MICRO FOCUS

PlateSpin® Protect 11.2 SP1

Guide de l'utilisateur

Décembre 2017

Mentions légales

Pour plus d'informations sur les mentions légales, les marques, les exclusions de garantie, les garanties, les limitations en matière d'exportation et d'utilisation, les droits du gouvernement américain, la politique relative aux brevets et la compatibilité avec la norme FIPS, consultez le site https://www.microfocus.com/about/legal/.

Copyright © 2017 NetIQ Corporation, une société Micro Focus. Tous droits réservés.

Octroi de licence

Les licences achetées pour PlateSpin Protect 11 et versions ultérieures ne peuvent pas être utilisées pour PlateSpin Protect 10.3 ou versions antérieures.

Table des matières

À propos de ce guide

Le *Guide de l'utilisateur* fournit des informations sur l'utilisation de PlateSpin Protect. Il présente des informations conceptuelles, un aperçu de l'interface utilisateur, ainsi que des procédures détaillées pour les tâches courantes. Il donne également une définition de la terminologie et comprend des informations de dépannage.

Public

Ce document s'adresse aux administrateurs et opérateurs de centres de données qui utilisent PlateSpin Protect dans leur solution quotidienne de reprise après sinistre et de protection de workloads.

Documentation supplémentaire

Pour obtenir la version la plus récente de ce guide et d'autres ressources de documentation relatives à PlateSpin Protect, visitez le site Web de documentation de PlateSpin Protect (https://www.netiq.com/documentation/platespin-protect/).

La documentation en ligne est disponible en anglais ainsi que dans les langues nationales suivantes : allemand, chinois simplifié, chinois traditionnel, espagnol, français et japonais.

Coordonnées

Nous sommes à l'écoute de vos commentaires et suggestions concernant ce manuel et les autres documentations fournies avec ce produit. N'hésitez pas à utiliser le lien **comment on this topic** (Ajouter un commentaire sur cette rubrique) situé au bas de chaque page de la documentation en ligne, ou à envoyer un message électronique à l'adresse Documentation-Feedback@microfocus.com.

Pour tout problème spécifique au produit, contactez le service clients de Micro Focus à l'adresse https://www.microfocus.com/support-and-services/.

Planification

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).

- Chapitre 1, « Planification de votre environnement PlateSpin », page 13
- Chapitre 2, « Workflow de base pour la protection et la récupération de workload », page 37

1 Planification de votre environnement PlateSpin

Utilisez les informations fournies dans cette section pour préparer votre environnement PlateSpin de protection et de récupération.

1.1 Configurations prises en charge

PlateSpin Protect prend en charge la plupart des versions principales des systèmes d'exploitation Microsoft Windows, SUSE Linux Enterprise Server et Red Hat Enterprise Linux. Il prend également en charge certaines versions sélectionnées des systèmes d'exploitation Novell Open Enterprise Server, Oracle Enterprise Linux et CentOS.

Cette section décrit les configurations de plate-forme prises en charge par PlateSpin Protect, ainsi que les logiciels, le matériel et les environnements de virtualisation requis pour la protection et la récupération des workloads. Certaines configurations, comme spécifié, nécessitent un traitement spécial pour la configuration et la récupération des workloads. Assurez-vous de passer en revue les informations référencées dans le reste de la documentation en ligne ou des articles de la base de connaissances avant d'essayer de configurer le workload.

REMARQUE : bien que les configurations non mentionnées ici ne soient pas prises en charge, la plupart des améliorations que nous apportons à PlateSpin Protect le sont en réponse directe aux suggestions de nos clients. Vous pouvez nous aider à faire en sorte que notre produit réponde à tous vos besoins. Si vous êtes intéressé par une configuration de plate-forme non répertoriée, contactez le support technique. Nous accordons une grande importance à vos commentaires et sommes impatients de connaître vos impressions.

1.1.1 Workloads Windows pris en charge

PlateSpin Protect prend en charge les workloads des versions de système d'exploitation Microsoft Windows répertoriées dans le Tableau 1-1.

Les réplications par fichier et par bloc sont prises en charge, moyennant certaines restrictions. Reportez-vous à la Section 1.2, « Méthodes de transfert des données prises en charge », page 23.

REMARQUE : la protection n'est pas prise en charge pour les workloads de bureau (postes de travail).

Tableau 1-1 *Workloads Windows pris en charge*

Système d'exploitation	Remarques
Serveurs	
Windows Server 2016	La protection des serveurs Windows Server 2016 nécessite VMware 6.0 ou version ultérieure.
Windows Server 2012 R2 Windows Server 2012	Y compris les éditions DC (contrôleurs de domaine) et SBS (Small Business Server). Pour plus d'informations sur la conversion de contrôleurs de domaine Active Directory, reportez-vous à l'article n° 7920501 de la base de connaissances (https://www.netiq.com/support/kb/doc.php?id=7920501).
Windows Server 2008 R2 (64 bits) Windows Server 2008 (64 bits) Windows Server 2008 SP le plus récent (32 bits)	Y compris les éditions DC (contrôleurs de domaine) et SBS (Small Business Server). Pour plus d'informations sur la conversion de contrôleurs de domaine Active Directory, reportez-vous à l'article n° 7920501 de la base de connaissances (https://www.netiq.com/support/kb/doc.php?id=7920501).
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.

Système d'exploitation	Remarques
Grappes	
Cluster de basculement Microsoft basé sur serveur Windows Server 2016	La protection des clusters Windows Server 2016 nécessite VMware 6.0 ou version ultérieure. Modèles pris en charge : *Quorum de disques et noeuds majoritaire* et *Pas de majorité : Disque quorum uniquement*. Le système prend en charge le transfert de données par bloc avec un pilote (SAN Fibre Channel uniquement) ou sans pilote pour les réplications incrémentielles de clusters. La réplication basée sur des fichiers n'est pas prise en charge. **AVERTISSEMENT :** n'essayez pas d'utiliser le pilote par bloc sur des grappes avec des disques iSCSI partagés. Cela rend les grappes inutilisables. Reportez-vous à la section « Préparation de la protection des clusters Windows » page 121.
Cluster de basculement Microsoft basé sur serveur Windows Server 2012 R2	
Cluster de basculement Microsoft basé sur serveur Windows Server 2008 R2	
Serveur de clusters Windows basé sur Windows Server 2003 R2	Modèle pris en charge : *Cluster de serveurs à quorum unique*. La prise en charge inclut uniquement le transfert de données par bloc sans pilote pour les réplications incrémentielles des clusters. La réplication basée sur des fichiers n'est pas prise en charge. Reportez-vous à la section « Préparation de la protection des clusters Windows » page 121.
Hôtes Hyper-V	
Windows Server 2012 R2 avec rôle Hyper-V Windows Server 2012 avec rôle Hyper-V	Protège un serveur Windows qui fonctionne comme un hôte Hyper-V et ses volumes. Protège les machines virtuelles séparément.

Configuration requise pour Windows

Mises à jour Windows

Assurez-vous d'appliquer les mises à jour Windows sur votre système source avant d'exécuter la première réplication complète.

Contrôleur de domaine et logiciel antivirus

Si la machine Windows est un contrôleur de domaine, veillez aussi à désactiver le logiciel antivirus sur le système pendant la réplication.

1.1.2 Workloads Linux pris en charge

PlateSpin Protect prend en charge les workloads des distributions de système d'exploitation Linux répertoriées dans le Tableau 1-2.

La réplication des workloads Linux protégés s'effectue uniquement en mode bloc. Reportez-vous à la section « Configuration requise pour un pilote `blkwatch` » page 17.

Tableau 1-2 *Workloads Linux pris en charge*

Système d'exploitation	Versions	Remarques
Serveurs		
Red Hat Enterprise Linux (RHEL)	7.0 à 7.3 6.0 à 6.9 5.x 4.x	Reportez-vous à la section « Distributions Linux prises en charge par Protect » page 137 pour obtenir la liste des versions et architectures de kernel Linux prises en charge pour les distributions RHEL. PlateSpin Protect ne prend pas en charge le système de fichiers XFS version 5 (v5) sous RHEL 7.3 et les distributions basées sous RHEL 7.3. Pour les workloads Red Hat Enterprise Linux 6.7, Oracle Linux 6.7 et CentOS 6.7 avec des volumes LVM, une réplication incrémentielle est prise en charge uniquement pour la dernière version du kernel disponible (version `2.6.32-642.13.1.el6.x86_64`) pour la distribution RHEL 6.7. Il s'agit du même kernel que celui utilisé par la distribution RHEL 6.8.
SUSE Linux Enterprise Server (SLES)	11 SP1 vers 11 SP4 10.x 9.x	Reportez-vous à la section « Distributions Linux prises en charge par Protect » page 137 pour obtenir la liste des versions et architectures de kernel Linux prises en charge pour les distributions SLES. la version 3.0.13 du kernel de SLES 11 SP3 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.
Open Enterprise Server (OES)	2015 SP1 11 SP1 vers 11 SP3 2 SP3 Reportez-vous à la SUSE Linux Enterprise Server (SLES).	Pour OES 2015 SP1, PlateSpin Protect prend en charge les réserves NSS 32 bits d'une taille maximale de 8 To ; les réserves NSS 64 bits ne sont pas prises en charge. Reportez-vous à la section « Distributions Linux prises en charge par Protect » page 137 pour obtenir la liste des versions et architectures de kernel Linux prises en charge pour les distributions SLES. La version de kernel par défaut 3.0.13 sous 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.

Système d'exploitation	Versions	Remarques
Oracle Linux (OL) (anciennement Oracle Enterprise Linux [OEL])	Reportez-vous à la Red Hat Enterprise Linux (RHEL).	Reportez-vous à la section « Distributions Linux prises en charge par Protect » page 137 pour obtenir la liste des versions et architectures de kernel Linux prises en charge pour les distributions RHEL. Les pilotes Blkwatch sont disponibles pour les kernels standard RHCK (Red Hat Compatible Kernel) et UEK (Unbreakable Enterprise Kernel) sous OEL 6 U7 et versions ultérieures, comme indiqué dans la « Liste des distributions » page 138. Les workloads utilisant le kernel UEK ne sont pas pris en charge pour PlateSpin Protect 11.2 et versions antérieures. Pour Oracle Linux 6 U7, les pilotes blkwatch pour le kernel version 2.6.32-573 n'assurent pas la prise en charge de la réplication incrémentielle des workloads avec des volumes LVM. Mettez à jour le kernel, puis utilisez des pilotes RHEL 6 U7 pour le kernel 2.6.32-642.
CentOS	Reportez-vous à la Red Hat Enterprise Linux (RHEL).	Reportez-vous à la section « Distributions Linux prises en charge par Protect » page 137 pour obtenir la liste des versions et architectures de kernel Linux prises en charge pour les distributions RHEL. CentOS 7.*x* nécessite VMware 5.5 ou version ultérieure.

Configuration requise pour les workloads Linux

Configuration requise pour un pilote `blkwatch`

Le transfert de données par bloc pour un workload Linux dans `PlateSpin Protect` requiert un pilote blkwatch spécialement compilé pour la distribution Linux faisant l'objet de la protection. Le logiciel PlateSpin Protect intègre des versions précompilées du pilote `blkwatch` pour de nombreuses distributions Linux de non-débogage (32 et 64 bits). Vous pouvez aussi créer un pilote personnalisé. Pour plus d'informations, reportez-vous à la section « Distributions Linux prises en charge par Protect » page 137.

1.1.3 Conteneurs de VM pris en charge

Un conteneur de machines virtuelles (Virtual Machine, VM) est une infrastructure de protection opérant en tant qu'hôte d'une réplique démarrable et régulièrement mise à jour d'un workload protégé.

- « Plates-formes VMware prises en charge » page 18
- « Prise en charge des grappes VMware DRS en tant que conteneurs » page 19
- « Prise en charge de VMware vCenter Site Recovery Manager » page 19
- « Prise en charge de la mutualisation de la protection sous VMware » page 19

Plates-formes VMware prises en charge

Reportez-vous au Tableau 1-3 pour la liste des plates-formes VMware prises en charge. Les plates-formes sont prises en charge en tant que conteneurs de protection et de rétablissement.

REMARQUE : la protection des workloads sur un conteneur de VM cible est soumise à la prise en charge du système d'exploitation invité sur l'hôte cible par le fournisseur de l'hôte. Pour plus d'informations sur les hôtes VMware cibles, reportez-vous au manuel *VMware Compatibility Guide* (http://www.vmware.com/resources/compatibility/) (Guide de compatibilité de VMware).

L'infrastructure de conteneur peut être un serveur VMware ESXi ou une grappe VMware DRS. Pour plus d'informations sur la configuration requise pour la grappe VMware DRS, reportez-vous à la section « Prise en charge des grappes VMware DRS en tant que conteneurs » page 19.

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

Conteneur	Versions	Remarques
VMware vCenter ou ESXi	NetWare 6.5	En tant que conteneur VM, la grappe DRS doit être constituée uniquement de serveurs ESXi 6.5 et peut uniquement être gérée par vCenter 6.5.
VMware vCenter ou ESXi	6.0 (GA2, U2, U3)	En tant que conteneur VM, la grappe DRS doit être constituée uniquement de serveurs ESXi 6.0 et peut uniquement être gérée par vCenter 6.0.
VMware vCenter ou ESXi	5.5 (GA2, U2, U3)	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.
VMware vCenter ou ESXi	5.1 (GA2, U2, U3)	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.
VMware vCenter ou ESXi	4.1 (GA2, U3)	En tant que conteneur VM, la grappe DRS doit être constituée uniquement de serveurs ESXi 4.1 et peut uniquement être gérée par vCenter 4.1.

REMARQUE : vos hôtes VMware ESXi doivent disposer d'une licence payante ; la protection n'est pas prise en charge sur ces systèmes s'ils fonctionnent avec une licence gratuite.

Prise en charge des grappes VMware DRS en tant que conteneurs

Pour être une cible de protection valide, votre grappe VMware DRS doit être ajoutée 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 96.

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

- L'option DRS doit être activée et définie sur **Partiellement automatisé** ou **Entièrement automatisé**. (Elle ne peut pas être configurée sur **Manuel**.)
- Les hôtes VMware de la grappe VMware doivent partager 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 hôtes VMware de la grappe VMware.
- Les workloads de basculement (VM) pour chaque contrat de protection doivent être placés exclusivement sur les banques de données, les vSwitch et les groupes de ports virtuels partagés par tous les hôtes VMware de la grappe VMware.

Prise en charge de VMware vCenter Site Recovery Manager

PlateSpin Protect prend en charge la copie de machines virtuelles répliquées vers un site de récupération à distance à l'aide de VMware vCenter Site Recovery Manager (SRM). Reportez-vous à la Section 6.7, « Configuration de la prise en charge de VMware vCenter Site Recovery Manager », page 76.

Prise en charge de la mutualisation de la protection sous VMware

PlateSpin Protect prend en charge la mutualisation sous VMware. Plusieurs serveurs Protect peuvent partager l'interface dorsale de grappe VMWare. Reportez-vous à la section « Configuration de la mutualisation de la protection sous VMware » page 57.

1.1.4 Architectures de workload prises en charge

PlateSpin Protect prend en charge les architectures informatiques x86 suivantes :

Architecture de système d'exploitation et processeur

PlateSpin Protect prend en charge la protection et la récupération des architectures x64 et x86 pour les workloads physiques et virtuels dans votre centre de données :

- 64 bits
- 32 bits

Noyaux et sockets pour les machines virtuelles cibles

Pour les conteneurs de machines virtuelles pris en charge qui utilisent VMware 5.1 et versions ultérieures, avec un matériel de machine virtuelle de niveau 8 minimum, PlateSpin Protect vous permet de spécifier le nombre de sockets, ainsi que le nombre de noyaux par socket pour le workload de basculement. Elle calcule automatiquement le nombre total de coeurs. Ce paramètre s'applique à la configuration initiale d'un workload avec une réplication initiale définie sur **Complète**.

REMARQUE : le nombre maximal de coeurs que le workload peut utiliser est soumis à des facteurs externes tels que le système d'exploitation invité, la version du matériel de machine virtuelle, la licence VMware pour l'hôte ESXi et les ressources informatiques maximales de l'hôte ESXi pour vSphere. Reportez-vous au document *ESX/ESXi Configuration Maximums* (https://kb.vmware.com/kb/1003497) (Limites de configuration d'EXS/ESXi) (Base de connaissances VMware 1003497).

Certaines distributions d'un système d'exploitation invité risquent de ne pas respecter la configuration des noyaux et des noyaux par socket. Par exemple, les systèmes d'exploitation invités SLES 10 SP4 et OES 2 SP3 conservent leurs paramètres de noyaux et de sockets d'origine, tels qu'installés, tandis que d'autres distributions SLES, RHEL et OES respectent la configuration.

Processeurs virtuels pour les machines virtuelles cibles

Pour les conteneurs de machines virtuelles utilisant VMware 4.1, PlateSpin Protect vous permet de spécifier le nombre requis de vCPU (processeurs virtuels) à assigner au workload de basculement. Ce paramètre s'applique à la configuration initiale d'un workload avec une réplication initiale définie sur **Complète**. Chaque vCPU est présentée au système d'exploitation invité sur le conteneur de machine virtuelle en tant que coeur unique, socket unique.

Microprogramme UEFI et BIOS

PlateSpin Protect prend en charge les interfaces de microprogramme UEFI et BIOS pour les workloads Windows et Linux.

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 envisager un conteneur vSphere 5.0 ou plus récent.

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

- Lorsque vous transférez un workload UEFI vers un conteneur VMware vSphere 4.*x* (qui ne prend pas en charge UEFI), 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, 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 signale que cette opération n'est pas valide. Autrement dit, la transition du microprogramme de BIOS vers UEFI n'est pas prise en charge, car Windows 2003 n'est pas compatible avec le mode de démarrage UEFI.
- Lorsque vous protégez une source UEFI sur une cible BIOS, PlateSpin 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.

Sur les workloads Windows, PlateSpin Protect met en miroir la prise en charge Microsoft des workloads Windows basés sur UEFI ou BIOS. Il transfère des workloads de la source vers la cible afin d'appliquer le microprogramme pris en charge pour les systèmes d'exploitation source et cible respectifs. Les transferts basés sur des fichiers et par bloc sont pris en charge. 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.

1.1.5 Stockage pris en charge

PlateSpin Protect prend en charge les configurations de stockage suivantes pour les workloads Windows et Linux.

Disques de stockage

PlateSpin Protect prend en charge plusieurs types de disques de stockage sources, notamment des disques de base, des disques dynamiques Windows, LVM2, RAID et SAN.

Vous pouvez spécifier si les disques virtuels sur la réplique de VM protégée ont fait l'objet d'un provisionnement léger ou lourd.

REMARQUE : les avertissements suivants s'appliquent pour les disques de stockage :

- **Disques dynamiques Windows :** PlateSpin Protect ne prend pas en charge les disques dynamiques Windows sur la cible.

  Pour les disques dynamiques, le stockage ne respecte pas la stratégie d'assignation Identique à la source. Tant les volumes dynamiques simples que les volumes dynamiques fractionnés résident sur le workload cible en tant que disques de volumes de base simples. Le disque cible est partitionné en tant que GPT si la taille totale combinée des disques membres du volume dynamique dépasse la limite de taille de partition MBR. Pour plus d'informations, reportez-vous au document *Microsoft TechNet: Understanding the 2 TB limit in Windows Storage* (https://blogs.technet.microsoft.com/askcore/2010/02/18/understanding-the-2-tb-limit-in-windows-storage/) (Microsoft TechNet : présentation de la limite de 2 To du stockage Windows).
- **RAID logiciel Linux :** PlateSpin Protect ne prend pas en charge les workloads Linux dont des volumes sont sur le RAID logiciel.

Modèles de partitionnement

PlateSpin Protect prend en charge les modèles de partitionnement MBR (Master Boot Record) et GPT (GUID Partition Table) pour les workloads Windows et Linux. Les workloads et le stockage pour la protection doivent être configurés sur des disques partitionnés avec le modèle MBR ou GPT. Bien que GPT permette jusqu'à 128 partitions par disque simple, PlateSpin Protect ne prend en charge que 57 partitions GPT ou moins par disque.

Systèmes de fichiers Windows

PlateSpin Protect ne prend en charge le système de fichiers NTFS que sur les systèmes Windows compatibles.

Systèmes de fichiers Linux

PlateSpin Protect prend en charge les systèmes de fichiers EXT2, EXT3, EXT4, REISERFS, XFS et NSS (Open Enterprise Server seulement) avec le transfert par bloc uniquement.

REMARQUE : le système de fichiers XFS v5 n'est pas pris en charge pour Red Hat Enterprise Linux 7.3 et les distributions basées sur cette version.

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

Fonctionnalités de stockage de Linux

Pour les workloads Linux, PlateSpin Protect fournit le support de stockage supplémentaire suivant :

- 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.
- Les volumes de disques bruts LVM sont pris en charge dans les configurations Identique à la source sur les workloads Linux.
- (OES 11) Les dispositions NLVM (Novell Linux Volume Management) des workloads sources sont conservées et recréées dans le conteneur de VM. Les réserves NSS sont copiées de la source vers la VM de récupération.
- (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.

1.1.6 Langues internationales prises en charge

Outre l'anglais, PlateSpin Protect fournit une prise en charge dans la langue nationale (National Language Support, NLS) pour l'installation et l'utilisation sur des machines configurées pour les langues internationales suivantes :

- Chinois simplifié (zh-cn)
- Chinois traditionnel (zn-tw)
- Français (fr)
- Allemand (de)
- Japonais (ja)

SUGGESTION : d'autres versions internationales bénéficient d'une prise en charge limitée ; la mise à jour des fichiers système peut être affectée dans les langues autres que celles répertoriées ci-dessus.

La documentation en ligne localisée est disponible dans ces langues, ainsi qu'en espagnol.

Pour utiliser l'interface Web dans l'une de ces langues, reportez-vous à la section « Configuration des paramètres de langue pour les versions internationales » page 65.

1.1.7 Navigateurs pris en charge

La plupart de vos interactions avec le produit s'effectuent via l'interface Web basée 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.

Pour utiliser l'interface Web de PlateSpin Protect dans une des langues internationales prises en charge, reportez-vous à la section « Configuration des paramètres de langue pour les versions internationales » page 65.

1.2 Méthodes de transfert des données prises en charge

La méthode de transfert des données correspond à la façon dont ces dernières 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.

1.2.1 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 au niveau du fichier.

- **Réplication au niveau du fichier Windows :** (Windows uniquement) les données sont répliquées fichier par 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 des données au niveau du bloc. Elle tire parti du service VSS (Volume Snapshot Service) de Microsoft et des 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. La réplication compare chaque bloc sur le disque et copie uniquement les modifications.

  Aucun redémarrage n'est nécessaire, mais les performances sont inférieures à celles obtenues avec le composant basé sur les blocs.

1.2.2 Méthode de transfert prises en charge pour les workloads Linux

Pour les workloads Linux, PlateSpin Protect prend en charge uniquement le transfert de données par bloc avec un pilote de surveillance des blocs (`blkwatch`).

REMARQUE : le déploiement ou la suppression du pilote `blkwatch` est transparent, n'a pas d'impact sur la continuité et ne nécessite aucune intervention ni redémarrage.

La distribution PlateSpin Protect inclut des pilotes `blkwatch` précompilés pour les workloads exécutant les kernels standard de non-débogage de distributions Linux prises en charge. Reportez-vous à la Section B.2, « Pilotes blkwatch précompilés pour les distributions Linux », page 138.

Si vos workloads ont un kernel non standard, personnalisé ou plus récent, vous pouvez générer un pilote `blkwatch` personnalisé pour votre kernel spécifique. Reportez-vous à l'article 7005873 de la base de connaissances *How to Build a Custom Block-Based Linux Kernel Driver (Procédure pour générer un pilote de kernel Linux personnalisé par bloc* (https://www.netiq.com/support/kb/doc.php?id=7005873).

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 Chiffrement des données lors d'une transmission

Le chiffrement du transfert sécurise la transmission de vos données de workload lors de la réplication du workload. Si le chiffrement est activé, le transfert de données sur le réseau depuis la source vers la cible est chiffré à l'aide de la norme AES (Advanced Encryption Standard).

REMARQUE : le chiffrement des données a un impact sur les performances et peut réduire la vitesse de transfert des données jusqu'à 30 %.

Vous pouvez activer ou désactiver le codage individuellement pour chaque workload en sélectionnant l'option **Coder le transfert des données**. Reportez-vous à la section « Détails de protection de workload » page 153.

1.3.2 Sécurité des communications client/serveur

Le serveur PlateSpin active le protocole SSL sur l'hôte du serveur PlateSpin, ce qui assure une transmission sécurisée des données entre votre navigateur Web et le serveur PlateSpin via 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

PlateSpin Protect protège les références en utilisant une connexion SSL pour les communications et la bibliothèque de chiffrement Windows pour chiffrer les mots de passe.

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 « Configuration de l'autorisation et de l'authentification utilisateur » page 53.

1.3.5 Authentification Windows pour la base de données Microsoft SQL Server

PlateSpin Protect offre la possibilité d'utiliser l'authentification Windows pour accéder à la base de données Microsoft SQL Server. Reportez-vous à la section « Exigences pour l'authentification Windows auprès de la base de données Microsoft SQL Server » page 34.

1.3.6 Pare-feu et paramètres de port

Le Tableau 1-4 répertorie les ports par défaut utilisés par PlateSpin Protect. Si vous configurez des ports personnalisés, vous devez plutôt ouvrir ces derniers. Pour les communications entre le serveur PlateSpin et les machines sources et cibles qu'il gère, veillez également à ouvrir les ports appropriés sur les pare-feu situés entre eux. Le trafic pour les communications est bidirectionnel (entrant et sortant). Reportez-vous également à la section « Conditions d'accès et de communication requises sur votre réseau de protection » page 31.

Tableau 1-4 *Ports par défaut utilisés par PlateSpin Protect*

Numéro de port	Protocole	Fonction	Détails
80	TCP	HTTP	(Non sécurisé) Utilisé pour les communications HTTP entre l'hôte du serveur PlateSpin et les machines sources et cibles qu'il gère. Ouvrez ce port sur votre hôte du serveur PlateSpin, les workloads source et cible, et les hôtes VMware ESXi.
443	TCP	HTTPS	(Sécurisé) Utilisé pour les communications HTTPS, si SSL est activé, entre l'hôte du serveur PlateSpin et les machines source et cible. Ouvrez ce port sur votre hôte du serveur PlateSpin, les workloads sources et cibles, les hôtes VMware ESXi et le serveur hôte vCenter.
3725	TCP	Transfert de données	Utilisé pour le transfert de données entre les machines source et cible, dont le transfert de fichiers et le transfert par bloc. Ouvrez ce port sur les machines sources et cibles pour tous les workloads. Tout pare-feu entre une source et sa cible doit également autoriser le port TCP 3725. Reportez-vous à la section « Configurations prises en charge » page 13.
135 445	TCP	RPC/DCOM	Utilisé pour les communications RPC/DCOM sur les machines Windows pendant le processus de découverte, ainsi que lors de la prise de contrôle et du redémarrage de la machine source. Ouvrez ces ports pour les communications entre les machines sources et cibles pour tous les workloads Windows. Reportez-vous à la section « Workloads Windows pris en charge » page 14.
137 138 139	TCP	NetBIOS	Utilisé pour les communications NetBIOS (service de noms, service de datagrammes et service de sessions). Ouvrez ces ports pour les communications entre les machines sources et cibles pour tous les workloads Windows. Reportez-vous à la section « Workloads Windows pris en charge » page 14.

