associée à votre conteneur de rétablissement pour le workload cible. **Assignation de volumes :** si la méthode de réplication initiale est définie comme étant « Incrémentielle », cette option vous permet de sélectionner des volumes sources et de les assigner à des volumes sur la cible de rétablissement en vue de la synchronisation. **Services/daemons à arrêter :** permet de sélectionner les services Windows ou daemons Linux à arrêter automatiquement pendant le rétablissement. Reportez-vous à la section « Contrôle des services et des daemons » page 79. **Adresse alternative pour la source :** accepte la saisie d'une adresse IP supplémentaire pour la machine virtuelle basculée, le cas échéant. Reportez-vous à la section « Protection sur des réseaux publics et privés via NAT » page 28.

Ensemble de paramètres (paramètres)	Détails
Workload	***Nombre d'UC :*** permet de spécifier le nombre requis d'UC assignées au workload cible. **Mémoire de la machine virtuelle :** permet d'assigner la quantité de mémoire virtuelle requise au workload cible. **Nom d'hôte, Domaine/groupe de travail :** utilisez ces options pour contrôler l'identité du workload cible et vérifiez son appartenance à un domaine/groupe de travail. Pour l'affiliation au domaine, les références de l'administrateur du domaine sont requises. **Connexions réseau :** utilisez ces options pour spécifier l'assignation réseau du workload cible sur la base des réseaux virtuels du conteneur de VM sous-jacent. **États des services à modifier :** permet de contrôler l'état de démarrage de services d'application (Windows) ou de daemons (Linux) spécifiques. Reportez-vous à la section « Contrôle des services et des daemons » page 79.
Post-rétablissement	**Reprotéger le workload :** utilisez cette option si vous envisagez de recréer le contrat de protection pour le workload cible après le déploiement. Cela permet de conserver un historique continu des événements pour le workload et d'assigner ou de désigner automatiquement une licence de workload. ◆ ***Protéger à nouveau après rétablissement :*** sélectionnez cette option si vous prévoyez de recréer un contrat de protection pour le workload cible. Une fois le basculement terminé, une commande *Reprotection* est disponible dans l'interface Web PlateSpin Protect pour le workload basculé. ◆ ***Aucune reprotection :*** sélectionnez cette option si vous n'avez pas l'intention de recréer un contrat de protection pour le workload cible. Pour protéger le workload basculé après avoir terminé, vous devrez le réinventorier et reconfigurer ses détails de protection.

4.8.2 Rétablissement semi-automatisé sur une machine physique

Utilisez la procédure suivante pour rétablir un workload sur une machine physique après un basculement. La machine physique peut être l'infrastructure d'origine ou une nouvelle.

1. Enregistrez la machine physique souhaitée auprès de votre serveur PlateSpin . Reportez-vous à la section « Rétablissement vers des machines physiques » page 82.
2. Si des pilotes sont incompatibles ou manquants, téléchargez les pilotes requis dans la base de données des pilotes de périphérique de PlateSpin Protect. Reportez-vous à la section « Gestion des pilotes de périphérique » page 91.
3. Après un basculement, sélectionnez le workload sur la page Workloads, puis cliquez sur *Rétablir*.
4. Spécifiez les ensembles de paramètres suivants :
   - **Paramètres du workload :** spécifiez le nom d'hôte ou l'adresse IP du workload de basculement et entrez les références d'un administrateur. Utilisez le format requis pour les références (reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 68).
   - **Paramètres cibles du rétablissement :** spécifiez les paramètres suivants.
     - ***Méthode de réplication*** **:** sélectionnez l'étendue de la réplication des données.

       Reportez-vous à la section « Méthode de réplication initiale (totale et incrémentielle) » page 77.

- ***Type de cible*** **:** sélectionnez l'option *Cible physique*, puis la machine physique que vous avez enregistrée à l'Étape 1.

5 Cliquez sur *Enregistrer et préparer* et surveillez la progression sur l'écran Détails de la commande.

   Une fois cette opération terminée, PlateSpin Protect charge l'écran Prêt pour le rétablissement et vous invite à spécifier les détails de l'opération de rétablissement.

6 Configurez les détails du rétablissement, puis cliquez sur *Enregistrer et rétablir*.

   Surveillez la progression de l'opération sur l'écran Détails de la commande.

4.8.3 Rétablissement semi-automatisé sur une machine virtuelle

Ce type de rétablissement suit un processus similaire au Rétablissement semi-automatisé sur une machine physique pour une cible VM autre qu'un conteneur VMware pris en charge en mode natif. Durant ce processus, vous ordonnez au système de considérer une cible VM en tant que machine physique.

Le rétablissement semi-automatisé sur une VM est pris en charge sur les plates-formes VM cibles suivantes :

- Xen sous SLES 10 SP2
- Serveur Microsoft Hyper-V 2008 (*non* R2)

vous pouvez également effectuer un basculement semi-automatisé vers un conteneur prenant en charge le basculement entièrement automatisé (cibles VMware ESX et cibles de grappe DRS).

4.9 Reprotection d'un workload

Une opération de *reprotection*, qui est l'étape logique après un *basculement*, termine le cycle de vie de protection du workload avant qu'un nouveau cycle ne commence. Lorsqu'une opération de basculement a réussi, une commande de *reprotection* est disponible dans l'interface Web de PlateSpin Protect et le système applique les mêmes détails de protection que ceux indiqués lors de la configuration initiale du contrat de protection.

REMARQUE : la commande de *reprotection* n'est disponible que si vous sélectionnez l'option *Reprotéger* dans les détails de basculement. Reportez-vous à la section « Rétablissement » page 60.

Le reste du workflow couvrant le cycle de vie de protection est identique à celui de protection d'un workload normal ; vous pouvez le répéter autant de fois que nécessaire.

5 Notions fondamentales concernant la protection de workload

Cette section fournit des informations sur les différents aspects fonctionnels d'un contrat de protection de workload.

5.1 Consommation de licences de workload

Votre licence pour le produit PlateSpin Protect vous donne droit à un nombre spécifique de workloads que vous pouvez protéger par des licences de workload. Chaque fois que vous ajoutez un workload à protéger, le système utilise une licence de workload unique dans votre réserve de licences. Vous pouvez récupérer une licence consommée jusqu'à cinq fois en supprimant un workload.

Pour plus d'informations sur l'acquisition des licences pour le produit et leur activation, reportez-vous à la section « Activation de la licence du produit » page 19.

5.2 Directives relatives aux références de workload et de conteneur

PlateSpin Protect doit disposer d'un accès aux workloads de niveau administrateur, ainsi que d'une configuration de rôle appropriée pour les conteneurs. Tout au long du workflow de protection et de récupération de workload, PlateSpin Protect vous invite à spécifier des références qui doivent être indiquées dans un format spécifique.

Tableau 5-1 *Références de workload et de conteneur*

À découvrir	Références	Remarques
Tous les workloads Windows	Références d'administrateur local ou de domaine	Pour le nom d'utilisateur, utilisez le format suivant : ◆ Pour les machines membres du domaine : *autorité\principal* ◆ Pour les machines membres du groupe de travail : *nom_hôte\principal*
Grappes Windows	Références d'administrateur de domaine	
Tous les workloads Linux	Nom d'utilisateur et mot de passe de niveau root	Les comptes non root ne sont pas correctement configurés pour utiliser `sudo`. Reportez-vous à l'article de la base de connaissances n° 7920711.
VMware ESX/ ESXi 4.1 ; ESXi 5.0, ESXi 5.1, ESXi 5.5	Compte VMware avec configuration de rôle appropriée. Reportez-vous à la Section 5.3.1, « Utilisation d'outils pour définir des rôles VMware », page 69.	Si ESX est configuré pour l'authentification d'un domaine Windows, vous pouvez aussi utiliser vos références de domaine Windows.
VMware vCenter Server	Compte VMware avec configuration de rôle appropriée. Reportez-vous à la Section 5.3.1, « Utilisation d'outils pour définir des rôles VMware », page 69.	

5.3 Configuration de la mutualisation de la protection sous VMware

PlateSpin Protect s'accompagne de rôles utilisateur uniques (et d'un outil pour les créer dans un datacenter VMware) qui permettent à des utilisateurs de VMware ne disposant pas de privilèges d'administration (ou « utilisateurs habilités ») d'effectuer des opérations de cycle de vie Protect dans l'environnement VMware. En votre qualité de fournisseur de service, ces rôles vous offrent la possibilité de segmenter votre grappe VMware pour permettre la mutualisation : cela signifie que plusieurs conteneurs Protect sont instanciés dans votre datacenter afin de prendre en charge les clients ou « locataires » Protect qui souhaitent que leurs données, et la preuve même de leur existence, soient séparées des autres clients qui utilisent également le datacenter.

Cette section présente les informations suivantes :

5.3.1 Utilisation d'outils pour définir des rôles VMware

PlateSpin Protect requiert certains privilèges pour accéder à des tâches de l'infrastructure VMware (c'est-à-dire des « conteneurs » VMware) et les exécuter. De cette manière, le workflow et les fonctionnalités Protect sont disponibles dans cet environnement. Compte tenu de l'abondance des privilèges requis, NetIQ a créé un fichier qui définit les privilèges minimums requis et les rassemble respectivement dans trois rôles VMware personnalisés :

- Gestionnaire de machines virtuelles PlateSpin
- Gestionnaire d'infrastructure PlateSpin
- Utilisateur PlateSpin

Ce fichier de définition, `PlateSpinRole.xml`, est inclus dans l'installation du serveur PlateSpin Protect. Il s'accompagne d'un exécutable,`PlateSpin.VMwareRoleTool.exe`, qui accède au fichier pour permettre la création de ces rôles PlateSpin personnalisés dans un environnement vCenter cible.

Cette section présente les informations suivantes :

- « Syntaxe de ligne de commande de base » page 69
- « Drapeaux et paramètres de ligne de commande supplémentaires » page 69
- « Exemple d'utilisation de l'outil » page 70
- « (Option) Définition manuelle de rôles PlateSpin dans vCenter » page 70

Syntaxe de ligne de commande de base

À partir de l'emplacement d'installation de l'outil de rôle, exécutez ce dernier via la ligne de commande en utilisant la syntaxe de base suivante :

```
PlateSpin.VMwareRoleTool.exe /host=[host name/IP] /user=[user name] /role=[the
role definition file name and location] /create
```

REMARQUE : par défaut, le fichier de définition du rôle est situé dans le même dossier que l'outil de définition.

Drapeaux et paramètres de ligne de commande supplémentaires

Appliquez les paramètres suivants en fonction des besoins lorsque vous utilisez `PlateSpin.VMwareRoleTool.exe` pour créer ou mettre à jour des rôles dans vCenter :

`/create`	(obligatoire) Crée les rôles définis par le paramètre `/role`.
`/get_all_prvileges`	Affiche tous les privilèges définis par le serveur.

Drapeaux facultatifs

`/interactive`	Exécute l'outil avec des options interactives qui vous permettent, au choix, de créer des rôles individuels, de vérifier la compatibilité des rôles ou de répertorier tous les rôles disponibles.
`/password=[mot de passe]`	Fournit le mot de passe VMware (ignore l'invite de mot de passe).
`/verbose`	Affiche des informations détaillées.

Exemple d'utilisation de l'outil

Syntaxe : `PlateSpin.VMwareRoleTool.exe /host=houston_sales /user=pedrom /role=PlateSpinRole.xml /create`

Actions consécutives :

1. L'outil de définition de rôle s'exécute sur le serveur vCenter `houston_sales`, dont un administrateur porte le nom d'utilisateur `pedrom`.
2. En l'absence du paramètre `/password`, l'outil demande la saisie du mot de passe utilisateur que vous spécifiez alors.
3. L'outil accède au fichier de définition de rôles, `PlateSpinRole.xml`, situé dans le même répertoire que l'exécutable (il n'était pas nécessaire de définir son chemin d'accès de manière plus détaillée).
4. L'outil localise le fichier de définition et est invité à créer (`/create`) les rôles définis dans le contenu de ce fichier dans l'environnement vCenter.
5. L'outil accède au fichier de définition et crée les rôles (y compris les privilèges minimums requis pour l'accès limité défini) dans vCenter.

   Les nouveaux rôles personnalisés devront être assignés ultérieurement à des utilisateurs dans vCenter.

(Option) Définition manuelle de rôles PlateSpin dans vCenter

Utilisez le client vCenter pour créer et assigner manuellement les rôles PlateSpin personnalisés. Cela suppose la création des rôles avec les privilèges énumérés, tels qu'ils sont définis dans le fichier `PlateSpinRole.xml`. Lorsque vous optez pour une création manuelle, il n'existe aucune restriction quant au nom du rôle. La seule limite est la suivante : les noms de rôle que vous créez comme équivalents des rôles du fichier de définition ont tous les privilèges minimums appropriés du fichier de définition.

Pour plus d'informations sur la création de rôles personnalisés dans vCenter, consultez le document *Managing VMWare VirtualCenter Roles and Permissions* (http://www.vmware.com/pdf/vi3_vc_roles.pdf) (Gestion de rôles et d'autorisations VMWare VirtualCenter) dans le Centre des ressources techniques VMware.

5.3.2 Assignation de rôles dans vCenter

Lorsque vous configurez un environnement de mutualisation, vous devez provisionner un seul serveur Protect par client ou « locataire ». Vous assignez à ce serveur Protect un utilisateur habilité avec des rôles Protect VMware particuliers. Cet utilisateur est celui qui crée le conteneur Protect. En tant que fournisseur de service, vous conservez les références de cet utilisateur et vous ne les divulguez pas à votre client locataire.

Le tableau ci-dessous répertorie les rôles que vous devez définir pour l'utilisateur habilité. Il contient également des informations supplémentaires sur la finalité du rôle :

Conteneur vCenter pour l'assignation de rôles	**Particularités de l'assignation de rôles**	**Instructions de propagation**	**Pour plus d'informations**
Racine de l'arborescence d'inventaire de vCenter.	Assignez à l'utilisateur habilité le rôle *Gestionnaire d'infrastructure PlateSpin* (ou équivalent).	Pour des raisons de sécurité, définissez l'autorisation sans l'attribut de propagation.	Ce rôle est nécessaire pour surveiller les tâches en cours d'exécution par le logiciel Protect et mettre fin à toute session VMware périmée.
Tous les objets du datacenter auxquels l'utilisateur habilité doit accéder.	Assignez à l'utilisateur habilité le rôle *Gestionnaire d'infrastructure PlateSpin* (ou équivalent).	Pour des raisons de sécurité, définissez l'autorisation sans l'attribut de propagation.	Ce rôle est nécessaire pour autoriser l'accès aux banques de données du datacenter en vue du téléchargement de fichiers. Définissez l'autorisation sans l'attribut de propagation.
Chaque grappe à ajouter à Protect en tant que conteneur et chaque hôte contenu dans la grappe.	Assignez à l'utilisateur habilité le rôle *Gestionnaire d'infrastructure PlateSpin* (ou équivalent).	La propagation est laissée à l'appréciation de l'administrateur VMware.	Pour assigner un élément à un hôte, propagez l'autorisation à partir de l'objet de grappe ou créez une autorisation supplémentaire sur chaque hôte de la grappe. Si le rôle est assigné sur l'objet de grappe et propagé, aucune autre modification n'est nécessaire lors de l'ajout d'un nouvel hôte à la grappe. La propagation de cette autorisation a toutefois des implications sur le plan de la sécurité.
Chaque réserve de ressources à laquelle l'utilisateur habilité doit accéder.	Assignez le rôle *Gestionnaire de machines virtuelles PlateSpin* (ou équivalent) à l'utilisateur habilité.	La propagation est laissée à l'appréciation de l'administrateur VMware.	Vous pouvez assigner l'accès à un nombre indéfini de réserves de ressources, à n'importe quel emplacement de l'arborescence. Cependant, vous devez assigner ce rôle à l'utilisateur habilité pour au moins une réserve de ressources.
Chaque dossier de machines virtuelles auquel l'utilisateur habilité doit accéder.	Assignez le rôle *Gestionnaire de machines virtuelles PlateSpin* (ou équivalent) à l'utilisateur habilité.	La propagation est laissée à l'appréciation de l'administrateur VMware.	Vous pouvez assigner l'accès à un nombre indéfini de dossiers de machines virtuelles, à n'importe quel emplacement de l'arborescence. Cependant, vous devez assigner ce rôle à l'utilisateur habilité pour au moins un dossier.

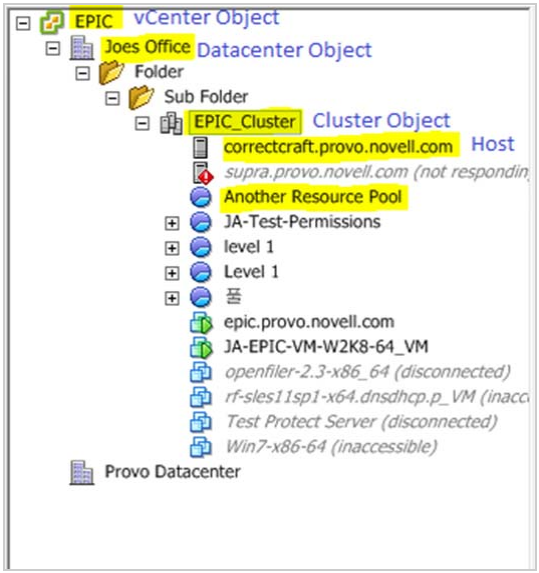
Conteneur vCenter pour l'assignation de rôles	Particularités de l'assignation de rôles	Instructions de propagation	Pour plus d'informations
Chaque réseau auquel l'utilisateur habilité doit accéder. Réseaux virtuels distribués avec dvSwitch et dvPortgroup.	Assignez le rôle *Gestionnaire de machines virtuelles PlateSpin* (ou équivalent) à l'utilisateur habilité.	La propagation est laissée à l'appréciation de l'administrateur VMware.	Vous pouvez assigner l'accès à un nombre indéfini de réseaux, à n'importe quel emplacement de l'arborescence. Cependant, vous devez assigner ce rôle à l'utilisateur habilité pour au moins un dossier. ◆ Pour assigner le rôle correct au paramètre dvSwitch, propagez le rôle sur le datacenter (un objet supplémentaire reçoit alors le rôle) ou placez le paramètre dvSwitch dans un dossier et assignez le rôle à ce dossier. ◆ Pour qu'un groupe de ports standard soit répertorié comme réseau disponible dans l'interface utilisateur de Protect, créez une définition correspondante sur chaque hôte de la grappe.
Chaque banque de données et chaque grappe de banques de données auxquelles l'utilisateur habilité doit accéder.	Assignez le rôle *Gestionnaire de machines virtuelles PlateSpin* (ou équivalent) à l'utilisateur habilité.	La propagation est laissée à l'appréciation de l'administrateur VMware.	Il faut que ce rôle ait été assigné à l'utilisateur habilité pour au moins une banque de données ou grappe de banques de données. Dans le cas des grappes de banques de données, l'autorisation doit être propagée aux banques de données qu'elles contiennent. Si l'accès n'est pas accordé à un membre de la grappe, la préparation et les réplications complètes échouent.

Le tableau ci-dessous indique le rôle que vous pouvez assigner au client ou à l'utilisateur locataire.

Conteneur vCenter pour l'assignation de rôles	Particularités de l'assignation de rôles	Instructions de propagation	Pour plus d'informations
Chaque réserve de ressources et chaque dossier dans lesquels les machines virtuelles du client seront créées.	Assignez le rôle *Utilisateur PlateSpin* (ou équivalent) à l'utilisateur locataire.	La propagation est laissée à l'appréciation de l'administrateur VMware.	Ce locataire est membre du groupe Administrateurs PlateSpin sur le serveur PlateSpin Protect. Il figure également sur le serveur vCenter. Si le locataire se voit accorder la possibilité de modifier les ressources utilisées par la machine virtuelle (en d'autres termes les réseaux, les images ISO, etc.), octroyez-lui les autorisations nécessaires sur ces ressources. Par exemple, si vous souhaitez autoriser le client à modifier le réseau auquel sa machine virtuelle est connectée, il doit se voir accorder, au minimum, le rôle Lecture seule sur tous les réseaux auxquels il a accès.

La figure ci-dessous illustre une infrastructure virtuelle dans la console vCenter. Le rôle Gestionnaire d'infrastructure est assigné aux objets avec un libellé bleu. Le libellé vert indique les objets auxquels le rôle Gestionnaire de machines virtuelles a été assigné. Les dossiers de machines virtuelles, les réseaux et les banques de données ne sont pas affichés dans l'arborescence. Ces objets se voient assigner le rôle *Gestionnaire de machines virtuelles PlateSpin*.

Figure 5-1 *Rôles assignés dans vCenter*



Implications de l'assignation de rôles VMware sur le plan de la sécurité

Dans le logiciel PlateSpin, seul un utilisateur habilité peut effectuer des opérations relatives au cycle de vie de protection. Du point de vue d'un fournisseur de service, un utilisateur final n'a jamais accès aux références de l'utilisateur habilité et n'est pas en mesure d'accéder au même ensemble de ressources VMware. Dans un environnement où plusieurs serveurs Protect sont configurés de manière à utiliser le même environnement vCenter, Protect empêche tout accès inter-clients. Les principales implications sur le plan de la sécurité sont les suivantes :

- Lorsque le rôle *Gestionnaire d'infrastructure PlateSpin* est assigné à l'objet vCenter, chaque utilisateur habilité peut voir les tâches effectuées par tous les autres, mais pas les influencer.
- Compte tenu de l'impossibilité de définir des autorisations sur les dossiers/sous-dossiers d'une banque de données, tous les utilisateurs habilités disposant d'autorisations sur la banque de données ont accès aux disques de tous leurs homologues stockés dans cette banque de données.
- Lorsque le rôle *Gestionnaire d'infrastructure PlateSpin* est assigné à l'objet Grappe, chaque utilisateur habilité est en mesure d'activer ou de désactiver HA ou DRS sur l'ensemble de la grappe.
- Lorsque le rôle *Utilisateur PlateSpin* est assigné au niveau de l'objet Grappe de stockage, chaque utilisateur habilité est en mesure d'activer ou de désactiver SDRS sur l'ensemble de la grappe.
- La définition du rôle *Gestionnaire d'infrastructure PlateSpin* sur l'objet Grappe DRS et la propagation de ce rôle permettent à l'utilisateur habilité de voir toutes les machines virtuelles placées dans la réserve de ressources et/ou le dossier de machines virtuelles par défaut. La propagation exige, en outre, que l'administrateur configure explicitement l'utilisateur habilité de telle sorte qu'il dispose d'un rôle de type « sans accès » sur les réserves de ressources/dossiers de machines virtuelles auxquels il ne doit pas accéder.
- La définition du rôle *Gestionnaire d'infrastructure PlateSpin* sur l'objet vCenter permet à l'utilisateur habilité de mettre fin aux sessions de tout autre utilisateur connecté à vCenter.

REMARQUE : pour rappel, dans ces scénarios, les différents utilisateurs habilités représentent, en réalité, des instances différentes du logiciel PlateSpin.

5.4 Transfert de données

Vous trouverez, dans les rubriques suivantes, des informations sur les mécanismes et les options de transfert des données depuis vos workloads vers leur répliques.

- Section 5.4.1, « Méthodes de transfert », page 74
- Section 5.4.2, « Chiffrement de données », page 75

5.4.1 Méthodes de transfert

La méthode de transfert correspond à la façon dont les données sont répliquées d'un workload source vers un workload cible. PlateSpin Protect propose différentes techniques de transfert des données en fonction du système d'exploitation du workload protégé.

- « Méthodes de transfert prises en charge pour les workloads Windows » page 75
- « Méthodes de transfert prises en charge pour les workloads Linux » page 75

Méthodes de transfert prises en charge pour les workloads Windows

S'agissant des workloads Windows, PlateSpin Protect fournit des mécanismes permettant de transférer des données de volume de workload au niveau du bloc ou du fichier.

- **Réplication au niveau du bloc Windows :** les données sont répliquées sur la base de blocs d'un volume. Pour cette méthode de transfert, PlateSpin Protect fournit deux mécanismes qui diffèrent sur le plan de l'impact et des performances. Vous pouvez basculer entre ces deux mécanismes en fonction des besoins.
  - **Réplication à l'aide du composant basé sur les blocs :** cette option utilise un composant logiciel dédié pour le transfert de données au niveau du bloc et tire parti du service VSS (Volume Snapshot Service) de Microsoft avec les applications et services qui le prennent en charge. L'installation du composant sur votre workload protégé est automatique.

    REMARQUE : l'installation et la désinstallation du composant basé sur les blocs nécessitent un redémarrage du workload protégé. Aucun redémarrage n'est nécessaire lorsque vous protégez des grappes Windows avec un transfert de données au niveau du bloc. Lorsque vous configurez les détails de protection du workload, vous pouvez choisir d'installer le composant ultérieurement, différant ainsi le redémarrage requis jusqu'à l'exécution de la première réplication.

  - **Réplication sans composant basé sur les blocs :** cette option utilise un mécanisme de « hachage » interne combiné au service VSS de Microsoft pour effectuer le suivi des modifications apportées aux volumes protégés.

    Aucun redémarrage n'est nécessaire, mais les performances sont inférieures à celles obtenues avec le composant basé sur les blocs.
- **Réplication au niveau du fichier Windows :** les données sont répliquées fichier par fichier (Windows seulement).

Méthodes de transfert prises en charge pour les workloads Linux

S'agissant des workloads Linux, PlateSpin Protect fournit un mécanisme permettant de transférer les données de volume de workload uniquement au niveau du bloc. Le transfert de données est effectué par un composant dédié qui tire parti d'instantanés LVM, s'ils sont disponibles (il s'agit de l'option par défaut dont l'utilisation est conseillée). Reportez-vous à l'article de la base de connaissances n° 7005872 (https://www.netiq.com/support/kb/doc.php?id=7005872).

Le composant basé sur les blocs Linux inclus dans votre distribution PlateSpin Protect est précompilé pour les kernels standard de non-débogage des distributions Linux prises en charge. Si vous disposez d'un kernel non standard, personnalisé ou plus récent, vous pouvez reconstruire le composant basé sur les blocs pour votre kernel spécifique. Reportez-vous à l'article de la base de connaissances n° 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873).

Le déploiement ou la suppression du composant sont transparents, n'ont pas d'impact sur la continuité et ne nécessitent aucune intervention ni redémarrage.

5.4.2 Chiffrement de données

Pour sécuriser davantage le transfert de données de workload, PlateSpin Protect permet de coder la réplication des données. Lorsque le codage est activé, le transfert de données sur le réseau de la source vers la cible est codé à l'aide de l'algorithme AES (Advanced Encryption Standard) ou 3DES si un codage compatible FIPS est activé (voir section « Activation de la prise en charge des algorithmes de codage de données conformes à la norme FIPS (facultatif) » du *Guide d'installation et de mise à niveau*).

REMARQUE : le codage de données a un impact sur les performances et peut ralentir considérablement le transfert des données.

5.5 Niveaux de protection

Un niveau de protection est une collection personnalisable de paramètres de protection de workload qui définissent :

- la fréquence et le schéma de récurrence des réplications ;
- s'il faut coder la transmission de données ;
- s'il faut appliquer la compression des données et comment ;
- s'il faut limiter la bande passante disponible à un débit défini durant le transfert des données ;
- les critères à appliquer par le système pour considérer un workload comme étant hors ligne (échec).

Un niveau de protection fait partie intégrante de chaque contrat de protection de workload. Durant la phase de configuration d'un contrat de protection de workload, vous pouvez sélectionner un ou plusieurs niveaux de protection intégrés et personnaliser les attributs comme requis par ce contrat spécifique de protection de workload.

Vous pouvez également créer des niveaux de protection personnalisés à l'avance :

1. Dans l'interface Web PlateSpin Protect, cliquez sur *Paramètres* > *Niveaux de protection* > *Créer un niveau de protection*.
2. Spécifiez les paramètres du nouveau niveau de protection :

Nom	Saisissez le nom que vous souhaitez utiliser pour le niveau.
Récurrence incrémentielle	Spécifiez la fréquence des réplications incrémentielles ainsi que le schéma de récurrence incrémentielle. Vous pouvez saisir les données directement dans le champ *Début de la récurrence* ou cliquer sur l'icône du calendrier pour sélectionner une date. Sélectionnez *Aucun* comme schéma de récurrence pour ne jamais utiliser la réplication incrémentielle.
Récurrence totale	Spécifiez la fréquence des réplications complètes ainsi que le schéma de récurrence totale.
Fenêtre d'interdiction	Ces paramètres permettent de forcer une interdiction de réplication (afin de suspendre les réplications planifiées pendant les heures de pointe ou d'éviter les conflits entre le logiciel compatible VSS et le composant PlateSpin VSS de transfert de données par bloc). Pour spécifier une fenêtre d'interdiction, cliquez sur *Éditer*, puis sélectionnez le schéma de récurrence d'interdiction (quotidien, hebdomadaire, etc.) ainsi que le début et la fin de la période d'interdiction. **REMARQUE :** les heures de début et de fin de l'interdiction sont basées sur l'horloge système de votre serveur PlateSpin .

Niveau de compression	Ces paramètres déterminent si les données de workload sont compressées avant la transmission et de quelle manière. Reportez-vous à la section « Compression des données » page 16. Sélectionnez l'une des options disponibles. *Rapide* exploite les ressources du processeur au minimum, mais applique un faible taux de compression ; *Maximum* exploite les ressources du processeur au maximum, mais applique un taux de compression élevé. *Optimal* est l'option intermédiaire recommandée.
Limitation de la bande passante	Ces paramètres définissent la limitation de bande passante. Reportez-vous à la section « Limitation de la bande passante » page 16. Pour limiter le débit des réplications, spécifiez une valeur en Mbits/s et indiquez le modèle temporel.
Points de reprise à conserver	Spécifiez le nombre de points de reprise à conserver pour les workloads utilisant ce niveau de protection. Reportez-vous à la section « Points de reprise » page 77.
Échec du workload	Spécifiez le nombre limite de tentatives de détection du workload avant qu'il ne soit considéré comme ayant échoué.
Détection de workload	Spécifiez l'intervalle de temps (en secondes) entre les tentatives de détection du workload.

5.6 Points de reprise

Un point de reprise est une copie instantanée d'un workload et permet de restaurer un workload répliqué dans un état spécifique.

Chaque workload protégé dispose au minimum d'un point de reprise et peut en compter au maximum 32.

AVERTISSEMENT : si vous accumulez de nombreux points de reprise au fil du temps, votre stockage PlateSpin Protect risque de manquer d'espace.

5.7 Méthode de réplication initiale (totale et incrémentielle)

Dans les opérations de protection et de rétablissement de workload, le paramètre Réplication initiale détermine l'étendue des données transférées depuis une source vers une cible.

- **Complète :** un transfert de volumes complet a lieu du workload de production vers sa réplique (le workload de basculement) ou du de basculement vers son infrastructure virtuelle ou physique d'origine.
- **Incrémentielle :** seules les différences sont transférées depuis une source vers sa cible, à condition qu'elles aient un système d'exploitation et des profils de volume similaires.
  - Au cours de la protection : le workload de production est comparé à une machine virtuelle dans le conteneur de machines virtuelles. La VM existante peut être :
    - une machine virtuelle de récupération d'un workload précédemment protégé (quand l'option *Supprimer la machine virtuelle* de la commande *Supprimer le workload* est désélectionnée) ;

- une machine virtuelle importée manuellement dans le conteneur de machines virtuelles, comme une machine virtuelle de workload déplacée physiquement, sur un support portable, du site de production vers un site de récupération distant.

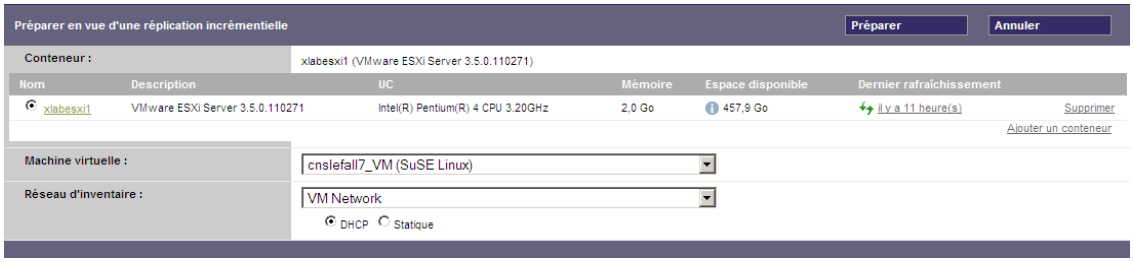
  Pour plus de détails, reportez-vous à la documentation de VMware.

- Au cours du rétablissement vers une machine virtuelle : le workload de basculement est comparé à une machine virtuelle dans un conteneur de rétablissement.
- Au cours du rétablissement vers une machine physique : le workload de basculement est comparé à un workload sur la machine physique cible, si elle est enregistrée auprès de PlateSpin Protect (reportez-vous à la section « Rétablissement semi-automatisé sur une machine physique » page 63).

Au cours de la protection de workload et du rétablissement vers un hôte de VM, la sélection de la méthode de réplication initiale *Incrémentielle* nécessite de rechercher la machine virtuelle cible pour la localiser et la préparer en vue de la synchronisation avec la source de l'opération sélectionnée.

1. Exécutez la commande de workload requise telle que *Configurer (Détails de la protection)* ou *Rétablissement*.
2. Choisissez comme *Méthode de réplication initiale* l'option *Réplication incrémentielle*.
3. Cliquez sur *Préparer un workload*.

   L'interface Web PlateSpin Protect affiche la page Préparer en vue d'une réplication incrémentielle.



4. Sélectionnez le conteneur requis, la machine virtuelle et le réseau d'inventaire à utiliser pour communiquer avec la machine virtuelle. Si le conteneur cible spécifié est une grappe DRS VMware, vous pouvez également spécifier une réserve de ressources cible auquel le système doit assigner le workload.
5. Cliquez sur *Préparer*.

   Attendez que le processus soit terminé et que l'interface utilisateur présente à nouveau la commande d'origine, puis sélectionnez le workload préparé.

REMARQUE : (réplications de données par bloc uniquement) la réplication incrémentielle initiale prend beaucoup plus de temps que les réplications suivantes. Cela est dû au fait que le système doit comparer les volumes sur la source et la cible bloc par bloc. Les réplications suivantes s'appuient sur les changements détectés par le composant basé sur les blocs pendant qu'il surveille un workload en cours d'exécution.

5.8 Contrôle des services et des daemons

PlateSpin Protect vous permet de contrôler les services et les daemons :

- **Contrôle des services et des daemons sources :** au cours du transfert de données, vous pouvez arrêter automatiquement les services Windows ou les daemons Linux qui s'exécutent sur votre workload source. Vous veillez ainsi à ce que le workload soit répliqué dans un état plus stable que lorsque les services restent en cours d'exécution.

  Par exemple, pour les workloads Windows, veillez à arrêter les logiciels Anti-virus ou les services des logiciels de sauvegarde tiers prenant en charge VSS.

  Pour obtenir un contrôle supplémentaire des sources Linux au cours de la réplication, pensez à la fonction d'exécution de scripts personnalisés sur vos workloads Linux au cours de chaque réplication. Reportez-vous à la section « Utilisation des scripts freeze et thaw pour chaque réplication (Linux) » page 79.

- **Contrôle de l'état de démarrage/du niveau d'exécution de la cible :** vous pouvez sélectionner l'état de démarrage (Windows) ou le niveau d'exécution (Linux) des services/daemons sur la machine virtuelle de basculement. Lorsque vous effectuez un basculement ou un test de basculement, vous pouvez spécifier les services ou daemons à exécuter ou à arrêter lorsque le workload de basculement est activé.

  Les services courants auxquels vous souhaiterez peut-être assigner un état de démarrage `désactivé` sont des services spécifiques au fournisseur liés à leur infrastructure physique sous-jacente et qui ne sont pas requis dans une machine virtuelle.

5.9 Utilisation des scripts freeze et thaw pour chaque réplication (Linux)

Pour les systèmes Linux, PlateSpin Protect propose la fonction d'exécution automatique de scripts personnalisés, `freeze` et `thaw`, qui s'ajoutent à la fonction de contrôle automatique du daemon.

Le script `freeze` est exécuté au début d'une réplication et `thaw`, à la fin.

Vous pouvez utiliser cette fonctionnalité pour compléter la fonction de contrôle du daemon automatisé proposée par le biais de l'interface utilisateur (reportez-vous à la section « Contrôle des services et des daemons sources : » page 79). Par exemple, cette fonction peut être intéressante pour suspendre temporairement certains daemons au lieu de les fermer pendant les réplications.

Pour implémenter la fonction, procédez comme suit avant de configurer votre protection de workload Linux :

1. Créez les fichiers suivants :
   - `platespin.freeze.sh` : script shell à exécuter au début de la réplication ;
   - `platespin.thaw.sh` : script shell à exécuter à la fin de la réplication ;
   - `platespin.conf` : fichier texte définissant tous les arguments requis ainsi qu'une valeur de timeout.

     La syntaxe requise pour le contenu du fichier `platespin.conf` est :

```
[ServiceControl]

FreezeArguments=<arguments>

ThawArguments=<arguments>

TimeOut=<timeout>
```

Remplacez *<arguments>* par les arguments de commande requis, en les séparant par un espace, et *<timeout>* par une valeur de timeout en secondes. Si aucune valeur n'est définie, le timeout par défaut s'applique (60 secondes).

2 Enregistrez les scripts, ainsi que le fichier `.conf` sur votre workload source Linux dans le répertoire suivant :

```
/etc/platespin
```

5.10 Volumes

Lors de l'ajout d'un workload à protéger, PlateSpin Protect établit l'inventaire du support de stockage de votre workload source et configure automatiquement les options dans l'interface Web PlateSpin Protect pour vous permettre de spécifier les volumes nécessitant une protection.

PlateSpin Protect prend en charge plusieurs types de stockage, notamment les disques dynamiques Windows, le gestionnaire de volumes logiques (LVM) (version 2 uniquement), ainsi que les systèmes RAID et SAN.