Numéro de port	Protocole	Fonction	Détails
137 138	UDP	SMB	Utilisé pour les communications SMB pour le transfert de fichiers du dossier et des fichiers Prise de contrôle, du serveur PlateSpin vers la machine source. Ouvrez ces ports sur l'hôte de votre serveur PlateSpin et sur les workloads sources.
139 445	TCP	SMB	
22	TCP		Utilisé pour les communications SSH et SCP sur les machines Linux pendant le processus de découverte. Ouvrez ce port sur les machines sources et cibles pour tous les workloads Linux. Reportez-vous à la section « Workloads Linux pris en charge » page 15.
25	TCP	SMTP	Utilisé pour le trafic SMTP si la notification par message électronique est activée. Ouvrez ce port sur l'hôte du serveur PlateSpin et l'hôte de relais de messagerie.
25	UDP	SMTP	
1433	TCP	SQL	Utilisé pour les communications Microsoft SQL Server pour l'authentification et l'échange de données avec un serveur SQL distant. Ouvrez les ports SQL sur l'hôte de votre serveur PlateSpin et sur l'hôte du serveur SQL distant, ainsi que sur les pare-feu situés entre eux. Pour plus d'informations sur les exigences du port du serveur SQL, reportez-vous à l'article *Configure the Firewall to Allow Server Access* (Configurer le pare-feu pour permettre l'accès au serveur) sur Microsoft Developers Network.
1434	TCP	SQL	Utilisé pour la connexion administrateur dédiée à Microsoft SQL Server.
1434	UDP	SQL	Utilisé pour les instances nommées Microsoft SQL Server. Ce port peut être requis lorsque vous utilisez des instances nommées sur un serveur SQL distant.
de 49152 à 65535	TCP	SQL	Utilisé pour Microsoft SQL Server ou RPC pour LSA, SAM et Netlogon. Si vous avez configuré Microsoft SQL Server de manière à utiliser un port TCP personnalisé, vous devez ouvrir ce dernier sur le pare-feu. Reportez-vous à la section « Exigences pour l'authentification Windows auprès de la base de données Microsoft SQL Server » page 34.

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 Spécifications RPO, RTO et TTO

Dans votre environnement de protection, vous avez des attentes différentes pour les points et temps de reprise requis pour divers workloads.

- **Perte de données maximale admissible (PDMA ou RPO – Recovery Point Objective) :** le paramètre RPO décrit la quantité tolérable de perte de données, mesurée en temps dans le cas d'une panne ou interruption informatique majeure. Vous définissez le RPO avec un intervalle configurable entre les réplications incrémentielles d'un workload protégé.

  La perte de données maximale admissible 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) :** le paramètre RTO décrit le temps hors service tolérable d'un workload et correspond au temps nécessaire à l'exécution d'une opération de basculement. L'opération de basculement met en ligne un workload de basculement pour remplacer temporairement un workload de production protégé.

  Le RTO est influencé par le temps nécessaire à la configuration et à l'exécution de l'opération de basculement (de 10 à 45 minutes). Reportez-vous à la section « Basculement » page 157.

- **Délai maximal de test admissible (DMTA ou TTO – Test Time Objective) :** le TTO décrit le temps nécessaire au test de la reprise après sinistre avec un certain niveau de confiance pour la restauration du service. Il est similaire au DMIA mais inclut le temps nécessaire à l'utilisateur pour tester le workload de basculement.

  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 158.

Parmi les facteurs influant sur le RPO, le RTO et le TTO 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.

Lorsque vous testez la réponse du basculement, notez les valeurs réelles associées aux RPO, RTO et TTO configurés :

- **Point de récupération réel (Recovery Point Actual, RPA) :** la valeur RPA est la perte de données réelle mesurée en temps et définie par l'intervalle mesuré réel entre les réplications incrémentielles d'un workload protégé qui se produit au cours d'un test de basculement. Le RPA est également appelé *RPO réel* (Actual Recovery Point Objective).
- **Délai de récupération réel (Recovery Time Actual, RTA) :** la valeur RTA est une mesure du temps hors service réel d'un workload, défini par la durée d'une opération de basculement. Le RTA est également appelé *RTO réel* (Actual Recovery Time Objective).
- **Délai de test réel (Test Time Actual, TTA) :** la valeur TTA est une mesure de la durée réelle du test d'un plan de reprise après sinistre. Cette mesure est similaire à la DMIA réelle, mais inclut le temps nécessaire à l'utilisateur pour tester le workload de basculement. Le TTA est également appelé *TTO réel* (Actual Test Time Objective).

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 178.

1.4.3 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 166.

1.4.4 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 166.

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.

1.4.6 Serveur de base de données

PlateSpin Protect inclut l'édition Microsoft SQL Server Express. Les fonctionnalités de SQL Server Express sont suffisantes pour un serveur PlateSpin unique qui protège jusqu'à 50 workloads (voir Section 1.4.5, « Évolutivité », page 30).

REMARQUE : Microsoft SQL Server Express a une limite de taille de base de données de 10 Go et ne peut utiliser qu'un seul noyau de processeur à la fois. Pour plus d'informations sur la configuration requise pour SQL Server Express et ses restrictions, consultez la documentation de Microsoft SQL Server Express 2014 (https://www.microsoft.com/en-us/download/details.aspx?id=42299).

L'instance de base de données du serveur PlateSpin peut croître jusqu'à 0,5 Go par mois et par workload, en fonction du nombre de réplications incrémentielles planifiées. Il est recommandé d'archiver ou de supprimer régulièrement les données de création de rapports historiques afin de libérer de l'espace pour les nouvelles données de création de rapports.

Dans une grappe VMware DRS, veillez à équilibrer les cibles de protection sur plusieurs hôtes de la grappe pour optimiser les performances.

Nous vous recommandons de configurer le serveur PlateSpin pour qu'il utilise une instance de base de données sur votre serveur de base de données existant utilisant l'édition standard ou entreprise de Microsoft SQL Server dans les environnements suivants :

- Déploiement de plusieurs serveurs PlateSpin qui utilisent le même serveur de base de données Microsoft SQL Server distant pour leurs instances de base de données
- Déploiements pour lesquels la conservation de tout l'historique des données de rapports est important

Bien que plusieurs serveurs PlateSpin puissent utiliser le même serveur de base de données distant, chaque serveur nécessite une instance de base de données séparée.

Afin de configurer une instance de base de données distante pour votre serveur PlateSpin, reportez-vous à la section « Configuration de votre serveur de base de données Microsoft SQL Server distant » du *Guide d'installation et de mise à niveau de PlateSpin Protect*.

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

Avant de définir la protection et la récupération des workloads, veillez à configurer votre réseau selon les conditions d'accès et de communication requises décrites dans cette section.

1.5.1 Configuration réseau pour l'interface Web de l'hôte du serveur PlateSpin

Le Tableau 1-5 décrit les ports qui doivent être ouverts sur l'hôte du serveur PlateSpin pour permettre l'accès à l'interface Web.

Tableau 1-5 *Exigences d'ouverture de ports pour l'hôte du serveur PlateSpin*

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

1.5.2 Configuration réseau requise pour les conteneurs

Le Tableau 1-6 liste les configurations logicielles, réseau et pare-feu requises pour les conteneurs de workloads pris en charge.

Tableau 1-6 *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).	
Tous les conteneurs VMware. Reportez-vous à la section « Conteneurs de VM pris en charge » page 17.	◆ 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)

1.5.3 Configuration réseau requise pour les workloads

Le Tableau 1-7 liste les configurations logicielles, réseau et pare-feu requises pour les workloads que vous souhaitez protéger à l'aide de PlateSpin Protect.

Tableau 1-7 *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. Reportez-vous à la section « Workloads Windows pris en charge » page 14.	◆ Microsoft .NET Framework 3.5 Service Pack 1 ◆ Microsoft .NET Framework 4.0 Pour la découverte, les workloads sources doivent exécuter Microsoft .NET Framework 2 SP2 ou version ultérieure.	
Tous les workloads de cluster Windows Server. Reportez-vous à Grappes dans la section « Workloads Windows pris en charge » page 14.	Assurez-vous que le serveur PlateSpin peut résoudre les recherches DNS directes et inversées pour les adresses IP du cluster Windows Server et de ses noeuds. Vous pouvez mettre à jour le serveur DNS ou mettre à jour le fichier `hosts` local (`%systemRoot%\system32\drivers\etc\hosts`) sur l'hôte du serveur PlateSpin.	

Type de workload	Conditions préalables	Ports requis (valeurs par défaut)
Tous les workloads Windows. Reportez-vous à la section « Workloads Windows pris en charge » page 14.	◆ Références de compte `Administrateur` ou d'administrateur de domaine (l'appartenance au groupe Administrateurs local uniquement est insuffisante). ◆ 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 (TCP 137 - 139) SMB (TCP 139, 445 et UDP 137, 138) RPC (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 : *The Netsh Command Line Utility* (http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx) (Utilitaire de ligne de commande Netsh).	TCP 3725, 135, 139, 445 UDP 137, 138, 139

Type de workload	Conditions préalables	Ports requis (valeurs par défaut)
Tous les workloads Linux. Reportez-vous à la section « Workloads Linux pris en charge » page 15.	Serveur Secure Shell (SSH)	TCP 22, 3725

1.5.4 Exigences pour l'authentification Windows auprès de la base de données Microsoft SQL Server

PlateSpin Protect offre la possibilité d'utiliser l'authentification Windows pour accéder à la base de données Microsoft SQL Server. Vous devez configurer les paramètres Active Directory et ouvrir des ports sur le pare-feu pour autoriser l'authentification.

Pour activer l'authentification Windows auprès de la base de données SQL :

1. Veillez à configurer Microsoft SQL Server pour qu'il autorise les connexions TCP/IP et de canal nommé.
2. (Conditionnel) Si vous prévoyez d'utiliser l'authentification Windows pour accéder à la base de données Microsoft SQL Server, vous devez configurer les éléments suivants dans Active Directory :
   - Vous devez ajouter le serveur de base de données Microsoft SQL Server au domaine.
   - Vous devez avoir deux comptes d'utilisateur de domaine pour l'installation de PlateSpin Protect.
     - **Un utilisateur de domaine pour lequel le rôle `sysadmin` est défini :** cet utilisateur doté de droits d'administrateur SQL est nécessaire pour créer des bases de données, des tables et d'autres objets de schéma.
     - **Un utilisateur du service PlateSpin :** l'utilisateur du service peut être un utilisateur du domaine bénéficiant de faibles privilèges. Cependant, il doit être un administrateur local sur le serveur PlateSpin Protect et cette autorisation doit lui être accordée avant l'installation.

       Si le mot de passe de l'utilisateur Windows change, vous devez le mettre à jour pour l'utilisateur du service PlateSpin et pour le pool d'applications IIS. Pensez à employer un utilisateur Windows dont le mot de passe n'expire jamais afin d'éviter ce genre de situation.

   REMARQUE : si vous utilisez l'authentification Windows, vous devez vous connecter en tant qu'utilisateur du domaine disposant de droits d'administrateur SQL lorsque vous effectuez une mise à niveau ou à jour de votre serveur PlateSpin.
3. Ouvrez les ports suivants sur le pare-feu pour prendre en charge l'authentification sur SQL Server :
   - **Ports 49152-65535/TCP :** autorise le trafic RPC pour LSA, SAM, Netlogon.
   - **Port 1433/TCP :** autorise le trafic pour Microsoft SQL Server.
   - **Ports personnalisés :** si vous configurez SQL Server pour utiliser un port TCP personnalisé, vous devez ouvrir ce port sur le pare-feu.

REMARQUE : si vous n'utilisez pas de ports dynamiques, vous devez spécifier le port dédié dans le champ **Serveur de base de données**.

4 (Conditionnel) Si vous voulez utiliser des ports dédiés avec PlateSpin Protect, vous devez ouvrir ces ports sur le pare-feu :

4a Sur le serveur de base de données, déterminez les ports qui doivent être ouverts :

4a1 Dans le Gestionnaire de configuration SQL Server, sélectionnez **Protocoles pour SQLExpress > TCP/IP**, puis cliquez avec le bouton droit et sélectionnez **Propriétés**.

4a2 Dans la boîte de dialogue, sélectionnez l'onglet **Adresses IP**.

4a3 Sous **IPAll** (ou sous le protocole de votre choix), si **Port TCP** ou **Ports dynamiques TCP** est défini sur une valeur autre que 0, ouvrez les ports du pare-feu spécifiés. Il s'agit des ports utilisés pour la connexion à SQL Server.

Par exemple, si le champ **Ports TCP dynamiques** est défini sur 60664 et que **Port TCP** est défini sur 1555, vous devez activer les ports 60664 et 1555 dans les règles de pare-feu sur le serveur SQL.

4b Ouvrez les ports sur le pare-feu.

REMARQUE : si une valeur est définie pour les ports dynamiques, il se peut que votre serveur ne figure pas dans la liste des serveurs SQL lorsque vous cliquez sur **Parcourir**. Dans ce cas, vous devez spécifier le serveur manuellement dans le champ de saisie **Serveur de base de données** de l'installation de PlateSpin Protect.

Par exemple, si le nom de votre serveur est `MYSQLSERVER`, le nom de l'instance de base de données `SQLEXPRESS` et le port dédié défini pour le port dynamique `60664`, entrez le texte suivant et sélectionnez ensuite le type d'authentification de votre choix :

```
MYSQLSERVER\SQLEXPRESS,60664
```

Vous devez ouvrir les ports sur le pare-feu.

1.5.5 Exigences pour la 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 :** à l'aide de l'outil de configuration de PlateSpin de votre serveur, enregistrez les adresses IP supplémentaires assignées à l'hôte du serveur PlateSpin. Reportez-vous à la section « Configuration requise pour le fonctionnement du serveur PlateSpin via NAT » page 36.
- **Conteneur cible :** lorsque vous essayez de découvrir un conteneur (tel que VMware ESX), spécifiez l'adresse IP publique (externe) de cet hôte dans les paramètres de découverte.
- **Solution :** 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 161) ».

- **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 PlateSpin, soit l'une de ses adresses publiques (externes) enregistrées dans la base de données de configuration de PlateSpin du serveur. Reportez-vous à la « Configuration requise pour le fonctionnement du serveur PlateSpin via NAT » page 36.

1.5.6 Configuration requise pour le fonctionnement du serveur PlateSpin via NAT

Le serveur PlateSpin a besoin d'adresses IP supplémentaires pour fonctionner dans des environnements pour lesquels la fonctionnalité de traduction d'adresses réseau (NAT) est activée. Reportez-vous à la « Configuration requise pour le fonctionnement du serveur PlateSpin via NAT » page 36.

1.5.7 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 *Linux Default Shell Override Procedure* (https://www.netiq.com/support/kb/doc.php?id=7010676) (Procédure de remplacement du shell par défaut de Linux) .

2 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. La plupart de ces étapes sont représentées par des commandes de workload sur la page Workloads. Reportez-vous à la section « Commandes de protection et de récupération de workload » page 45.

Tableau 2-1 *Cycle de protection et de récupération*

Tâche	Opération	Remarques
Préparation Assurez-vous que vos workloads, vos conteneurs et votre environnement répondent aux critères requis.		
	1. Vérifiez que PlateSpin Protect prend en charge votre workload.	Reportez-vous à la section « Configurations prises en charge » page 13.
	2. Assurez-vous que vos workloads et conteneurs de machines virtuelles 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 31.
Inventaire 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.		
	3. Ajoutez des conteneurs cibles au serveur PlateSpin.	Reportez-vous à la section « Ajout de conteneurs (cibles de protection) » page 96.
	4. Ajoutez des workloads sources au serveur PlateSpin.	Reportez-vous à la section « Ajout de workloads (sources de protection) » page 100.
	5. Pour une cible de protection physique, préparez des pilotes de périphérique.	Reportez-vous au Chapitre 11, « Préparation des pilotes de périphérique pour les cibles de rétablissement physiques », page 105.
	6. Pour un workload Linux, préparez la protection de workload :	Reportez-vous au Chapitre 12, « Préparation des workloads Linux pour la protection », page 117.
	7. Pour les workloads de cluster Windows Server, préparez la protection de workload de grappe.	Reportez-vous au Chapitre 13, « Préparation de la protection des clusters Windows », page 121.

Tâche	Opération	Remarques
Définition du contrat de protection		
	8. Définissez les détails et spécifications d'un contrat de protection.	Reportez-vous à la section « Configuration des détails de protection et préparation de la réplication » page 151.
	9. Préparez la réplication.	
Lancement de la protection		
	10. Commencez le contrat de protection en fonction de vos besoins.	Reportez-vous à la section « Démarrage de la protection du workload » page 156.
Tâches du cycle protection (facultatives) 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.		
	11. *Réplication incrémentielle manuelle*. Vous pouvez exécuter une réplication incrémentielle manuellement, en dehors du contrat de protection de workload.	Sélectionnez le workload, puis cliquez sur **Exécuter la migration incrémentielle**.
	12. *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.
Basculement		
	13. 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 157.
Rétablissement		
	14. 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 159.
Reprotection		
	15. 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 164. La commande **Reprotéger** devient disponible après une opération de rétablissement réussie.

Gestion du serveur PlateSpin

Cette section fournit les informations dont vous avez besoin pour activer votre licence PlateSpin Protect et pour personnaliser le produit PlateSpin en fonction de votre environnement. Familiarisez-vous avec les outils de PlateSpin et les options de configuration. Vous pouvez revenir à cette section à chaque fois que vous avez besoin de gérer les licences ou les utilisateurs, de personnaliser les paramètres.

3 Utilisation des outils PlateSpin

La plupart de vos interactions avec le produit s'effectuent via l'interface Web basée sur un navigateur. Vous pouvez également configurer les paramètres globaux de l'application PlateSpin Server à l'aide de la page de configuration de PlateSpin basée sur le Web.

3.1 Lancement de l'interface Web

1. (Facultatif) Configurez le serveur PlateSpin et votre navigateur Web pour utiliser l'une des langues internationales prises en charge au lieu de l'anglais. Reportez-vous à la « Configuration des paramètres de langue pour les versions internationales » page 65.
2. Ouvrez un navigateur Web pris en charge et rendez-vous sur le site :

   `https://votre_serveur_PlateSpin/Protect`

   Remplacez *`votre_serveur_PlateSpin`* par le nom d'hôte DNS ou l'adresse IP de l'hôte du serveur PlateSpin.

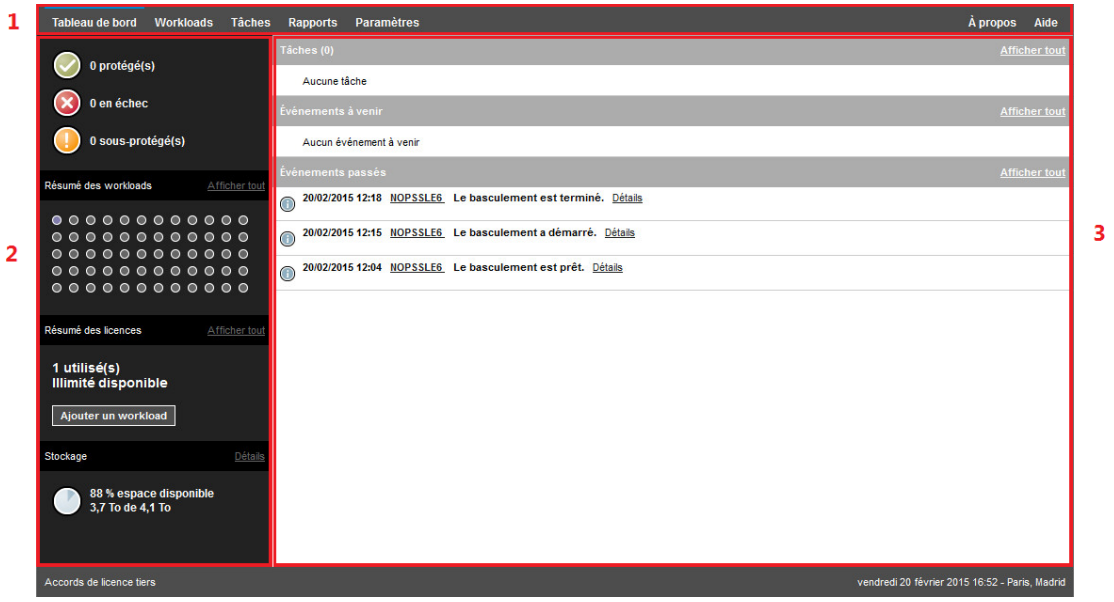
   Si SSL n'est pas activé, utilisez le protocole `http` dans l'URL.
3. Connectez-vous à l'aide des références de l'utilisateur administrateur local pour l'hôte du serveur PlateSpin.

   Pour plus d'informations sur la configuration des utilisateurs supplémentaires de PlateSpin, reportez-vous au Chapitre 5, « Configuration de l'autorisation et de l'authentification utilisateur », page 53.

3.2 Présentation du tableau de bord

La page Tableau de bord de l'interface Web de PlateSpin Protect 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 43
- Section 3.2.2, « Panneau de résumé visuel », page 43
- Section 3.2.3, « Panneau Tâches et événements », page 44

REMARQUE : vous pouvez modifier certains éléments de l'interface Web afin de les faire correspondre à la stratégie de marque de votre entreprise. Pour plus d'informations, reportez-vous à la section « Application de votre marque à l'interface Web de PlateSpin Protect » page 87.

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 « Présentation des workloads » page 45.
- **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 178.
- **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 166.
  - **Balises de workload :** reportez-vous à la section « Création et gestion des balises de workload » page 79.
  - **Autorisations :** reportez-vous à la section « Configuration de l'autorisation et de l'authentification utilisateur » page 53.
  - **Conteneurs :** reportez-vous à la section « Ajout de conteneurs (cibles de protection) » page 96.
  - **Paramètres de notification :** reportez-vous à la section « Activation des notifications d'événement » page 68.
  - **Paramètres des rapports de réplication :** reportez-vous à la section « Activation de rapports de réplication » page 69
  - **SMTP :** reportez-vous à la section « Configuration de SMTP pour le service de notification par message électronique » page 67.
  - **Licences :** reportez-vous à la section « Activation de la licence de votre produit » page 49.

3.2.2 Panneau de résumé visuel

Le panneau de résumé visuel fournit un état de protection de haut niveau des workloads inventoriés, l'état de chaque workload sous licence, un résumé de l'utilisation des licences et la capacité de stockage disponible.

État de protection

L'état de protection global des workloads inventoriés est représenté par 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.

Résumé des workloads

Le résumé des workloads présente l'état de santé de chaque workload sous licence répertorié dans la page Workloads. Le nombre maximum d'icônes en forme de point indiquant l'état des workloads correspond au nombre de licences de workload installées sur le serveur PlateSpin. Pour une licence illimitée, le résumé affiche 96 icônes en forme de point. Le Tableau 3-1 décrit les différents états des workloads représentés par les icônes en forme de point.

Ces icônes représentent les workloads par ordre alphabétique, selon leur nom. 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.

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

Protégé	Non protégé
Ayant échoué	Non protégé - Erreur
Sous-protégé	Expiré
	Inutilisé

Résumé des licences

Le résumé des licences affiche le nombre de licences installées, ainsi que le nombre de licences en cours d'utilisation par les workloads.

Stockage

Stockage fournit des informations sur la quantité totale d'espace de stockage du conteneur disponible pour PlateSpin Protect ainsi que sur la quantité d'espace actuellement utilisée.

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 services de notification par message électronique pour les événements et les rapports de réplication » page 67.

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

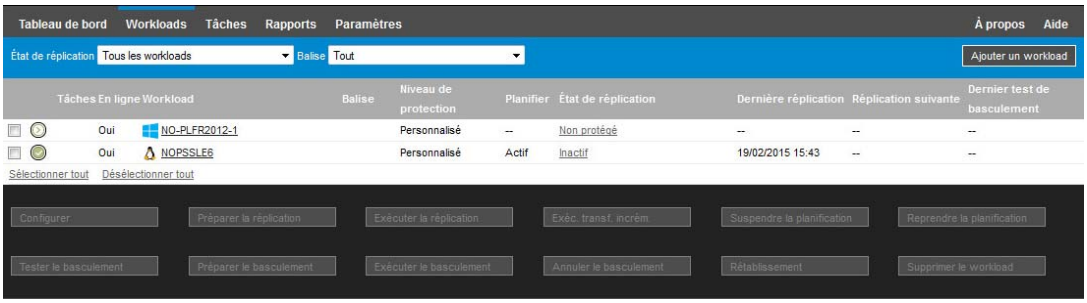
`Marquer le test comme échoué`. Un clic sur une de ces tâches entraîne l'annulation de l'opération Tester le basculement et l'enregistrement d'un événement dans l'historique. Autre exemple, l'événement `FullReplicationFailed`, qui est illustré en liaison avec une tâche `StartFull`. Vous trouverez la 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 Présentation des workloads

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. La liste Workloads affiche des informations sur la disponibilité de chaque workload (en ligne ou hors ligne), sa balise, son niveau de protection, son état de réplication et les temps d'exécution, ainsi que l'heure du dernier test de basculement.

Figure 3-2 *Page Workloads*

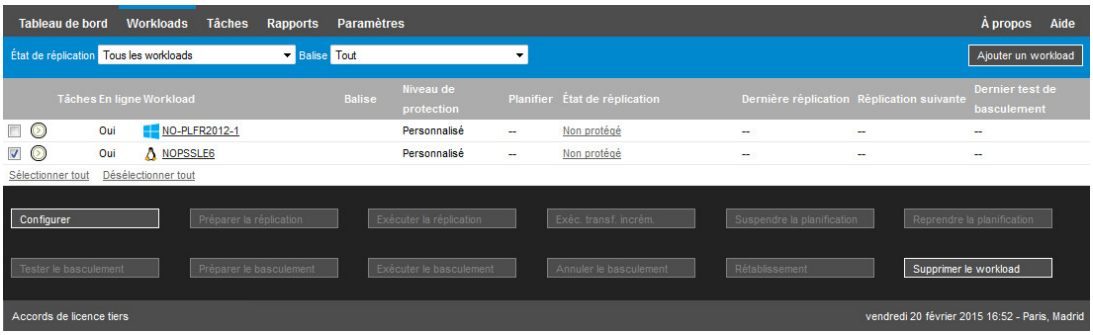


REMARQUE : tous les tampons horaire reflètent le fuseau horaire de l'hôte du serveur PlateSpin, lequel peut être différent du fuseau horaire du workload protégé ou de celui de l'hôte sur lequel vous exécutez l'interface Web . La date et l'heure du serveur s'affichent en bas en droite de la fenêtre du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

3.4 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 3-2 présente un résumé des commandes de workload, accompagné de 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).
Reprotéger	Après une opération de rétablissement réussie, l'option Reprotéger devient disponible.
Supprimer le workload	Supprime un workload de l'inventaire.

3.5 Autres outils de gestion du serveur PlateSpin

3.5.1 Configuration de PlateSpin

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 à l'adresse :

`https://Votre_serveur_PlateSpin/platespinconfiguration/`

REMARQUE : dans des circonstances normales, vous n'avez pas besoin de modifier ces paramètres, sauf si le support PlateSpin vous le recommande.

Pour modifier et appliquer des paramètres de configuration :

1. À partir de n'importe quel navigateur Web, ouvrez

   `https://Votre_serveur_PlateSpin/platespinconfiguration/`
2. Recherchez le paramètre de serveur requis et modifiez sa valeur.
3. Enregistrez vos paramètres et quittez la page.

   Un redémarrage des services PlateSpin n'est pas nécessaire pour appliquer les modifications.

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

- « Configuration requise pour le fonctionnement du serveur PlateSpin via NAT » page 36
- « Optimisation du transfert de données sur les connexions WAN » page 71
- « Optimisation des performances de l'environnement de réplication » page 74
- « Définition de la méthode de redémarrage pour le service de configuration » page 75
- « Configuration de la prise en charge de VMware vCenter Site Recovery Manager » page 76
- « Application de votre marque à l'interface Web grâce aux paramètres de configuration » page 87
- « Configuration de la découverte des noeuds actifs Windows » page 127
- « Dépannage du service de configuration » page 180

3.5.2 Utilitaire Protect Agent

L'utilitaire Protect Agent (ProtectAgent.cli.exe) est un utilitaire de ligne de commande que vous pouvez utiliser pour installer, mettre à niveau, interroger ou désinstaller les pilotes de transfert par bloc. Bien qu'un redémarrage soit toujours requis lors de l'installation, de la désinstallation ou de la mise à niveau des pilotes, cet utilitaire vous permet de mieux contrôler le moment où se produit l'opération et, par conséquent, le moment du redémarrage du serveur. Vous pouvez, par exemple, employer l'utilitaire Protect Agent pour installer les pilotes pendant le temps hors service planifié, au lieu de le faire lors de la première réplication. Reportez-vous à l'Annexe D, « Utilitaire Protect Agent », page 143.

3.5.3 Outil de rôles VMware

L'outil de rôles VMware (PlateSpin.VMwareRoleTool.exe) est un utilitaire de ligne de commande que vous pouvez utiliser pour créer des rôles utilisateur uniques dans un centre de données VMware afin de soutenir la mutualisation. Les rôles permettent d'autoriser des utilisateurs VMware non-administrateurs (« utilisateurs habilités ») à effectuer des opérations de cycle de vie Protect dans l'environnement VMware. Reportez-vous à la Section 5.4, « Configuration de la mutualisation de la protection sous VMware », page 57.

4 Gestion des licences

Après avoir activé une licence pour le produit, vous pouvez surveiller la disponibilité des licences de workload, ajouter de nouvelles licences et supprimer les licences expirées.

4.1 Activation de la licence de votre produit

Votre licence pour le produit PlateSpin Protect vous donne droit à un nombre spécifique ou illimité de workloads que vous pouvez protéger par des licences de workload.

Pour activer la licence du produit PlateSpin Protect, vous devez disposer d'un code d'activation. Si ce n'est pas le cas, demandez-en un via le Novell Customer Center (http://www.netiq.com/customercenter/). Un représentant du service clients vous recontactera et vous indiquera le code d'activation de la licence.

REMARQUE : si vous existez déjà en tant que client PlateSpin mais ne disposez pas encore de compte Novell Customer Center, commencez par en créer un à l'aide de l'adresse électronique spécifiée sur votre bon de commande. Pour plus d'informations, reportez-vous à la section Création d'un compte (https://www.netiq.com/selfreg/jsp/createAccount.jsp).

Vous pouvez activer votre produit en ligne ou hors ligne.

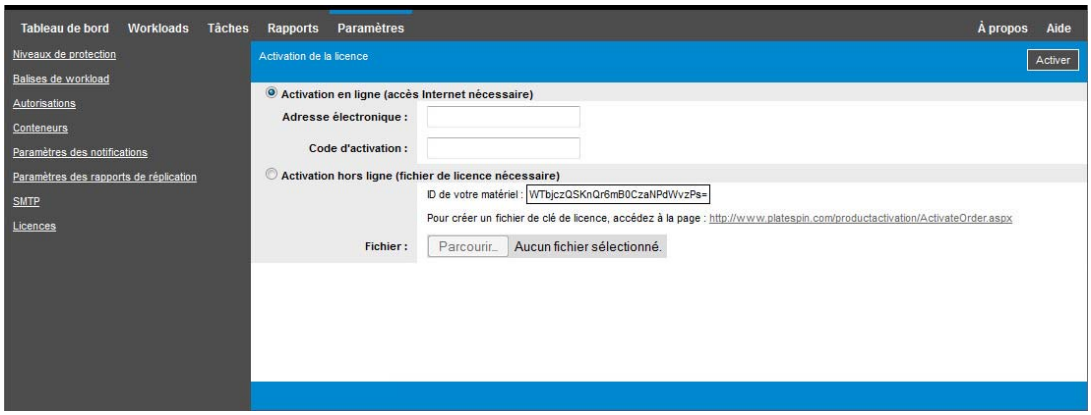
4.1.1 Activation en ligne de la licence

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.

Pour configurer l'activation de licence en ligne :

1 Dans l'interface Web, sélectionnez **Paramètres > Licences**, puis cliquez sur **Ajouter une licence**.



2 Sélectionnez **Activation en ligne**.

3 Indiquez l'adresse électronique spécifiée lorsque vous avez passé votre commande, ainsi que le code d'activation reçu, puis cliquez sur **Activer**.

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

4.1.2 Activation hors ligne de la licence

Pour une activation hors ligne, vous devez obtenir une clé de licence PlateSpin Protect à l'aide d'un ordinateur connecté à Internet.

1 Dans l'interface Web, sélectionnez **Paramètres > Licences**, puis cliquez sur **Ajouter une licence**.

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). Connectez-vous en utilisant votre nom d'utilisateur et votre mot de passe Customer Center.

4 Utilisez l'ID matériel pour créer un fichier de clé de licence. Ce processus requiert les informations suivantes :

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

5 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.

6 Sur la page Activation de la licence de l'interface Web de , entrez le chemin d'accès au fichier ou accédez à son emplacement, puis cliquez sur **Activer**.

   Le fichier de clé de licence est enregistré et le produit est activé sur la base de ce fichier.

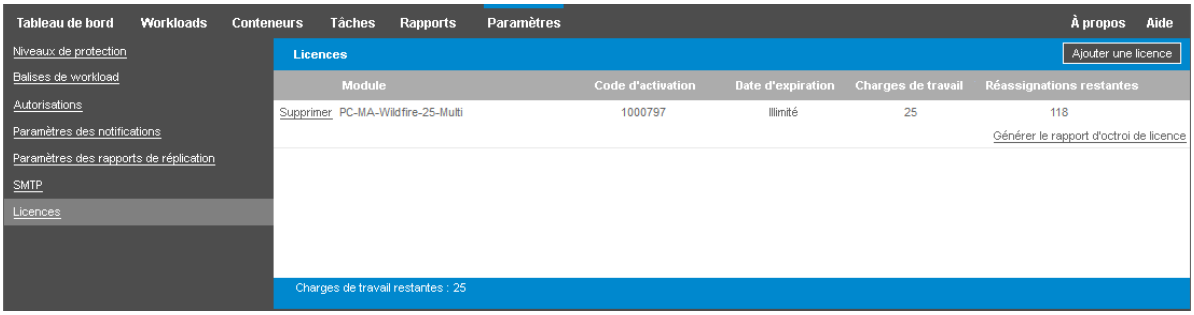
4.2 À propos de la consommation des licences de workload

Votre licence pour le produit PlateSpin Protect vous donne droit à un nombre spécifique ou illimité 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.

Dans la page Tableau de bord de l'interface Web de PlateSpin Protect, le résumé des licences affiche le nombre actuel de licences installées et consommées.

La page Licences (**Paramètres** > **Licences**) répertorie chaque licence installée avec son nombre actuel de licences de workload consommées et nombre de réassignations restantes disponibles pour ces licences. La page affiche également le nombre total de licences de workload inutilisées restant pour le serveur PlateSpin.

Figure 4-1 *Nombre de licences et de réassignations restantes*



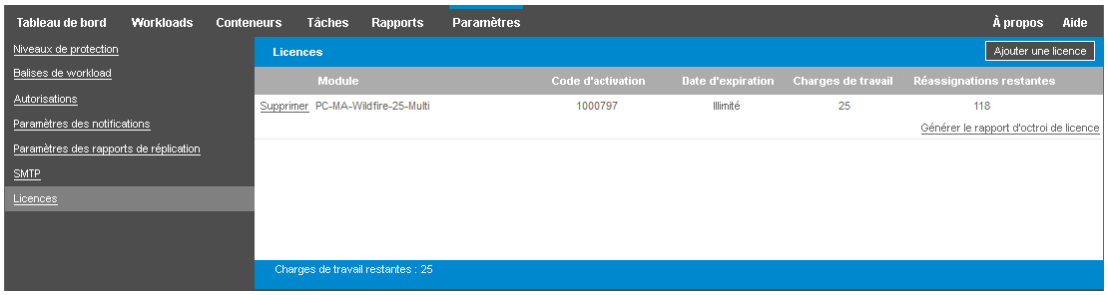
4.3 Affichage des informations de licence

Le Tableau de bord du produit fournit un résumé des licences qui affiche le nombre total de licences installées et le nombre actuel de licences consommées.

Vous pouvez consulter des informations sur les licences de workload installées sur un serveur PlateSpin dans la page Licences. Pour chaque licence, vous pouvez afficher le nombre actuel de licences de workload utilisées et le nombre actuel de réassignations restantes disponibles pour les licences utilisées.

Pour afficher les informations de licence :

1. Dans l'interface Web, sélectionnez **Paramètres > Licences**.



2. Affichez les informations de licence :
   - Code d'activation
   - Date d'expiration
   - Workloads
   - Réassignations restantes
3. Affichez les **Charges de travail restantes** pour le nombre de licences inutilisées disponibles.

4.4 Ajout d'une licence

Pour ajouter une licence, vous utilisez le même processus pour l'activation de la première licence. Pour plus d'informations, reportez-vous aux suivantes :

- Section 4.1.1, « Activation en ligne de la licence », page 49
- Section 4.1.2, « Activation hors ligne de la licence », page 50

4.5 Suppression d'une licence

Vous pouvez supprimer une licence expirée de la page Licences.

1. Dans l'interface Web, sélectionnez **Paramètres > Licences**.
2. Affichez les informations de licence.
3. Cliquez sur **Supprimer** en regard de la licence expirée, puis confirmez la suppression.

4.6 Génération d'un rapport sur les licences pour le support technique

Si vous avez des problèmes de licences, il se peut que le support technique vous demande de générer un rapport sur les licences. Ce rapport de diagnostic contient des informations de produit chiffrées sur les licences que vous avez activées pour votre serveur PlateSpin.

1. Dans l'interface Web, sélectionnez **Paramètres > Licences**.
2. Sous la liste des licences, cliquez sur **Afficher le rapport d'octroi de licence**.

   Le fichier `LicenseReport.txt` s'ouvre dans une nouvelle fenêtre ou un nouvel onglet de navigateur, selon les paramètres de votre navigateur.
3. Enregistrez le fichier `LicenseReport.txt` sous `LicenseReport.psl` sur votre ordinateur local.

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

Cette section comprend les informations suivantes :

5.1 À propos de l'accès basé sur le rôle 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 5-1 *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
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.

Pour configurer un accès basé sur les rôles à PlateSpin Protect :

1. Ajoutez des utilisateurs aux groupes d'utilisateurs appropriés repris dans le Tableau 5-1. Reportez-vous à la documentation relative à votre produit Windows.
2. Créez des 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 56.

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

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

- Section 5.2.1, « Ajout d'utilisateurs PlateSpin Protect », page 55
- Section 5.2.2, « Assignation d'un rôle de protection de workload à un utilisateur PlateSpin Protect », page 55

5.2.1 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 55.

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**.
3. 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 55.

5.2.2 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 5-1, « Détails des rôles de protection de workload et des autorisations », page 54.

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. Sous l'onglet **Membre de**, cliquez sur **Ajouter**.
4. Recherchez le groupe Protection des workloads souhaité et assignez-le à l'utilisateur.

Plusieurs minutes peuvent être nécessaires pour que le changement soit pris en compte. Pour tenter d'appliquer les modifications manuellement, redémarrez votre serveur en utilisant l'exécutable `RestartPlateSpinServer.exe`.

Pour redémarrer le serveur PlateSpin :

1. Avant de tenter de redémarrer le serveur PlateSpin, suspendez l'ensemble de vos contrats ou vérifiez qu'aucune réplication, aucun basculement ni aucun rétablissement n'est en cours. Ne continuez pas tant que toutes les charges ne sont pas inactives.
2. Sur l'hôte du serveur PlateSpin, accédez au sous-répertoire `..\bin\RestartPlateSpinServer`.
3. Double-cliquez sur l'exécutable `RestartPlateSpinServer.exe`.

   Une fenêtre d'invite de commande s'ouvre et vous demande confirmation.
4. 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 56.

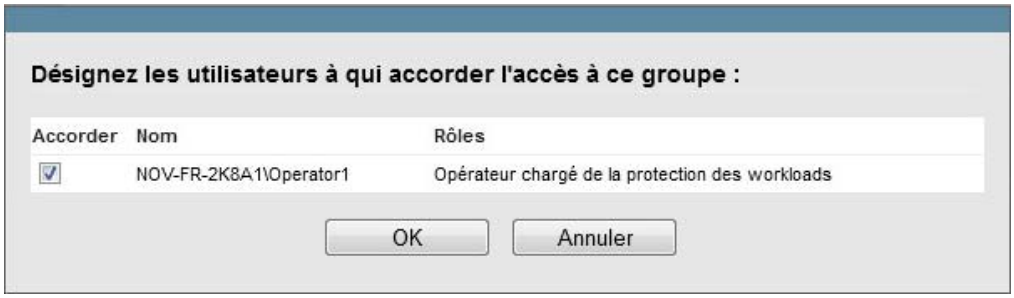
5.3 Gestion des groupes de sécurité et des autorisations de workload de PlateSpin Protect

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*.

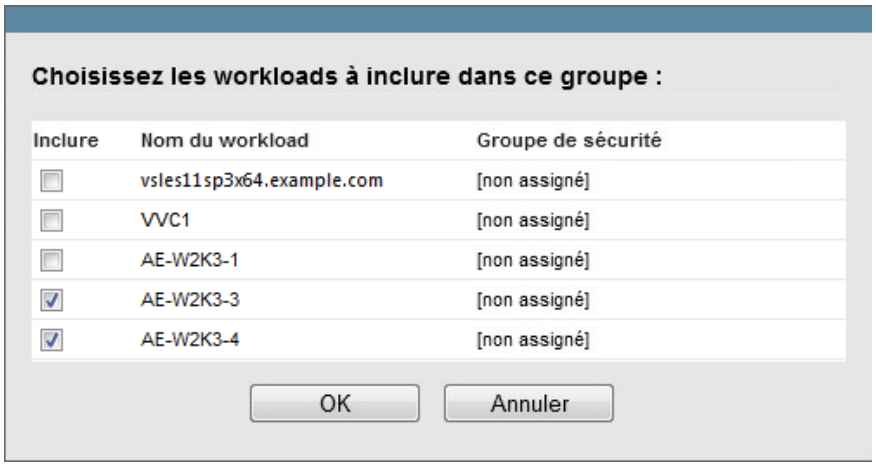
1. Assignez à un utilisateur PlateSpin Protect un rôle de protection de workload dont les autorisations sont les plus adaptées à ce rôle dans votre organisation. Reportez-vous à la section « Assignation d'un rôle de protection de workload à un utilisateur PlateSpin Protect » page 55.
2. Accédez à PlateSpin 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 Protect récemment ajouté à l'hôte du serveur PlateSpin, 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.

5.4 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 centre de données 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 centre de données 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 centre de données.

Cette section présente les informations suivantes :

- Section 5.4.1, « Définition de rôles VMware pour la mutualisation », page 57
- Section 5.4.2, « Assignation de rôles dans vCenter », page 61

5.4.1 Définition de rôles VMware pour la mutualisation

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

par défaut, le fichier de définition de rôle (`PlateSpinRole.xml`) et l'outil de définition de rôle (`PlateSpin.VMwareRoleTool.exe`) sont situés dans le dossier `VMwareRolesTool` :

`<répertoire_installation>\PlateSpin Protect Server\bin\VMwareRolesTool`

Cette section présente les informations suivantes :

- « Syntaxe de ligne de commande de base » page 58
- « Drapeaux et paramètres de ligne de commande supplémentaires » page 58
- « Exemple d'utilisation de l'outil » page 58
- « (Option) Définition manuelle de rôles PlateSpin dans vCenter » page 59
- « Utilisation de vCenter pour afficher les privilèges pour les rôles personnalisés PlateSpin » page 59

Syntaxe de ligne de commande de base

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

```
PlateSpin.VMware.Role.Tool.exe /host=[host name or IP address of vCenter or ESX host] /user=[user name] /role=[PlateSpinRole.xml] /create
```

Où `PlateSpinRole.xml` est le nom de fichier de la définition de rôle.

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.VMware.Role.Tool.exe` pour créer ou mettre à jour des rôles dans vCenter :

Paramètres

`/create`	(Obligatoire) Crée les rôles définis par le paramètre `/role`.
`/get_all_prvileges`	Affiche tous les privilèges définis par le serveur.
`/get_compatible_roles`	Affiche tous les rôles compatibles à celui défini par `/role`.
`/check_role=[`*`nom_rôle`*`]`	Vérifie la compatibilité du rôle donné avec le rôle défini par `/role`.

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. Pour plus d'informations sur l'utilisation de l'outil en mode interactif, reportez-vous au document *VMware Role Tool to Verify Permissions to Roles* (Outil de rôles VMware pour la vérification des autorisations de rôles (article de la Base de connaissances n° 7018547) (https://www.netiq.com/support/kb/doc.php?id=7018547).
`/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.VMware.Role.Tool.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

Le client vCenter vous permet de créer et d'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.

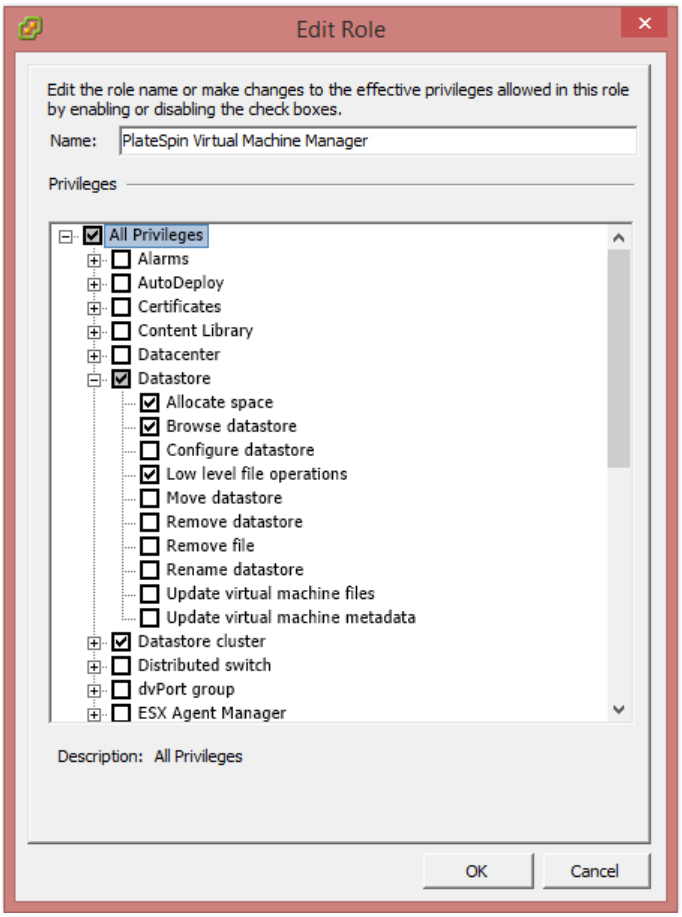
Utilisation de vCenter pour afficher les privilèges pour les rôles personnalisés PlateSpin

Le client vCenter permet de visualiser les privilèges minimaux définis pour les rôles personnalisés PlateSpin.

1 Dans vCenter, sélectionnez un rôle personnalisé :
   - Gestionnaire de machines virtuelles PlateSpin
   - Gestionnaire d'infrastructure PlateSpin
   - Utilisateur PlateSpin

2 Cliquez sur **Éditer** pour afficher les paramètres de privilèges dans la boîte de dialogue Modifier le rôle.

Par exemple, la figure suivante montre certains des privilèges définis pour le rôle PlateSpin Virtual Machine Manager.



5.4.2 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 de centre de données 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 centre de données 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.

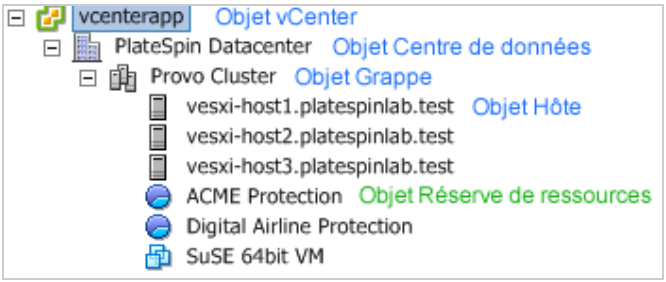
Conteneur vCenter pour l'assignation de rôles	Particularités de l'assignation de rôles	Instructions de propagation	Pour plus d'informations
Chaque réseau auquel l'utilisateur habilité doit accéder. Réseaux virtuels distribués avec dvSwitch et dvPortgroup.	Assignez le rôle *Gestionnaire de machines virtuelles 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 centre de données (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. Les objets VCenter, Centre de données, Grappe et Hôte étiquetés en bleu sont assignés au rôle Gestionnaire d'infrastructure. Les objets Réserve de ressources étiquetés en vert sont assignés au rôle Gestionnaire de machines virtuelles. 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.

---

6 Configuration de l'application PlateSpin Server

Cette section décrit la configuration requise et l'installation pour PlateSpin Protect.

6.1 Configuration des paramètres de langue pour les versions internationales

Outre l'anglais, PlateSpin Protect fournit une prise en charge dans la langue nationale (National Language Support, NLS) pour les langues internationales suivantes :

- Chinois simplifié
- Chinois traditionnel
- Français
- Allemand
- Japonais

Pour gérer votre serveur PlateSpin dans une de ces langues prises en charge, configurez le code de langue du système d'exploitation sur l'hôte du serveur PlateSpin et dans votre navigateur Web.

6.1.1 Définition de la langue sur le système d'exploitation

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

Pour changer la langue du système d'exploitation :

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.

6.1.2 Définition de la langue dans votre navigateur Web

Pour utiliser l'interface Web de PlateSpin Protect dans l'une de ces langues, vous devez ajouter la langue correspondante 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 :
   - **Chrome :**
     1. Dans le menu Chrome, cliquez sur **Paramètres**, faites défiler la page vers le bas, puis cliquez sur **Afficher les paramètres avancés**.
     2. Faites défiler jusqu'à **Langues**, puis cliquez sur **Paramètres de langue et de saisie**.
   - **Firefox :**
     1. Dans le menu **Outils**, sélectionnez **Options**, puis cliquez sur l'onglet **Contenu**.
     2. Sous **Langues**, cliquez sur **Choisir**.
   - **Internet Explorer :**
     1. Dans le menu **Outils**, sélectionnez **Options Internet**, puis cliquez sur l'onglet **Général**.
     2. Sous **Apparence**, cliquez sur **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 » page 41.

REMARQUE : (pour les utilisateurs des langues en chinois traditionnel et en chinois simplifié) les tentatives de connexion au serveur PlateSpin avec un navigateur n'intégrant pas une version spécifique du chinois 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]`.

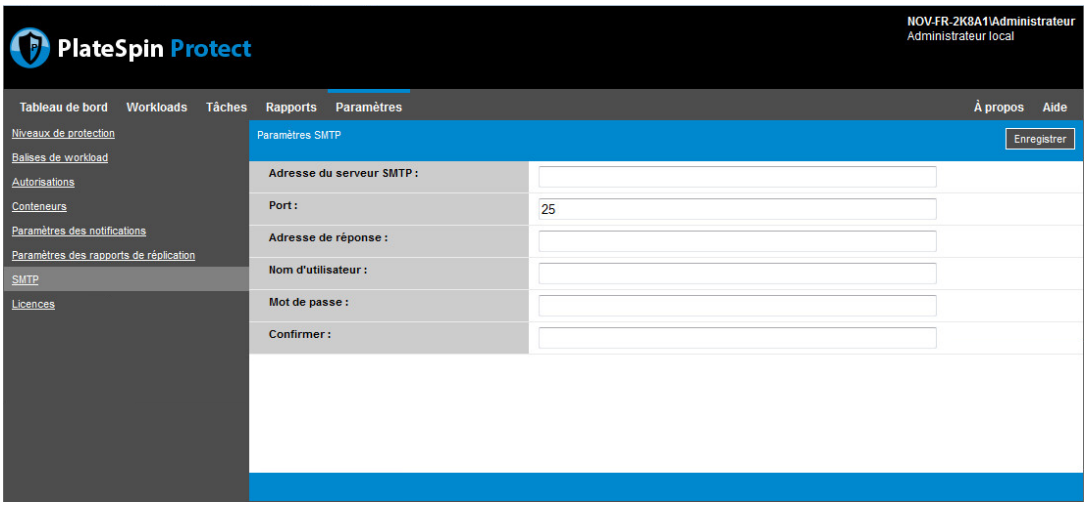
6.2 Configuration des services de notification par message électronique pour les événements et les rapports de réplication

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

6.2.1 Configuration de SMTP pour le service de notification par message électronique

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 6-1 *Paramètres SMTP (Simple Mail Transfer Protocol)*



Pour configurer les paramètres SMTP :

1. Dans votre interface Web PlateSpin Protect, cliquez sur **Paramètres > SMTP**.
2. Spécifiez les paramètres du serveur SMTP pour recevoir des notifications de progression et d'événement par message électronique :
   - **Adresse**
   - **Port** (la valeur par défaut est 25)
   - **Adresse de réponse**
3. Saisissez un nom d'utilisateur et un mot de passe, puis confirmez le mot de passe.
4. Cliquez sur **Enregistrer**.