Pour les workloads Linux, PlateSpin Protect fournit les fonctions supplémentaires suivantes :

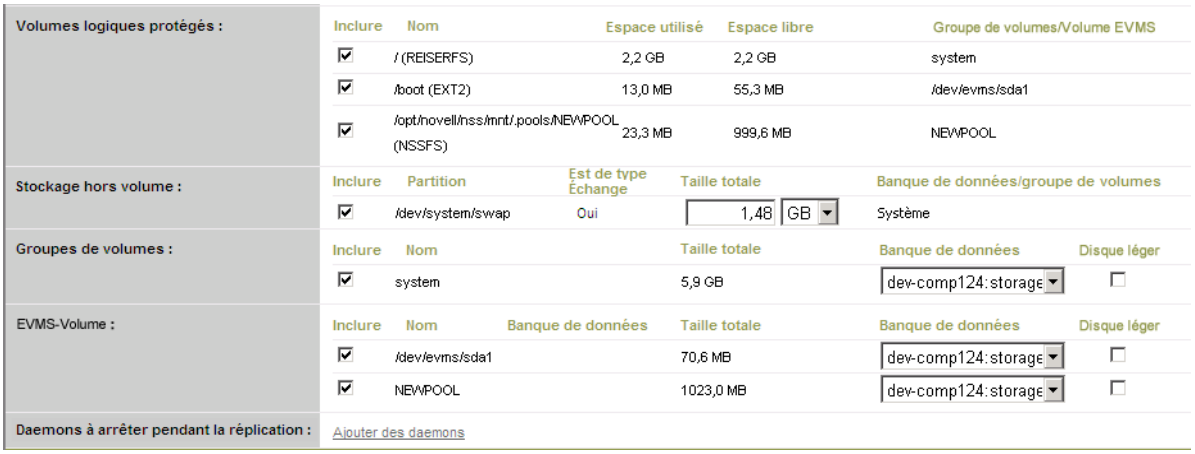
- Une zone de stockage (autre qu'un volume), telle qu'une partition d'échange associée au workload source, est recréée dans le workload de basculement.
- La disposition des groupes de volumes et des volumes logiques est conservée pour vous permettre de la recréer pendant le rétablissement.
- (Workloads OES 2) Les dispositions EVMS de workloads sources sont conservées et recréées dans le conteneur de VM. Les réserves NSS sont copiées de la source vers la VM de récupération.

Les figures suivantes affichent l'ensemble des paramètres de réplication pour un workload Linux avec plusieurs volumes et deux volumes logiques dans un groupe de volumes.

Figure 5-2 *Volumes, volumes logiques et groupes de volumes d'un workload Linux protégé*

La figure suivante affiche les options de protection de volume d'un workload OES 2 avec des options spécifiant que la disposition EVMS doit être conservée et recréée pour le workload de basculement :

Figure 5-3 *Paramètres de réplication, options de volume (workload OES 2)*



5.11 Réseautique

PlateSpin Protect permet de contrôler l'identité réseau et les paramètres LAN de votre workload de basculement de manière à éviter que le trafic de réplication interfère avec le trafic LAN ou WAN principal.

Vous pouvez spécifier des paramètres de réseautique distincts dans vos détails de protection de workload à utiliser à différents stades du workflow de protection et de récupération de workload.

- **Réplication :** (ensemble des paramètres Réplication) pour séparer le trafic de réplication habituel de votre trafic de production.
- **Basculement :** (ensemble des paramètres Basculement) pour que le workload de basculement intègre votre réseau de production lorsqu'il est actif.
- **Préparer le basculement :** (paramètre réseau Préparer le basculement) pour les paramètres réseau pendant l'opération facultative de préparation du basculement.
- **Tester le basculement :** (ensemble des paramètres Test de basculement) pour que les paramètres réseau s'appliquent au workload de basculement pendant le test de basculement.

5.12 Rétablissement vers des machines physiques

Si l'infrastructure cible requise pour une opération de rétablissement est une machine physique, vous devez l'enregistrer auprès de PlateSpin Protect.

L'enregistrement d'une machine physique s'effectue en démarrant la machine physique cible avec l'image ISO de démarrage PlateSpin.

- Section 5.12.1, « Téléchargement de l'image ISO de démarrage PlateSpin », page 82
- Section 5.12.2, « Insertion de pilotes de périphérique supplémentaires dans l'image ISO de démarrage », page 82
- Section 5.12.3, « Enregistrement de machines physiques en tant que cibles de rétablissement avec PlateSpin Protect », page 84

5.12.1 Téléchargement de l'image ISO de démarrage PlateSpin

Vous pouvez télécharger les images ISO de démarrage PlateSpin (`bootofx.x2p.iso` pour les cibles basées sur des microprogrammes BIOS et `bootofx.x2p.uefi.iso` pour les cibles basées sur des microprogrammes UEFI) à partir de la zone PlateSpin Protect des téléchargements Novell (http://download.novell.com) en effectuant une recherche à l'aide des paramètres suivants :

- *Produit ou technologie :* `PlateSpin Protect`
- *Sélectionner une version :* `PlateSpin Protect 11.0`
- *Date Range :* `(Plage de dates) All Dates (Toutes les dates)`

5.12.2 Insertion de pilotes de périphérique supplémentaires dans l'image ISO de démarrage

Vous pouvez faire appel à un utilitaire personnalisé pour créer un paquetage avec des pilotes de périphérique Linux supplémentaires et les insérer dans l'image de démarrage PlateSpin avant de la graver sur un CD :

1. Obtenez ou compilez des fichiers de pilotes `*.ko` appropriés pour le fabricant du matériel cible.

IMPORTANT : assurez-vous que les pilotes sont valides pour le kernel inclus dans le fichier ISO (`3.0.93-0.8-pae` pour les systèmes x86 ; `3.0.93-0.8-default` pour les systèmes x64) et qu'ils conviennent à l'architecture cible. Reportez-vous également à l'article de la base de connaissances n° 7005990.

2 Montez l'image sur une machine Linux (références `root` requises). Utilisez la syntaxe de commande suivante :

```
mount -o loop <chemin_fichier_ISO> <point_montage>
```

3 Copiez le script `rebuildiso.sh` du sous-répertoire `/tools` du fichier ISO monté dans un répertoire de travail temporaire. Lorsque vous avez terminé, démontez le fichier ISO (exécutez la commande `unmount <point_montage>`).

4 Créez un autre répertoire de travail pour les fichiers de pilotes requis et enregistrez-les dans ce répertoire.

5 Dans le répertoire dans lequel vous avez enregistré le script `rebuildiso.sh`, exécutez le script `rebuildiso.sh` en tant qu'utilisateur `root` à l'aide de la syntaxe suivante :

```
./rebuildiso.sh <ARGS> [-v] -m32|-m64 -i <fichier_ISO>
```

Le tableau ci-dessous répertorie les options de ligne de commande possibles pour cette commande :

Option	Description
`-i <fichier_ISO>`	<*fichier_ISO*> correspond au fichier ISO à modifier, répertorier, etc.
`-v`	Utilisée avec l'argument `-l`, cette option entraîne l'utilisation de modinfo afin d'obtenir des informations sur le pilote en mode verbeux.
`-o`	Si cette option est utilisée avec l'argument `-c` ou `-d`, l'ancienne copie du fichier ISO est conservée.
`-m32`	Spécifie une insertion initrd 32 bits.
`-m64`	Spécifie une insertion initrd 64 bits.

Le tableau ci-dessous répertorie les arguments utilisables avec cette commande : Vous devez utiliser au moins l'un des arguments suivants dans la commande :

Argument	Description
`-d <chemin>`	<*chemin*> indique le répertoire qui contient les pilotes (en d'autres termes, les fichiers `*.ko`) que vous souhaitez insérer. Lors de l'exécution de la commande, le fichier ISO est mis à jour avec les pilotes ajoutés.
`-c <chemin>`	<*chemin*> indique l'emplacement où réside un fichier `ConfigureTakeControl.xml`.

Argument	Description

`-l [<type>]`	<*type*> indique un sous-ensemble de pilotes que vous souhaitez répertorier. La valeur par défaut est « Tous » les types.
	
	Les types de pilotes répertoriés qui commencent par une barre oblique (/) sont censés être situés à l'emplacement `<répertoire_module_kernel>/kernel/`.
	
	Les types de pilotes répertoriés qui ne commencent pas par une barre oblique (/) sont censés être situés à l'emplacement `<répertoire_module_kernel/kernel/drivers/`
	
	Exemples de sous-ensembles de pilotes :
	
	`-l scsi`
	`-l 'net|video'`
	`-l '/net|net'`
	
	Utilisation spéciale de cet argument :
	
	si vous souhaitez répertorier les sous-répertoires disponibles de chacun des sous-ensembles, utilisez l'argument comme suit : `-l INDEX`

Exemples de syntaxe

- Pour répertorier un index de pilotes 32 bits :

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m32 -l INDEX
```

- Pour répertorier les pilotes trouvés dans le dossier /misc :

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m32 -l misc
```

- Pour insérer des pilotes 32 bits à partir du dossier /oem-drivers :

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m32 -d oem-drivers
```

- Pour insérer des pilotes 64 bits à partir d'un dossier /oem-drivers et insérer également un fichier ConfigureTakeControl.xml personnalisé :

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m64 -c ConfigureTakeControl.xml -d
oem-drivers
```

5.12.3 Enregistrement de machines physiques en tant que cibles de rétablissement avec PlateSpin Protect

1. Gravez l'image ISO de démarrage PlateSpin sur un CD ou enregistrez-la sur le support à partir duquel votre cible peut démarrer.
2. Veillez à ce que le port réseau commuté connecté à la cible soit défini sur *Duplex intégral - Automatique*.
3. Démarrez la machine physique cible à l'aide du CD de démarrage, puis attendez l'ouverture de la fenêtre d'invite de commande.
4. (Linux uniquement) Pour les systèmes 64 bits, à l'invite de démarrage initiale, tapez ce qui suit :
   - `ps64` (pour les systèmes ayant jusqu'à 512 Mo de RAM)
   - `ps64_512m` (pour les systèmes ayant plus de 512 Mo de RAM)
5. Appuyez sur Entrée.

6 Lorsque vous y êtes invité, entrez le nom d'hôte ou l'adresse IP de l'hôte de votre serveur PlateSpin .

7 Fournissez vos références d'administrateur pour l'hôte du serveur PlateSpin , en spécifiant une autorité. Pour le compte utilisateur, utilisez le format suivant :

   domaine\nom_utilisateur ou *nom_hôte\nom_utilisateur*

   Les cartes réseau disponibles sont détectées et affichées selon leur adresse MAC.

8 Si DHCP est disponible sur la carte réseau à utiliser, appuyez sur Entrée pour continuer. Si DHCP n'est pas disponible, sélectionnez la carte réseau requise à configurer avec une adresse IP statique.

9 Entrez un nom d'hôte pour la machine physique ou appuyez sur Entrée pour accepter les valeurs par défaut.

10 Lorsque vous êtes invités à indiquer si vous souhaitez utiliser HTTPS, entrez `Y` (Oui) si vous avez activé SSL et `N` (Non) dans le cas contraire.

Après quelques instants, la machine physique doit être disponible dans les paramètres de rétablissement de l'interface Web PlateSpin Protect.

5.13 Sections sur la protection de workload avancée

5.13.1 Protection des grappes Windows

prend en charge la protection des services métiers d'une grappe (cluster) Microsoft Windows. Les technologies de mise en grappe prises en charge sont les suivantes :

- Cluster de basculement Microsoft Windows 2008 R2 Server

Cette section présente les informations suivantes :

REMARQUE : pour plus d'informations sur la reconstruction de l'environnement de cluster de basculement Windows 2008/2008R2 après sa protection par PlateSpin Forge lors d'un basculement/rétablissement, reportez-vous à l'article de la base de connaissances décrivant la procédure.

Protection de workload

La protection d'une grappe s'effectue par le biais de réplications incrémentielles de changements sur le noeud actif transmises en continu à une grappe virtuelle à noeud unique que vous pouvez utiliser lors du dépannage de l'infrastructure source.

L'étendue de la prise en charge des migrations de grappe dans la version actuelle est soumise aux conditions suivantes :

- Lorsque vous effectuez une opération *Ajouter un workload*, vous devez identifier le noeud actif, à savoir le noeud qui détient actuellement la ressource quorum de la grappe, identifié par l'adresse IP de la grappe (*adresse IP virtuelle*). En spécifiant l'adresse IP des résultats d'un noeud individuel, ce noeud est inventorié en tant que workload Windows ordinaire ne prenant pas en charge les grappes.
- Une ressource quorum de grappe doit être colocalisée avec le groupe de ressources (services) de la grappe protégé.

Lorsque vous utilisez le transfert par bloc, les composants de pilote par bloc ne sont pas installés sur les noeuds de grappe. Le transfert par bloc s'effectue au moyen d'une synchronisation sans pilote avec une réplication basée sur MD5. Dans la mesure où le pilote par bloc n'est pas installé, aucun redémarrage n'est nécessaire sur les noeuds de grappe sources.

REMARQUE : le transfert basé sur les fichiers n'est pas pris en charge pour la protection des grappes Microsoft Windows.

---

si un basculement de noeud se produit entre les réplications incrémentielles d'une grappe protégée et si le profil du nouveau noeud actif est semblable au noeud actif qui a échoué, le contrat de protection se poursuit comme prévu. Dans le cas contraire, la commande échoue. Les profils des noeuds de grappe sont considérés similaires si :

- ils ont le même nombre de volumes ;
- chaque volume a exactement la même taille sur chaque noeud ;
- ils ont un nombre identique de connexions réseau.
- Les numéros de série des volumes locaux (volume Système et volume Système réservé) doivent être identiques sur chaque noeud de grappe.

  Si les unités locales sur chaque noeud de la grappe ont des numéros de série différents, vous ne pouvez pas exécuter de réplication incrémentielle après le basculement du noeud actif dans le cas d'un échec. Par exemple, le noeud actif est le noeud 1 et il « bascule » ensuite vers le noeud 2.

  Dans le cas de Protect 11.0.1, deux solutions sont acceptées pour la prise en charge des grappes dans ce scénario :

  - (Recommandé) Utilisez l'utilitaire *Gestionnaire de volumes* personnalisé afin de modifier les numéros de série des volumes locaux pour qu'ils correspondent à chaque noeud de la grappe. Pour plus d'informations, reportez-vous à l'Annexe B, « Synchronisation du stockage local du noeud de grappe », page 125.
  - (Conditionnel et facultatif) Si cette erreur est affichée :

    ```
    Volume mappings does not contain source serial number: xxxx-xxxx,
    ```

    elle est peut-être due à un changement dans le noeud actif antérieur à l'exécution de la réplication incrémentielle. Dans ce cas, vous pouvez exécuter une réplication complète afin de vous assurer que la grappe est à nouveau protégée. Les réplications incrémentielles devraient fonctionner à nouveau après la réplication complète.

Si vous choisissez de ne pas faire correspondre les numéros de série de volume de chaque noeud de la grappe, une réplication complète est requise avant chaque réplication incrémentielle lorsque le noeud actif bascule vers un nouveau noeud de la grappe.

Si un basculement de noeud se produit avant la fin du processus de copie au cours d'une réplication complète ou incrémentielle, la commande est annulée et un message s'affiche pour indiquer la nécessité d'exécuter à nouveau la réplication.

Pour protéger une grappe Windows, suivez le workflow de protection du workload normal (reportez-vous à la section « Workflow de base pour la protection et la récupération de workload » page 49).

Basculement de protection

Lorsque la machine de basculement est mise en ligne à la suite d'une opération de basculement, une grappe à noeuds multiples avec un seul noeud actif (tous les autres noeuds sont indisponibles) est visible.

Pour faire basculer un cluster Windows (ou tester le basculement sur cette grappe), il doit être en mesure de se connecter à un contrôleur de domaine. Pour tirer parti de la fonctionnalité de basculement de test, vous devez protéger le contrôleur de domaine avec la grappe. Au cours du test, mettez en service le contrôleur de domaine, suivi du workload de cluster Windows (sur un réseau isolé).

Rétablissement de protection

Seul un rétablissement à l'aide d'une réplication complète des workloads de cluster Windows est pris en charge pour cette version.

Si vous configurez le rétablissement en tant que réplication complète sur une cible physique, vous pouvez utiliser l'une des méthodes suivantes :

- Assignez tous les disques de la machine de basculement à un disque local unique sur la cible du rétablissement.
- Ajoutez un autre disque (`Disque 2`) à la machine physique du rétablissement. Vous pouvez ensuite configurer l'opération de rétablissement afin de restaurer le volume système du basculement sur le `Disque 1` et les autres disques du basculement (disques partagés précédents) sur le `Disque 2`. De cette façon, le disque système peut être restauré sur le disque de stockage présentant la même taille que la source initiale.

Une fois le rétablissement effectué, vous pouvez joindre à nouveau d'autres noeuds à la grappe que vous venez de restaurer.

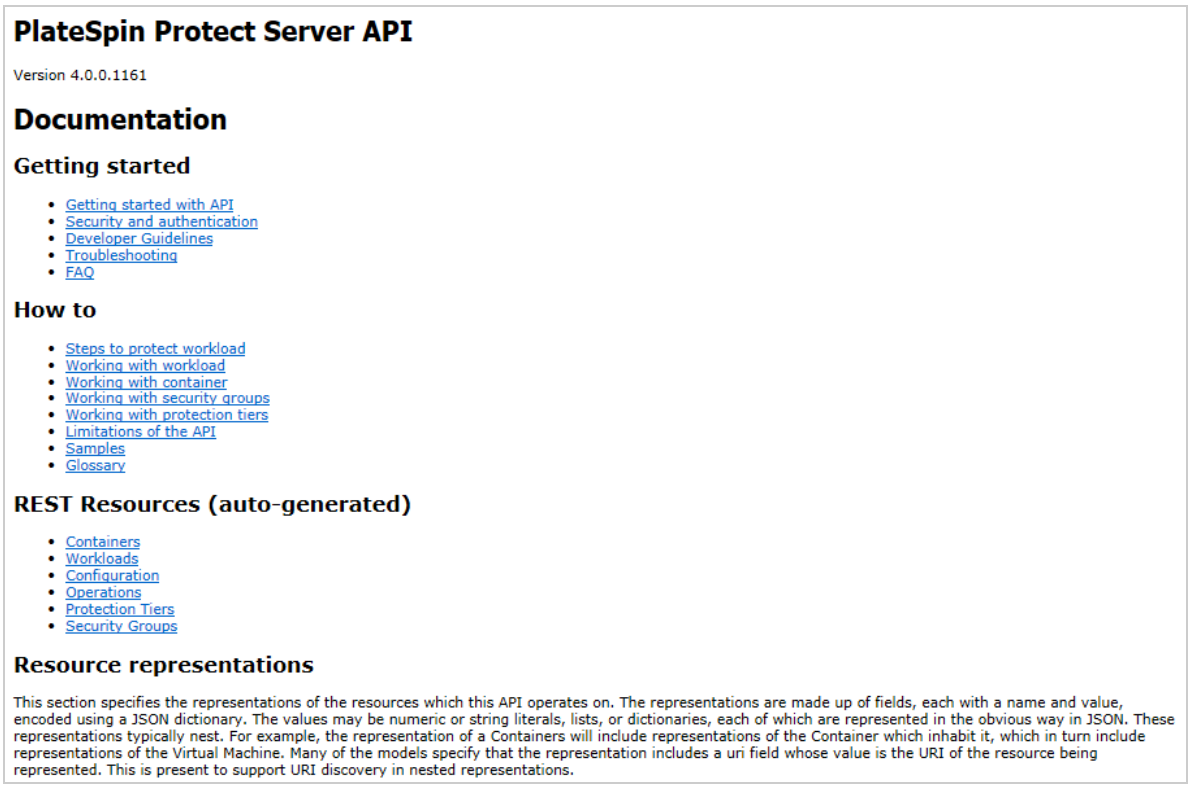
5.13.2 Utilisation des fonctions de protection de workload à l'aide des API de services Web de PlateSpin Protect

Vous pouvez utiliser la fonctionnalité de protection de workload par programmation, via l'API `protectionservices`, depuis vos applications. Vous pouvez utiliser tout langage de programmation ou de script prenant en charge un client HTTP et la structure de sérialisation JSON.

`https://`*<nom_hôte | adresse_IP>*`/protectionservices`

Remplacez *<nom_hôte | adresse_IP>* par le nom d'hôte et l'adresse IP de l'hôte du serveur PlateSpin . Si SSL n'est pas activé, utilisez le protocole `http` dans l'URI.