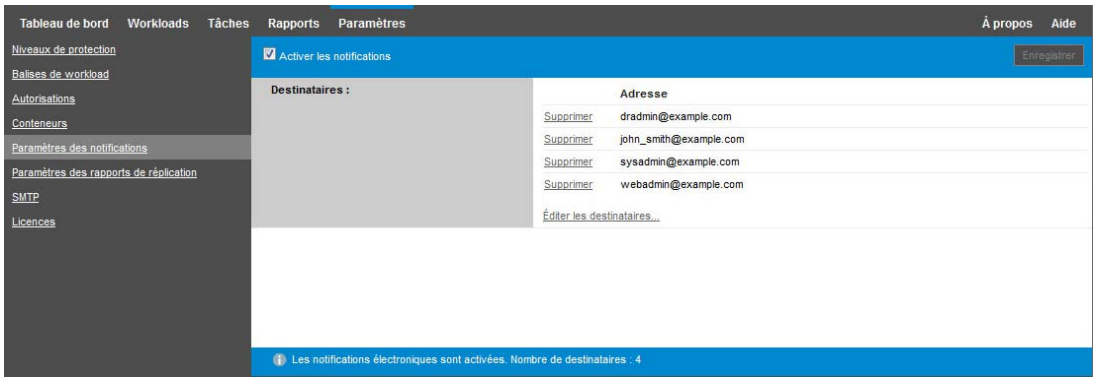
6.2.2 Activation des notifications d'événement

Les événements sont toujours ajoutés au journal des événements de l'application système, selon les types d'entrée de journal Avertissement, Erreur et Information. Vous pouvez également activer les notifications de manière à envoyer automatiquement des notifications d'événement aux destinataires appropriés.

1. Configurez le serveur SMTP que PlateSpin Protect doit utiliser.

   Reportez-vous à la section « Configuration de SMTP pour le service de notification par message électronique » page 67.

2. Dans votre interface Web PlateSpin Protect, cliquez sur **Paramètres > 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 les adresses électroniques répertoriées, cliquez sur **Supprimer** en regard de l'adresse.

Les types d'événements affichés dans le Tableau 6-1 peuvent déclencher des notifications par message électronique si ces notifications sont activées.

REMARQUE : même si les entrées de journal des événements ont des identifiants uniques, ces derniers sont susceptibles de changer dans de futures versions.

Tableau 6-1 *Types d'événements organisés par types d'entrée de journal*

Types d'événement	Remarques
Type d'entrée de journal : Avertissement	
`FullReplicationMissed`	Similaire à l'événement `Réplication incrémentielle manquée`.

Types d'événement	Remarques
`IncrementalReplicationMissed`	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.
`WorkloadOfflineDetected`	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**.
Type d'entrée de journal : Erreur	
`FailoverFailed`	
`FullReplicationFailed`	
`IncrementalReplicationFailed`	
`PrepareFailoverFailed`	
Type d'entrée de journal : Information	
`FailoverCompleted`	
`FullReplicationCompleted`	
`IncrementalReplicationCompleted`	
`PrepareFailoverCompleted`	
`TestFailoverCompleted`	Généré lors du marquage manuel d'une opération de test de basculement comme réussie ou échouée.
`WorkloadOnlineDetected`	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**.

6.2.3 Activation de rapports de réplication

Vous pouvez activer les rapports de réplication pour envoyer automatiquement des rapports aux destinataires appropriés.

1. Configurez le serveur SMTP que PlateSpin Protect doit utiliser.

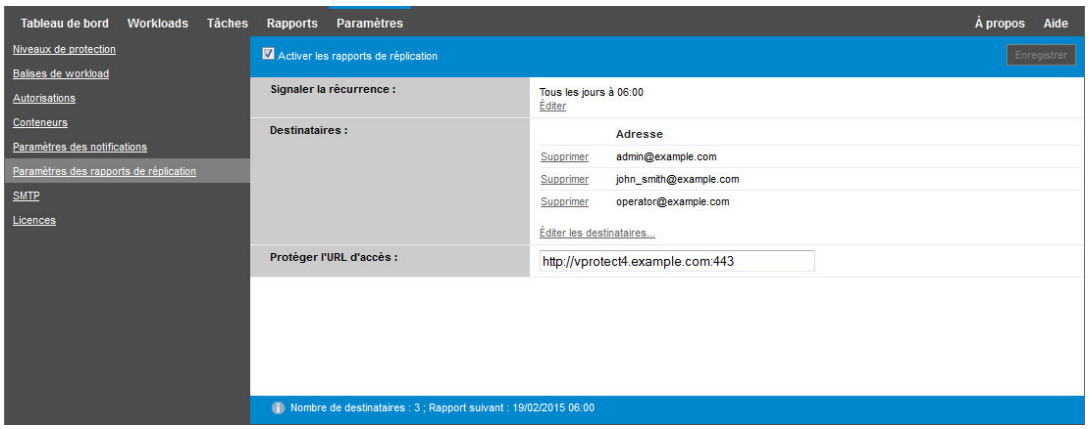
   Reportez-vous à la section « Configuration de SMTP pour le service de notification par message électronique » page 67.

2. Dans l'interface Web de PlateSpin Protect, cliquez sur **Paramètres > Paramètres des rapports de réplication**.

3 Sélectionnez l'option **Activer les rapports de réplication**.

4 Dans la section **Signaler la récurrence**, cliquez sur **Éditer**, puis spécifiez le schéma de récurrence approprié pour les rapports. Vous pouvez cliquer sur **Fermer** pour réduire la section.

5 Dans la section **Destinataires**, cliquez sur **Éditer les destinataires**, entrez les adresses électroniques appropriées en les séparant par des virgules, puis cliquez sur **OK**. Vous pouvez cliquer sur **Supprimer** en regard d'une adresse électronique pour supprimer ce destinataire de la liste.



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 178.

6.3 Configuration d'adresses IP de remplacement pour le serveur PlateSpin

Vous pouvez ajouter des adresses IP de remplacement pour le paramètre `AlternateServerAddresses` de la configuration de PlateSpin afin de permettre au serveur PlateSpin de fonctionner au sein d'environnements NAT.

Pour ajouter des adresses IP de remplacement pour le serveur PlateSpin :

1 À partir de n'importe quel navigateur Web, ouvrez la page suivante :

`https://Votre_serveur_PlateSpin/platespinconfiguration/`

2 Recherchez le paramètre `AlternateServerAddresses` et ajoutez des adresses IP pour le serveur PlateSpin.

3 Enregistrez vos paramètres et quittez la page.

Un redémarrage des services PlateSpin n'est pas nécessaire pour appliquer les modifications.

6.4 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 plus d'informations, reportez-vous au Section 3.5.1, « Configuration de PlateSpin », page 47.

6.4.1 Réglage des paramètres

Les paramètres de configuration du transfert de fichier permettent d'optimiser les transferts de données via un réseau étendu (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 6-2 répertorie les paramètres de la page de configuration de PlateSpin (`https://votre_serveur_PlateSpin/platespinconfiguration/`) qui contrôlent les vitesses des transferts de fichiers avec les valeurs par défaut et les valeurs maximales. Vous pouvez modifier ces valeurs en procédant par essais-erreurs afin d'optimiser le fonctionnement dans un environnement WAN à latence élevée.

Tableau 6-2 *Paramètres de configuration du transfert de fichier par défaut et optimisés*

Paramètre	Valeur par défaut	Valeur maximale
`AlwaysUseNonVSSFileTransferForWindows2003`	Faux	
`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
`FileTransferBufferThresholdPercentage` Détermine la quantité de données minimale devant être mise en tampon avant la création et l'envoi de nouveaux paquets réseau.	10	
`FileTransferKeepAliveTimeOutMilliSec` Indique le délai d'attente avant de commencer à envoyer des messages de maintien de connexion en cas de timeout du TCP.	120000	

Paramètre	Valeur par défaut	Valeur maximale
`FileTransferLongerThan24HoursSupport`	True (vrai)	
`FileTransferLowMemoryThresholdInBytes` Détermine le moment où le serveur se considère en état de mémoire faible, ce qui provoque l'augmentation d'un comportement réseau particulier.	536870912	
`FileTransferMaxBufferSizeForLowMemoryInBytes` Indique la taille du tampon interne utilisé en état de mémoire faible.	5242880	
`FileTransferMaxBufferSizeInBytes` Indique la taille du tampon interne pour la conservation des données de paquet.	31457280	
`FileTransferMaxPacketSizeInButes` Détermine les paquets les plus volumineux qui seront envoyés.	1048576	
`FileTransferMinCompressionLimit` Spécifie en octets le seuil de compression au niveau des paquets.	0 (désactivé)	65 536 max (64 Ko)
`FileTransferPort`	3725	

`FileTransferSendReceiveBufferSize`
 	
Définit la taille maximale (en octets) des tampons d'envoi et de réception pour les connexions TCP dans le réseau de réplication. La taille des tampons affecte la taille de la fenêtre de réception (RWIN) TCP, qui définit le nombre d'octets pouvant être envoyés sans accusé de réception TCP. Ce paramètre est utile à la fois pour les transferts basés sur les fichiers et ceux par bloc. Le réglage de la taille des tampons en fonction de la bande passante et de la latence de votre réseau améliore le débit et réduit l'utilisation de l'UC.
 	
Lorsque la valeur est définie sur zéro (désactivé), la taille de la fenêtre TCP par défaut est utilisée (8 Ko). Pour personnaliser les tailles, spécifiez-les en octets.
 	
Utilisez la formule suivante pour déterminer la valeur appropriée :
 	
((VITESSE_LIAISON en Mbit/s/8) * DÉLAI en s)) * 1 000 * 1 024
 	
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 * 1 000 * 1 024 = 128 000 octets`
 	
Pour des informations sur le réglage, reportez-vous à la Section 6.4.2, « Réglage du paramètre FileTransferSendReceiveBufferSize », page 73.
	0 (8 192 octets)	5 242 880 max
		(5 Mo)

Paramètre	Valeur par défaut	Valeur maximale
`FileTransferSendReceiveBufferSizeLinux` Indique la taille de la fenêtre de réception TCP/IP des connexions de transfert de fichiers pour Linux. Cette valeur contrôle le nombre d'octets envoyés sans accusé de réception TCP, en octets. Lorsque la valeur est définie sur zéro (désactivé), la valeur de taille de la fenêtre TCP/IP pour Linux est automatiquement calculée à partir du paramètre `FileTransferSendReceiveBufferSize`. Si les deux paramètres sont définis sur zéro (désactivé), la valeur par défaut est 248 Ko. Pour personnaliser les tailles, spécifiez-les en octets. **REMARQUE :** dans les versions précédentes, vous deviez définir ce paramètre sur la 1/2 de la valeur désirée, mais ce n'est plus nécessaire.	0 (253952 octets)	
`FileTransferShutDownTimeOutInMinutes`	1090	
`FileTransferTCPTimeOutMilliSec` Permet de définir les valeurs de timeout pour l'envoi et la réception TCP.	30000	
`PostFileTransferActionsRequiredTimeInMinutes`	60	

6.4.2 Réglage du paramètre FileTransferSendReceiveBufferSize

Le paramètre FileTransferSendReceiveBufferSize définit la taille maximale (en octets) des tampons d'envoi et de réception pour les connexions TCP dans le réseau de réplication. La taille des tampons affecte la taille de la fenêtre de réception (RWIN) TCP, qui définit le nombre d'octets pouvant être envoyés sans accusé de réception TCP. Ce paramètre est utile à la fois pour les transferts basés sur les fichiers et ceux par bloc. Le réglage de la taille des tampons en fonction de la bande passante et de la latence de votre réseau améliore le débit et réduit l'utilisation de l'UC.

Vous pouvez régler le paramètre FileTransferSendReceiveBufferSize de manière à optimiser le transfert de fichiers ou de blocs à partir des serveurs sources vers les serveurs cibles au sein de votre environnement de réplication. Définissez le paramètre sur la page de configuration de PlateSpin (`https://`*`votre_serveur_PlateSpin`*`/platespinconfiguration/`).

Pour calculer la taille optimale des tampons :

1. Déterminez le temps de latence (délai) entre le serveur source et le serveur cible.

   L'objectif est de découvrir le temps de latence pour une taille de paquet qui se rapproche le plus de l'unité de transmission maximale (Maximum Transmission Unit, MTU).

   1a Connectez-vous au serveur source en tant qu'administrateur.

   1b À l'invite, entrez la commande suivante :

   ```
   # ping <target-server-ip-address> -f -l <MTU_minus_28> -n 10
   ```

   Généralement, l'option `-l` de la commande `ping` ajoute 28 octets dans les en-têtes de la charge utile spécifiée pour *adresse_IP_serveur_cible*. Par conséquent, une bonne valeur initiale pour essayer correspond à la taille en octets de la `MTU moins 28`.

1c Modifiez à plusieurs reprises la charge utile et entrez à nouveau la commande de l'Étape 1b jusqu'à ce que vous obteniez le message suivant :

```
Le paquet doit être fragmenté.
```

1d Notez la latence en secondes.

Par exemple, si la latence est de 35 ms (millisecondes), notez 0,035.

2 Calculez une valeur (en octets) pour la taille de tampon initiale :

```
Taille de tampon = (bande passante en Mbit/s / 8) * latence en secondes * 1 000
* 1 024
```

Utilisez des valeurs binaires pour la bande passante réseau. Autrement dit, 10 Gbit/s = 10 240 Mbit/s et 1 Gbit/s = 1 024 Mbit/s.

Par exemple, le calcul pour un réseau de 10 Gbit/s avec une latence de 35 ms serait le suivant :

```
Taille de tampon = (10 240 / 8) * 0,035 * 1 000 * 1 024 = 45 875 200 octets
```

3 (Facultatif) Calculez une taille de tampon optimale en arrondissant à un multiple de la taille de segment maximale (Maximum Segment Size, MSS).

3a Déterminez la MSS :

```
MSS = taille de la MTU en octets - (taille de l'en-tête IP + taille de l'en-
tête TCP)
```

La taille de l'en-tête IP est de 20 octets. La taille de l'en-tête TCP est de 20 octets plus les octets des options comme le tampon horaire.

Par exemple, si la taille de la MTU est de 1 470, votre MSS est généralement de 1 430.

```
MSS = 1 470 octets - (20 octets + 20 octets) = 1 430 octets
```

3b Calculez la taille de tampon optimale :

```
Taille de tampon optimale = (arrondissement (taille du tampon / MSS)) * MSS
```

Si nous continuons avec l'exemple, cela donne ceci :

```
Taille de tampon optimale = (arrondissement (45 875 200 / 1 430)) * 1 430 =
32 081 * 1 430 = 45 875 830
```

Vous devez arrondir vers l'unité supérieure car si vous arrondissez à l'unité inférieure, vous obtenez un multiple de la MSS qui est plus petit que la taille du tampon de 45 875 200 :

```
Taille de tampon non optimale = 32 080 * 1 430 = 45 874 400
```

6.5 Optimisation des performances de l'environnement de réplication

Les définitions des paramètres de configuration de prise de contrôle et d'instantané permettent d'optimiser les performances de réplication. Ces paramètres sont globaux et affectent toutes les réplications.

Le Tableau 6-3 répertorie les paramètres de la page de configuration de PlateSpin (`https://` *`votre_serveur_PlateSpin`*`/platespinconfiguration/`) qui contrôlent l'environnement de réplication avec les valeurs par défaut.

Tableau 6-3 Paramètres de configuration par défaut de l'environnement de réplication

Paramètre	Valeur par défaut
`TakeControlMemorySizeInMB` Taille de la mémoire (en Mo) à définir lors de la prise de contrôle pour la réplication.	768
`TakeControlCoresPerSocket` Nombre de noyaux virtuels par socket à utiliser pour la prise de contrôle lorsque la cible est démarrée avec l'option de démarrage LRD ou `bootofx.iso`.	1
`TakeControlSockets` Nombre de sockets virtuels à utiliser pour la prise de contrôle lorsque la cible est démarrée avec l'option LRD ou `bootofx.iso`.	1
`MaximumConcurrentReplications` Nombre de réplications simultanées pouvant s'exécuter simultanément.	25
`VssSnapshotCreationDelay` Nombre de secondes d'attente entre les tentatives lors de la création d'un instantané VSS pendant la réplication.	120
`VssSnapshotCreationRetryCount` Nombre maximal de tentatives de création d'un instantané VSS lors de la réplication avant l'échec de l'opération.	5

6.6 Définition de la méthode de redémarrage pour le service de configuration

Lors d'une opération de basculement, le service de configuration optimise les redémarrages en réduisant autant que possible le nombre de redémarrages et en contrôlant le moment auquel ils se produisent. Si le service de configuration se bloque lors du basculement d'un workload Windows en indiquant l'erreur `Configuration Service Not Started` (Service de configuration non démarré), vous devrez peut-être autoriser que les redémarrages se produisent comme indiqué lors de la configuration. Vous pouvez configurer le seul workload affecté pour ignorer l'optimisation du redémarrage, ou configurer un paramètre global `SkipRebootOptimization` sur le serveur PlateSpin pour ignorer l'optimisation du redémarrage pour tous les workloads Windows.

Pour ignorer l'optimisation du redémarrage pour un seul workload Windows, procédez comme suit :

1. Connectez-vous en tant qu'administrateur au workload source.
2. Ajoutez un fichier à la racine du lecteur système (généralement `C:`) appelé `PlateSpin.ConfigService.LegacyReboot` sans extension de fichier. À partir d'une invite de commande, entrez

   ```
   echo $null >> %SYSTEMDRIVE%\PlateSpin.ConfigService.LegacyReboot
   ```
3. Exécutez le test de basculement ayant échoué ou réexécutez le basculement.

Pour ignorer l'optimisation de redémarrage pour tous les workloads Windows, procédez comme suit :

1. Connectez-vous au serveur PlateSpin, puis ouvrez la page de configuration du serveur PlateSpin à l'adresse :

   `https://Votre_serveur_PlateSpin/platespinconfiguration/`
2. Recherchez le paramètre de configuration **ConfigurationServiceValues**, puis cliquez sur **Éditer** pour ce paramètre.
3. Pour le paramètre **SkipRebootOptimization**, remplacez la valeur `false` par `true`.
4. Cliquez sur **Enregistrer**.
5. Exécutez une réplication incrémentielle ou complète.

   La réplication propage également les paramètres de configuration modifiés à la machine virtuelle cible.
6. Exécutez le test de basculement ou réexécutez le basculement pour les workloads Windows affectés.

6.7 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.

Les workloads répliqués par PlateSpin Protect et gérés par VMware vCenter SRM peuvent fonctionner en toute transparence si vous configurez PlateSpin Protect de manière à prendre en charge le gestionnaire SRM en faisant 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.

- Section 6.7.1, « Configuration des fichiers de workload dans la même banque de données », page 76
- Section 6.7.2, « Configuration des outils VMware pour les cibles de basculement », page 77
- Section 6.7.3, « Accélération du processus de configuration », page 78

6.7.1 Configuration des fichiers de workload dans la même banque de données

Pour faire en sorte 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, repérez 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.

6.7.2 Configuration des outils VMware pour les cibles de basculement

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. Lorsque cela n'est pas le cas, vous devez préparer votre environnement avant la réplication.

Pour préparer votre environnement :

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.*x* et versions ultérieures** les paquetages d'installation sont `setup.exe` et `setup64.exe`.
- **VMware 4.*x* :** 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 :

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 approprié (`1.package`) dans le répertoire `%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 d'outils VMware, comme indiqué dans le Tableau 6-4. Utilisez la valeur GUID appropriée pour copier le paquetage dans le répertoire approprié.

Tableau 6-4 *GUID pour les noms de répertoire d'outils VMware*

Version du serveur VMware	Architecture des outils VMware	GUID
NetWare 6.5	x86	`D61C0FCA-058B-42C3-9F02-898F568A3071`
NetWare 6.5	x64	`5D3947B7-BE73-4A00-A549-B15E84B98803`
NetWare 6.0	x86	`311E672E-05BA-4CAF-A948-B26DF0C6C5A6`
NetWare 6.0	x64	`D7F55AED-DA64-423F-BBBE-F1215529AD03`
5.5	x86	`660C345A-7A91-458b-BC47-6A3914723EF7`
5.5	x64	`8546D4EF-8CA5-4a51-A3A3-6240171BE278`
5.1	x86	`34DD2CBE-183E-492f-9B36-7A8326080755`
5.1	x64	`AD4FDE1D-DE86-4d05-B147-071F4E1D0326`
5	x86	`AD4FDE1D-DE86-4d05-B147-071F4E1D0326`
5	x64	`F7C9BC91-7733-4790-B7AF-62E074B73882`
4.1	x86	`F2957064-65D7-4bda-A52B-3F5859624602`
4.1	x64	`80B1C53C-6B43-4843-9D63-E9911E9A15D5`
4.0	x86	`D052CBAC-0A98-4880-8BCC-FE0608F0930F`
4.0	x64	`80B50267-B30C-4001-ABDF-EA288D1FD09C`

6.7.3 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, repérez le paramètre de configuration `ConfigurationServiceValues` et remplacez la valeur de son sous-paramètre `WaitForFloppyTimeoutInSecs` par zéro (0).
2. Dans la page Web de configuration, repérez 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.

7 Configuration de l'interface Web de PlateSpin

L'interface Web de PlateSpin permet de configurer des balises à utiliser pour assurer le suivi des associés logiques parmi les workloads. En outre, vous pouvez contrôler les fréquences de rafraîchissement d'écran pour plusieurs pages. Utilisez les informations de cette section pour configurer votre interface Web.

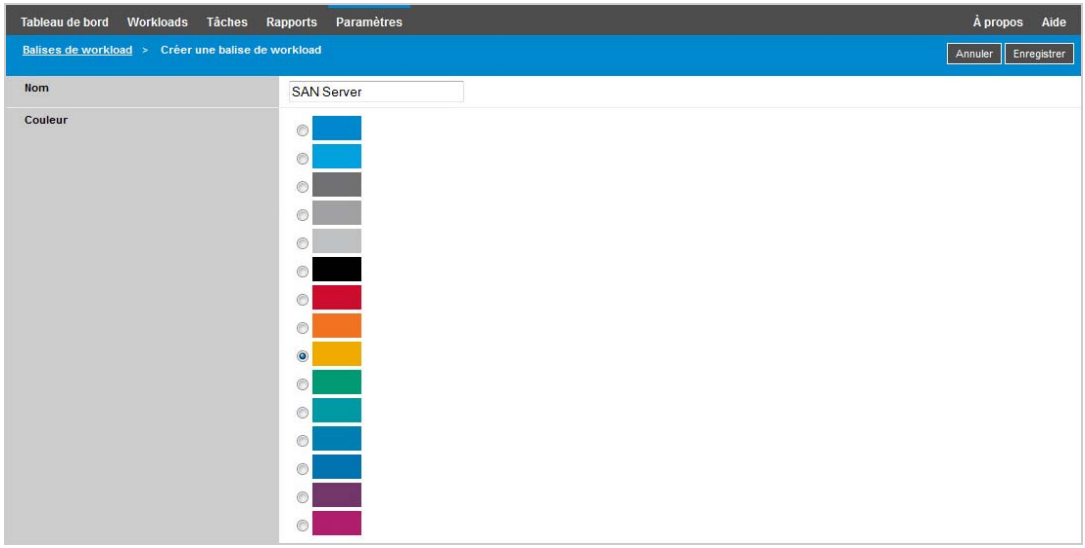
7.1 Création et gestion des balises de workload

Lorsque vous avez un grand nombre de workloads à gérer, parcourir la liste et sélectionner des workloads similaires pour des opérations simultanées peut prendre beaucoup de temps. Trier en fonction du nom ou de la fonctionnalité peut vous aider. Une autre solution consiste à utiliser une balise pour définir une association personnalisée parmi les workloads que vous souhaitez gérer en tant que groupe. Vous pouvez facilement trier les workloads grâce à la colonne Balise, sélectionner les workloads appropriés et exécuter les opérations disponibles simultanément sur ces workloads balisés.

Une balise peut représenter toute association logique ou physique pertinente pour vous. Vous attribuez une couleur et un nom uniques à chaque balise. Vous pouvez créer autant de balises uniques que vous le souhaitez, bien que le choix de couleurs uniques soit limité. Chaque workload peut être associé à une balise unique. Lorsque vous exportez un workload vers un nouveau serveur, ses paramètres de balise sont conservés.

7.1.1 Création d'une balise de workload

1 Dans l'interface Web de PlateSpin Protect, cliquez sur **Paramètres** > **Balises de workload** > **Créer une balise de workload**.



2 Indiquez un nom de balise unique (25 caractères maximum) et associez une couleur à cette description.

3 Cliquez sur **Enregistrer** pour ajouter cette nouvelle balise à la liste des balises de workloads disponibles dans la vue Balises de workload de la page Paramètres.

7.1.2 Modification d'une balise de workload

1 Dans l'interface Web de PlateSpin Protect, cliquez sur **Paramètres** > **Balises de workload**.

2 Modifiez l'une des balises disponibles. Cliquez sur le nom de la balise, modifiez son nom ou la couleur associée, puis cliquez sur **Enregistrer**.

7.1.3 Ajout d'une balise à un workload

1 Dans la liste des workloads, sélectionnez le workload actif que vous souhaitez baliser, puis cliquez sur **Configurer** pour ouvrir la page de configuration correspondante.

2 Développez la section **Balise** pour afficher la liste déroulante **Balise**.

3 Sélectionnez le nom de la balise que vous souhaitez associer au workload, puis cliquez sur **Enregistrer**.

7.1.4 Retrait d'une balise d'un workload

1 Dans la liste des workloads, sélectionnez le workload, puis cliquez sur **Configurer** pour ouvrir la page de configuration correspondante.

2 Développez la section **Balise** pour afficher la liste déroulante **Balise**.

3 Sélectionnez la ligne « vide » dans la liste des noms de balises disponibles, puis cliquez sur **Enregistrer**.

7.1.5 Suppression d'une balise de workload

Vous pouvez supprimer n'importe quelle balise que vous n'utilisez plus. Vous ne pouvez pas supprimer une balise qui est associée à un workload.

1 Dans l'interface Web de PlateSpin Protect, cliquez sur **Paramètres** > **Balises de workload**.

2 Dissociez la balise souhaitée des workloads.

3 Cliquez sur **Supprimer** en regard de la balise, puis cliquez sur **OK** pour confirmer.

7.2 Configuration des fréquences de rafraîchissement de l'interface Web

L'intervalle de rafraîchissement peut être configuré sur plusieurs pages de l'interface Web, comme l'indique le Tableau 7-1. Vous pouvez modifier le paramètre d'intervalle en fonction des besoins de votre environnement PlateSpin.

Tableau 7-1 *Intervalles de rafraîchissement par défaut de l'interface Web*

Paramètre de l'interface Web	Intervalle de rafraîchissement par défaut (en secondes)
DashboardUpdateIntervalSeconds	60
WorkloadsUpdateIntervalSeconds	60
WorkloadTargetsUpdateIntervalSeconds	30
WorkloadDetailsUpdateIntervalSeconds	15
TasksUpdateIntervalSeconds	15

1 Ouvrez le fichier suivant dans un éditeur de texte :

```
\Program Files\PlateSpin Protect Server\Platespin Forge\web\web.config
```

2 Modifiez la valeur des paramètres d'intervalle suivants en fonction des besoins de votre environnement PlateSpin :

```
<add key="DashboardUpdateIntervalSeconds" value="60" /> <add
key="WorkloadsUpdateIntervalSeconds" value="60" /> <add
key="WorkloadTargetsUpdateIntervalSeconds" value="30" /> <add
key="WorkloadDetailsUpdateIntervalSeconds" value="15" /> <add
key="TasksUpdateIntervalSeconds" value="15" />
```

3 Enregistrez le fichier.

Les nouveaux paramètres prendront effet lors de votre prochaine session de l'interface Web. Il n'est pas nécessaire de redémarrer le serveur ni le service PlateSpin Server.

7.3 Personnalisation de l'interface utilisateur pour l'interface Web

Vous pouvez modifier l'apparence de l'interface Web de PlateSpin pour qu'elle reflète l'identité de votre entreprise. Vous pouvez ainsi changer les couleurs, le logo ou encore le nom du produit. Pour plus d'informations, reportez-vous à l'Annexe A, « Application de votre marque à l'interface Web de PlateSpin Protect », page 87.

8 Gestion de plusieurs serveurs PlateSpin dans la console de gestion

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 et PlateSpin Forge, 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.

8.1 Utilisation de la console de gestion de PlateSpin Protect

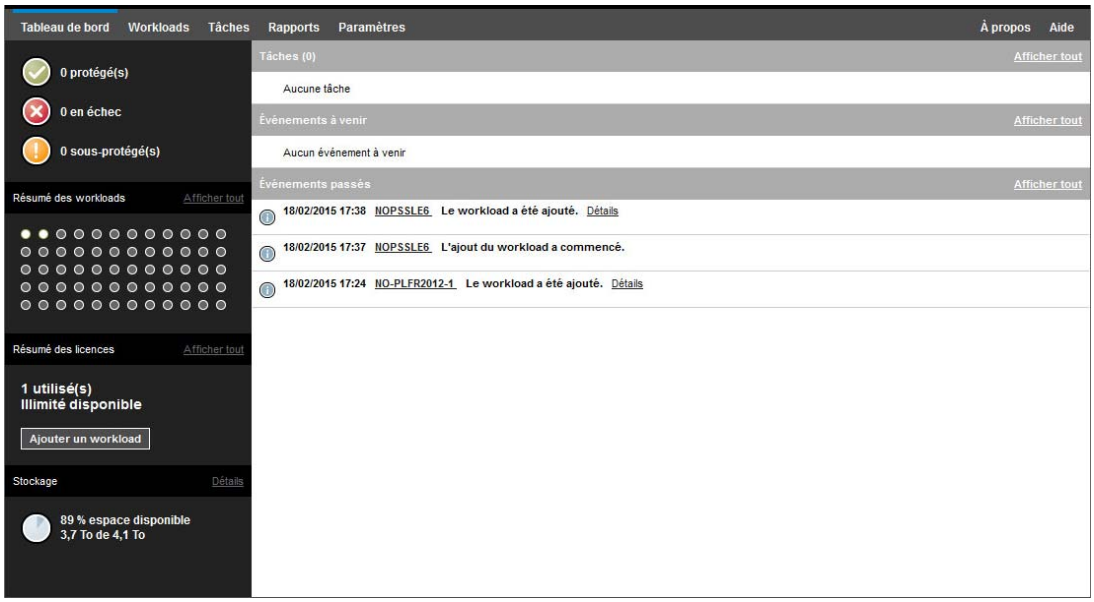
Pour utiliser la console de gestion :

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

   `https://`*votre_serveur_PlateSpin*`/console`

   Remplacez *votre_serveur_PlateSpin* par l'adresse IP ou le nom d'hôte DNS de l'hôte du serveur PlateSpin désigné comme gestionnaire.
2. Connectez-vous en utilisant votre nom d'utilisateur et votre mot de passe
3. (Connexion initiale) Sur la page de bienvenue, cliquez sur **Ajouter un serveur PlateSpin**, puis configurez une instance de serveur PlateSpin comme décrit à la Section 8.3, « Ajout d'instances de PlateSpin Protect et PlateSpin Forge à la console de gestion », page 85.

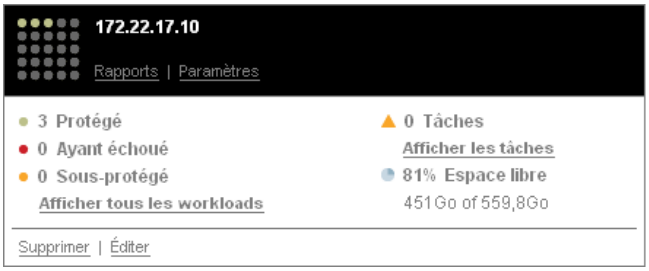
4 (Connexions ultérieures) Affichez le tableau de bord.



8.2 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 8-1 *Carte de l'instance PlateSpin Protect*



La carte affiche les informations de base relatives à l'instance correspondante de PlateSpin Protect et 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.

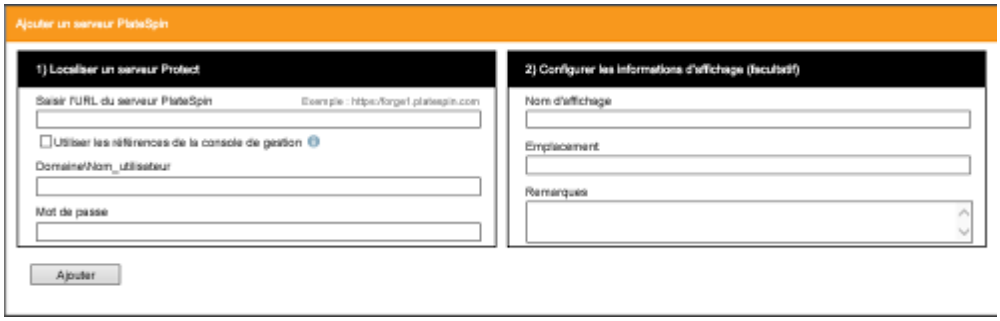
8.3 Ajout d'instances de PlateSpin Protect et PlateSpin Forge à la console de gestion

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**.



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) Saisissez un **Nom d'affichage** descriptif unique (15 caractères maximum) pour le serveur PlateSpin, son **Emplacement** (20 caractères maximum) et les éventuelles **Remarques** que vous souhaitez ajouter (400 caractères maximum).

6 Cliquez sur **Ajouter**.

Une nouvelle carte est ajoutée au tableau de bord.

8.4 Modification des cartes dans la console de gestion

Pour modifier les détails d'une carte sur la console de gestion :

1 Dans la console de gestion, recherchez l'instance de carte du serveur PlateSpin Protect ou PlateSpin Forge que vous souhaitez modifier.

2 Cliquez sur le lien hypertexte **Éditer** de la carte.

   La page **Ajouter/éditer** de la console s'affiche.

3 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.

8.5 Suppression de cartes dans la console de gestion

Pour supprimer une carte de la console de gestion :

1 Dans la console de gestion, recherchez l'instance de carte du serveur PlateSpin Protect ou PlateSpin Forge que vous souhaitez supprimer.

2 Cliquez sur le lien hypertexte **Supprimer** de la carte.

   Une invite de confirmation s'affiche.

3 Cliquez sur **OK** pour confirmer.

   L'instance de carte est supprimée du tableau de bord.

A Application de votre marque à l'interface Web de PlateSpin Protect

Vous pouvez modifier l'apparence de l'interface Web de pour l'adapter à l'identité de votre entreprise, ce qui inclut les couleurs, le logo et le nom de produit. Vous pouvez même supprimer les liens vers les onglets **À propos de** et **Aide** dans l'interface du produit.

Les informations de cette section vous aident à modifier l'identification de marque appliquée au produit :

A.1 Application de votre marque à l'interface Web grâce aux paramètres de configuration

Vous pouvez modifier l'apparence de l'interface Web pour qu'elle corresponde à celle des sites Web de l'entreprise. Pour personnaliser la marque de l'interface Web, modifiez les paramètres de configuration de l'hôte de votre serveur PlateSpin.

Pour modifier les paramètres de personnalisation de l'interface Web :

1. Ouvrez la page `https://votre_serveur_PlateSpin/platespinconfiguration/` dans le navigateur Web de votre choix, puis connectez-vous en tant qu'administrateur.
2. Recherchez le paramètre de serveur requis, cliquez sur **Éditer** et modifiez ensuite sa valeur.

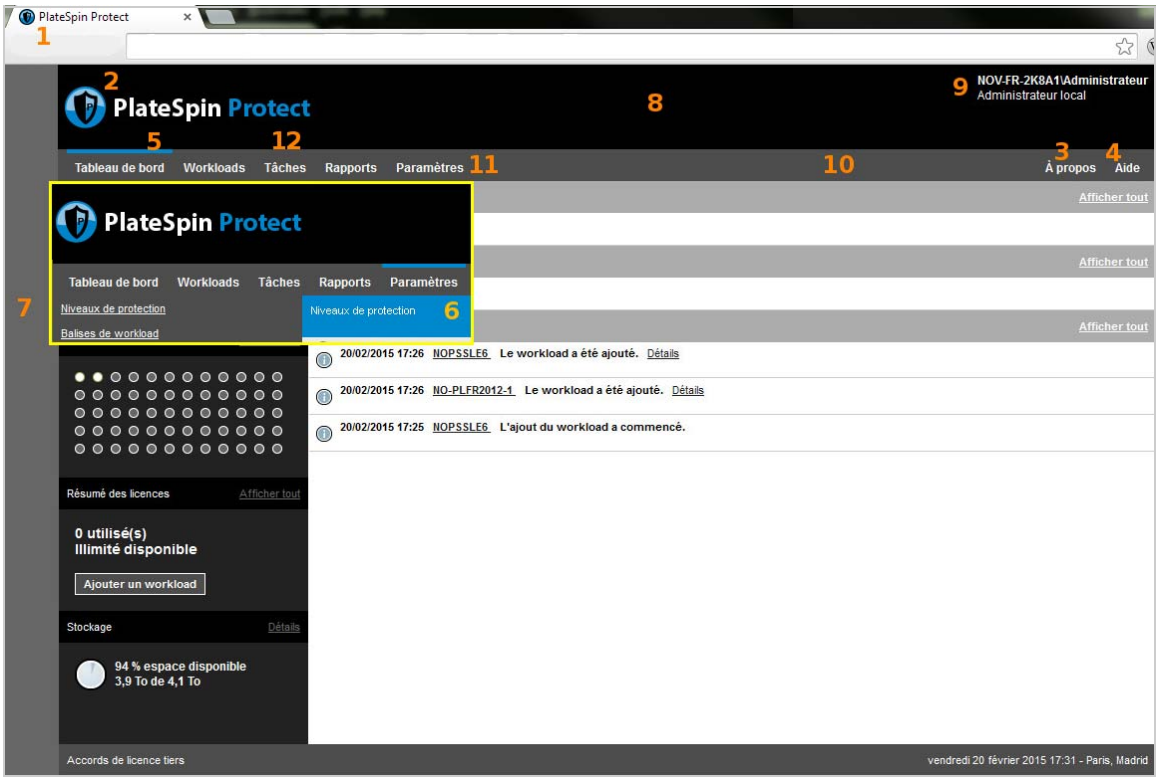
   Pour plus d'informations, reportez-vous à la Figure A-1 afin d'identifier les éléments configurables dans l'interface utilisateur. Reportez-vous au Tableau A-1 pour afficher le nom du paramètre, la description et les informations sur la valeur par défaut pour chaque élément configurable.
3. Enregistrez vos paramètres et quittez la page.

   Bien qu'aucun redémarrage des services ne soit nécessaire après avoir effectué des modifications dans l'outil de configuration, il peut s'écouler jusqu'à 30 secondes avant que les modifications ne soient prises en compte dans l'interface.

A.1.1 Éléments configurables de l'interface Web

L'aspect de l'interface Web est cohérent dans l'ensemble. L'illustration du tableau de bord de PlateSpin Protect de la Figure A-1 identifie les éléments que vous pouvez modifier au moyen de légendes numérotées. L'incrustation affiche les éléments configurables dans le panneau Paramètres.

Figure A-1 *Interface Web de Protect avec identification des éléments configurables*



A.1.2 Paramètres configurables de l'interface Web

Le tableau ci-dessous identifie l'élément d'interface (ID) dans la capture d'écran ci-dessus et affiche le nom du paramètre, une description et la valeur par défaut. Utilisez la page des paramètres de configuration du serveur PlateSpin pour modifier ces valeurs (dans la page des paramètres, cliquez sur **Éditer** sur une valeur de configuration) en fonction de la nouvelle apparence que vous souhaitez appliquer.

Tableau A-1 *Paramètres de configuration de l'interface Web et valeurs par défaut*

ID	Définition du nom et de la description	Valeur par défaut

1	`WebUIFaviconUrl`
	
	Emplacement d'un fichier graphique `.ico` valide. Spécifiez l'un des éléments suivants :
	
	◆ Une URL valide vers le fichier `.ico` approprié sur un autre ordinateur.
	
	Par exemple : https://myserver.example.com/dir1/dir2/icons/mycompany_favicon.ico
	
	◆ Un chemin d'accès relatif sous la racine du serveur Web local où vous avez téléchargé le fichier `.ico` approprié.
	
	Par exemple, si vous créez un chemin d'accès appelé `mycompany\images\icons` à la racine du serveur Web pour stocker votre fichier d'icône personnalisé :
	
	`~/mycompany/images/icons/mycompany_favicon.ico`
	
	Dans cet exemple, le chemin d'accès réel au fichier est `C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\mycompany\images\icons\mycompany_favicon.ico`.
		`~/doc/en/favicon.ico` [1]

2	`WebUILogoUrl`
	
	Emplacement du fichier graphique du logo du produit. Spécifiez l'un des éléments suivants :
	
	◆ Une URL valide vers le fichier graphique approprié sur un autre ordinateur.
	
	Par exemple : https://myserver.example.com/dir1/dir2/logos/mycompany_logo.png
	
	◆ Un chemin d'accès relatif sous la racine du serveur Web local où vous avez téléchargé le fichier graphique approprié.
	
	Par exemple, si vous créez un chemin d'accès appelé `mycompany\images\logos` à la racine du serveur Web pour stocker vos images de logo personnalisées :
	
	`~/mycompany/images/logos/mycompany_logo.png`
	
	Dans cet exemple, le chemin d'accès réel au fichier est `C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\mycompany\images\logos\mycompany_logo.png`.
		`~/Resources/protectLogo.png` [2]

3	`WebUIShowAboutTab` Permet d'afficher ou de masquer l'onglet **À propos de** en définissant **True** ou **False**.	True (vrai)

ID	Définition du nom et de la description	Valeur par défaut
4	`WebUIShowHelpTab` Permet d'afficher ou de masquer l'onglet **Aide** en définissant **True** ou **False**.	True (vrai)
5	`WebUISiteAccentColor` Couleur d'accentuation (valeur hexadécimale RVB)	#0088CE
6	`WebUISiteAccentFontColor` Couleur de police à afficher avec la couleur d'accentuation dans l'interface utilisateur Web (valeur hexadécimale RVB)	#FFFFFF
7	`WebUISiteBackgroundColor` Couleur d'arrière-plan du site (valeur hexadécimale RVB)	#666666
8	`WebUISiteHeaderBackgroundColor` Couleur d'arrière-plan de l'en-tête du site (valeur hexadécimale RVB)	#000000
9	`WebUISiteHeaderFontColor` Couleur de police de l'en-tête du site dans l'interface utilisateur Web (valeur hexadécimale RVB)	#FFFFFF
10	`WebUISiteNavigationBackgroundColor` Couleur de l'arrière-plan de navigation du site dans l'interface utilisateur Web (valeur hexadécimale RVB)	#4D4D4D
11	`WebUISiteNavigationFontColor` Couleur de la police du lien de navigation du site dans l'interface utilisateur Web (valeur hexadécimale RVB)	#FFFFFF
12	`WebUISiteNavigationLinkHoverBackgroundColor` Couleur de l'arrière-plan du lien de navigation du site en mode survol de la souris (valeur hexadécimale RVB)	#808080

[1] Le chemin d'accès réel est `C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\doc\en\favicon.ico`.

[2] Le chemin d'accès réel est `C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\Resources\protectLogo.png`.

A.2 Changement du nom de produit dans le Registre Windows

Le titre situé dans la partie supérieure de l'interface du produit offre suffisamment d'espace pour le logo de l'entreprise et pour le nom du produit. Vous pouvez changer le logo, qui inclut généralement le nom du produit, à l'aide d'un paramètre de configuration. Pour modifier ou supprimer le nom du produit dans un onglet du navigateur, vous devez effectuer une modification dans le Registre Windows.

Pour modifier le nom du produit :

1. Exécutez `regedit` sur le serveur PlateSpin.
2. Dans l'Éditeur du Registre Windows, accédez à la clé de Registre suivante :

   `HKEY_LOCAL_MACHINE\SOFTWARE\PlateSpin\ProtectServer\ProductName`

   REMARQUE : dans certains cas, la clé de Registre se trouve à l'emplacement suivant :

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PlateSpin\Protect`
3. Double-cliquez sur la clé `ProductName` et entrez le nom de votre choix dans le champ **Données de la valeur**, puis cliquez sur **OK**.
4. Redémarrez le serveur IIS pour que le changement d'interface soit pris en compte.

Préparation des sources et des cibles de protection

Avant de pouvoir configurer des contrats de protection, vous devez identifier les conteneurs cibles et workloads sources prévus. Vous pouvez obtenir les détails concernant les cibles et les workloads via un processus d'inventaire.

9 Préparation 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. L'ajout d'un conteneur cible remplit la base de données PlateSpin Protect avec des informations d'inventaire détaillées sur le conteneur et ses ressources. L'inventaire fournit les données nécessaires pour déterminer l'utilisation du conteneur et configurer correctement un ou plusieurs contrats de protection de workload pour le conteneur cible.

9.1 À propos des conteneurs (cibles de protection)

L'interface Web de PlateSpin permet l'inventaire automatisé des plates-formes des conteneurs cibles pris en charge.

9.1.1 Conteneurs pris en charge

Avant d'ajouter un conteneur au serveur PlateSpin, assurez-vous que la version du conteneur de machines virtuelles est prise en charge. Reportez-vous à la section « Conteneurs de VM pris en charge » page 17.

9.1.2 Conditions d'accès réseau pour les conteneurs

Avant de commencer les opérations d'inventaire, assurez-vous que le serveur PlateSpin peut communiquer avec vos workloads sources et vos cibles. Reportez-vous à la Section 1.5.2, « Configuration réseau requise pour les conteneurs », page 32.

9.1.3 Directives concernant les paramètres des conteneurs

Le Tableau 9-1 fournit des directives pour la sélection du type de machine, le format des références et la syntaxe des paramètres d'inventaire pour les hôtes cibles qui utilisent l'interface Web.

Tableau 9-1 *Directives pour les paramètres de découverte de l'interface Web concernant les conteneurs cibles*

À découvrir	Type de cible	Références
Grappe VMware vCenter	**Grappe VMware DRS**	Références du service Web VMware vCenter (nom d'utilisateur et mot de passe)
VMware ESXi Server	**Serveur VMware ESX**	Compte ESX avec rôle d'administrateur OU Références de domaine Windows (versions 4 et 4.1 uniquement)

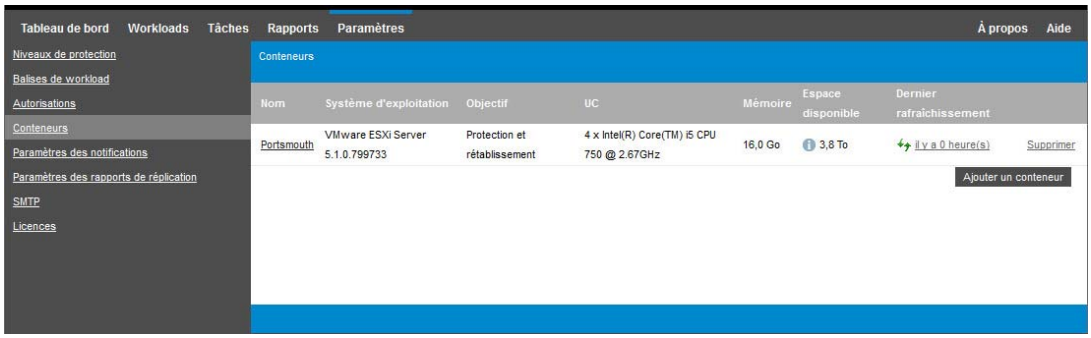
9.2 Ajout de conteneurs (cibles de protection)

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. PlateSpin Protect vous permet d'utiliser des conteneurs pour la protection et le rétablissement.

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, sélectionnez **Paramètres > Conteneurs > Ajouter un conteneur**.



2 Spécifiez le type de conteneur :

- **Serveur VMware ESX**
- **Grappe VMware DRS**

3 Selon le type de cibles sélectionnées à l'étape précédente, spécifiez les informations d'accès suivantes.

Tableau 9-2 *Options pour une cible de grappe DRS VMware*

Option	Description
Nom d'hôte vCenter ou IP	Spécifiez le nom d'hôte ou l'adresse IP du serveur vCenter.

Option	Description
Nom d'hôte vCenter ou IP	Spécifiez le nom d'hôte ou l'adresse IP du serveur vCenter.

- **Grappe VMware DRS:** Reportez-vous au Tableau 9-3.
- **Serveur VMware ESX:** Reportez-vous au Tableau 9-4.

Tableau 9-3 *Options pour une cible de grappe DRS VMware*

Option	Description
Nom d'hôte vCenter ou IP	Spécifiez le nom d'hôte ou l'adresse IP du serveur vCenter.

Option	Description
Nom d'hôte vCenter ou IP	Spécifiez le nom d'hôte ou l'adresse IP du serveur vCenter.

Tableau 9-4 *Options pour une cible de serveur VMware ESX*

Option	Description
Nom d'hôte ou adresse IP	Spécifiez le nom d'hôte ou l'adresse IP du serveur vMware ESX.
Nom d'utilisateur et mot de passe	Spécifiez les références de niveau administrateur pour accéder au conteneur cible. Reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 165.

4 Cliquez sur **Tester les références** pour valider les valeurs de référence spécifiées.

5 Sélectionnez l'objectif du conteneur de machines virtuelles :

- **Protection**
- **Rétablissement**
- **Protection et rétablissement**

Si vous sélectionnez les deux éléments (**Protection** et **Rétablissement**), le conteneur peut être sélectionné en tant que cible pour les opérations de protection et de rétablissement.

6 Cliquez sur **Ajouter** pour ajouter et découvrir des détails concernant le conteneur et les répertorier dans la page Conteneurs.

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**.

9.3 Rafraîchissement des détails des conteneurs

Vous devez régulièrement rafraîchir les détails concernant vos conteneurs cibles avant de configurer ou d'exécuter un contrat de protection. L'interface Web de PlateSpin permet de rafraîchir les ressources découvertes pour les conteneurs cibles virtuels.

Lorsque vous rafraîchissez la cible, ses ressources associées sont automatiquement redécouvertes et mises à jour. Vous pouvez rafraîchir un conteneur à la fois.

Pour rafraîchir les détails d'un conteneur cible :

1. Dans l'interface Web de PlateSpin, sélectionnez **Paramètres > Conteneurs**.
2. Cliquez sur l'icône **Rafraîchir** en regard de ce conteneur.

   Cela exécute un nouvel inventaire du conteneur.
3. Développez les panneaux de la page des détails du conteneur pour plus d'informations sur les modifications de l'inventaire.

9.4 Suppression de conteneurs (cibles de protection)

Si vous supprimez tous les contrats de protection d'un conteneur cible, vous pouvez supprimer ce dernier (annuler sa découverte). Vous pouvez également supprimer un conteneur qui ne sera pas utilisé.

IMPORTANT : avant de supprimer un conteneur cible qui est en cours d'utilisation pour un contrat de protection de workload configuré, vous devez vous assurer que tous les contrats concernés sont supprimés ou reconfigurés pour un autre conteneur cible.

Pour supprimer une cible via l'interface Web :

1. Dans l'interface Web de PlateSpin, sélectionnez **Paramètres > Conteneurs**.
2. Dans la page Conteneurs, cliquez sur **Supprimer** en regard du conteneur que vous souhaitez supprimer de Protect.

10 Préparation des workloads (sources de protection)

Pour tout contrat de protection, vous devez disposer d'un workload source et d'un conteneur cible. L'ajout d'un workload au serveur PlateSpin Protect remplit la base de données PlateSpin avec les informations d'inventaire détaillées concernant la machine. Ces informations fournissent les données nécessaires pour déterminer l'utilisation de la machine et configurer correctement un contrat de protection.

10.1 À propos des workloads (sources de protection)

L'interface Web de PlateSpin permet l'inventaire automatisé des configurations des workloads sources pris en charge.

10.1.1 Workloads pris en charge

Avant d'ajouter un workload au serveur PlateSpin, assurez-vous que le matériel et la version du système d'exploitation du workload sont pris en charge. Reportez-vous aux rubriques suivantes de la Section 1.1, « Configurations prises en charge », page 13 :

- « Workloads Windows pris en charge » page 14
- « Workloads Linux pris en charge » page 15
- « Architectures de workload prises en charge » page 19
- « Stockage pris en charge » page 21

10.1.2 Conditions d'accès réseau pour les workloads sources

Pour plus d'informations sur les conditions d'accès réseau concernant l'inventaire des workloads Windows et Linux, reportez-vous à la Section 1.5.3, « Configuration réseau requise pour les workloads », page 32.

10.1.3 Directives concernant les paramètres des workloads sources

Le Tableau 10-1 fournit des directives pour la sélection du type de machine, le format des références et la syntaxe des paramètres d'inventaire pour les workloads.

Tableau 10-1 *Directives pour les paramètres de découverte des workloads*

À découvrir	Type de machine	Références	Remarques
Tous les workloads Windows	**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*
Tous les workloads Linux	**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 n° 7920711 de la base de connaissances (https://www.netiq.com/support/kb/doc.php?id=7920711).

10.2 Ajout de workloads (sources de protection)

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.