Figure 5-4 *Page d'accueil de l'API du serveur Protect*



PlateSpin Protect Server API

Version 4.0.0.1161

Documentation

Getting started

- Getting started with API
- Security and authentication
- Developer Guidelines
- Troubleshooting
- FAQ

How to

- Steps to protect workload
- Working with workload
- Working with container
- Working with security groups
- Working with protection tiers
- Limitations of the API
- Samples
- Glossary

REST Resources (auto-generated)

- Containers
- Workloads
- Configuration
- Operations
- Protection Tiers
- Security Groups

Resource representations

This section specifies the representations of the resources which this API operates on. The representations are made up of fields, each with a name and value, encoded using a JSON dictionary. The values may be numeric or string literals, lists, or dictionaries, each of which are represented in the obvious way in JSON. These representations typically nest. For example, the representation of a Containers will include representations of the Container which inhabit it, which in turn include representations of the Virtual Machine. Many of the models specify that the representation includes a uri field whose value is the URI of the resource being represented. This is present to support URI discovery in nested representations.

Pour créer un script des opérations courantes de protection de workload, aidez-vous des modèles de référence écrits en Python. Une application Microsoft Silverlight est également fournie, avec son code source, à titre de référence.

Aperçu des API

PlateSpin Protect propose un aperçu de la technologie API basée sur REST que les développeurs peuvent utiliser pour concevoir leurs propres applications destinées à fonctionner avec le produit. L'API contient des informations sur les opérations suivantes :

- découverte de conteneurs
- découverte de workloads
- configuration de la protection
- exécution des réplications, opérations de basculement et de rétablissement
- demande de l'état d'un workload et d'un conteneur
- demande de l'état d'opérations en cours
- demande de groupes de sécurité et de leurs liens de protection

Les administrateurs protégés peuvent générer un échantillon Jscript (`https://localhost/protectionservices/Documentation/Samples/protect.js`) à partir de la ligne de commande pour accéder au produit via l'API. L'échantillon peut vous aider à rédiger des scripts afin de faciliter votre travail sur le produit. L'utilitaire de ligne de commande vous permet d'effectuer les opérations suivantes :

- ajout d'un workload seul

- ajout d'un conteneur seul
- exécution d'opérations de réplication, de basculement et de rétablissement
- ajout simultané de plusieurs workloads et conteneurs

  REMARQUE : pour plus d'informations sur cette opération, consultez la documentation relative à l'API à l'adresse `https://localhost/protectionservices/Documentation/AddWorkloadsAndContainersFromCsvFile.htm`.

- suppression simultanée de tous les workloads
- suppression simultanée de tous les conteneurs

La page d'accueil de l'API REST de PlateSpin Protect (`https://localhost/protectionservices/` ou `https://<page_serveur>/protectionservices/`) inclut des liens vers du contenu utile pour les développeurs et les administrateurs.

Cet aperçu technologique sera complété avec d'autres fonctionnalités dans les prochaines versions.

6 Outils auxiliaires pour l'utilisation de machines physiques

Votre distribution PlateSpin Protect inclut des outils à employer lorsque vous utilisez des machines physiques en tant que cibles de rétablissement.

6.1 Gestion des pilotes de périphérique

PlateSpin Protect est fourni avec une bibliothèque de pilotes de périphérique et installe automatiquement les pilotes adéquats sur les workloads cibles. Si certains pilotes sont manquants ou incompatibles ou si vous avez besoin de pilotes spécifiques pour votre infrastructure cible, il se peut que vous deviez ajouter (télécharger) des pilotes dans la base de données de pilotes de PlateSpin Forge/PlateSpin Protect.

Pour plus d'informations, reportez-vous aux sections suivantes :

6.1.1 Création d'un paquetage contenant les pilotes de périphérique pour les systèmes Windows

Pour créer un paquetage contenant vos pilotes de périphérique Windows en vue de les télécharger dans la base de données des pilotes de PlateSpin Protect :

1. Préparez tous les fichiers de pilote interdépendants (`*.sys`, `*.inf`, `*.dll`, etc.) pour votre infrastructure et votre périphérique cibles. Si vous avez obtenu des pilotes spécifiques à un fabricant sous la forme d'une archive `.zip` ou d'un exécutable, veillez à les extraire au préalable.
2. Enregistrez les fichiers de pilote dans des dossiers distincts, en créant un dossier par périphérique.

Les pilotes sont à présent prêts à être téléchargés. Reportez-vous à la section « Téléchargement de pilotes dans la base de données des pilotes de périphérique de PlateSpin Protect » page 92.

REMARQUE : pour garantir le bon fonctionnement de votre tâche de protection et de votre workload cible, téléchargez uniquement les pilotes à signature numérique pour :

- l'ensemble des systèmes Windows 64 bits ;
- les versions 32 bits des systèmes Windows Vista et Windows Server 2008, ainsi que Windows 7.

6.1.2 Création d'un paquetage contenant les pilotes de périphérique pour les systèmes Linux

Pour réaliser un paquetage de vos pilotes de périphériques Linux afin de les télécharger dans la base de données de pilotes PlateSpin Protect, vous pouvez utiliser un utilitaire personnalisé inclus dans votre image ISO de démarrage PlateSpin.

1. Sur un poste de travail Linux, créez un répertoire pour vos fichiers de pilote de périphérique. Tous les pilotes du répertoire doivent être destinés au même kernel et à la même architecture.
2. Téléchargez l'image de démarrage et montez-la.

   Par exemple, en partant de l'hypothèse que l'image ISO a été copiée dans le répertoire `/root`, émettez la commande suivante pour les cibles basées sur des microprogrammes BIOS :

   ```
   # mkdir /mnt/ps # mount -o loop /root/bootofx.x2p.iso /mnt/ps
   ```

   ou cette commande pour les cibles basées sur des microprogrammes UEFI :

   ```
   # mkdir /mnt/ps # mount -o loop /root/bootofx.x2p.uefi.iso /mnt/ps
   ```

3. Dans le sous-répertoire `/tools` de l'image ISO montée, copiez l'archive `packageModules.tar.gz` dans un autre répertoire de travail et extrayez-la.

   Par exemple, si le fichier `.gz` se trouve dans votre répertoire de travail actuel, exécutez la commande suivante :

   ```
   tar -xvzf packageModules.tar.gz
   ```

4. Entrez le répertoire de travail et exécutez la commande suivante :

   `./PackageModules.sh –d <chemin_répertoire_pilote> -o <nom_paquetage>`

   Remplacez *<chemin_répertoire_pilote>* par le chemin d'accès au répertoire dans lequel vous avez enregistré les fichiers de pilote et *<nom_paquetage>* par le nom du paquetage, en vous conformant à ce format :

   Nompilote-versionpilote-dist-versionkernel-arch.pkg

   Par exemple, `bnx2x-1.48.107-RHEL4-2.6.9-11.EL-i686.pkg`

Le paquetage est à présent prêt à être téléchargé. Reportez-vous à la section « Téléchargement de pilotes dans la base de données des pilotes de périphérique de PlateSpin Protect » page 92.

6.1.3 Téléchargement de pilotes dans la base de données des pilotes de périphérique de PlateSpin Protect

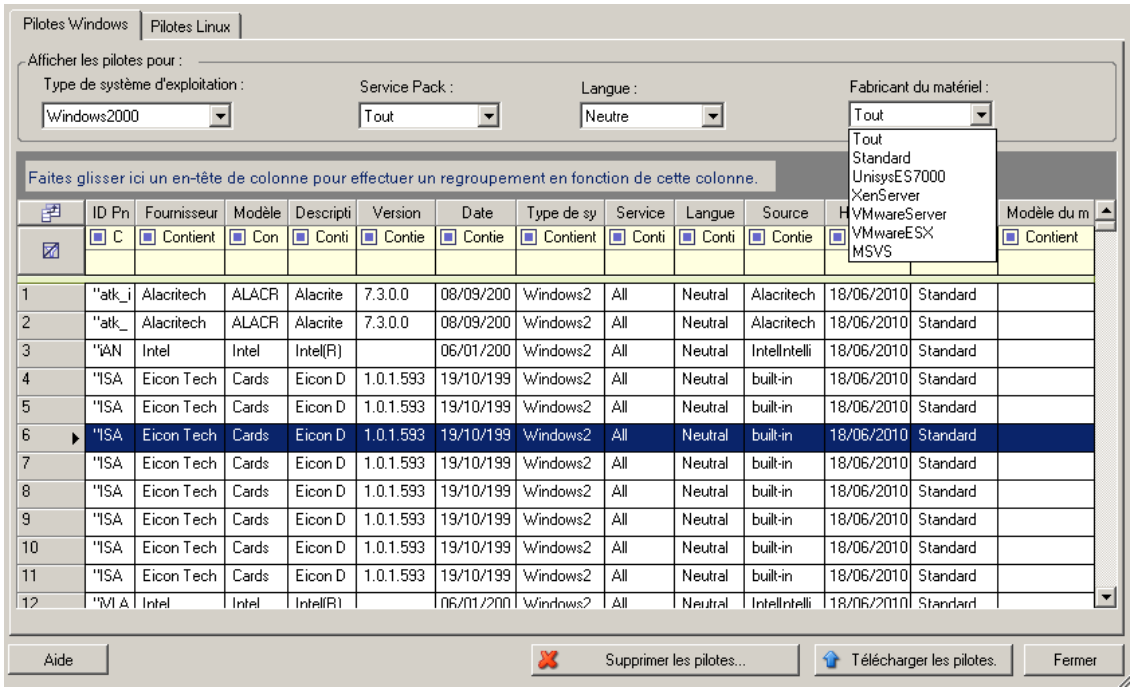
Le gestionnaire de pilotes PlateSpin permet de télécharger les pilotes de périphériques dans la base de données des pilotes.

REMARQUE : lors du téléchargement, PlateSpin Protect ne valide pas les pilotes par rapport aux types de systèmes d'exploitation sélectionnés ou à leurs spécifications au niveau des bits. Veillez donc à télécharger uniquement des pilotes convenant à votre infrastructure cible.

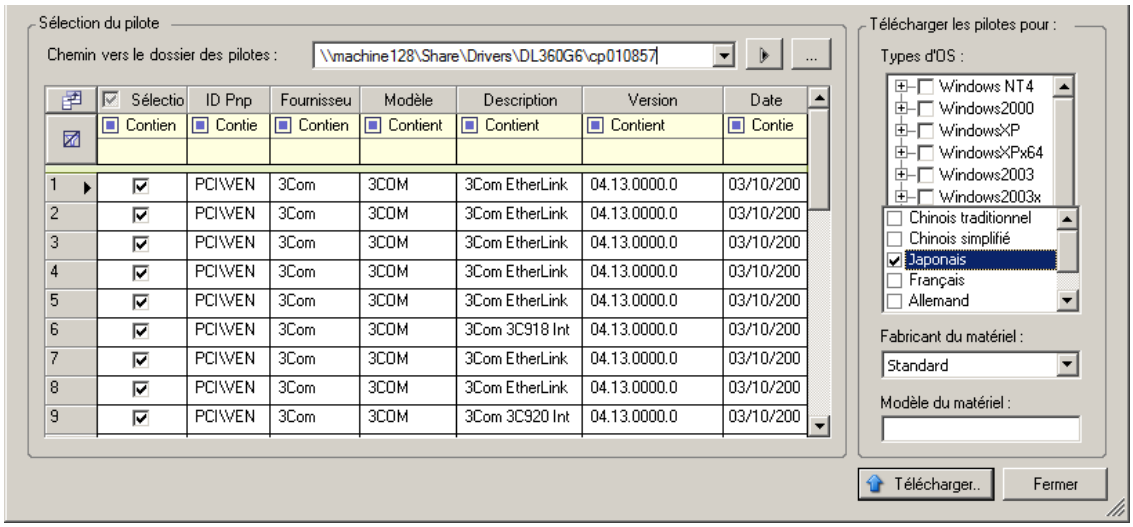
Procédure de téléchargement de pilotes de périphérique (Windows)

1 Procurez-vous les pilotes de périphérique requis et préparez-les. Reportez-vous à la section Création d'un paquetage contenant les pilotes de périphérique pour les systèmes Windows.

2 Sur votre hôte PlateSpin Server, sous `\Program Files\PlateSpin Protect Server\DriverManager`, démarrez le programme `DriverManager.exe`, puis cliquez sur l'onglet *Pilotes Windows*.



3 Cliquez sur *Télécharger les pilotes*, accédez au dossier contenant les fichiers de pilote requis, puis sélectionnez les options appropriées concernant le type de système d'exploitation, la langue et le fabricant du matériel.



Sélectionnez *Standard* pour l'option *Fabricant du matériel*, sauf si vos pilotes sont spécifiquement conçus pour l'un des environnements cibles répertoriés.

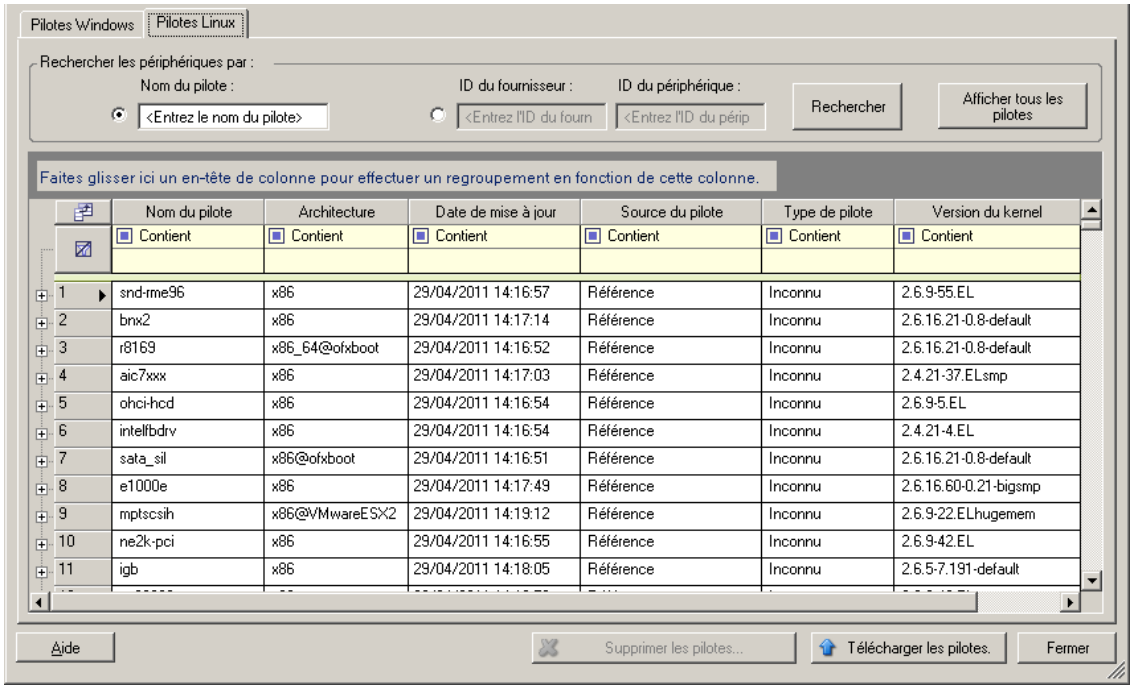
4 Cliquez sur *Télécharger* et confirmez vos sélections quand vous y êtes invité.

Le système télécharge les pilotes sélectionnés dans la base de données des pilotes.

Procédure de téléchargement de pilotes de périphérique (Linux)

1 Procurez-vous les pilotes de périphérique requis et préparez-les. Reportez-vous à la section Création d'un paquetage contenant les pilotes de périphérique pour les systèmes Linux.

2 Cliquez sur *Outils* > *Gérer les pilotes de périphérique*, puis cliquez sur l'onglet *Pilotes Linux* :



3 Cliquez sur *Télécharger les pilotes*, accédez au dossier contenant le paquetage de pilote requis (`*.pkg`), puis cliquez sur *Télécharger tous les pilotes*.

Le système télécharge les pilotes sélectionnés dans la base de données des pilotes.

6.1.4 Utilisation de la fonction de traduction d'ID Plug-and-Play (PnP)

« Plug-and-Play » (PnP) désigne la fonctionnalité du système d'exploitation Windows qui prend en charge la connectivité, la configuration et la gestion avec des périphériques Plug-and-Play natifs. Sous Windows, cette fonctionnalité facilite la découverte des périphériques matériels compatibles PnP connectés à un bus PnP. Le fabricant des périphériques compatibles PnP leur assigne un ensemble de chaînes d'identification de périphérique. Ces chaînes sont intégrées dans le périphérique lors de la fabrication. Elles sont essentielles au fonctionnement de PnP : elles font partie de la source d'informations de Windows utilisée pour faire correspondre le périphérique au pilote approprié.

Lorsque le serveur PlateSpin découvre des workloads et le matériel correspondant disponible, la découverte inclut ces ID PnP et le stockage des données en tant que détails de ces workloads. PlateSpin utilise ces ID pour déterminer les pilotes qui doivent être insérés, le cas échéant, au cours d'une opération de basculement/rétablissement. Le serveur PlateSpin gère une base de données d'ID

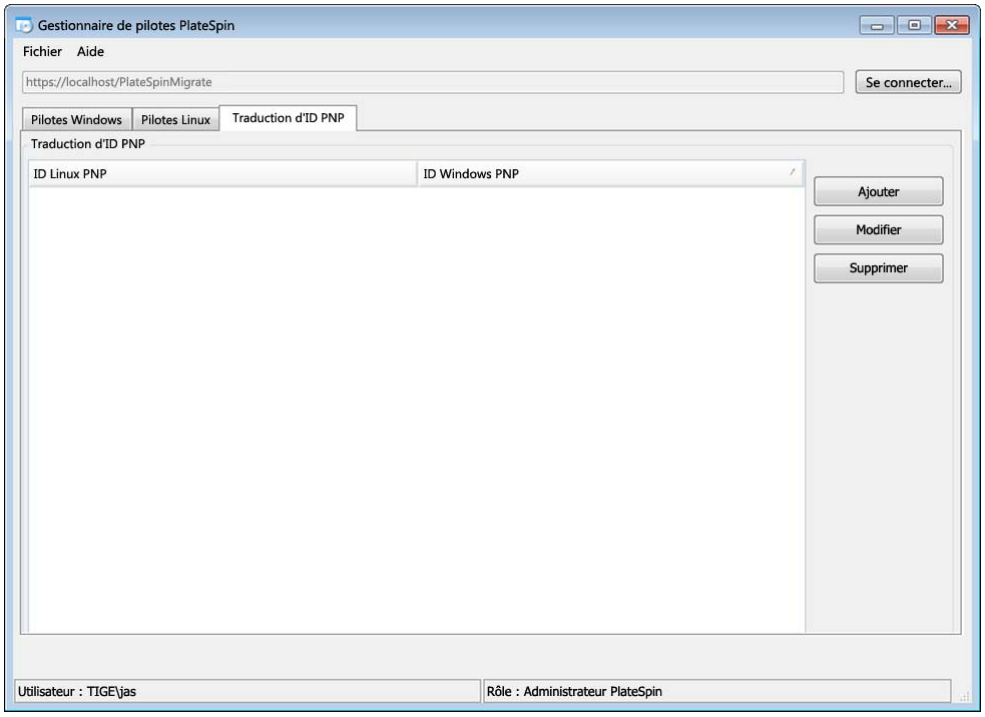
PnP pour les pilotes associés de chacun des systèmes d'exploitation pris en charge. Dans la mesure où Windows et Linux utilisent des formats différents pour les ID PnP, un workload Windows découvert par le disque virtuel Linux Protect contient des ID PnP de type Linux.

Ces ID adoptent un format cohérent, de sorte que PlateSpin puisse appliquer une transformation standard à chacun d'eux afin de déterminer l'ID PnP Windows correspondant. La transaction s'effectue automatiquement à l'intérieur du produit PlateSpin. La fonctionnalité vous permet (à vous ou à un technicien de l'équipe d'assistance) d'ajouter, de modifier ou de supprimer des assignations PnP personnalisées.

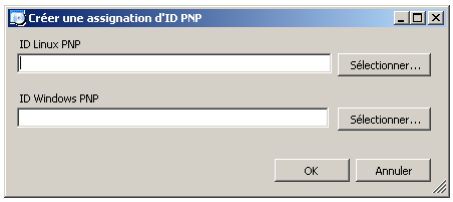
Procédez comme suit pour utiliser la fonction Traduction d'ID PnP :

1 Lancez l'outil Gestionnaire de pilotes PlateSpin et connectez-vous au serveur PlateSpin.

2 Dans l'outil Gestionnaire de pilotes PlateSpin, sélectionnez l'onglet Traduction d'ID PNP pour ouvrir la liste *Traduction d'ID PNP* qui contient les assignations d'ID PnP personnalisées connues.



3 Cliquez sur *Ajouter* dans la liste pour ouvrir la boîte de dialogue de création d'assignation d'ID PNP.



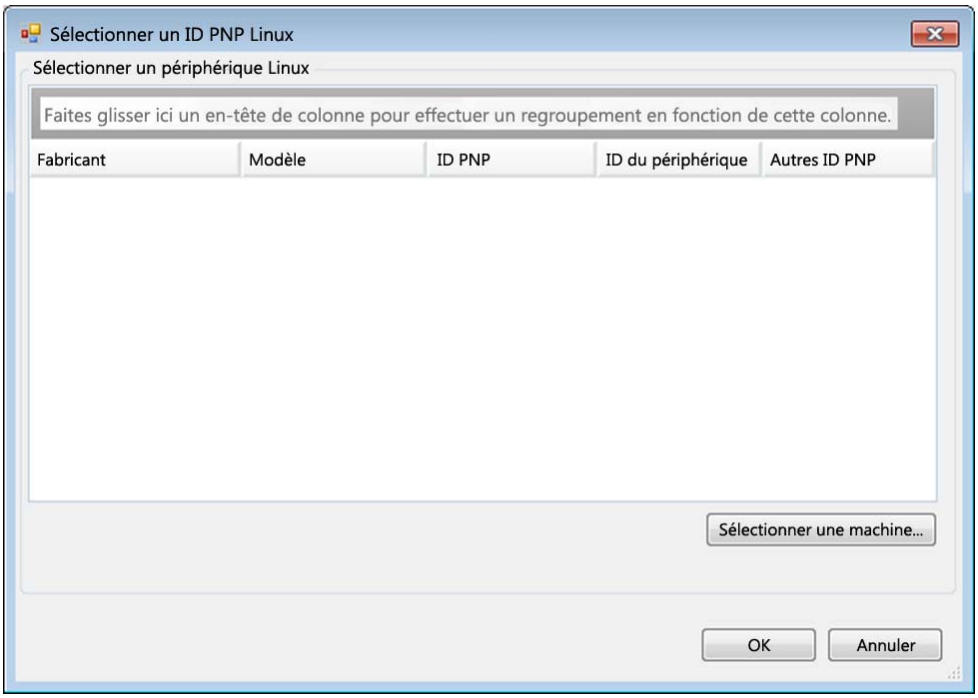
4 Ajoutez un ID PnP Linux dans le champ d'*ID PnP Linux*.

4a (Conditionnel) Entrez l'ID PnP Linux que vous souhaitez utiliser, si vous le connaissez.

ou

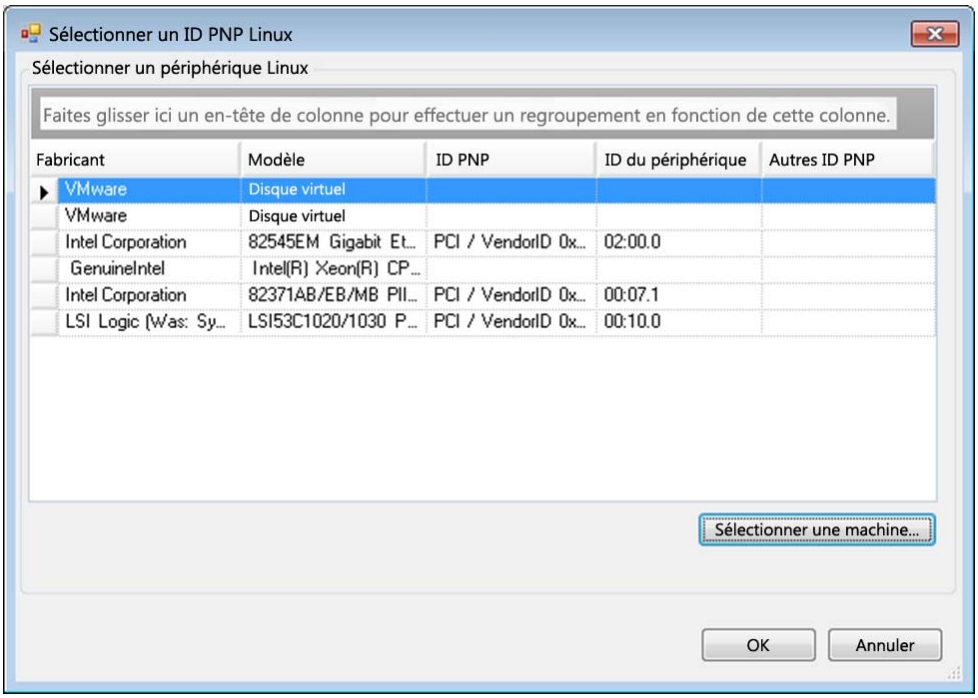
4b (Conditionnel) Sélectionnez un ID d'un workload découvert précédemment :

4b1 Cliquez sur *Sélectionner* en regard du champ d'*ID PnP Linux* pour ouvrir la boîte de dialogue de sélection de l'ID PnP Linux.



4b2 Dans la boîte de dialogue, cliquez sur l'option de *sélection de la machine* pour afficher la liste des machines découvertes précédemment par le disque virtuel Linux PlateSpin.

4b3 Mettez en surbrillance l'un des périphériques de la liste, puis cliquez sur *Sélectionner* pour remplir la liste dans la boîte de dialogue de sélection de l'ID PnP Linux.



4b4 Sélectionnez un périphérique dans la liste, puis cliquez sur *OK* pour appliquer la transformation standard à l'ID PnP et l'afficher dans la boîte de dialogue de création d'une assignation d'ID PNP.

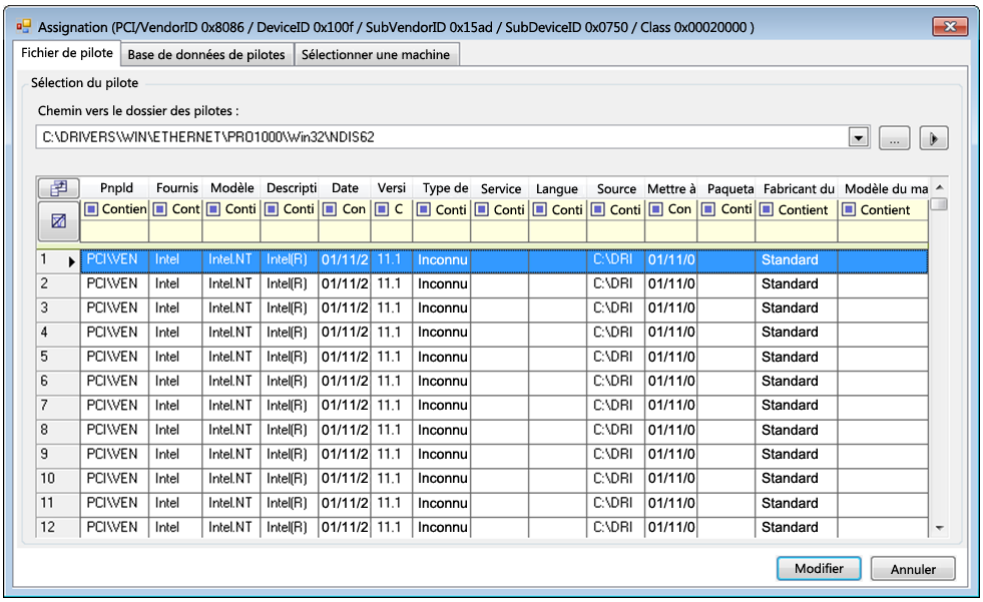
5 Ajoutez un ID PnP Windows dans le champ d'*ID PNP Windows*.

5a (Conditionnel) Entrez l'ID PnP Windows que vous souhaitez utiliser, si vous le connaissez.

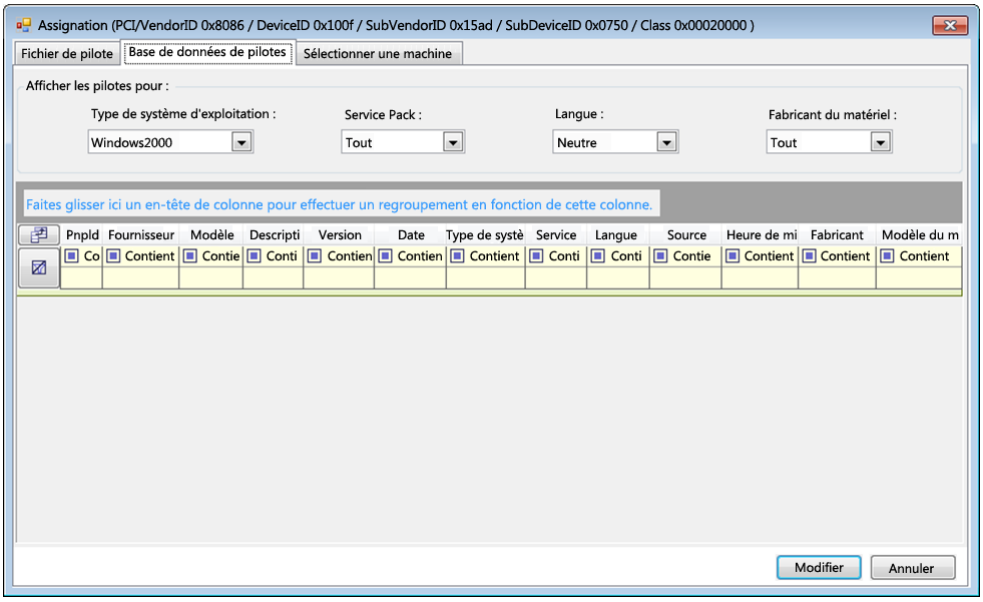
ou

5b (Conditionnel) Cliquez sur *Sélectionner* en regard du champ d'*ID PnP Windows* pour ouvrir un outil d'assignation présentant trois méthodes qui facilitent l'assignation d'un ID PnP Windows :

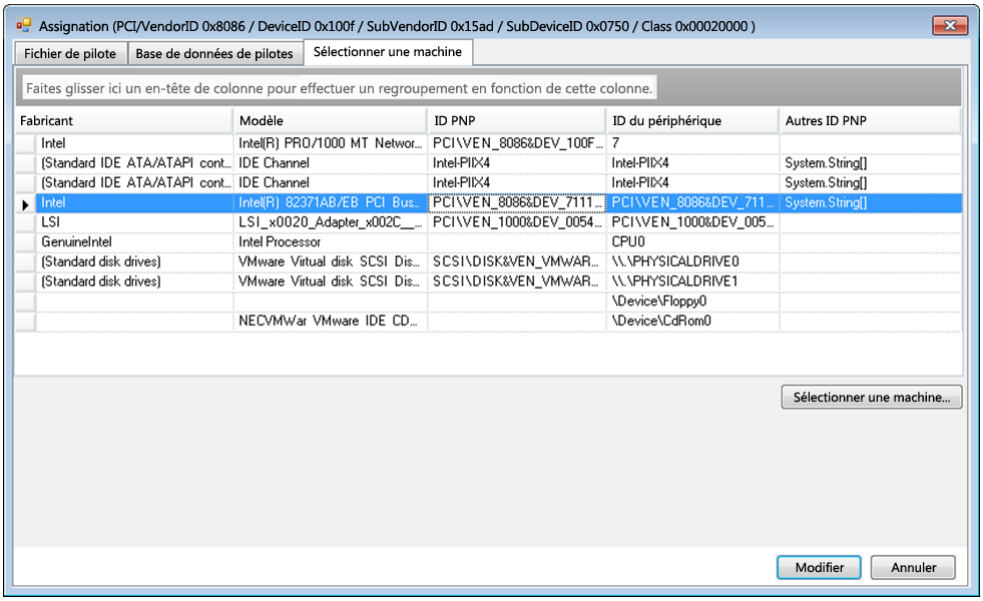
- Sous l'onglet *Fichier de pilote*, recherchez et sélectionnez un fichier de pilote Windows (c'est-à-dire un fichier portant l'extension *.`inf`), sélectionnez l'ID PnP de votre choix, puis cliquez sur *Modifier*.



- Sous l'onglet *Base de données des pilotes*, recherchez et sélectionnez la base de données de pilotes existante, sélectionnez l'ID PnP correct, puis cliquez sur *Modifier*.

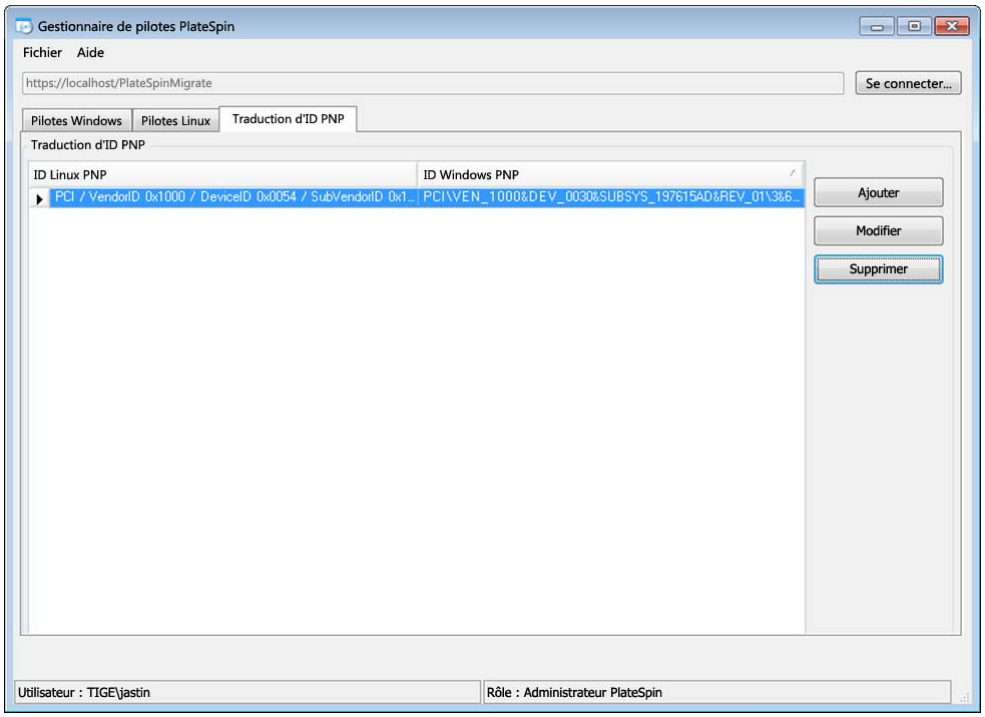


- Sous l'onglet *Sélectionner la machine*, cliquez sur *Sélectionner la machine*, puis dans la liste des machines Windows découvertes à l'aide de la découverte dynamique, sélectionnez une machine, cliquez sur *OK* pour en afficher les périphériques, sélectionnez l'ID PnP de votre choix et cliquez enfin sur Modifier.



IMPORTANT : si vous sélectionnez un ID PnP Windows pour lequel aucun paquetage de pilotes n'est installé, une erreur risque de se produire lors du basculement/rétablissement.

6 Dans la boîte de dialogue de création d'une assignation d'ID PNP, vérifiez que les ID PnP Linux et Windows corrects sont sélectionnés, puis cliquez sur *OK* pour afficher la page « Traduction d'ID PNP » du Gestionnaire de pilotes PlateSpin.



7 (Facultatif) Pour modifier ou supprimer l'assignation dans la liste Traduction d'ID PNP, sélectionnez le modèle d'assignation, puis cliquez sur *Supprimer* ou *Modifier* en fonction de l'opération que vous souhaitez effectuer.

L'option *Supprimer* supprime simplement l'assignation (après l'affichage d'une boîte de dialogue de confirmation).

Pour modifier l'assignation :

7a Cliquez sur *Modifier* pour ouvrir la boîte de dialogue de création d'une assignation d'ID PNP.

7b Effectuez à nouveau l'Étape 5 page 97 pour modifier l'ID PnP Windows.

REMARQUE : l'ID PnP Linux ne peut être ni sélectionné, ni modifié.

---

7 Dépannage

Cette section présente les informations suivantes :

7.1 Dépannage de l'inventaire de workload (Windows)

Vous devrez peut-être résoudre les problèmes courants suivants durant l'inventaire de workload.

Problèmes ou messages	Solutions
`Le domaine dans les références n'est pas valide ou est vide`	Cette erreur se produit lorsque le format des références est incorrect. Essayez d'effectuer la découverte à l'aide d'un compte d'administrateur local utilisant pour ses références le format `nom_hôte\AdminLocal` Ou essayez d'effectuer la découverte à l'aide d'un compte d'administrateur de domaine utilisant pour ses références le format `domaine\AdminDomaine`
`Impossible de se connecter au serveur Windows… L'accès est refusé`	Le compte utilisé lors de la tentative d'ajout du workload n'était pas un compte d'administrateur. Utilisez un compte d'administrateur ou ajoutez l'utilisateur au groupe des administrateurs, puis réessayez. Ce message peut également indiquer un échec de connectivité WMI. Pour chacun des cas de figure possibles suivants, essayez la solution, puis réexécutez le « Test de connectivité WMI » page 103. Si le test réussit, réessayez d'ajouter le workload. ◆ « Dépannage de la connectivité DCOM » page 103 ◆ « Dépannage de la connectivité du service RPC » page 103

Problèmes ou messages	Solutions
`Connexion impossible au serveur Windows… Le chemin d'accès réseau est introuvable`	Échec de la connectivité réseau Effectuez les tests de la section « Exécution des tests de connectivité » page 102. En cas d'échec du test, vérifiez si PlateSpin Protect et le workload se trouvent sur le même réseau. Reconfigurez le réseau, puis réessayez.
`« Découvrir les détails du serveur {nom_hôte} » - Échec Progression : 0 % État : NotStarted`	Cette erreur peut se produire pour plusieurs raisons et chacune a sa propre solution : ◆ Pour les environnements qui utilisent un proxy local avec une authentification, ignorez le proxy ou ajoutez les autorisations appropriées. Pour plus de détails, reportez-vous à l'article de la base de connaissances 7920339 (https://www.netiq.com/support/kb/doc.php?id=7920339). ◆ Si des restrictions de stratégies locales ou de domaine nécessitaient des autorisations, suivez la procédure décrite dans l'article de la base de connaissances n°7920862 (https://www.netiq.com/support/kb/doc.php?id=7920862).