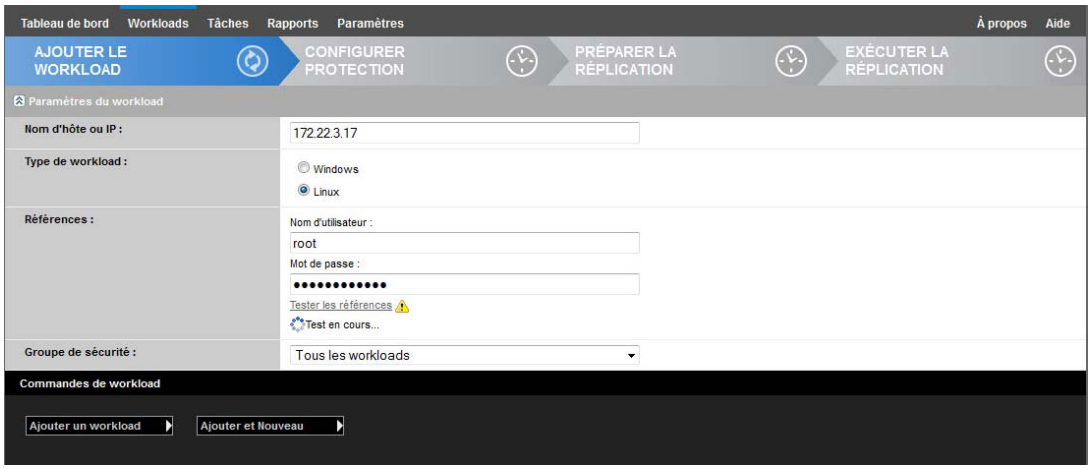
Pour protéger un workload, un workload et un conteneur doivent être inventoriés par le serveur PlateSpin (ou y être *ajoutés*).

Pour ajouter un workload :

1. Suivez les étapes préparatoires requises.

   Reportez-vous au point Préparation de la section « Workflow de base pour la protection et la récupération de workload » page 37.
2. Sur la page Tableau de bord ou Workloads, cliquez sur **Ajouter un workload**.

   L'interface Web affiche la page Ajouter un workload.



3 Spécifiez les détails de workload requis.

- **Paramètres du workload :** spécifiez le nom d'hôte ou 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 165.

  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 de prenne fin. 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.

5 (Conditionnel) Si vous n'avez pas encore ajouté de conteneur à utiliser avec ce workload, faites-le afin de préparer la protection du workload. Reportez-vous à la section « Préparation de conteneurs (cibles de protection) » page 95.

6 Passez à la section « Configuration des détails de protection et préparation de la réplication » page 151.

10.3 Ajout de balises à des workloads

Dans l'interface Web de PlateSpin , il se peut que la page Workloads affiche une longue liste de workloads. Parcourir ces workloads afin de gérer des opérations pour des workloads similaires peut prendre beaucoup de temps. Afin de résoudre ce problème, vous pouvez créer des balises pour les différentes catégories de workloads, des services distincts ou d'autres associations logiques appropriées à votre environnement.

Pour plus d'informations sur la création, la modification ou la suppression de balises de workload, reportez-vous à la Section 7.1, « Création et gestion des balises de workload », page 79.

Une fois des balises créées, elles sont disponibles au bas de la page de modification des détails cibles où vous pouvez assigner une balise aux workloads appropriés. La page Workloads comprend une colonne **Balise** dans laquelle est affichée la balise unique que vous associez à un workload. Vous pouvez effectuer un tri sur la base de cette colonne afin de regrouper les workloads similaires. Cela vous permet de localiser et d'exécuter des opérations simultanées sur les workloads associés à une balise.

REMARQUE : lorsque vous exportez un workload avec un paramètre de balise vers un nouveau serveur, ses paramètres de balise sont conservés.

Pour associer une balise à un workload au cours de la configuration de la protection :

1. Dans l'interface Web de PlateSpin Protect, cliquez sur **Workloads**.
2. Dans la liste des workloads, sélectionnez celui auquel vous souhaitez ajouter une balise, puis cliquez sur **Configurer la protection**.
3. Configurez le workload.
4. Dans la section Balise au bas de la page de modification des détails cibles, sélectionnez le nom de la balise que vous souhaitez associer au workload.
5. Cliquez sur **Enregistrer**.

Pour ajouter ou modifier une balise associée à un workload configuré :

1. Dans l'interface Web de PlateSpin Protect, cliquez sur **Workloads**.
2. Dans la liste des workloads, cliquez sur celui auquel vous souhaitez ajouter une balise pour ouvrir la page Détails cibles.
3. Cliquez sur **Éditer**.
4. Dans la section Balise au bas de la page de modification des détails cibles, sélectionnez le nom de la balise que vous souhaitez associer au workload.
5. Cliquez sur **Enregistrer**.

Pour dissocier une balise d'un workload :

1. Dans l'interface Web de PlateSpin Protect, cliquez sur **Workloads**.
2. Dans la liste des workloads, sélectionnez celui dont vous souhaitez supprimer la balise, puis cliquez sur **Configurer la protection**.
3. Dans la section Balise de la page de configuration, sélectionnez la chaîne vide, puis cliquez sur **Enregistrer**.

10.4 Rafraîchissement des détails des workloads

L'interface Web de PlateSpin ne prend pas en charge les détails de rafraîchissement des workloads découverts. Pour mettre à jour les détails concernant un workload découvert, vous devez supprimer le workload, puis l'ajouter à nouveau et redécouvrir ses détails. Les détails de la configuration sont perdus si le workload est dans un état configuré lors de sa suppression. Si une licence de protection est en cours d'utilisation, elle est supprimée du workload et renvoyée dans la réserve de licences. Reportez-vous à la Section 10.5, « Suppression de workloads », page 103.

10.5 Suppression de workloads

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

1. Dans la page Workloads, sélectionnez le workload à retirer, puis cliquez sur **Supprimer le workload**.
2. (Conditionnel, Windows) Pour les workloads Windows auparavant protégés par la réplication par bloc, l'interface Web 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.
3. À la page Confirmation de commande, cliquez sur **Confirmer** pour exécuter la commande.

   Attendez que le processus de prenne fin.
4. (Conditionnel, Linux) Pour les workloads Linux, vous devez désinstaller manuellement le pilote par bloc du workload source. Reportez-vous à la section Logiciel de transfert de données par bloc dans la section Nettoyage des workloads Linux.

11 Préparation des pilotes de périphérique pour les cibles de rétablissement physiques

PlateSpin Protect fournit une bibliothèque de pilotes de périphérique et d'ID PnP (Plug-and-Play) nécessaires si vous disposez de machines physiques en tant que cibles de rétablissement. Vous pouvez ajouter des pilotes de périphérique personnalisés et des assignations d'ID PnP à l'aide de l'outil de pilote de périphérique de PlateSpin (`DeviceDriver.exe`).

11.1 Gestion des pilotes de périphérique

PlateSpin Protect est fourni avec une bibliothèque de pilotes de périphérique. Il installe automatiquement les pilotes de périphérique appropriés sur les workloads cibles. Si certains pilotes sont manquants ou incompatibles sur la machine physique cible du rétablissement, 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 Protect.

11.1.1 Création d'un paquetage contenant les pilotes de périphérique pour les workloads Windows

Vous devez créer un paquetage contenant vos pilotes de périphérique Windows afin de les préparer pour le téléchargement dans la base de données des pilotes de PlateSpin Protect.

REMARQUE : pour garantir le bon fonctionnement de votre tâche de protection et de votre workload cible, créez un paquetage contenant et permettant de télécharger uniquement des pilotes à signature numérique pour :

- l'ensemble des systèmes Windows 64 bits ;
- les versions 32 bits des systèmes Windows Server 2008.

Pour créer un paquetage contenant les pilotes de périphérique Windows :

1. Préparez tous les fichiers de pilote interdépendants (`*.sys`, `*.inf`, `*.dll`, etc.) pour votre infrastructure et votre périphérique cible.

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.

Le paquetage est à présent prêt à être téléchargé. Reportez-vous à la section « Téléchargement de paquetages de pilotes dans la base de données des pilotes de périphérique de PlateSpin » page 106.

11.1.2 Création d'un paquetage contenant les pilotes de périphérique pour les workloads Linux

Vous devez créer un paquetage contenant vos pilotes de périphérique Linux afin de les préparer pour le téléchargement dans la base de données des pilotes de PlateSpin Protect. Pour ce faire, votre image ISO de démarrage PlateSpin (`bootofx.x2p.iso`) contient un utilitaire personnalisé.

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 et UEFI :

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

   Exemples :

   ```
   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 paquetages de pilotes dans la base de données des pilotes de périphérique de PlateSpin » page 106.

11.1.3 Téléchargement de paquetages de pilotes dans la base de données des pilotes de périphérique de PlateSpin

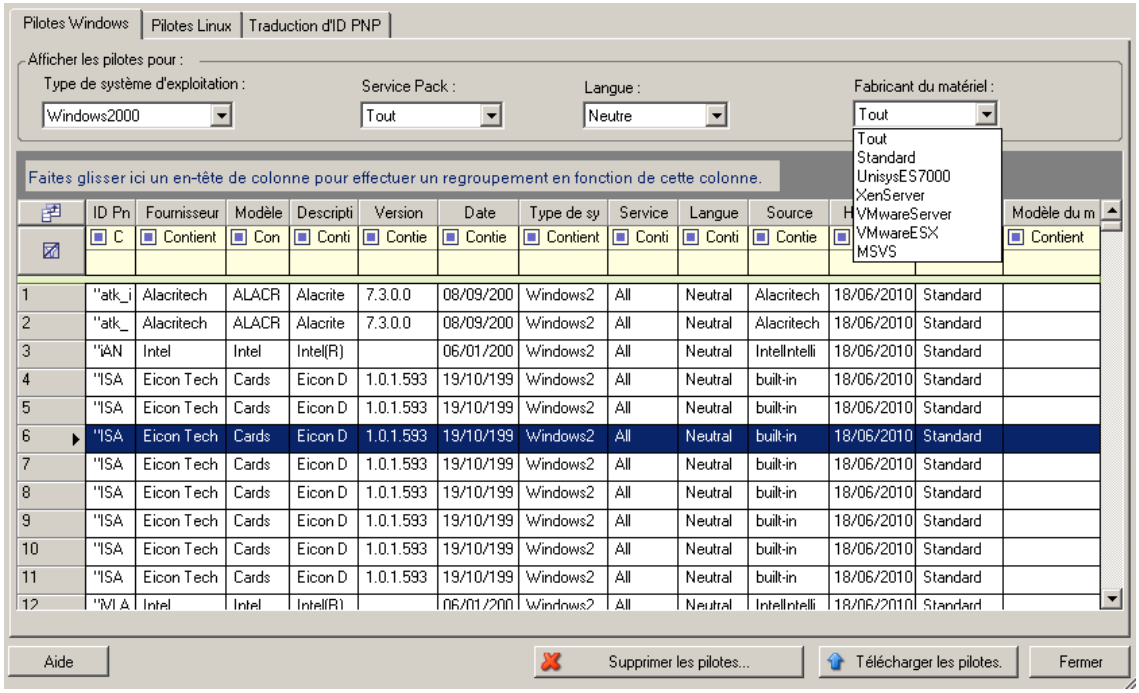
L'outil Gestionnaire de pilotes PlateSpin permet de télécharger les pilotes de périphérique dans la base de données des pilotes.

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

- « Procédure de téléchargement de pilotes de périphérique (Windows) » page 107
- « Procédure de téléchargement de pilotes de périphérique (Linux) » page 108

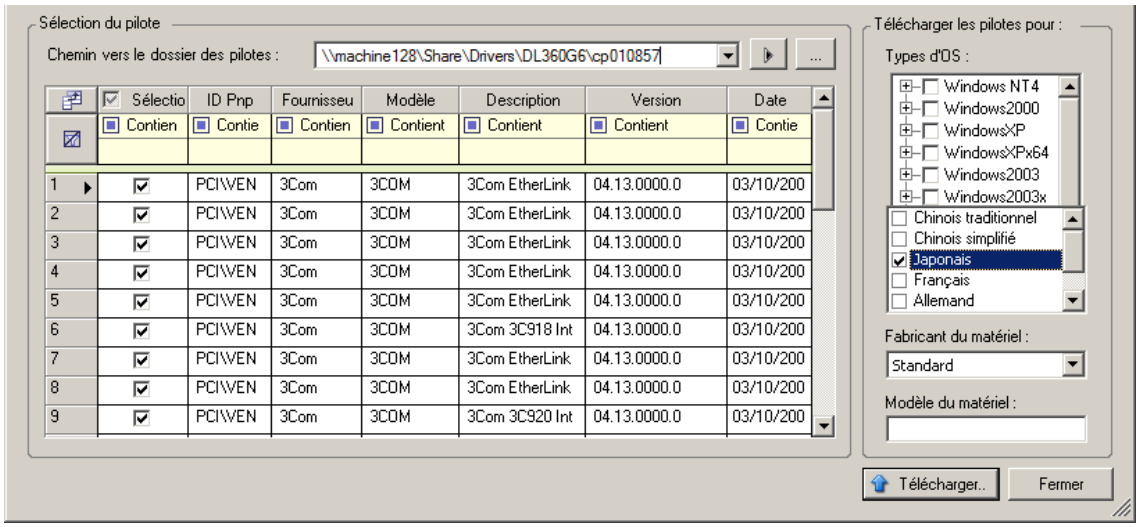
Procédure de téléchargement de pilotes de périphérique (Windows)

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 workloads Windows ».
2. Connectez-vous en tant qu'administrateur à l'hôte du serveur PlateSpin.
3. Lancez l'outil Gestionnaire de pilotes PlateSpin. Accédez au dossier `C:\Program Files\PlateSpin Protect Server\DriverManager`, puis lancez le programme `DriverManager.exe`.
4. Sélectionnez **Outils** > **Gérer les pilotes de périphérique**, puis cliquez sur l'onglet **Pilotes Windows**.



5. Au bas de la boîte de dialogue, cliquez sur **Télécharger les pilotes**.
6. Dans la boîte de dialogue Sélection du pilote, 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.