La découverte du workload échoue avec le message d'erreur
`Fichier output.xml introuvable`
ou
`Chemin d'accès réseau introuvable`
ou (lors d'une tentative de découverte d'une grappe Windows)
`L'inventaire n'a pas pu être découvert. Le résultat d'inventaire n'a renvoyé aucune donnée.`
	Plusieurs explications sont possibles pour l'erreur `Fichier output.xml introuvable` :
	◆ Le logiciel Anti-virus sur la source peut interférer avec la découverte. Désactivez le logiciel Anti-virus pour déterminer s'il s'agit de la cause du problème. Reportez-vous à la section « Désactivation du logiciel anti-virus » page 104.
	◆ Il se peut que le partage de fichiers et d'imprimantes pour les réseaux Microsoft ne soit pas activé. Activez-le dans les propriétés de la carte d'interface réseau.
	◆ Les partages Admin$ sur la source ne sont peut-être pas accessibles. Vérifiez que PlateSpin Protect peut accéder à ces partages. Reportez-vous à la section « Activation des autorisations et de l'accès aux fichiers/partages » page 104.
	◆ Il se peut que le service du serveur ou du poste de travail ne soit pas en cours d'exécution. Dans ce cas, activez-les et définissez le mode de démarrage sur `Automatique`.
	◆ Le service d'accès à distance au Registre Windows est désactivé. Démarrez le service et définissez le type de démarrage sur Automatique.

Vous trouverez des informations de dépannage sur les workloads Windows dans les sections suivantes :

7.1.1 Exécution des tests de connectivité

Test de connectivité réseau

Effectuez ce test de connectivité réseau de base pour déterminer si PlateSpin Protect peut communiquer avec le workload que vous tentez de protéger.

1. Accédez à votre hôte de serveur PlateSpin .
2. Ouvrez une invite de commande et effectuez un test ping sur votre workload :

   `ping` *IP_workload*

Test de connectivité WMI

1. Accédez à votre hôte de serveur PlateSpin .
2. Cliquez sur *Démarrer* > *Exécuter*, tapez `Wbemtest` et appuyez sur `Entrée`.
3. Cliquez sur *Connecter*.
4. Dans l'*espace de noms*, tapez le nom du workload que vous tentez de découvrir et ajoutez-y `\root\cimv2`. Par exemple, si le nom d'hôte est `win2k`, tapez :

   `\\win2k\root\cimv2`
5. Entrez les références appropriées, en utilisant le format `nom_hôte\AdminLocal` ou `domaine\AdminDomaine`.
6. Cliquez sur *Connexion* pour tester la connexion WMI.

   Si un message d'erreur est renvoyé, aucune connexion WMI ne peut être établie entre PlateSpin Protect et votre workload.

Dépannage de la connectivité DCOM

1. Loguez-vous au workload à protéger.
2. Cliquez sur *Démarrer* > *Exécuter*.
3. Saisissez `dcomcnfg` et appuyez sur Entrée.
4. Vérifiez la connectivité :
   - Pour les systèmes Windows (XP/Vista/2003/2008/7), la fenêtre Services de composants s'affiche. Dans le dossier *Ordinateurs* de l'arborescence de la console de l'outil d'administration Services de composants, cliquez avec le bouton droit sur l'ordinateur dont vous souhaitez vérifier la connectivité DCOM, puis cliquez sur *Propriétés*. Cliquez sur l'onglet *Propriétés par défaut* et vérifiez que l'option *Activer Distributed COM (DCOM) sur cet ordinateur* est sélectionnée.
   - Sur la machine d'un serveur Windows 2000, la boîte de dialogue Configuration DCOM s'affiche. Cliquez sur l'onglet *Propriétés par défaut* et vérifiez que l'option *Activer Distributed COM (DCOM) sur cet ordinateur* est sélectionnée.
5. Si DCOM n'était pas activé, activez-le et redémarrez le serveur ou le service d'instrumentation WMI (Windows Management Instrumentation). Tentez de nouveau d'ajouter le workload.

Dépannage de la connectivité du service RPC

Différents éléments sont susceptibles de bloquer le service RPC :

- le service Windows ;
- un pare-feu Windows ;
- un pare-feu réseau.

Pour le service Windows, assurez-vous que le service RPC est en cours d'exécution sur le workload. Pour accéder au panneau de service, exécutez le fichier `services.msc` à partir d'une invite de commande. Pour un pare-feu Windows, ajoutez une exception RPC. Pour les pare-feu matériels, vous pouvez essayer les stratégies suivantes :

- Placez PlateSpin Protect et le workload du même côté du pare-feu.
- Ouverture de ports spécifiques entre PlateSpin Protect et le workload (reportez-vous à la section « Conditions d'accès et de communication requises sur votre réseau de protection » page 25).

7.1.2 Désactivation du logiciel anti-virus

Le logiciel Anti-virus peut parfois bloquer certaines fonctionnalités de PlateSpin Protect liées à WMI et à l'accès à distance au Registre. Pour assurer la réussite de l'inventaire de workloads, il peut être nécessaire de d'abord désactiver le service Anti-virus sur un workload. En outre, le logiciel Anti-virus peut parfois verrouiller l'accès à certains fichiers et ne permettre l'accès qu'à certains processus ou exécutables, ce qui peut empêcher la réplication des données basée sur les fichiers. Dans ce cas, lorsque vous configurez la protection du workload, vous pouvez sélectionner les services à désactiver, tels que les services installés et utilisés par votre logiciel Anti-virus. Ces services ne sont désactivés que pour la durée du transfert de fichiers et sont redémarrés une fois le processus terminé. Cette précaution n'est pas nécessaire pendant la réplication des données par bloc.

7.1.3 Activation des autorisations et de l'accès aux fichiers/partages

Pour protéger efficacement un workload, PlateSpin Protect doit déployer et installer le logiciel sur le workload. Lors du déploiement de ces composants sur un workload, de même que pendant le processus Ajouter le workload, PlateSpin Protect utilise les partages administratifs du workload. Pour pouvoir fonctionner, PlateSpin Protect requiert un accès aux partages, par le biais d'un compte d'administrateur local ou d'un compte d'administrateur de domaine.

Pour vérifier que les partages administratifs sont activés :

1. Cliquez avec le bouton droit sur *Ordinateur* sur le bureau et sélectionnez *Gérer*.
2. Développez *Outils système* > *Dossiers partagés* > *Partages*
3. Le répertoire `Dossiers partagés` doit notamment contenir les partages Admin$.

Après avoir confirmé que ces partages sont activés, veillez à ce qu'ils soient accessibles à partir de l'hôte du serveur PlateSpin :

1. Accédez à votre hôte de serveur PlateSpin .
2. Cliquez sur *Démarrer* > *Exécuter*, tapez `\\<hôte_serveur>\Admin$`, puis cliquez sur *OK*.
3. Si vous recevez une invite, utilisez les mêmes références que celles que vous utiliserez pour ajouter le workload à l'inventaire de workloads de PlateSpin Protect.

   Le répertoire s'ouvre vous permettant de le parcourir et de modifier son contenu.
4. Répétez le processus pour tous les partages à l'exception du partage IPC$.

   Windows utilise le partage IPC$ pour la validation des références et pour l'authentification. Il n'est pas assigné à un dossier ou fichier sur le workload, de sorte que le test échoue toujours. Toutefois, le partage reste visible.

PlateSpin Protect ne modifie pas le contenu existant du volume. Il crée cependant son propre répertoire pour lequel il nécessite un accès et des autorisations.

7.2 Dépannage de l'inventaire de workload (Linux)

Problèmes ou messages	Solutions
`Impossible de se connecter ni au serveur SSH qui s'exécute sur <adresse_IP> ni aux services Web VMware Virtual Infrastructure à <adresse_ip>/sdk`	Les causes possibles pouvant avoir généré l'envoi de ce message sont les suivantes : ◆ le workload est inaccessible ; ◆ SSH ne s'exécute pas sur le workload ; ◆ le pare-feu est activé et les ports requis n'ont pas été ouverts ; ◆ le système d'exploitation spécifique du workload n'est pas pris en charge. Pour les conditions d'accès et de réseau d'un workload, reportez-vous à la section « Conditions d'accès et de communication requises sur votre réseau de protection » page 25.
`Accès refusé`	Ce problème d'authentification est dû à un nom d'utilisateur ou un mot de passe non valide. Pour plus d'informations sur les références d'accès des workloads, reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 68.

7.3 Dépannage des problèmes pendant l'exécution de la commande Préparer la réplication (Windows)

Problèmes ou messages	Solutions
Erreur d'authentification lors de la vérification de la connexion du contrôleur pendant la configuration de ce dernier sur la source.	Le compte utilisé pour ajouter un workload doit être autorisé par cette stratégie. Reportez-vous à la section « Stratégie de groupe et droits utilisateur » page 106.
Impossible de déterminer si .NET Framework est installé (à l'exception de `Échec de la relation d'approbation entre le poste de travail et le domaine principal`).	Vérifiez si le service d'accès à distance au Registre est activé et exécuté. Reportez-vous également à la section « Dépannage de l'inventaire de workload (Windows) » page 101.

7.3.1 Stratégie de groupe et droits utilisateur

Étant donné la façon dont PlateSpin Protect interagit avec le système d'exploitation du workload source, le compte administrateur utilisé pour ajouter un workload doit disposer de certains droits utilisateur sur la machine source. Pour la plupart des instances, ces paramètres sont ceux utilisés par défaut pour la stratégie de groupe. Toutefois, si l'environnement a été verrouillé, les assignations suivantes des droits utilisateur ont peut-être été supprimées :

- Bypass Traverse Checking (Ignorer la vérification transversale)
- Replace Process Level Token (Remplacer le token au niveau du processus)
- Act as part of the Operating System (Agir en tant qu'élément du système d'exploitation)

Pour vérifier si ces paramètres de stratégie de groupe ont été définis, vous pouvez exécuter `gpresult /v` à partir de la ligne de commande sur la machine source ou alternativement `RSOP.msc`. Si la stratégie n'a pas été définie ou a été désactivée, elle peut être activée par le biais de la stratégie de sécurité locale de la machine ou par le biais des stratégies de groupe du domaine appliquées à la machine.

Vous pouvez rafraîchir la stratégie immédiatement à l'aide de la commande `gpudate /force` (pour Windows 2003/XP) ou `secedit /refreshpolicy machine_policy /enforce` (pour Windows 2000).

7.4 Dépannage de la réplication de workload

Problèmes ou messages	Solutions
Erreur pouvant être corrigée au cours de la réplication pendant la *Planification de la prise d'un instantané de la machine virtuelle* ou la *Planification du rétablissement de la machine virtuelle selon l'instantané avant le démarrage*.	Ce problème survient lorsque le serveur est surchargé et que le processus dure plus longtemps que prévu. Attendez que la réplication soit terminée.
Un problème de workload nécessite une intervention de l'utilisateur.	Plusieurs types de problèmes peuvent être à l'origine de ce message. Dans la plupart des cas, le message doit contenir des détails sur la nature du problème et à quel niveau il se situe (connectivité, références, etc.). Patientez quelques minutes après le dépannage. Contactez le support PlateSpin si le message persiste.
Tous les workloads signalent des erreurs récupérables en raison de l'espace disque insuffisant.	Vérifiez l'espace disponible. Si vous avez besoin de plus d'espace, supprimez un workload.
Le réseau est très lent (vitesse inférieure à 1 Mo).	Vérifiez si le paramètre de duplex de la carte d'interface réseau de la machine source est activé et si le commutateur auquel elle est connectée dispose d'un paramètre correspondant. En effet, si le paramètre est configuré sur Automatique, la source ne peut pas être définie sur 100 Mo.

Problèmes ou messages	Solutions
Le réseau est très lent (vitesse supérieure à 1 Mo).	Mesurez le temps de réponse en exécutant la commande suivante à partir du workload source : `ping ip -t` (remplacez *ip* par l'adresse IP de votre hôte de serveur PlateSpin). Autorisez-le à exécuter 50 itérations et la moyenne indique la latence. Reportez-vous également à la section « Optimisation du transfert de données sur les connexions WAN » page 34.

`Le transfert de fichiers ne peut pas commencer - le port 3725 est déjà utilisé.`
 	
ou
 	
`3725 : connexion impossible`
	Assurez-vous que le port est ouvert et écoute :
	
	Exécutez `netstat -ano` sur le workload.
	
	Vérifiez le pare-feu.
	
	Réessayez la réplication.

`Connexion du contrôleur non établie` La réplication échoue à l'étape *Prise de contrôle de la machine virtuelle*.	Cette erreur se produit lorsque les informations de réseautique de réplication ne sont pas valides. Soit le serveur DHCP n'est pas disponible ou le réseau virtuel de réplication ne peut pas être routé vers l'hôte du serveur PlateSpin . Remplacez l'adresse IP de réplication par une adresse IP statique ou activez le serveur DHCP. Assurez-vous que le réseau virtuel sélectionné pour la réplication peut être routé vers l'hôte du serveur PlateSpin.

Problèmes ou messages	Solutions
La tâche de réplication ne démarre pas (bloquée à 0 %)	Cette erreur peut se produire pour diverses raisons et chacune a sa propre solution : ◆ Pour les environnements qui utilisent un proxy local avec une authentification, ignorez le proxy ou ajoutez les autorisations appropriées pour résoudre ce problème. Pour plus de détails, reportez-vous à l'article de la base de connaissances n° 20339 (https://www.netiq.com/support/kb/doc.php?id=7920339). ◆ Si des restrictions de stratégies locales ou de domaine nécessitaient des autorisations, suivez la procédure décrite dans l'article de la base de connaissances n°7920862 (https://www.netiq.com/support/kb/doc.php?id=7920862). Il s'agit d'un problème courant lorsque l'hôte du serveur PlateSpin est affilié à un domaine alors que les stratégies de domaine sont appliquées avec des restrictions. Reportez-vous à la section « Stratégie de groupe et droits utilisateur » page 106.
À la suite d'une mise à jour Windows, certains fichiers du dossier `C:\Windows\SoftwareDistribution` ne sont pas transférés vers la machine cible pendant la réplication incrémentielle basée sur les fichiers.	Il s'agit d'une pratique courante de Microsoft Windows : pour des besoins d'optimisation, certains fichiers sont marqués pour suppression dans la clé de registre `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot` afin d'éviter leur inclusion dans les instantanés VSS. Pour plus d'informations, consultez l'article MSDN en anglais, *Excluding Files from Shadow Copies* (Exclusion de fichiers des clichés instantanés). Ces fichiers sont généralement utilisés pour installer les mises à jour Windows avant d'être supprimés et ne sont plus nécessaires après la mise à jour. Si vous choisissez de restaurer ces fichiers, exécutez la mise à jour Windows sur la machine cible après le basculement pour réapprovisionner le dossier `SoftwareDistribution`.

7.5 Dépannage des workloads de transfert de trafic

dans certains scénarios, la réplique d'un workload qui transfère le trafic réseau (par exemple, si l'objectif du workload est de faire office de pont réseau pour NAT, VPN ou un pare-feu) peut voir ses performances réseau se dégrader sensiblement. Cela est dû à un problème lié aux adaptateurs VMXNET 2 et VMXNET 3 pour lesquels la fonction LRO (Large Receive Offload, déchargement de réception volumineux) est activée.

Pour résoudre ce problème, vous devez désactiver la fonction LRO sur l'adaptateur réseau virtuel. Pour plus d'informations, consultez l'article de la base de connaissances n° 7005495.

7.6 Aide en ligne pour le dépannage

sur certains systèmes comportant des paramètres de sécurité de navigateur améliorés (tels qu'Internet Explorer 8 sous Windows Server 2008), les icônes Développer et Réduire (+ et -) du sommaire risquent de ne pas fonctionner. Pour résoudre ce problème, activez JavaScript dans votre navigateur :

- **Internet Explorer :** cliquez sur *Outils* > *Options Internet* > *onglet Sécurité* > zone *Internet* > *Personnaliser le niveau*, puis sélectionnez l'option *Activé* pour la fonction *Scripts ASP*.
- **Firefox :** cliquez sur *Outils* > *Options* > *onglet Contenu*, puis sélectionnez l'option *Activer JavaScript*.

7.7 Génération et affichage de rapports de diagnostic

Dans l'interface Web PlateSpin Protect, après avoir exécuté une commande, vous pouvez générer des rapports de diagnostic détaillés sur la commande.

1 Cliquez sur *Détails de la commande*, puis sur le lien *Générer des diagnostics*.

La page se rafraîchit après quelques instants et propose un lien *Afficher* au-dessus du lien *Diagnostics générés*.

2 Cliquez sur *Afficher*.

Une nouvelle page s'ouvre et reprend des informations de diagnostic complètes sur la commande en cours.

3 Enregistrez la page des diagnostics et conservez-la si vous devez contacter le support technique.

7.8 Suppression de workloads

Il peut parfois être nécessaire de supprimer un workload de l'inventaire PlateSpin Protect et de le rajouter ultérieurement.

1 À la page Workloads, sélectionnez le workload à retirer, puis cliquez sur *Supprimer le workload*.

(Conditionnel) Pour les workloads Windows auparavant protégés par la réplication par bloc, l'interface Web PlateSpin Protect vous invite à indiquer si les composants basés sur les blocs doivent aussi être supprimés. Vous pouvez faire les sélections suivantes :

- **Ne pas supprimer les composants :** les composants ne seront pas supprimés.

- **Supprimer les composants, mais ne pas redémarrer le workload :** les composants seront supprimés. Toutefois, un redémarrage du workload sera nécessaire pour terminer le processus de désinstallation.
- **Supprimer les composants et redémarrer le workload :** les composants seront supprimés et le workload redémarrera automatiquement. Veillez à exécuter cette opération durant le temps hors service planifié.

2 À la page Confirmation de commande, cliquez sur *Confirmer* pour exécuter la commande.

Attendez que le processus se termine.

7.9 Nettoyage de workload de post-protection

Ces étapes permettent de nettoyer votre workload source en supprimant tous les composants logiciels de PlateSpin si nécessaire, par exemple après un échec de protection ou une protection problématique.

Pour plus d'informations, reportez-vous aux sections suivantes :

- Section 7.9.1, « Nettoyage des workloads Windows », page 110
- Section 7.9.2, « Nettoyage des workloads Linux », page 111

7.9.1 Nettoyage des workloads Windows

Composant	Instructions de suppression
Composant de transfert par bloc PlateSpin	Reportez-vous à l'article de la base de connaissances n° 7005616 (https://www.netiq.com/support/kb/doc.php?id=7005616).
Composant tiers de transfert par bloc (discontinué)	1. Utilisez l'applet Ajout/Suppression de programmes de Windows (exécutez le fichier `appwiz.cpl`) et supprimez le composant. Selon la source, vous pouvez disposer de l'une des versions suivantes : ◆ SteelEye Data Replication pour Windows v6 Update2 ◆ SteelEye DataKeeper pour Windows v7 2. Redémarrez la machine.
Composant de transfert basé sur les fichiers	Au niveau de la racine de chaque volume protégé, supprimez tous les fichiers nommés `PlateSpinCatalog*.dat`.
Logiciel d'inventaire de workloads	Dans le répertoire `Windows` du workload : ◆ Supprimez tous les fichiers nommés `machinediscovery*`. ◆ Supprimez le sous-répertoire nommé `platespin`.

Composant	Instructions de suppression
Logiciel contrôleur	1. Ouvrez une invite de commande et remplacez le répertoire actuel par : ◆ `\Program Files\platespin*` (systèmes 32 bits) ◆ `\Program Files (x86)\platespin*` (systèmes 64 bits) 2. Exécutez la commande suivante : `ofxcontroller.exe /uninstall` 3. Supprimez le répertoire `platespin*`.

7.9.2 Nettoyage des workloads Linux

Composant	Instructions de suppression
Logiciel contrôleur	◆ Détruisez les processus suivants : ◆ `pkill -9 ofxcontrollerd` ◆ `pkill -9 ofxjobexec` ◆ Supprimez le paquetage RPM du contrôleur OFX : `rpm -e ofxcontrollerd` ◆ Dans le système de fichiers du workload , supprimez le répertoire `/usr/lib/ofx` et son contenu.