7 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.

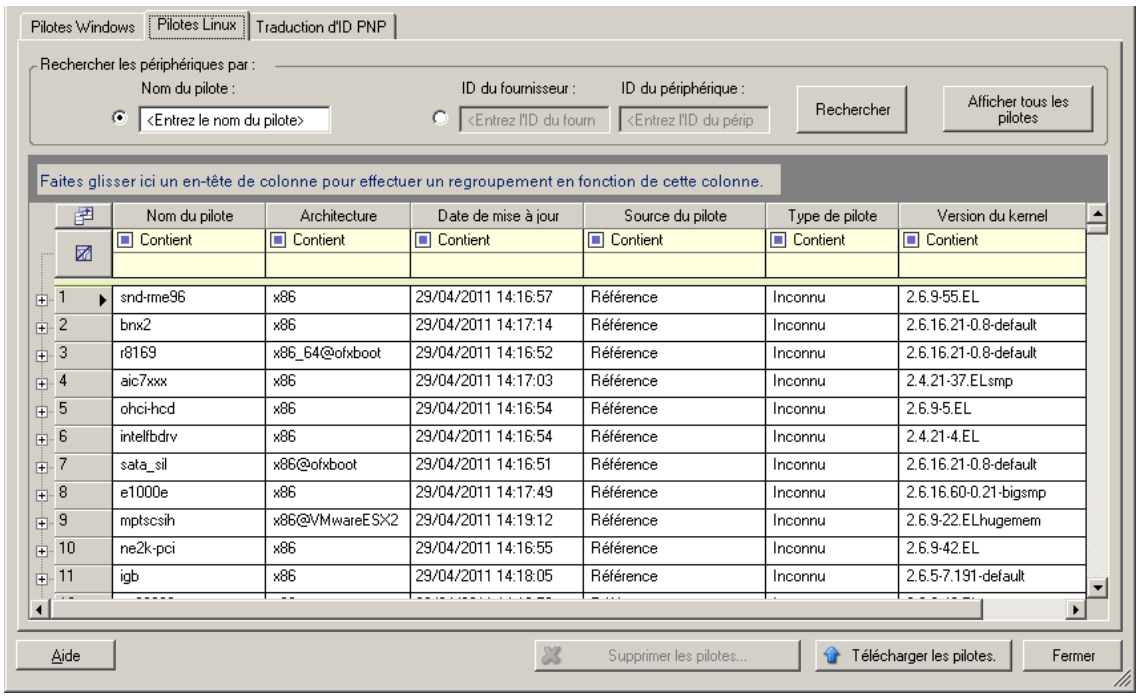
Procédure de téléchargement de pilotes de périphérique (Linux)

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 workloads Linux ».

2 Connectez-vous en tant qu'administrateur à l'hôte du serveur PlateSpin.

3 Lancez l'outil Gestionnaire de pilotes PlateSpin. Accédez au dossier `C:\Program Files\PlateSpin Protect Server\DriverManager`, puis lancez le programme `DriverManager.exe`.

4 Sélectionnez **Outils** > **Gérer les pilotes de périphérique**, puis cliquez sur l'onglet **Pilotes Linux**.



5 Au bas de la boîte de dialogue, cliquez sur **Télécharger les pilotes**.

6 Accédez au dossier contenant le paquetage de pilotes requis (`*.pkg`), puis cliquez sur **Télécharger tous les pilotes**.

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

11.2 Gestion des assignations d'ID PnP PlateSpin

« 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 (Linux RAM Disk, LRD) 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.

Vous (ou un technicien du support) pouvez utiliser l'option Traduction d'ID PNP dans l'outil de pilote de périphérique de PlateSpin pour ajouter, modifier ou supprimer des assignations d'ID PnP personnalisées.

Pour ajouter des assignations d'ID PnP personnalisées :

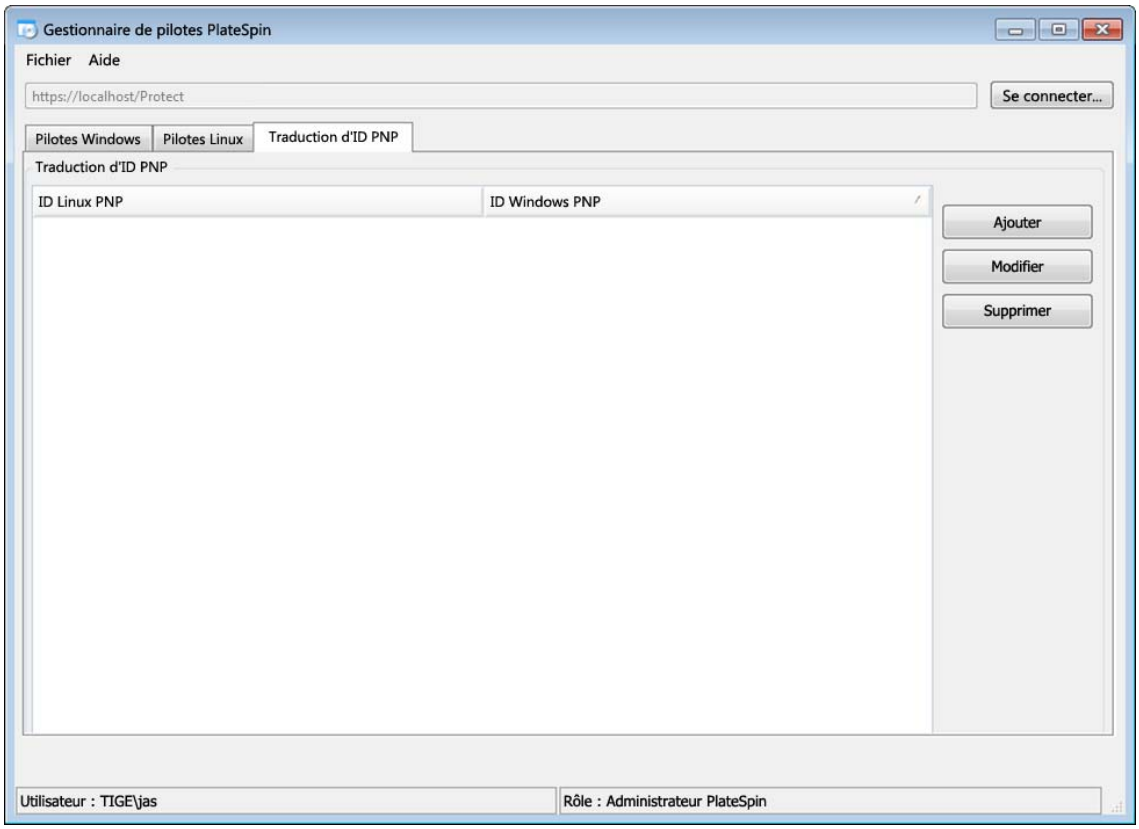
1 Connectez-vous en tant qu'administrateur à l'hôte du serveur PlateSpin.

2 Lancez l'outil Gestionnaire de pilotes PlateSpin. Accédez au dossier `C:\Program Files\PlateSpin Protect Server\DriverManager`, puis lancez le programme `DriverManager.exe`.

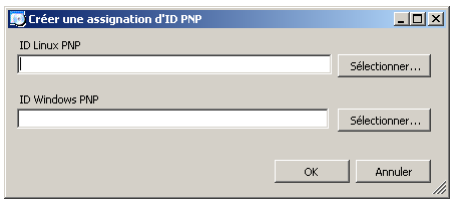
3 Connectez-vous au serveur PlateSpin.

`https://localhost/Protect`

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



5 Cliquez sur **Ajouter** dans la liste pour ouvrir la boîte de dialogue Créer une assignation d'ID PNP.



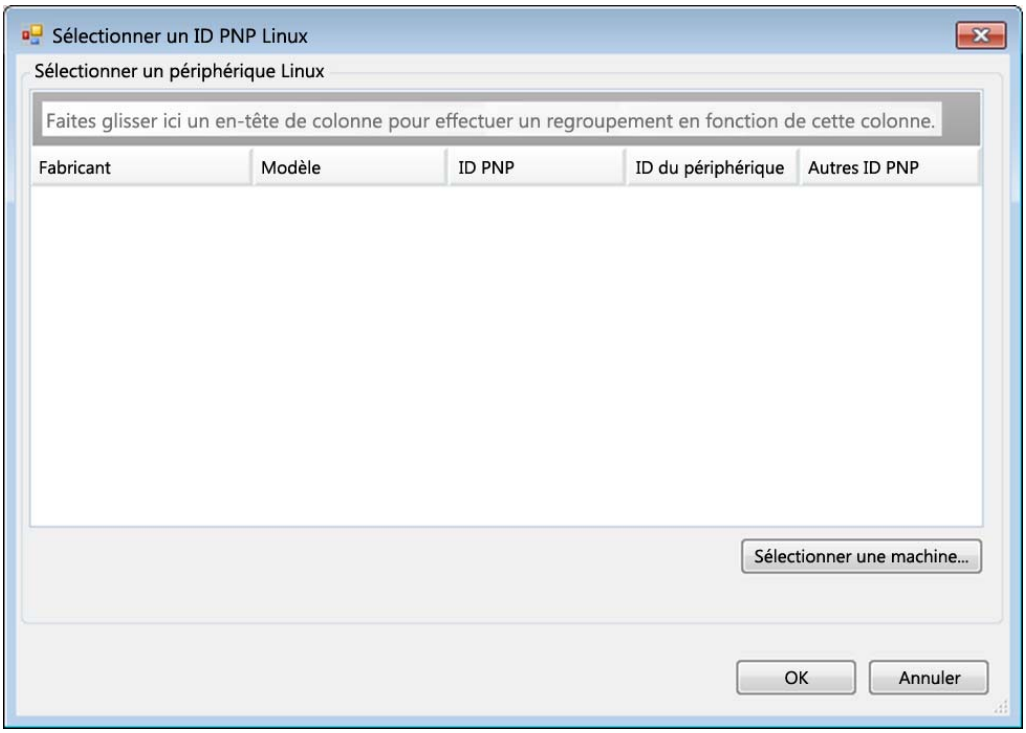
6 Ajoutez un ID PnP Linux dans le champ d'**ID PnP Linux**.

6a (Conditionnel) Entrez l'ID PnP Linux que vous souhaitez utiliser, si vous le connaissez.

ou

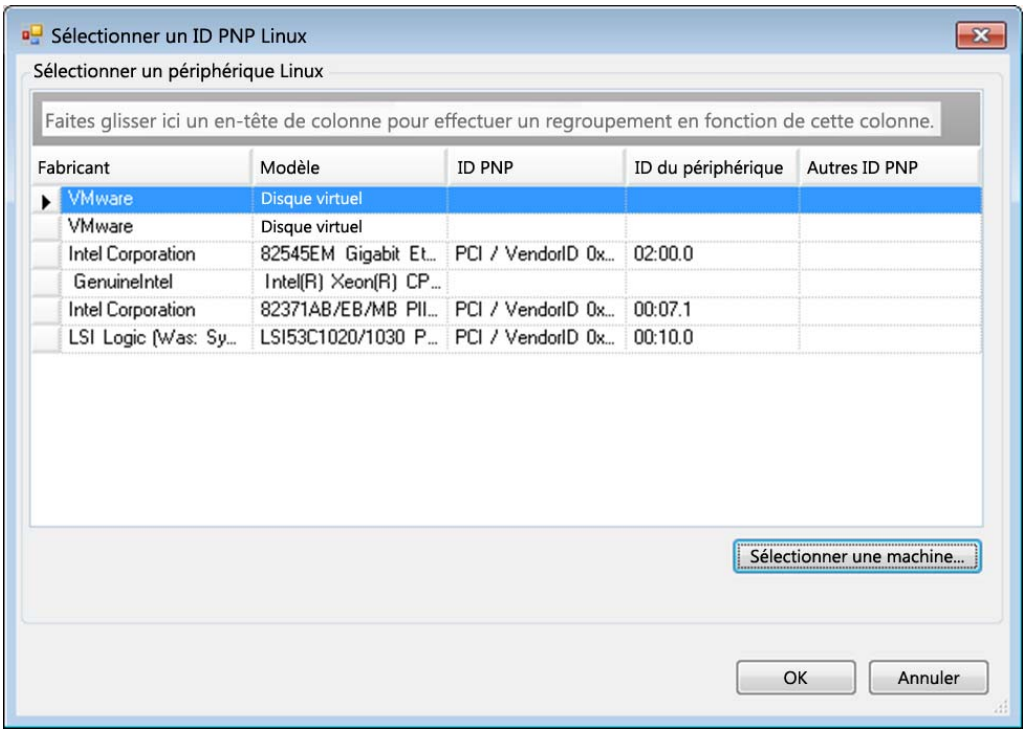
6b (Conditionnel) Sélectionnez un ID d'un workload découvert précédemment :

6b1 Cliquez sur **Sélectionner** en regard du champ **ID PnP Linux** pour ouvrir la boîte de dialogue Sélectionner un ID PNP Linux.



6b2 Dans la boîte de dialogue, cliquez sur l'option **Sélectionner une machine** pour afficher la liste des machines découvertes précédemment par le disque virtuel Linux PlateSpin.

6b3 Mettez en surbrillance l'un des périphériques de la liste, puis cliquez sur **Sélectionner** pour remplir la liste dans la boîte de dialogue Sélectionner un ID PNP Linux.



6b4 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 Créer une assignation d'ID PNP.

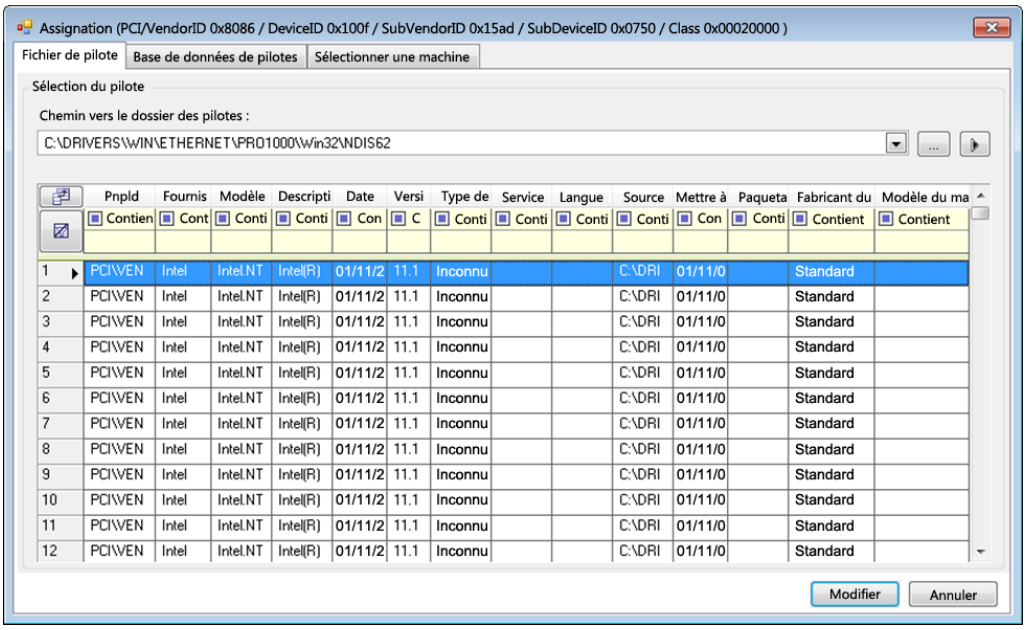
7 Ajoutez un ID PnP Windows dans le champ d'**ID PNP Windows**.

7a (Conditionnel) Entrez l'ID PnP Windows que vous souhaitez utiliser, si vous le connaissez.

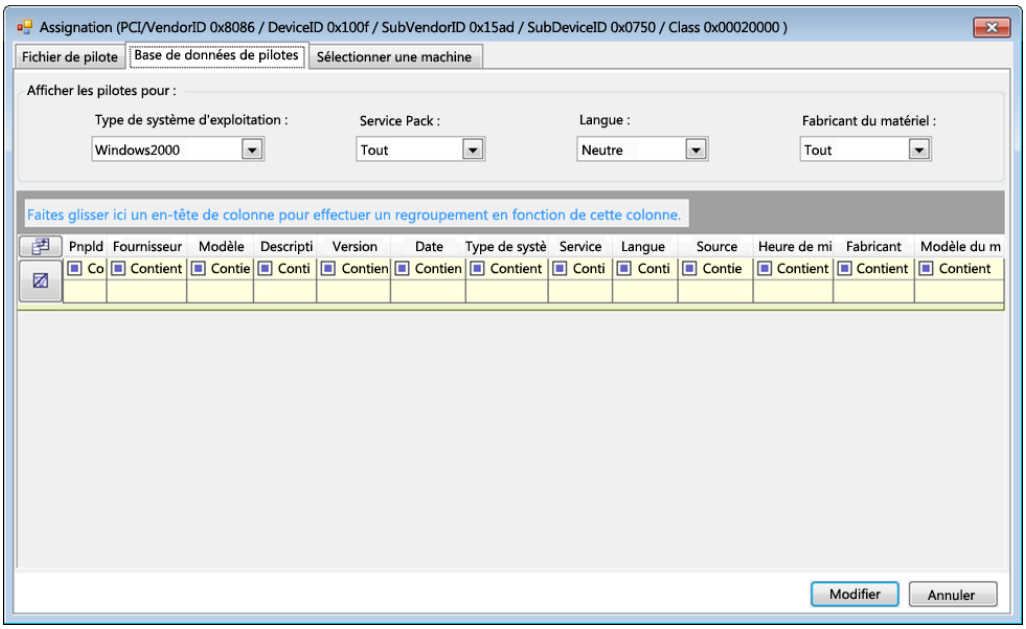
ou

7b (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 :

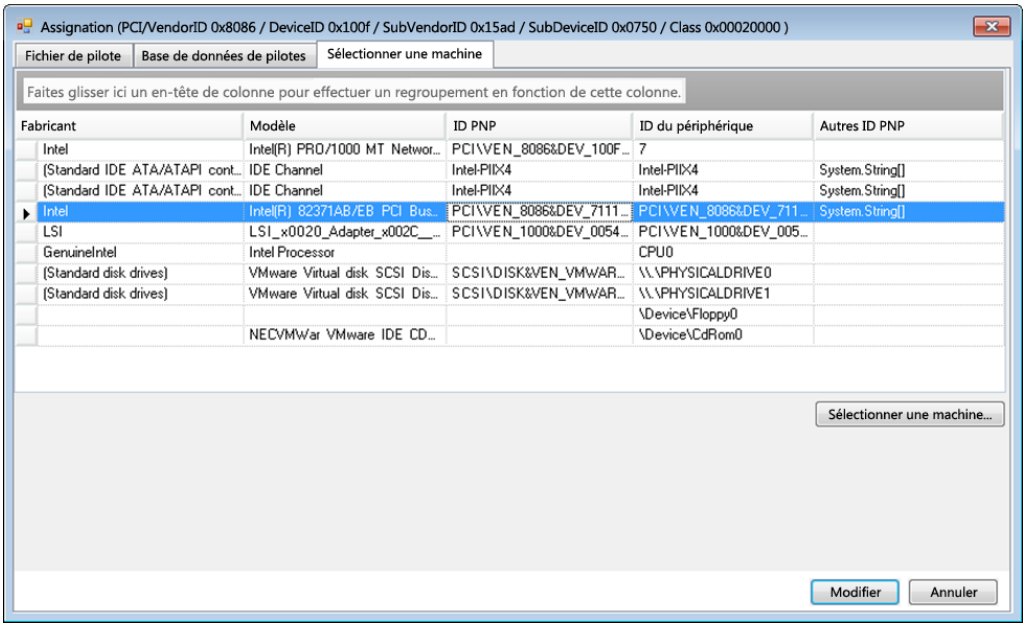
- Sous l'onglet **Fichier de pilote**, recherchez et sélectionnez un fichier de pilote Windows (c'est-à-dire un fichier portant l'extension `*.inf`), sélectionnez l'ID PnP de votre choix, puis cliquez sur **Modifier**.



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

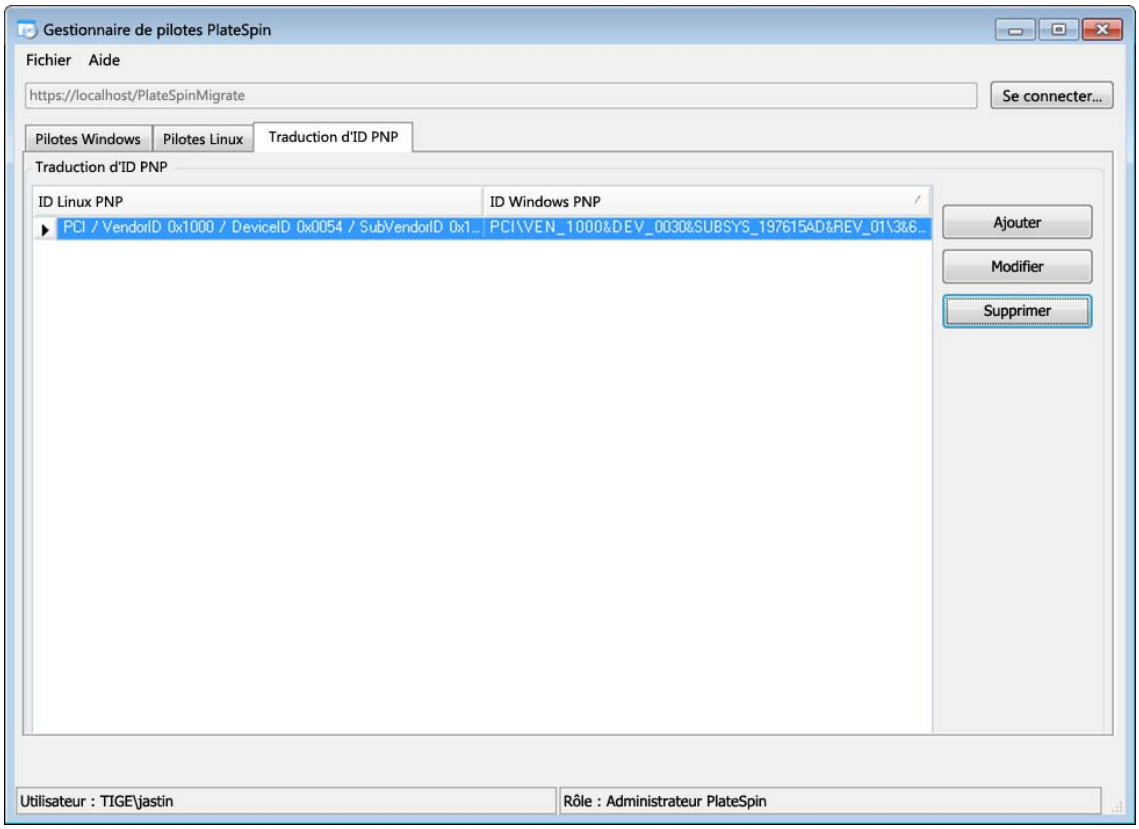


- Sous l'onglet **Sélectionner la machine**, cliquez sur **Sélectionner la machine**, puis dans la liste des machines Windows découvertes à l'aide de la découverte dynamique, sélectionnez une machine, cliquez sur **OK** pour en afficher les périphériques, sélectionnez l'ID PnP de votre choix et cliquez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

8 Dans la boîte de dialogue Créer 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.



9 (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 :

9a Cliquez sur **Modifier** pour ouvrir la boîte de dialogue Créer une assignation d'ID PNP.

9b Effectuez à nouveau l'Étape 7 page 112 pour modifier l'ID PnP Windows.

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

---

12 Préparation des workloads Linux pour la protection

Effectuez les tâches décrites dans cette section afin de préparer vos workloads Linux pour la protection dans PlateSpin Protect.

12.1 Vérification des pilotes par bloc pour Linux

Vérifiez qu'un module blkwatch est disponible pour la distribution Linux du workload. Pour obtenir la liste des pilotes préconfigurés, reportez-vous à la section « Distributions Linux prises en charge par Protect » page 137.

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 7005873 de la base de connaissances (https://www.netiq.com/support/kb/doc.php?id=7005873).

12.2 Préparation des instantanés pour le transfert par bloc (Linux)

Il est recommandé de préparer des instantanés pour le transfert des données par bloc. Assurez-vous que chaque groupe de volumes dispose de suffisamment d'espace libre pour accueillir les instantanés (au moins 10 % de la somme de toutes les partitions). Si les instantanés ne sont pas disponibles, PlateSpin Protect verrouille, puis libère chaque bloc un à un sur le workload source pour le transfert des données.

12.2.1 Configuration des instantanés LVM pour la réplication de volumes Linux

Le pilote `blkwatch` exploite les instantanés LVM s'ils sont disponibles. La copie de blocs à partir de l'instantané permet d'éviter d'éventuels conflits d'ouverture de fichiers.

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

12.2.2 Configuration d'instantanés NSS pour la réplication de réserves NSS

Pour les workloads Linux exécutant OES (Open Enterprise Server), la solution d'instantanés LVM n'est pas disponible pour les réserves NSS. Lors de la réplication de réserves NSS, PlateSpin Protect verrouille, puis libère chaque bloc un à un pour le transfert des données. Pour éviter d'éventuels conflits d'ouverture de fichiers et améliorer les performances de la réplication, vous pouvez exploiter des instantanés de réserve NSS.

Vous pouvez ajouter un disque unique non formaté que vous utilisez avec tous les instantanés de réserve NSS, ou vous pouvez ajouter un disque non formaté distinct pour chaque réserve NSS. Les meilleures performances sont obtenues lorsque vous ajoutez un disque distinct pour chaque réserve. Ajoutez le disque avant de configurer la protection de workload. Vous préparez le disque à utiliser et PlateSpin configurera les instantanés NSS pour la réserve lors de la réplication.

REMARQUE : par défaut, PlateSpin utilise le disque géré NLVM qui a le plus d'espace disponible (espace non partitionné) pour les instantanés de réserve NSS. Si vous constatez que les instantanés de réserve NSS pour la réplication sont situés sur le même disque que votre système de fichiers racine ou sur un autre disque qui recevra constamment des entrées/sorties, utilisez le fichier `/etc/platespin/platespin.conf` pour diriger les instantanés NSS sur un disque approprié.

Pour plus d'informations sur la manière dont les instantanés NSS fonctionnent sous OES, reportez-vous à la section « Guidelines for Using and Managing Pool Snapshots » (http://www.novell.com/documentation/oes2015/stor_nss_lx/data/br18up4.html) (Directives pour l'utilisation et la gestion des instantanés de réserve) du manuel *NSS File System Administration Guide for Linux* (Guide d'administration du système de fichiers NSS pour Linux).

Pour configurer un ou plusieurs disques à utiliser pour les instantanés de réserves NSS :

1. Sur le workload source OES, ajoutez un disque Linux non formaté à utiliser pour les instantanés de toutes les réserves NSS. Autre solution, vous pouvez créer un disque distinct pour chaque réserve NSS.

   La taille du disque doit correspondre environ à 20 % de la quantité de données utilisées dans la réserve NSS. Ajustez la taille en fonction de la quantité de modifications de données ou de leur croissance attendue pendant l'intervalle de réplication.

2. Pour chaque disque créé à l'Étape 1, initialisez le disque à gérer via NLVM.

   L'initialisation peut être effectuée à l'aide de NSSMU ou des commandes NLVM. Le format du périphérique peut être GPT ou DOS.

   - Pour utiliser NSSMU :
     1. Lancez l'utilitaire NSSMU, puis sélectionnez **Périphériques**.
     2. Sélectionnez le nouveau disque, puis appuyez sur F3 pour l'initialiser.
   - Pour utiliser les commandes NLVM :
     1. Sur la ligne de commande , entrez

        ```
        NLVM init <device_name> [format]
        ```

3 Il se peut que vous deviez spécifier le disque à utiliser pour les instantanés de chaque réserve NSS. Créez un fichier `platespin.conf` sur le workload source OES et associez les réserves NSS avec les nouveaux disques :

3a Dans un éditeur de texte, créez un fichier `/etc/platespin/platespin.conf`.

3b Pour chaque réserve NSS, ajoutez les informations de taille et de périphérique sous le paramètre `Customlocation` à l'aide de la syntaxe suivante :