Logiciel de transfert de données par bloc	1. Vérifiez si le pilote est actif :
	`lsmod | grep blkwatch`
	Si le pilote est toujours chargé en mémoire, le résultat devrait contenir une ligne similaire à celle-ci :
	`blkwatch_7616 70924 0`
	2. (Conditionnel) Si le pilote est toujours chargé, supprimez-le de la mémoire :
	`rmmod blkwatch_7616`
	3. Supprimez le pilote de la séquence de démarrage :
	`blkconfig -u`
	4. Supprimez les fichiers de pilote en supprimant le répertoire suivant avec son contenu :
	`/lib/modules/`*`[Version_Kernel]`*`/Platespin`
	5. Supprimez le fichier suivant :
	`/etc/blkwatch.conf`

Composant	Instructions de suppression
Instantanés du gestionnaire de volumes logiques (LVM)	Les instantanés LVM utilisés par les réplications en cours sont nommés sur la base de la convention suivante *nom_volume*-PS-snapshot. Par exemple, le nom de l'instantané d'un volume LogVol01 est LogVol01-PS-snapshot. Pour supprimer les instantanés LVM : 1. Générez une liste d'instantanés sur le workload requis à l'aide de l'une des méthodes suivantes : ◆ Utilisez l'interface Web PlateSpin Protect pour générer un rapport pour la tâche ayant échoué. Le rapport doit contenir des informations sur les instantanés LVM et leurs noms. - OU - ◆ Sur le workload Linux requis, exécutez la commande suivante pour afficher une liste de tous les volumes et instantanés : `# lvdisplay -a` 2. Notez le nom et l'emplacement des instantanés à supprimer. 3. Supprimez-les à l'aide de la commande suivante : `lvremove` *nom_instantané*
Fichiers Bitmap	À la racine de chaque volume protégé, supprimez le fichier .blocks_bitmap correspondant.
Outils	Sur le workload source, sous /sbin, supprimez les fichiers suivants : ◆ bmaputil ◆ blkconfig

7.10 Réduction de la taille des bases de données PlateSpin Protect

Lorsque les bases de données PlateSpin Protect (OFX, PortabilitySuite et Protection) atteignent une capacité prédéfinie, un nettoyage est effectué à intervalles réguliers. S'il s'avère nécessaire de réguler davantage la taille ou le contenu de ces bases de données, Protect propose un utilitaire (PlateSpin.DBCleanup.exe) qui permet de les nettoyer et de réduire leur taille. L'article 7006458 de la Base de connaissances (https://www.netiq.com/support/kb/doc.php?id=7006458) indique l'emplacement de l'outil, ainsi que les options disponibles, si vous décidez de l'utiliser pour des opérations de base de données hors ligne.

A Distributions Linux prises en charge par Protect

Le logiciel PlateSpin ForgeProtect intègre des versions précompilées du pilote `blkwatch` pour de nombreuses distributions Linux de non-débogage (32 et 64 bits). Cette section présente les informations suivantes :

- Section A.1, « Analyse de votre workload Linux », page 113
- Section A.2, « Version précompilée du pilote « blkwatch » Protect (Linux) », page 114

A.1 Analyse de votre workload Linux

Avant de déterminer si PlateSpin Protect dispose d'un pilote `blkwatch` pour votre distribution, vous devez obtenir de plus amples informations sur le kernel de votre workload Linux afin de pouvoir l'utiliser comme critère pour effectuer une recherche dans la liste des distributions prises en charge. Cette section présente les informations suivantes :

- Section A.1.1, « Détermination de la chaîne de version », page 113
- Section A.1.2, « Détermination de l'architecture », page 114

A.1.1 Détermination de la chaîne de version

Vous pouvez déterminer la chaîne de version du kernel de votre workload Linux en exécutant la commande suivante sur le terminal Linux du workload :

```
uname -r
```

Par exemple, si vous exécutez `uname -r`, le résultat suivant peut être renvoyé :

```
3.0.76-0.11-default
```

Si vous effectuez une recherche dans la liste de distributions, vous pouvez constater que deux entrées correspondent à cette chaîne :

- `SLES11SP3-GA-3.0.76-0.11-default-x86`
- `SLES11SP3-GA-3.0.76-0.11-default-x86_64`

Les résultats de la recherche indiquent que le produit intègre des pilotes pour les architectures 32 bits (x86) et 64 bits (x86_64).

A.1.2 Détermination de l'architecture

Vous pouvez déterminer l'architecture de votre workload Linux en exécutant la commande suivante sur le terminal Linux du workload :

```
uname -m
```

Par exemple, si vous exécutez la commande `uname -m`, le résultat suivant peut être renvoyé :

```
x86_64
```

Sur la base de ces informations, il vous est possible de déterminer que le workload a une architecture 64 bits.

A.2 Version précompilée du pilote « blkwatch » Protect (Linux)

Vous trouverez, ci-après, la liste des distributions Linux de non-débogage pour lesquelles Protect offre un pilote `blkwatch`. Vous pouvez effectuer une recherche dans cette liste afin de déterminer si la chaîne de version et l'architecture du kernel de votre workload Linux correspondent à une distribution prise en charge de la liste. Si vous trouvez votre chaîne de version et votre architecture dans la liste, cela signifie que PlateSpin Protect intègre une version précompilée du pilote `blkwatch`.

Si votre recherche ne renvoie aucun résultat, vous avez la possibilité de créer un pilote `blkwatch` personnalisé en suivant la procédure décrite dans l'article de la base de connaissances KB 7005873.

Syntaxe des éléments de liste

Chaque élément de liste est formaté à l'aide de la syntaxe suivante :

<Distribution>-<Correctif>-<Chaîne_version_kernel>-<Architecture_kernel>

Ainsi, pour une distribution SLES 9 SP1 avec une chaîne de version de kernel `2.6.5-7.139-bigsmp` et une architecture 32 bits (x86), l'élément est listé dans un format similaire à celui-ci :

```
SLES9-SP1-2.6.5-7.139-bigsmp-x86
```

Liste des distributions

```
RHEL4-GA-2.6.9-5.EL-x86
RHEL4-GA-2.6.9-5.EL-x86_64
RHEL4-GA-2.6.9-5.ELhugemem-x86
RHEL4-GA-2.6.9-5.ELsmp-x86
RHEL4-GA-2.6.9-5.ELsmp-x86_64
RHEL4-U1-2.6.9-11.EL-x86
RHEL4-U1-2.6.9-11.EL-x86_64
RHEL4-U1-2.6.9-11.ELhugemem-x86
RHEL4-U1-2.6.9-11.ELsmp-x86
RHEL4-U1-2.6.9-11.ELsmp-x86_64
RHEL4-U2-2.6.9-22.EL-x86
RHEL4-U2-2.6.9-22.EL-x86_64
RHEL4-U2-2.6.9-22.ELhugemem-x86
RHEL4-U2-2.6.9-22.ELsmp-x86
RHEL4-U2-2.6.9-22.ELsmp-x86_64
```

```
RHEL4-U3-2.6.9-34.EL-x86
RHEL4-U3-2.6.9-34.EL-x86_64
RHEL4-U3-2.6.9-34.ELhugemem-x86
RHEL4-U3-2.6.9-34.ELlargesmp-x86_64
RHEL4-U3-2.6.9-34.ELsmp-x86
RHEL4-U3-2.6.9-34.ELsmp-x86_64
RHEL4-U4-2.6.9-42.EL-x86
RHEL4-U4-2.6.9-42.EL-x86_64
RHEL4-U4-2.6.9-42.ELhugemem-x86
RHEL4-U4-2.6.9-42.ELlargesmp-x86_64
RHEL4-U4-2.6.9-42.ELsmp-x86
RHEL4-U4-2.6.9-42.ELsmp-x86_64
RHEL4-U5-2.6.9-55.EL-x86
RHEL4-U5-2.6.9-55.EL-x86_64
RHEL4-U5-2.6.9-55.ELhugemem-x86
RHEL4-U5-2.6.9-55.ELlargesmp-x86_64
RHEL4-U5-2.6.9-55.ELsmp-x86
RHEL4-U5-2.6.9-55.ELsmp-x86_64
RHEL4-U6-2.6.9-67.EL-x86
RHEL4-U6-2.6.9-67.EL-x86_64
RHEL4-U6-2.6.9-67.ELhugemem-x86
RHEL4-U6-2.6.9-67.ELlargesmp-x86_64
RHEL4-U6-2.6.9-67.ELsmp-x86
RHEL4-U6-2.6.9-67.ELsmp-x86_64
RHEL4-U7-2.6.9-78.EL-x86
RHEL4-U7-2.6.9-78.EL-x86_64
RHEL4-U7-2.6.9-78.ELhugemem-x86
RHEL4-U7-2.6.9-78.ELlargesmp-x86_64
RHEL4-U7-2.6.9-78.ELsmp-x86
RHEL4-U7-2.6.9-78.ELsmp-x86_64
RHEL4-U8-2.6.9-89.EL-x86
RHEL4-U8-2.6.9-89.EL-x86_64
RHEL4-U8-2.6.9-89.ELhugemem-x86
RHEL4-U8-2.6.9-89.ELlargesmp-x86_64
RHEL4-U8-2.6.9-89.ELsmp-x86
RHEL4-U8-2.6.9-89.ELsmp-x86_64
RHEL4-U9-2.6.9-100.EL-x86
RHEL4-U9-2.6.9-100.EL-x86_64
RHEL4-U9-2.6.9-100.ELhugemem-x86
RHEL4-U9-2.6.9-100.ELlargesmp-x86_64
RHEL4-U9-2.6.9-100.ELsmp-x86
RHEL4-U9-2.6.9-100.ELsmp-x86_64
RHEL5-GA-2.6.18-8.el5-x86
RHEL5-GA-2.6.18-8.el5-x86_64
RHEL5-GA-2.6.18-8.el5PAE-x86
RHEL5-U1-2.6.18-53.el5-x86
RHEL5-U1-2.6.18-53.el5-x86_64
```

```
RHEL5-U1-2.6.18-53.el5PAE-x86
RHEL5-U10-2.6.18-371.el5-x86
RHEL5-U10-2.6.18-371.el5-x86_64
RHEL5-U10-2.6.18-371.el5PAE-x86
RHEL5-U2-2.6.18-92.el5-x86
RHEL5-U2-2.6.18-92.el5-x86_64
RHEL5-U2-2.6.18-92.el5PAE-x86
RHEL5-U3-2.6.18-128.el5-x86
RHEL5-U3-2.6.18-128.el5-x86_64
RHEL5-U3-2.6.18-128.el5PAE-x86
RHEL5-U4-2.6.18-164.el5-x86
RHEL5-U4-2.6.18-164.el5-x86_64
RHEL5-U4-2.6.18-164.el5PAE-x86
RHEL5-U5-2.6.18-194.el5-x86
RHEL5-U5-2.6.18-194.el5-x86_64
RHEL5-U5-2.6.18-194.el5PAE-x86
RHEL5-U6-2.6.18-238.el5-x86
RHEL5-U6-2.6.18-238.el5-x86_64
RHEL5-U6-2.6.18-238.el5PAE-x86
RHEL5-U7-2.6.18-274.el5-x86
RHEL5-U7-2.6.18-274.el5-x86_64
RHEL5-U7-2.6.18-274.el5PAE-x86
RHEL5-U8-2.6.18-308.el5-x86
RHEL5-U8-2.6.18-308.el5-x86_64
RHEL5-U8-2.6.18-308.el5PAE-x86
RHEL5-U9-2.6.18-348.el5-x86
RHEL5-U9-2.6.18-348.el5-x86_64
RHEL5-U9-2.6.18-348.el5PAE-x86
RHEL6-GA-2.6.32-71.el6.i686-x86
RHEL6-GA-2.6.32-71.el6.x86_64-x86_64
RHEL6-U1-2.6.32-131.0.15.el6.i686-x86
RHEL6-U1-2.6.32-131.0.15.el6.x86_64-x86_64
RHEL6-U2-2.6.32-220.el6.i686-x86
RHEL6-U2-2.6.32-220.el6.x86_64-x86_64
RHEL6-U3-2.6.32-279.el6.i686-x86
RHEL6-U3-2.6.32-279.el6.x86_64-x86_64
RHEL6-U4-2.6.32-358.el6.i686-x86
RHEL6-U4-2.6.32-358.el6.x86_64-x86_64
RHEL6-U5-2.6.32-431.el6.i686-x86
RHEL6-U5-2.6.32-431.el6.x86_64-x86_64
SLES10-GA-2.6.16.21-0.8-bigsmp-x86
SLES10-GA-2.6.16.21-0.8-default-x86
SLES10-GA-2.6.16.21-0.8-default-x86_64
SLES10-GA-2.6.16.21-0.8-smp-x86
SLES10-GA-2.6.16.21-0.8-smp-x86_64
SLES10-GA-2.6.16.21-0.8-xen-x86
SLES10-GA-2.6.16.21-0.8-xen-x86_64
```

SLES10-GA-2.6.16.21-0.8-xenpae-x86
SLES10-SP1-2.6.16.46-0.12-bigsmp-x86
SLES10-SP1-2.6.16.46-0.12-default-x86
SLES10-SP1-2.6.16.46-0.12-default-x86_64
SLES10-SP1-2.6.16.46-0.12-smp-x86
SLES10-SP1-2.6.16.46-0.12-smp-x86_64
SLES10-SP1-2.6.16.46-0.12-xen-x86
SLES10-SP1-2.6.16.46-0.12-xen-x86_64
SLES10-SP1-2.6.16.46-0.12-xenpae-x86
SLES10-SP2-2.6.16.60-0.21-bigsmp-x86
SLES10-SP2-2.6.16.60-0.21-default-x86
SLES10-SP2-2.6.16.60-0.21-default-x86_64
SLES10-SP2-2.6.16.60-0.21-smp-x86
SLES10-SP2-2.6.16.60-0.21-smp-x86_64
SLES10-SP2-2.6.16.60-0.21-xen-x86
SLES10-SP2-2.6.16.60-0.21-xen-x86_64
SLES10-SP2-2.6.16.60-0.21-xenpae-x86
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-bigsmp-x86
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-default-x86
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-default-x86_64
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-smp-x86
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-smp-x86_64
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-xen-x86
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-xen-x86_64
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-xenpae-x86
SLES10-SP3-2.6.16.60-0.54.5-bigsmp-x86
SLES10-SP3-2.6.16.60-0.54.5-default-x86
SLES10-SP3-2.6.16.60-0.54.5-default-x86_64
SLES10-SP3-2.6.16.60-0.54.5-smp-x86
SLES10-SP3-2.6.16.60-0.54.5-smp-x86_64
SLES10-SP3-2.6.16.60-0.54.5-xen-x86
SLES10-SP3-2.6.16.60-0.54.5-xen-x86_64
SLES10-SP3-2.6.16.60-0.54.5-xenpae-x86
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-bigsmp-x86
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-default-x86
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-default-x86_64
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-smp-x86
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-smp-x86_64
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-xen-x86
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-xen-x86_64
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-xenpae-x86
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-bigsmp-x86
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-default-x86
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-default-x86_64
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-smp-x86
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-smp-x86_64
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-xen-x86

```
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-xen-x86_64
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-xenpae-x86
SLES10-SP4-2.6.16.60-0.85.1-bigsmp-x86
SLES10-SP4-2.6.16.60-0.85.1-default-x86
SLES10-SP4-2.6.16.60-0.85.1-default-x86_64
SLES10-SP4-2.6.16.60-0.85.1-smp-x86
SLES10-SP4-2.6.16.60-0.85.1-smp-x86_64
SLES10-SP4-2.6.16.60-0.85.1-xen-x86
SLES10-SP4-2.6.16.60-0.85.1-xen-x86_64
SLES10-SP4-2.6.16.60-0.85.1-xenpae-x86
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-bigsmp-x86
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-default-x86
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-default-x86_64
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-smp-x86
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-smp-x86_64
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-xen-x86
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-xen-x86_64
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-xenpae-x86
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-bigsmp-x86
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-default-x86
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-default-x86_64
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-smp-x86
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-smp-x86_64
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-xen-x86
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-xen-x86_64
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-xenpae-x86
SLES10-SP4_U4-2.6.16.60-0.93.1-bigsmp-x86
SLES10-SP4_U4-2.6.16.60-0.93.1-default-x86
SLES10-SP4_U4-2.6.16.60-0.93.1-default-x86_64
SLES10-SP4_U4-2.6.16.60-0.93.1-smp-x86
SLES10-SP4_U4-2.6.16.60-0.93.1-smp-x86_64
SLES10-SP4_U4-2.6.16.60-0.93.1-xen-x86
SLES10-SP4_U4-2.6.16.60-0.93.1-xen-x86_64
SLES10-SP4_U4-2.6.16.60-0.93.1-xenpae-x86
SLES10-SP4_U5-2.6.16.60-0.97.1-bigsmp-x86
SLES10-SP4_U5-2.6.16.60-0.97.1-default-x86
SLES10-SP4_U5-2.6.16.60-0.97.1-default-x86_64
SLES10-SP4_U5-2.6.16.60-0.97.1-smp-x86
SLES10-SP4_U5-2.6.16.60-0.97.1-smp-x86_64
SLES10-SP4_U5-2.6.16.60-0.97.1-xen-x86
SLES10-SP4_U5-2.6.16.60-0.97.1-xen-x86_64
SLES10-SP4_U5-2.6.16.60-0.97.1-xenpae-x86
SLES10-SP4_U6-2.6.16.60-0.99.1-bigsmp-x86
SLES10-SP4_U6-2.6.16.60-0.99.1-default-x86
SLES10-SP4_U6-2.6.16.60-0.99.1-default-x86_64
SLES10-SP4_U6-2.6.16.60-0.99.1-smp-x86
SLES10-SP4_U6-2.6.16.60-0.99.1-smp-x86_64
```

SLES10-SP4_U6-2.6.16.60-0.99.1-xen-x86
SLES10-SP4_U6-2.6.16.60-0.99.1-xen-x86_64
SLES10-SP4_U6-2.6.16.60-0.99.1-xenpae-x86
SLES10-SP4_U7-2.6.16.60-0.101.1-bigsmp-x86
SLES10-SP4_U7-2.6.16.60-0.101.1-default-x86
SLES10-SP4_U7-2.6.16.60-0.101.1-default-x86_64
SLES10-SP4_U7-2.6.16.60-0.101.1-smp-x86
SLES10-SP4_U7-2.6.16.60-0.101.1-smp-x86_64
SLES10-SP4_U7-2.6.16.60-0.101.1-xen-x86
SLES10-SP4_U7-2.6.16.60-0.101.1-xen-x86_64
SLES10-SP4_U7-2.6.16.60-0.101.1-xenpae-x86
SLES10-SP4_U8-2.6.16.60-0.103.1-bigsmp-x86
SLES10-SP4_U8-2.6.16.60-0.103.1-default-x86
SLES10-SP4_U8-2.6.16.60-0.103.1-default-x86_64
SLES10-SP4_U8-2.6.16.60-0.103.1-smp-x86
SLES10-SP4_U8-2.6.16.60-0.103.1-smp-x86_64
SLES10-SP4_U8-2.6.16.60-0.103.1-xen-x86
SLES10-SP4_U8-2.6.16.60-0.103.1-xen-x86_64
SLES10-SP4_U8-2.6.16.60-0.103.1-xenpae-x86
SLES11-GA-2.6.27.19-5-default-x86
SLES11-GA-2.6.27.19-5-default-x86_64
SLES11-GA-2.6.27.19-5-pae-x86
SLES11-SP1-2.6.32.12-0.6-default-x86
SLES11-SP1-2.6.32.12-0.6-default-x86_64
SLES11-SP1-2.6.32.12-0.6-pae-x86
SLES11-SP1_LTSS_U1-2.6.32.59-0.9-default-x86
SLES11-SP1_LTSS_U1-2.6.32.59-0.9-default-x86_64
SLES11-SP1_LTSS_U1-2.6.32.59-0.9-pae-x86
SLES11-SP1_LTSS_U2-2.6.32.59-0.13-default-x86
SLES11-SP1_LTSS_U2-2.6.32.59-0.13-default-x86_64
SLES11-SP1_LTSS_U2-2.6.32.59-0.13-pae-x86
SLES11-SP1_U14-2.6.32.54-0.3-default-x86
SLES11-SP1_U14-2.6.32.54-0.3-default-x86_64
SLES11-SP1_U14-2.6.32.54-0.3-pae-x86
SLES11-SP1_U15-2.6.32.59-0.3-default-x86
SLES11-SP1_U15-2.6.32.59-0.3-default-x86_64
SLES11-SP1_U15-2.6.32.59-0.3-pae-x86
SLES11-SP1_U16-2.6.32.59-0.7-default-x86
SLES11-SP1_U16-2.6.32.59-0.7-default-x86_64
SLES11-SP1_U16-2.6.32.59-0.7-pae-x86
SLES11SP2-GA-3.0.13-0.27-default-x86
SLES11SP2-GA-3.0.13-0.27-default-x86_64
SLES11SP2-GA-3.0.13-0.27-pae-x86
SLES11SP2-GA-3.0.13-0.27-xen-x86
SLES11SP2-GA-3.0.13-0.27-xen-x86_64
SLES11SP2-LTSS_U1-3.0.101-0.7.19-default-x86
SLES11SP2-LTSS_U1-3.0.101-0.7.19-default-x86_64

```
SLES11SP2-LTSS_U1-3.0.101-0.7.19-pae-x86
SLES11SP2-LTSS_U1-3.0.101-0.7.19-xen-x86
SLES11SP2-LTSS_U1-3.0.101-0.7.19-xen-x86_64
SLES11SP2-LTSS_U2-3.0.101-0.7.21-default-x86
SLES11SP2-LTSS_U2-3.0.101-0.7.21-default-x86_64
SLES11SP2-LTSS_U2-3.0.101-0.7.21-pae-x86
SLES11SP2-LTSS_U2-3.0.101-0.7.21-xen-x86
SLES11SP2-LTSS_U2-3.0.101-0.7.21-xen-x86_64
SLES11SP2-U1-3.0.26-0.7-default-x86
SLES11SP2-U1-3.0.26-0.7-default-x86_64
SLES11SP2-U1-3.0.26-0.7-pae-x86
SLES11SP2-U1-3.0.26-0.7-xen-x86
SLES11SP2-U1-3.0.26-0.7-xen-x86_64
SLES11SP2-U10-3.0.74-0.6.8-default-x86
SLES11SP2-U10-3.0.74-0.6.8-default-x86_64
SLES11SP2-U10-3.0.74-0.6.8-pae-x86
SLES11SP2-U10-3.0.74-0.6.8-xen-x86
SLES11SP2-U10-3.0.74-0.6.8-xen-x86_64
SLES11SP2-U11-3.0.74-0.6.10-default-x86
SLES11SP2-U11-3.0.74-0.6.10-default-x86_64
SLES11SP2-U11-3.0.74-0.6.10-pae-x86
SLES11SP2-U11-3.0.74-0.6.10-xen-x86
SLES11SP2-U11-3.0.74-0.6.10-xen-x86_64
SLES11SP2-U12-3.0.80-0.5-default-x86
SLES11SP2-U12-3.0.80-0.5-default-x86_64
SLES11SP2-U12-3.0.80-0.5-pae-x86
SLES11SP2-U12-3.0.80-0.5-xen-x86
SLES11SP2-U12-3.0.80-0.5-xen-x86_64
SLES11SP2-U13-3.0.80-0.7-default-x86
SLES11SP2-U13-3.0.80-0.7-default-x86_64
SLES11SP2-U13-3.0.80-0.7-pae-x86
SLES11SP2-U13-3.0.80-0.7-xen-x86
SLES11SP2-U13-3.0.80-0.7-xen-x86_64
SLES11SP2-U14-3.0.93-0.5-default-x86
SLES11SP2-U14-3.0.93-0.5-default-x86_64
SLES11SP2-U14-3.0.93-0.5-pae-x86
SLES11SP2-U14-3.0.93-0.5-xen-x86
SLES11SP2-U14-3.0.93-0.5-xen-x86_64
SLES11SP2-U15-3.0.101-0.5-default-x86
SLES11SP2-U15-3.0.101-0.5-default-x86_64
SLES11SP2-U15-3.0.101-0.5-pae-x86
SLES11SP2-U15-3.0.101-0.5-xen-x86
SLES11SP2-U15-3.0.101-0.5-xen-x86_64
SLES11SP2-U16-3.0.101-0.7.15-default-x86
SLES11SP2-U16-3.0.101-0.7.15-default-x86_64
SLES11SP2-U16-3.0.101-0.7.15-pae-x86
SLES11SP2-U16-3.0.101-0.7.15-xen-x86
```

SLES11SP2-U16-3.0.101-0.7.15-xen-x86_64
SLES11SP2-U17-3.0.101-0.7.17-default-x86
SLES11SP2-U17-3.0.101-0.7.17-default-x86_64
SLES11SP2-U17-3.0.101-0.7.17-pae-x86
SLES11SP2-U17-3.0.101-0.7.17-xen-x86
SLES11SP2-U17-3.0.101-0.7.17-xen-x86_64
SLES11SP2-U2-3.0.31-0.9-default-x86
SLES11SP2-U2-3.0.31-0.9-default-x86_64
SLES11SP2-U2-3.0.31-0.9-pae-x86
SLES11SP2-U2-3.0.31-0.9-xen-x86
SLES11SP2-U2-3.0.31-0.9-xen-x86_64
SLES11SP2-U3-3.0.34-0.7-default-x86
SLES11SP2-U3-3.0.34-0.7-default-x86_64
SLES11SP2-U3-3.0.34-0.7-pae-x86
SLES11SP2-U3-3.0.34-0.7-xen-x86
SLES11SP2-U3-3.0.34-0.7-xen-x86_64
SLES11SP2-U4-3.0.38-0.5-default-x86
SLES11SP2-U4-3.0.38-0.5-default-x86_64
SLES11SP2-U4-3.0.38-0.5-pae-x86
SLES11SP2-U4-3.0.38-0.5-xen-x86
SLES11SP2-U4-3.0.38-0.5-xen-x86_64
SLES11SP2-U5-3.0.42-0.7-default-x86
SLES11SP2-U5-3.0.42-0.7-default-x86_64
SLES11SP2-U5-3.0.42-0.7-pae-x86
SLES11SP2-U5-3.0.42-0.7-xen-x86
SLES11SP2-U5-3.0.42-0.7-xen-x86_64
SLES11SP2-U6-3.0.51-0.7.9-default-x86
SLES11SP2-U6-3.0.51-0.7.9-default-x86_64
SLES11SP2-U6-3.0.51-0.7.9-pae-x86
SLES11SP2-U6-3.0.51-0.7.9-xen-x86
SLES11SP2-U6-3.0.51-0.7.9-xen-x86_64
SLES11SP2-U7-3.0.58-0.6.2-default-x86
SLES11SP2-U7-3.0.58-0.6.2-default-x86_64
SLES11SP2-U7-3.0.58-0.6.2-pae-x86
SLES11SP2-U7-3.0.58-0.6.2-xen-x86
SLES11SP2-U7-3.0.58-0.6.2-xen-x86_64
SLES11SP2-U8-3.0.58-0.6.6-default-x86
SLES11SP2-U8-3.0.58-0.6.6-default-x86_64
SLES11SP2-U8-3.0.58-0.6.6-pae-x86
SLES11SP2-U8-3.0.58-0.6.6-xen-x86
SLES11SP2-U8-3.0.58-0.6.6-xen-x86_64
SLES11SP2-U9-3.0.74-0.6.6-default-x86
SLES11SP2-U9-3.0.74-0.6.6-default-x86_64
SLES11SP2-U9-3.0.74-0.6.6-pae-x86
SLES11SP2-U9-3.0.74-0.6.6-xen-x86
SLES11SP2-U9-3.0.74-0.6.6-xen-x86_64
SLES11SP3-GA-3.0.76-0.11-default-x86

```
SLES11SP3-GA-3.0.76-0.11-default-x86_64
SLES11SP3-GA-3.0.76-0.11-pae-x86
SLES11SP3-GA-3.0.76-0.11-xen-x86
SLES11SP3-GA-3.0.76-0.11-xen-x86_64
SLES11SP3-U1-3.0.82-0.7-default-x86
SLES11SP3-U1-3.0.82-0.7-default-x86_64
SLES11SP3-U1-3.0.82-0.7-pae-x86
SLES11SP3-U1-3.0.82-0.7-xen-x86
SLES11SP3-U1-3.0.82-0.7-xen-x86_64
SLES11SP3-U2-3.0.93-0.8-default-x86
SLES11SP3-U2-3.0.93-0.8-default-x86_64
SLES11SP3-U2-3.0.93-0.8-pae-x86
SLES11SP3-U2-3.0.93-0.8-xen-x86
SLES11SP3-U2-3.0.93-0.8-xen-x86_64
SLES11SP3-U3-3.0.101-0.8-default-x86
SLES11SP3-U3-3.0.101-0.8-default-x86_64
SLES11SP3-U3-3.0.101-0.8-pae-x86
SLES11SP3-U3-3.0.101-0.8-xen-x86
SLES11SP3-U3-3.0.101-0.8-xen-x86_64
SLES11SP3-U4-3.0.101-0.15-default-x86
SLES11SP3-U4-3.0.101-0.15-default-x86_64
SLES11SP3-U4-3.0.101-0.15-pae-x86
SLES11SP3-U4-3.0.101-0.15-xen-x86
SLES11SP3-U4-3.0.101-0.15-xen-x86_64
SLES11SP3-U5-3.0.101-0.21-default-x86
SLES11SP3-U5-3.0.101-0.21-default-x86_64
SLES11SP3-U5-3.0.101-0.21-pae-x86
SLES11SP3-U5-3.0.101-0.21-xen-x86
SLES11SP3-U5-3.0.101-0.21-xen-x86_64
SLES11SP3-U6-3.0.101-0.29-default-x86
SLES11SP3-U6-3.0.101-0.29-default-x86_64
SLES11SP3-U6-3.0.101-0.29-pae-x86
SLES11SP3-U6-3.0.101-0.29-xen-x86
SLES11SP3-U6-3.0.101-0.29-xen-x86_64
SLES11SP3-U7-3.0.101-0.31-default-x86
SLES11SP3-U7-3.0.101-0.31-default-x86_64
SLES11SP3-U7-3.0.101-0.31-pae-x86
SLES11SP3-U7-3.0.101-0.31-xen-x86
SLES11SP3-U7-3.0.101-0.31-xen-x86_64
SLES11SP3-U8-3.0.101-0.35-default-x86
SLES11SP3-U8-3.0.101-0.35-default-x86_64
SLES11SP3-U8-3.0.101-0.35-pae-x86
SLES11SP3-U8-3.0.101-0.35-xen-x86
SLES11SP3-U8-3.0.101-0.35-xen-x86_64
SLES9-GA-2.6.5-7.97-bigsmp-x86
SLES9-GA-2.6.5-7.97-default-x86
SLES9-GA-2.6.5-7.97-default-x86_64
```

```
SLES9-GA-2.6.5-7.97-smp-x86
SLES9-GA-2.6.5-7.97-smp-x86_64
SLES9-SP1-2.6.5-7.139-bigsmp-x86
SLES9-SP1-2.6.5-7.139-default-x86
SLES9-SP1-2.6.5-7.139-default-x86_64
SLES9-SP1-2.6.5-7.139-smp-x86
SLES9-SP1-2.6.5-7.139-smp-x86_64
SLES9-SP2-2.6.5-7.191-bigsmp-x86
SLES9-SP2-2.6.5-7.191-default-x86
SLES9-SP2-2.6.5-7.191-default-x86_64
SLES9-SP2-2.6.5-7.191-smp-x86
SLES9-SP2-2.6.5-7.191-smp-x86_64
SLES9-SP3-2.6.5-7.244-bigsmp-x86
SLES9-SP3-2.6.5-7.244-default-x86
SLES9-SP3-2.6.5-7.244-default-x86_64
SLES9-SP3-2.6.5-7.244-smp-x86
SLES9-SP3-2.6.5-7.244-smp-x86_64
SLES9-SP4-2.6.5-7.308-bigsmp-x86
SLES9-SP4-2.6.5-7.308-default-x86
SLES9-SP4-2.6.5-7.308-default-x86_64
SLES9-SP4-2.6.5-7.308-smp-x86
SLES9-SP4-2.6.5-7.308-smp-x86_64
```

B Synchronisation du stockage local du noeud de grappe

Cette section décrit, de manière détaillée, la procédure à suivre pour modifier les numéros de série des volumes locaux afin de les faire correspondre à chaque noeud du cluster Windows à protéger. Il y est notamment question de l'emploi de l'utilitaire Gestionnaire de volumes (`VolumeManager.exe`) pour synchroniser le stockage local du noeud de grappe.

Pour télécharger et exécuter l'utilitaire :

1. Recherchez le produit Protect 11 sur le site de téléchargement de NetIQ, puis cliquez sur **Submit Query** (Envoyer la requête).
2. Sélectionnez **PlateSpin Protect 11.0** sous l'onglet des produits, puis cliquez sur **proceed to download** (procéder au téléchargement).
3. Dans la page de téléchargement, cliquez sur **download** (télécharger) dans la ligne *VolumeManager.exe* ou sélectionnez le lien du gestionnaire de téléchargement comparable.
4. Téléchargez l'utilitaire, puis copiez-le dans un emplacement accessible sur chaque noeud de grappe.
5. Sur le noeud actif de la grappe, ouvrez une invite de commande d'administration, accédez à l'emplacement de l'utilitaire téléchargé, puis exécutez la commande suivante :

   ```
   VolumeManager.exe -l
   ```

   La liste des volumes locaux et des numéros de série correspondants s'affiche. Par exemple :

   ```
   Volume Listing:

   --------------------

   DriveLetter (*:) VolumeId="System Reserved" SerialNumber: AABB-CCDD

   DriveLetter (C:) VolumeId=C:\ SerialNumber: 1122-3344
   ```

   Prenez note de ces numéros de série ou laissez-les à l'écran en vue d'une comparaison ultérieure.
6. Vérifiez que tous les numéros de série de stockage local du noeud actif correspondent bien à ceux des autres noeuds de la grappe.
   - **6a** Sur chaque noeud de grappe, exécutez la commande `VolumeManager.exe -l` afin d'obtenir les numéros de série de volume correspondants.
   - **6b** Comparez les numéros de série de stockage local du noeud actif (Étape 5) à ceux du noeud (Étape 6a).
   - **6c** (Conditionnel) En cas de divergence entre les numéros de série du noeud actif et de ce noeud, prenez note du numéro de série à propager sur ce noeud et exécutez la commande suivante afin de définir le numéro en question, puis de le vérifier :

     ```
     VolumeManager -s <ID_volume> <numéro-série>
     ```

Vous trouverez, ci-dessous, deux exemples d'utilisation de cette commande :

- `VolumeManager -s "Système réservé" AAAA-AAAA`
- `VolumeManager -s C:\ 1111-1111`

6d Après avoir modifié tous les numéros de série de volume d'un noeud de la grappe, vous devez redémarrer ce noeud.

6e Effectuez à nouveau la procédure de l'Étape 6a à l'Étape 6d pour chaque noeud de la grappe.

7 (Conditionnel) Si la grappe a déjà été protégée dans un environnement PlateSpin, il est conseillé d'exécuter une réplication complète sur le noeud actif afin de s'assurer que les éventuelles modifications sont propagées à la base de données.

Glossaire

Basculement. Reprise de la fonction métier d'un workload qui a échoué par un workload de basculement figurant dans un conteneur de VM de PlateSpin Protect.

Cible. Workload ou son infrastructure qui constitue le résultat d'une commande de PlateSpin Protect. Par exemple, lors de la protection initiale d'un workload, la cible est le workload de basculement dans le conteneur. Pour une opération de rétablissement, il s'agit de l'infrastructure d'origine de votre workload de production ou tout conteneur pris en charge inventorié par PlateSpin Protect.

Voir également Source.

Conteneur. Infrastructure de protection du workload PlateSpin Protect, telle que l'hôte de la machine virtuelle.

Contrat de protection. Collecte des paramètres activés relatifs au cycle de vie complet de la protection d'un workload (*Ajout d'un inventaire*, *Réplications* initiales et en cours, *Basculement*, *Rétablissement* et *Reprotection*).

Délai maximal d'interruption admissible (DMIA ou RTO – Recovery Time Objective). Mesure du temps hors service tolérable d'un workload défini par la durée d'une opération basculement. Également connue sous l'abréviation anglaise RTO (Recovery Time Objective).

Délai maximal de test admissible (DMTA ou TTO – Test Time Objective). Mesure de la facilité de test d'un plan de reprise après sinistre. Également connue sous l'abréviation anglaise TTO (Test Time Objective). Il est similaire au DMIA mais inclut le temps nécessaire à l'utilisateur pour tester le workload de basculement.

Événement. Message du serveur PlateSpin contenant des informations sur les étapes importantes du cycle de vie de protection de workload.

Incrémentiel. 1. (Nom) Transfert isolé planifié ou transfert manuel des différences entre un workload protégé et sa réplique (le workload de basculement).

2. (Adjectif) Décrit la portée de la *réplication (1)* dans laquelle la réplique initiale d'un workload est créée de façon différentielle, selon les différences entre le workload et son homologue préparé.

Niveau de protection. Collection personnalisable des paramètres de protection de workload qui définit la fréquence des réplications et les critères dont le système doit tenir compte pour considérer qu'un workload a échoué.

Perte de données maximale admissible (PDMA ou RPO – Recovery Point Objective). Perte de données tolérable mesurée en temps et définie par un intervalle configurable entre les réplications incrémentielles d'un workload protégé.

Planification de réplication. Planification configurée pour contrôler la fréquence et la portée des réplications.

Point de reprise. Instantané permettant la restauration d'un workload répliqué à son état précédent.

Préparation au basculement. Opération de PlateSpin Protect qui démarre le workload de basculement pour préparer une opération complète de basculement.

Réplication. 1. *Réplication initiale* : création d'une copie de base initiale d'un workload. Peut être effectuée en tant que *Réplication complète* (toutes les données de workload sont transférées sur une machine virtuelle de basculement « vide ») ou en tant que *Réplication incrémentielle* [voir Incrémentiel (2)].

2. Tout transfert de données modifiées d'un workload protégé vers sa réplique dans le conteneur.

Reprotéger. Commande PlateSpin Protect qui rétablit un contrat de protection pour un workload à la suite des opérations de basculement et de rétablissement.

Rétablissement. Restauration de la fonction métier d'un workload qui a échoué dans son environnement d'origine lorsque la fonction métier d'un workload de basculement temporaire au sein de PlateSpin Protect n'est plus requise.

Source. Workload ou son infrastructure qui constitue le point de départ d'une opération dans PlateSpin Protect. Par exemple, lors de la protection initiale d'un workload, la source est votre workload de production. Pour une opération de rétablissement, il s'agit du workload de basculement dans le conteneur.

Voir également Cible.

Test de basculement. Opération de PlateSpin Protect qui démarre un workload de basculement dans un environnement réseau isolé pour tester la fonctionnalité du basculement et vérifier l'intégrité du workload de basculement.

Workload. Objet de base pour la protection d'une banque de données. Système d'exploitation, ainsi que ses applications et données, dissocié de son infrastructure physique ou virtuelle sous-jacente.

Workload de basculement. Réplique virtuelle démarrable d'un workload protégé.