```
[Customlocation] /dev/pool/
<nom_réserve>=<périphérique>:<taille_max_non_partitionnée_en_Mo>
```

Par exemple, spécifiez l'entrée suivante pour une réserve nommée `NSSPOOL` pour ajouter des instantanés sur le périphérique `sdc` avec une taille maximale de 12 228 Mo.

```
[Customlocation] /dev/pool/NSSPOOL=sdc:12288
```

4 Enregistrez le fichier.

5 Passez à la configuration de la protection pour le workload OES source.

12.3 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 169). 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`

13 Préparation de la protection des clusters Windows

PlateSpin Protect prend en charge la protection des services métiers d'une grappe (cluster) Microsoft Windows. Les systèmes d'exploitation de cluster Microsoft Windows pris en charge sont les suivants :

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2008 R2
- Windows Server 2003 R2

Pour plus d'informations, reportez-vous à la rubrique « Grappes » de la Section 1.1.1, « Workloads Windows pris en charge », page 14.

REMARQUE : le logiciel de gestion de clusters Windows contrôle le basculement et le rétablissement pour les ressources exécutées sur les noeuds de ses clusters. Ce document réfère à cette opération en tant que *basculement de noeud de grappe* ou *rétablissement de noeud de grappe*.

Le serveur PlateSpin contrôle le basculement et le rétablissement pour le workload protégé qui représente la grappe. Ce document réfère à cette opération en tant que *basculement PlateSpin* ou *rétablissement PlateSpin*.

13.1 Planification de la protection de workload de grappe

Lorsque la découverte de noeud actif est activée (valeur par défaut) pour l'environnement PlateSpin, la protection d'un cluster Windows s'effectue via des réplications incrémentielles des changements sur le noeud actif transmises en continu à une grappe virtuelle à noeud unique que vous pouvez utiliser pendant le dépannage de l'infrastructure source. Si vous désactivez la découverte de noeud actif, chaque noeud de cluster Windows peut être découvert et protégé en tant que noeud autonome.

Avant de configurer la protection des clusters Windows, assurez-vous que votre environnement répond aux conditions requises et que vous comprenez les conditions nécessaires à la protection des workloads de grappe.

13.1.1 Conditions requises pour la protection de grappes

L'étendue de la prise en charge de la protection des grappes est soumise aux conditions décrites dans le Tableau 13-1. Tenez compte de ces conditions lorsque vous configurez la protection de grappes dans votre environnement PlateSpin.

Tableau 13-1 *Conditions requises pour la protection de grappes*

Configuration requise	Description
Découvrir le noeud actif comme cluster Windows	Le paramètre de configuration globale de PlateSpin `DiscoverActiveNodeAsWindowsCluster` détermine si les clusters Windows sont protégés en tant que grappes ou en tant que machines autonomes distinctes : ◆ **True (Vrai - Valeur par défaut) :** le noeud actif est découvert en tant que cluster Windows. ◆ **False (faux) :** les noeuds individuels peuvent être découverts en tant que machines autonomes. Reportez-vous à la Section 13.2, « Configuration de la découverte des noeuds actifs Windows », page 127.
Valeurs de recherche de nom de ressource	Le paramètre de configuration globale de PlateSpin `MicrosoftClusterIPAddressNames` détermine les noms de ressources de grappes qui peuvent être découverts dans votre environnement PlateSpin. Vous devez configurer des valeurs de recherche qui aident à différencier le nom de la ressource partagée d'adresse IP de grappe du nom des autres ressources d'adresse IP sur la grappe. Reportez-vous à la Section 13.4, « Ajout de valeurs de recherche de nom de ressource », page 128.

Configuration requise	Description
Mode Cluster Windows	Le paramètre de configuration globale de PlateSpin `WindowsClusterMode` détermine la méthode de transfert de données par bloc pour les réplications incrémentielles : ◆ **Par défaut :** synchronisation sans pilote. ◆ **SingleNodeBBT :** transfert par bloc basé sur le pilote. Reportez-vous aux rubriques suivantes : ◆ « Transfert par bloc pour les grappes » page 123 ◆ « Configuration de la méthode de transfert par bloc pour les grappes » page 128
Nom d'hôte ou adresse IP du noeud actif	Vous devez indiquer le nom d'hôte ou l'adresse IP du noeud actif de la grappe lorsque vous effectuez une opération **Ajouter un workload**. Du fait des modifications de sécurité apportées par Microsoft, les clusters Windows ne peuvent plus être détectés en utilisant le nom du cluster virtuel (soit l'adresse IP de cluster partagé).
Nom d'hôte résolvable	Le serveur PlateSpin doit être en mesure de résoudre le nom d'hôte de chacun des noeuds de la grappe en fonction de leur adresse IP. **REMARQUE :** les recherches DNS directes et inverses sont requises pour résoudre le nom d'hôte par son adresse IP.
Ressource de quorum	une ressource de quorum d'une grappe doit être colocalisée sur le noeud avec le groupe de ressources (services) de la grappe qui est protégé.
Similarité des noeuds de grappe	Dans le mode Cluster Windows par défaut, la synchronisation sans pilote peut se poursuivre à partir de n'importe quel noeud qui devient actif si les noeuds sont similaires. S'ils ne correspondent pas, les réplications peuvent se produire uniquement sur le noeud actif découvert initialement. Reportez-vous à la section « Similarité de noeud de grappe » page 126.
PowerShell 2.0	Windows PowerShell 2.0 doit être installé sur chaque noeud de la grappe.

13.1.2 Transfert par bloc pour les grappes

Le transfert par bloc pour les grappes fonctionne différemment de celui des serveurs autonomes. La réplication initiale effectue une copie complète ou utilise une méthode de synchronisation sans pilote exécutée sur le noeud actif de la grappe. Les réplications incrémentielles suivantes peuvent utiliser une méthode sans pilote ou une méthode basée sur le pilote pour le transfert de données par bloc.

REMARQUE : PlateSpin Protect ne prend pas en charge le transfert basé sur des fichiers pour les grappes.

Le paramètre de configuration globale de PlateSpin `WindowsClusterMode` détermine la méthode de transfert de données par bloc pour les réplications incrémentielles :

- **Par défaut :** synchronisation sans pilote.
- **SingleNodeBBT :** transfert par bloc basé sur le pilote. À utiliser uniquement avec des SAN (sous-réseaux de stockage) Fibre Channel.

AVERTISSEMENT : n'essayez pas d'utiliser SingleNodeBBT sur des grappes avec des disques iSCSI partagés. Cela rend les grappes inutilisables.

Le Tableau 13-2 décrit et compare les deux méthodes.

Tableau 13-2 *Comparaison des méthodes de transfert de données par bloc pour la réplication incrémentielle*

Considérations	Transfert par bloc par défaut	Transfert par bloc à noeud unique
Méthode de transfert des données	Utilise la synchronisation sans pilote avec une réplication basée sur MD5 sur le noeud actuellement actif.	Utilise un pilote de transfert par bloc (Block-Based Transfer, BBT) installé sur le noeud actif découvert à l'origine.
Performances	Réplications incrémentielles potentiellement lentes.	Amélioration significative des performances pour les réplications incrémentielles.
Pilotes	◆ Aucun pilote BBT à installer. ◆ Aucun redémarrage requis sur les noeuds de grappe sources.	◆ L'utilitaire Protect Agent permet d'installer un pilote BBT sur le noeud actif de la grappe découvert à l'origine. ◆ Redémarrez le noeud pour appliquer le pilote. Cela lance un basculement vers un autre noeud de la grappe. Après le redémarrage, faites à nouveau du noeud découvert à l'origine le noeud actif. ◆ Pour que les réplications aient lieu et utilisent le transfert par bloc de noeud unique, le même noeud doit rester actif. ◆ Après avoir installé le pilote BBT, une réplication complète ou une réplication incrémentielle sans pilote doit avoir lieu avant que les réplications incrémentielles basée sur le pilote puissent commencer.
Clusters Windows pris en charge	Fonctionne avec n'importe quel cluster de serveur Windows pris en charge.	Fonctionne avec les clusters Windows Server 2008 R2 et versions ultérieures. Les autres clusters Windows pris en charge utilisent la méthode de synchronisation sans pilote pour la réplication.
Première réplication incrémentielle	Utilise la synchronisation sans pilote sur le noeud actif.	Utilise le transfert par bloc basé sur le pilote sur le noeud actif découvert à l'origine, si une réplication complète a été effectuée après l'installation du pilote BBT. Dans le cas contraire, il utilise la synchronisation sans pilote sur le noeud actif découvert à l'origine.

Considérations	Transfert par bloc par défaut	Transfert par bloc à noeud unique
Réplication incrémentielle suivante	Utilise la synchronisation sans pilote sur le noeud actif.	Utilise le transfert par bloc basé sur le pilote sur le noeud actif découvert à l'origine. Si une grappe bascule des noeuds, la méthode de synchronisation sans pilote est utilisée pour la première réplication incrémentielle après la réactivation du noeud actif à l'origine. Reportez-vous à la section « Impact du basculement de noeud de grappe sur la réplication » page 125.

13.1.3 Impact du basculement de noeud de grappe sur la réplication

Le Tableau 13-3 décrit l'impact du basculement de noeud de grappe sur la réplication et les opérations requises pour l'administrateur de PlateSpin Protect.

Tableau 13-3 *Impact du basculement de noeud de grappe sur la réplication*

Basculement ou rétablissement de noeud de grappe	Transfert par bloc par défaut	Transfert par bloc à noeud unique
Basculement de noeud de grappe lors de la première réplication complète	La réplication échoue. La première réplication complète doit aboutir et se terminer sans basculement de noeud de grappe. 1. Supprimez la grappe de PlateSpin Protect. 2. (Facultatif) Réactivez le noeud actif découvert à l'origine. 3. Ajoutez à nouveau la grappe en utilisant le noeud actif. 4. Exécutez à nouveau la première réplication complète.	

Basculement ou rétablissement de noeud de grappe	Transfert par bloc par défaut	Transfert par bloc à noeud unique
Basculement de noeud de grappe au cours d'une réplication complète ou incrémentielle ultérieure	La commande de réplication est annulée et un message s'affiche pour indiquer que la réplication doit être exécutée à nouveau. Si le profil du nouveau noeud actif est similaire à celui qui a échoué, le contrat de protection reste valide. 1. Exécutez à nouveau la réplication sur le noeud à présent actif. Si le profil du nouveau noeud actif n'est pas semblable à celui du noeud actif ayant échoué, le contrat de protection est valide uniquement sur le noeud actif à l'origine. 1. Réactivez le noeud actif découvert à l'origine. 2. Exécutez à nouveau la réplication sur le noeud actif.	La commande de réplication est annulée et un message s'affiche pour indiquer que la réplication doit être exécutée à nouveau. Le contrat de protection est valide uniquement sur le noeud actif découvert à l'origine. 1. Réactivez le noeud actif découvert à l'origine. 2. Exécutez à nouveau la réplication sur le noeud actif. Cette première réplication incrémentielle après un événement de basculement/ rétablissement de grappe utilise automatiquement la synchronisation sans pilote. Les réplications incrémentielles ultérieures utiliseront le pilote par bloc comme spécifié par le transfert par bloc à noeud unique.
Basculement de noeud de grappe entre les réplications	Si le profil du nouveau noeud actif est similaire à celui qui a échoué, le contrat de protection se poursuit comme prévu pour la réplication incrémentielle suivante. Dans le cas contraire, la commande de la prochaine réplication incrémentielle échoue. En cas d'échec d'une réplication incrémentielle planifiée : 1. Réactivez le noeud actif découvert à l'origine. 2. Exécutez une réplication incrémentielle.	La réplication incrémentielle échoue si le noeud actif change entre les réplications. 1. Veillez à ce que le noeud actif découvert à l'origine redevienne le noeud actif. 2. Exécutez une réplication incrémentielle. Cette première réplication incrémentielle après un événement de basculement/ rétablissement de grappe utilise automatiquement la synchronisation sans pilote. Les réplications incrémentielles ultérieures utiliseront le pilote par bloc comme spécifié par le transfert par bloc à noeud unique.

13.1.4 Similarité de noeud de grappe

Dans le mode Cluster Windows par défaut, les noeuds de grappe doivent avoir des profils similaires pour éviter les interruptions dans le processus de réplication. Les profils des noeuds de grappe sont considérés comme semblables si toutes les conditions suivantes sont remplies :

- Les numéros de série des volumes locaux (volume système et volume réservé au système) des noeuds doivent être identiques sur chaque noeud de grappe.

REMARQUE : employez l'utilitaire *Gestionnaire de volumes* personnalisé pour modifier les numéros de série des volumes locaux afin qu'ils correspondent à chaque noeud de la grappe. Reportez-vous à la section « Synchronisation des numéros de série sur le stockage local du noeud de grappe » page 141.

Si les volumes locaux sur chaque noeud de la grappe possèdent des numéros de série différents, vous ne pouvez pas exécuter de réplication après le basculement d'un noeud de grappe. Par exemple, pendant un basculement de noeud de grappe, le noeud actif, Noeud 1, échoue et le logiciel de la grappe fait du Noeud 2 le noeud actif. Si les unités locales sur les deux noeuds possèdent des numéros de série différents, la commande de la prochaine réplication du workload échoue.

- Les noeuds doivent avoir le même nombre de volumes.
- Chaque volume doit avoir exactement la même taille sur chaque noeud.
- Les noeuds doivent avoir le même nombre de connexions réseau.

13.1.5 Configuration de la protection

Pour configurer la protection d'un cluster Windows, suivez le flux de travail normal de la protection de workload. Veillez à bien spécifier le nom d'hôte ou l'adresse IP du noeud actif de la grappe. Reportez-vous à la section « Workflow de base pour la protection et la récupération de workload » page 37.

13.2 Configuration de la découverte des noeuds actifs Windows

Selon le paramètre de configuration globale de PlateSpin `DiscoverActiveNodeAsWindowsCluster`, vous pouvez découvrir les clusters Windows Server en tant que grappes ou en tant que machines autonomes individuelles.

Pour découvrir les clusters Windows en tant que grappes, définissez le paramètre `DiscoverActiveNodeAsWindowsCluster` sur `True` (Vrai). Ce mode correspond au paramétrage par défaut. La détection de grappe, l'inventaire et la protection de workload utilisent le nom d'hôte ou l'adresse IP du noeud actif d'une grappe, au lieu d'utiliser son nom de grappe et un partage administratif. Vous ne configurez pas de workloads distincts pour les noeuds non actifs de la grappe. Pour connaître les autres exigences de protection de workload de grappe, consultez la section « Conditions requises pour la protection de grappes » page 122.

Pour découvrir tous les clusters Windows en tant que machines autonomes individuelles, définissez le paramètre `DiscoverActiveNodeAsWindowsCluster` sur `False` (Faux). Ce paramètre permet au serveur PlateSpin de détecter tous les noeuds d'un cluster de basculement Windows comme des machines autonomes. Autrement dit, il inventorie le noeud actif et les noeuds non actifs d'un cluster comme un workload Windows régulier et sans lien avec le cluster.

Pour activer ou désactiver la détection de grappe :

1. Accédez à la page de configuration du serveur PlateSpin à l'adresse

   https://<*adresse-ip-serveur-platespin*>/PlateSpinConfiguration
2. Recherchez `DiscoverActiveNodeAsWindowsCluster`, puis cliquez sur **Éditer**.
3. Dans le champ **Valeur**, sélectionnez **True** pour activer la détection de grappe ou sélectionnez **False** pour désactiver la détection de grappe.
4. Cliquez sur **Enregistrer**.

13.3 Configuration de la méthode de transfert par bloc pour les grappes

Les réplications incrémentielles de clusters Windows peuvent utiliser une méthode sans pilote (valeur par défaut) ou une méthode basée sur le pilote (SingleNodeBBT) pour le transfert de données par bloc, en fonction du paramètre de configuration globale de PlateSpin `WindowsClusterMode`. Pour plus d'informations, reportez-vous à la section « Transfert par bloc pour les grappes » page 123.

Pour configurer WindowsClusterMode :

1. Accédez à la page de configuration du serveur PlateSpin à l'adresse

   https://<*adresse-ip-serveur-platespin*>/PlateSpinConfiguration
2. Recherchez `WindowsClusterMode`, puis cliquez sur **Éditer**.
3. Dans le champ **Valeur**, sélectionnez **Par défaut** pour utiliser la synchronisation sans pilote pour la réplication incrémentielle, ou sélectionnez **SingleNodeBBT** pour employer les pilotes par bloc pour la réplication incrémentielle.
4. Cliquez sur **Enregistrer**.

13.4 Ajout de valeurs de recherche de nom de ressource

Pour permettre d'identifier le noeud actif dans un cluster de basculement Windows, PlateSpin Protect doit faire la différence entre le nom de la ressource partagée d'adresse IP de grappe et les noms des autres ressources d'adresse IP sur la grappe. La ressource partagée d'adresse IP de grappe se trouve sur le noeud actif de la grappe.

Le paramètre global `MicrosoftClusterIPAddressNames` dans la page de configuration du serveur PlateSpin contient une liste de valeurs de recherche à utiliser pour la détection d'un workload de cluster Windows. Lorsque vous ajoutez un workload de cluster Windows, vous devez indiquer l'adresse IP du noeud actuellement actif du cluster. PlateSpin Protect recherche les noms des ressources d'adresse IP de la grappe sur ce noeud pour en trouver un qui *commence par* les caractères spécifiés de n'importe quelle valeur de la liste. Ainsi, chaque valeur de recherche doit contenir suffisamment de caractères pour différencier la ressource partagée d'adresse IP de grappe sur une grappe donnée, mais elle peut être assez courte pour s'appliquer à la détection dans d'autres clusters Windows.

Par exemple, une valeur de recherche `Clust IP Address` ou `Clust IP` correspond aux noms de ressource *Clust IP Address* pour 10.10.10.201 et *Clust IP Address* pour 10.10.10.101.

Le nom par défaut de la ressource partagée d'adresse IP de grappe est `Cluster IP Address` en anglais, ou l'équivalent si le noeud de grappe est configuré dans une autre langue. Les valeurs de recherche par défaut dans la liste `MicrosoftClusterIPAddressNames` incluent le nom de ressource `Cluster IP Address` en anglais et chacune des langues prises en charge.

Comme le nom de la ressource partagée d'adresse IP de grappe peut être configuré par l'utilisateur, vous devez ajouter d'autres valeurs de recherche à la liste, le cas échéant. Si vous modifiez le nom de ressource, vous devez ajouter une valeur de recherche liée à la liste `MicrosoftClusterIPAddressNames`. Par exemple, si vous indiquez un nom de ressource `Win2012-CLUS10-IP-ADDRESS`, vous devez ajouter cette valeur à la liste. Si vous disposez de plusieurs grappes utilisant la même convention de dénomination, une entrée `Win2012-CLUS` correspond à n'importe quel nom de ressource commençant par cette série de caractères.

Pour ajouter des valeurs de recherche dans la liste `MicrosoftClusterIPAddressNames` :

1. Accédez à la page de configuration du serveur PlateSpin à l'adresse https://<*adresse-ip-serveur-platespin*>/PlateSpinConfiguration
2. Recherchez `MicrosoftClusterIPAddressNames`, puis cliquez sur **Éditer**.
3. Dans le champ **Valeur**, ajoutez une ou plusieurs valeurs de recherche à la liste.
4. Cliquez sur **Enregistrer**.

13.5 Timeout d'arbitrage du quorum

Vous pouvez définir la clé de registre QuorumArbitrationTimeMax pour les clusters de basculement Windows Server dans votre environnement PlateSpin en utilisant le paramètre global `FailoverQuorumArbitrationTimeout` dans la page de configuration du serveur PlateSpin. Le timeout par défaut est 60 secondes, conformément à la valeur par défaut de Microsoft pour ce paramètre. Consultez la section *QuorumArbitrationTimeMax* (https://msdn.microsoft.com/en-us/library/aa369123%28v=vs.85%29.aspx?f=255&MSPPError=-2147217396) sur le site Web Microsoft Developer Network. L'intervalle de timeout spécifié est respecté pour l'arbitrage du quorum lors du basculement et du rétablissement.

Pour définir le timeout d'arbitrage du quorum pour tous les clusters de basculement Windows :

1. Accédez à la page de configuration du serveur PlateSpin à l'adresse https://<p*latespin-server-ip-address*>/PlatespinConfiguration
2. Recherchez `FailoverQuorumArbitrationTimeout`, puis cliquez sur **Éditer**.
3. Dans le champ **Valeur**, indiquez le nombre maximal de secondes à octroyer à l'arbitrage du quorum.
4. Cliquez sur **Enregistrer**.

13.6 Paramétrage des numéros de série des volumes locaux

Vous pouvez utiliser l'utilitaire *Gestionnaire de volumes* personnalisé pour modifier les numéros de série des volumes locaux afin qu'ils correspondent à chaque noeud de la grappe. Reportez-vous à la section « Synchronisation des numéros de série sur le stockage local du noeud de grappe » page 141.

13.7 Basculement PlateSpin

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

Pour effectuer le basculement PlateSpin (ou tester le basculement PlateSpin) sur un cluster Windows, celui-ci 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).

13.8 Rétablissement PlateSpin

Une opération de rétablissement PlateSpin nécessite une réplication complète pour les workloads de cluster Windows.

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

- Assignez tous les disques de la grappe PlateSpin virtuelle à un noeud 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 PlateSpin afin de restaurer le volume système de la machine de basculement sur le `Disque 1` et les autres disques de la machine de 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.

Après la fin d'un rétablissement PlateSpin, vous devez rattacher le stockage partagé et recréer l'environnement de grappe avant de pouvoir joindre à nouveau des noeuds supplémentaires à la grappe nouvellement restaurée.

REMARQUE : lorsque la grappe est dans la phase **Prêt pour la reprotection**, assurez-vous de commencer par reconstruire et restaurer la cible de rétablissement afin qu'elle soit découverte en tant que grappe. Vous devez désinstaller manuellement le pilote de grappe PlateSpin grappe au cours du processus de reconstruction.

Pour plus d'informations sur la reconstruction de l'environnement de grappe après un basculement et un rétablissement de PlateSpin, reportez-vous aux ressources suivantes :

- **Cluster de basculement Windows Server 2012 R2 (rétablissement vers une reconstruction physique ou virtuelle) :** reportez-vous à l'article 7016770 de la base de connaissances (http://www.netiq.com/support/kb/doc.php?id=7016770).
- **Cluster de basculement Windows Server 2008 R2 (rétablissement vers une reconstruction physique ou virtuelle) :** reportez-vous à l'article n° 7015576 de la base de connaissances (http://www.netiq.com/support/kb/doc.php?id=7015576).

---

14 Dépannage de la découverte et de l'inventaire de workloads

Cette section peut vous aider à résoudre les problèmes courants survenant lors de la découverte et de l'inventaire des workloads.

14.1 Dépannage de la découverte pour les workloads Windows

Les informations de cette section peuvent vous aider à résoudre les problèmes lors de la découverte et de l'inventaire de workloads Windows :

14.1.1 Problèmes courants et solutions

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`.

Problèmes ou messages	Solutions
`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 133. Si le test réussit, réessayez d'ajouter le workload. ◆ « Dépannage de la connectivité DCOM » page 134 ◆ « Dépannage de la connectivité du service RPC » page 134
`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 133. 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 pour {hostname} Échec de la 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 n° 7920339 de la base de connaissances (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 7920862 de la base de connaissances (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 134.
	◆ 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 Protect peut accéder à ces partages. Reportez-vous à la section « Activation des autorisations et de l'accès aux fichiers/partages » page 135.
	◆ 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.

14.1.2 Modification du délai de démarrage de la pulsation du contrôleur OFX

Pour éviter les échecs de découverte dus à des problèmes de minutage, un délai par défaut de 15 secondes (15 000 ms) est défini sur le contrôleur OFX pour le démarrage de la pulsation. Ce paramètre peut être configuré en ajoutant la clé de Registre `HeartbeatStartupDelayInMS` sur le workload source. Cette clé de Registre n'est pas configurée par défaut.

Pour activer un délai de pulsation d'une durée inférieure ou supérieure :

1. Sur le workload source, ouvrez l'éditeur du Registre de Windows.
2. Accédez à l'emplacement suivant dans l'éditeur du Registre, selon l'architecture du système d'exploitation sur le workload source :

   Chemin d'accès pour un workload source 64 bits :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PlateSpin\OperationsFramework\Controller
   ```

   Chemin d'accès pour un workload source 32 bits :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\PlateSpin\OperationsFramework\Controller
   ```

3. Ajoutez une clé nommée `HeartbeatStartupDelayInMS` de type `REG_SZ` et définissez sa valeur sur le nombre de millisecondes souhaité. Le paramètre par défaut doit être 15 000.

   ```
   REG_SZ: HeartbeatStartupDelayInMS Value: "15000"
   ```

4. Redémarrez le workload source.

14.1.3 Exécution des tests de connectivité

- « Test de connectivité réseau » page 133
- « Test de connectivité WMI » page 133
- « Dépannage de la connectivité DCOM » page 134
- « Dépannage de la connectivité du service RPC » page 134

Test de connectivité réseau

Effectuez ce test de connectivité réseau de base pour déterminer si 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 Protect et votre workload.

Dépannage de la connectivité DCOM

1 Connectez-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 une machine Windows 2000 Server, 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 Protect et le workload du même côté du pare-feu.
- Ouverture de ports spécifiques entre Protect et le workload (reportez-vous à la section « Conditions d'accès et de communication requises sur votre réseau de protection » page 31).

14.1.4 Désactivation du logiciel anti-virus

Le logiciel Anti-virus peut parfois bloquer certaines fonctionnalités de 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.

14.1.5 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, Protect utilise les partages administratifs du workload. Pour pouvoir fonctionner, 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 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.

14.2 Dépannage de la découverte pour les workloads 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 31.
`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 165.

14.3 Dépannage de la découverte pour les hôtes cibles

Problèmes ou messages	Solutions
Pour ESXi 4.1, des groupes de ports de machine virtuelle sont manquants dans la découverte d'hôte directe si des groupes de ports dvSwitch partagent le même nom.	Assurez-vous que les noms de groupes de ports sont uniques sur l'hôte VMware cible.

B Distributions Linux prises en charge par Protect

Le logiciel PlateSpin Protect intègre des versions précompilées du pilote `blkwatch` pour de nombreuses distributions Linux de non-débogage (32 et 64 bits).

B.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.

B.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).

B.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.

B.2 Pilotes blkwatch précompilés pour les distributions Linux

PlateSpin Protect fournit des pilotes blkwatch précompilés pour de nombreuses distributions Linux sans débogage. Vous pouvez effectuer une recherche dans la Liste des distributions afin de déterminer si la chaîne de version et l'architecture du kernel de votre workload Linux correspondent à une distribution prise en charge dans 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 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873). Les pilotes compilés automatiquement sont uniquement pris en charge pour les versions principale et secondaire du kernel Linux reprises dans la Listes des distributions, ou une version corrigée de celle-ci. Si les versions principale et secondaire du kernel dans la chaîne de version du kernel de votre workload Linux correspondent aux versions principale et secondaire d'un kernel dans la liste, votre pilote auto-compilé sera pris en charge.

- Section B.2.1, « Syntaxe des éléments de liste », page 138
- Section B.2.2, « Liste des distributions », page 138
- Section B.2.3, « Autres distributions Linux qui utilisent des pilotes blkwatch », page 138

B.2.1 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`

B.2.2 Liste des distributions

Pour connaître la liste des distributions de kernels prises en charge, consultez la « Liste des distributions » (https://www.netiq.com/documentation/platespin-protect-11-2-1/protect_user/data/blkwatch-drivers.html#blkwatch-dist-list) du *Guide de l'utilisateur de PlateSpin Protect*.

B.2.3 Autres distributions Linux qui utilisent des pilotes blkwatch

PlateSpin Protect prend en charge d'autres distributions Linux que celles répertoriées dans le Tableau B-1 si la distribution est basée sur une version prise en charge de Red Hat Enterprise Linux ou SUSE Linux Enterprise Server. Vous pouvez utiliser le pilote blkwatch précompilé pour la distribution Linux prise en charge.

Tableau B-1 *Prise en charge du pilote blkwatch pour d'autres distributions Linux*

Autre distribution Linux	Selon la version prise en charge pour RHEL ou SLES	Remarques
CentOS	Red Hat Enterprise Linux	
Open Enterprise Server (OES)	SUSE Linux Enterprise Server 11 SP 1 ou version ultérieure	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.
Oracle Linux (OL) (anciennement Oracle Enterprise Linux [OEL])	Red Hat Enterprise Linux	Les pilotes blkwatch sont disponibles pour le kernel et UEK (Unbreakable Enterprise Kernel) comme indiqué à la Section B.2.2, « Liste des distributions », page 138. Pour les autres distributions Linux d'Oracle, des pilotes précompilés sont disponibles uniquement pour le kernel Red Hat compatible correspondant (RHCK). Les workloads utilisant le kernel Oracle Linux Unbreakable Enterprise Kernel ne sont pas pris en charge dans PlateSpin Protect 11.2 ni dans les versions antérieures.

Pour connaître la liste des distributions de kernels prises en charge, consultez la « Liste des distributions » (https://www.netiq.com/documentation/platespin-protect-11-2-1/protect_user/data/blkwatch-drivers.html#blkwatch-dist-list) du *Guide de l'utilisateur de PlateSpin Protect*.

C Synchronisation des numéros de série sur le 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 les numéros de série sur le stockage local du noeud de grappe.

Pour télécharger et exécuter l'utilitaire :

1. Téléchargez le fichier `VolumeManager.exe` à partir de la page de téléchargement de PlateSpin Protect :
   - **1a** Accédez au site de téléchargement Micro Focus (https://www.microfocus.com/support-and-services/download/).
   - **1b** Sélectionnez PlateSpin Protect dans la liste **Parcourir par produit**, ou saisissez le nom du produit dans le champ **Parcourir par produit** pour rechercher le produit, puis sélectionnez-le.
   - **1c** Si la liste des versions est disponible, sélectionnez PlateSpin Protect 11.2.1.
   - **1d** Sur la page de présentation du téléchargement, cliquez sur **proceed to download** (Lancer le téléchargement), puis connectez-vous à l'aide de vos références de compte client.
   - **1e** Cliquez sur **accept** (Accepter) pour confirmer que vous acceptez la législation et la réglementation américaines en matière d'exportation.
   - **1f** Sur la page de téléchargement, cliquez sur **download** (Télécharger) en regard du fichier `VolumeManager.exe`, puis enregistrez-le.
2. Copiez le fichier téléchargé à un emplacement accessible sur chaque noeud de grappe.
3. 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 :

   ```
   Liste des volumes : ------------------- 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.
4. Vérifiez que tous les numéros de série de stockage local du noeud actif correspondent bien à ceux des autres noeuds de la grappe.
   - **4a** Sur chaque noeud de grappe, exécutez la commande `VolumeManager.exe -l` afin d'obtenir les numéros de série de volume correspondants.
   - **4b** Comparez les numéros de série de stockage local du noeud actif (Étape 3) à ceux du noeud (Étape 4a).

4c (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`

4d Après avoir modifié tous les numéros de série de volume d'un noeud de la grappe, vous devez redémarrer ce noeud.

4e Effectuez à nouveau la procédure de l'Étape 4a à l'Étape 4d pour chaque noeud de la grappe.

5 (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.

D Utilitaire Protect Agent

Protect Agent est un utilitaire de ligne de commande que vous pouvez utiliser pour installer, mettre à niveau, interroger ou désinstaller les pilotes de transfert par bloc.

Bien qu'un redémarrage soit toujours requis lors de l'installation, de la désinstallation ou de la mise à niveau des pilotes, cet utilitaire vous permet de mieux contrôler le moment où se produit l'opération et, par conséquent, le moment du redémarrage du serveur. Vous pouvez, par exemple, employer Protect Agent pour installer les pilotes pendant le temps hors service planifié, au lieu de le faire lors de la première réplication.

D.1 Utilisation de l'utilitaire Protect Agent pour Windows

Pour télécharger l'utilitaire Protect Agent pour Windows sur le workload source :

1. Connectez-vous à l'ordinateur Windows source en tant qu'administrateur.
2. Dans un navigateur Web, lancez l'interface Web et connectez-vous.
3. Cliquez sur l'onglet **Téléchargements**.
4. Cliquez sur le lien de l'application Protect Agent pour la plate-forme cible Windows, puis enregistrez le fichier compressé `ProtectAgent.cli.exe`.
5. Extrayez le contenu du fichier pour accéder au fichier exécutable.
6. (Facultatif) Affichez l'Aide de l'utilitaire Protect Agent en entrant :

   ```
   Protect.Agent.cli.exe -h
   ```

L'utilitaire est disponible sur l'hôte du serveur PlateSpin dans un fichier compressé. Extrayez le contenu du fichier pour accéder au fichier exécutable.

```
C:\Program Files\PlateSpin Protect Server\bin\ProtectAgent
```

Pour exécuter l'utilitaire Protect Agent pour Windows, utilisez la syntaxe suivante :

```
ProtectAgent.cli.exe {command} [command_option] [/psserver=%IP%]
```

Le Tableau D-1 décrit les commandes, l'option de commande et le paramètre disponibles pour la commande `ProtectAgent.cli.exe`.

Tableau D-1 *Commandes, option de commande et paramètre de l'utilitaire Protect Agent pour Windows*

Syntaxe	Description
Commandes	
`h |? | help`	Affiche la syntaxe et les options de la commande.

Syntaxe	Description
`logs|view-logs`	Ouvre le répertoire des journaux de l'application.

`status`
 	
`/status [/psserver=%IP%]`
	Affiche l'état d'installation du contrôleur et des pilotes PlateSpin sur ce workload.
	
	Si vous spécifiez le serveur PlateSpin, l'utilitaire recherche les mises à niveau de pilote à partir du serveur.

`din|driver-install`
 	
`/din [/psserver=%IP%]`
	Installe les pilotes PlateSpin.
	
	Si vous spécifiez le serveur PlateSpin, l'utilitaire recherche les mises à niveau de pilote à partir du serveur.

`dup|driver-upgrade`
 	
`/dup [/psserver=%IP%]`
	Met à niveau les pilotes PlateSpin.
	
	Si vous spécifiez le serveur PlateSpin, l'utilitaire recherche les mises à niveau de pilote à partir du serveur.

`dun|driver-uninstall`
 	
`[/dun /psserver=%IP%]`
	Désinstalle les pilotes PlateSpin.

`con | config`
 	
`/con /setting=<`*`nom_paramètre`*`>:<`*`valeur`*`>`
 	
Exemple :
 	
`ProtectAgent.cli.exe /config /setting=psserver:10.10.10.202`
	Indique le nom du paramètre et sa valeur à modifier dans le fichier de configuration sur ce workload.
	
	L'option `psserver` arrête le service du contrôleur OFX (`ofxcontroller`), modifie le fichier `OfxController.exe.config` en indiquant la nouvelle adresse IP et redémarre le service. Si vous modifiez l'adresse IP publique du serveur PlateSpin, vous devez exécuter cette commande sur chacun des workloads sources configurés pour le serveur.

Paramètre	
`/psserver=%IP%`	Télécharge les pilotes de transfert par bloc du serveur spécifié lorsque vous invoquez les options `status`, `driver-install` ou `driver-upgrade`.
Option de commande	

`setting`
 	
`/setting=<`*`nom_paramètre`*`>:<`*`valeur`*`>`
	Spécifie le nom du paramètre et la valeur du paramètre de configuration à modifier.
	
	Les noms de paramètre pris en charge sont les suivants :
	
	`psserver`
	`altAddress`
	`heartbeat`

D.2 Utilisation de l'utilitaire Protect Agent avec les pilotes de transfert par bloc

Une copie des pilotes de transfert par bloc est fournie avec l'utilitaire Protect Agent. Vous pouvez également spécifier le paramètre de ligne de commande `/psserver=` afin de télécharger les pilotes du serveur PlateSpin lorsque vous invoquez les options `status`, `driver-install` ou `driver-upgrade`. Cela se révèle particulièrement utile lorsqu'un nouveau paquetage de pilotes est appliqué comme correctif au serveur, mais pas à l'utilitaire de ligne de commande Protect Agent.

REMARQUE : pour éviter toute confusion, il est conseillé d'utiliser l'utilitaire Protect Agent pour installer, désinstaller ou mettre à niveau les pilotes, puis procéder à un redémarrage avant d'effectuer une réplication.

Il est conseillé de redémarrer le workload source chaque fois que vous installez, désinstallez ou mettez à niveau les pilotes. Le redémarrage force l'arrêt du pilote en cours d'exécution. Le nouveau pilote est alors appliqué au redémarrage du système. Si vous ne redémarrez pas le système avant d'effectuer une réplication, la source continue à se comporter comme si l'opération n'était pas terminée. Si, par exemple, vous installez des pilotes sans redémarrer le système, la source se comporte comme si aucun pilote n'avait été installé lors de la réplication. De même, si vous mettez à niveau les pilotes sans redémarrer le système, la source continue à utiliser le pilote en cours d'exécution lors de la réplication jusqu'au prochain redémarrage.

Si la version du pilote installé n'est pas la même que celle du pilote en cours d'exécution, l'option `status` rappelle à l'utilisateur qu'il doit redémarrer. Par exemple :

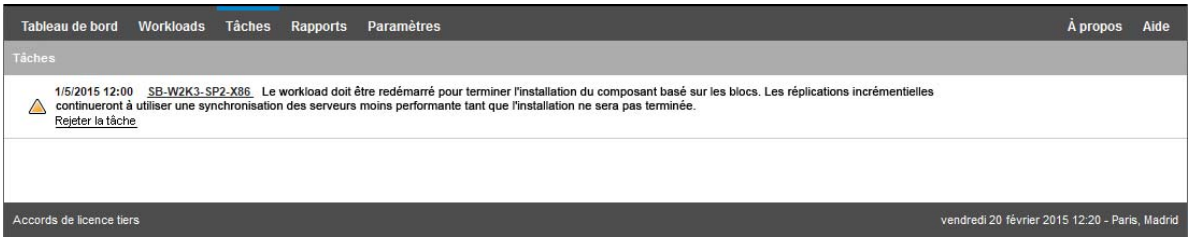
```
C:\ProtectAgent\ProtectAgent.cli.exe status
Step 1 of 2: Querying the PlateSpin controller service
   Done
Step 2 of 2: Querying the installed PlateSpin driver version
   Done

The task completed successfully
PlateSpin Controller Service Status
    Status: Running
    Version: 9.9.9.9
    Last Successful Contact: 1/5/2015 12:14:25 PM

PlateSpin Driver Status
    Installed Driver Version: 8.0.0.11
    Running Driver Version: Not running. Reboot to load the driver.
    Upgrade Available: No
```

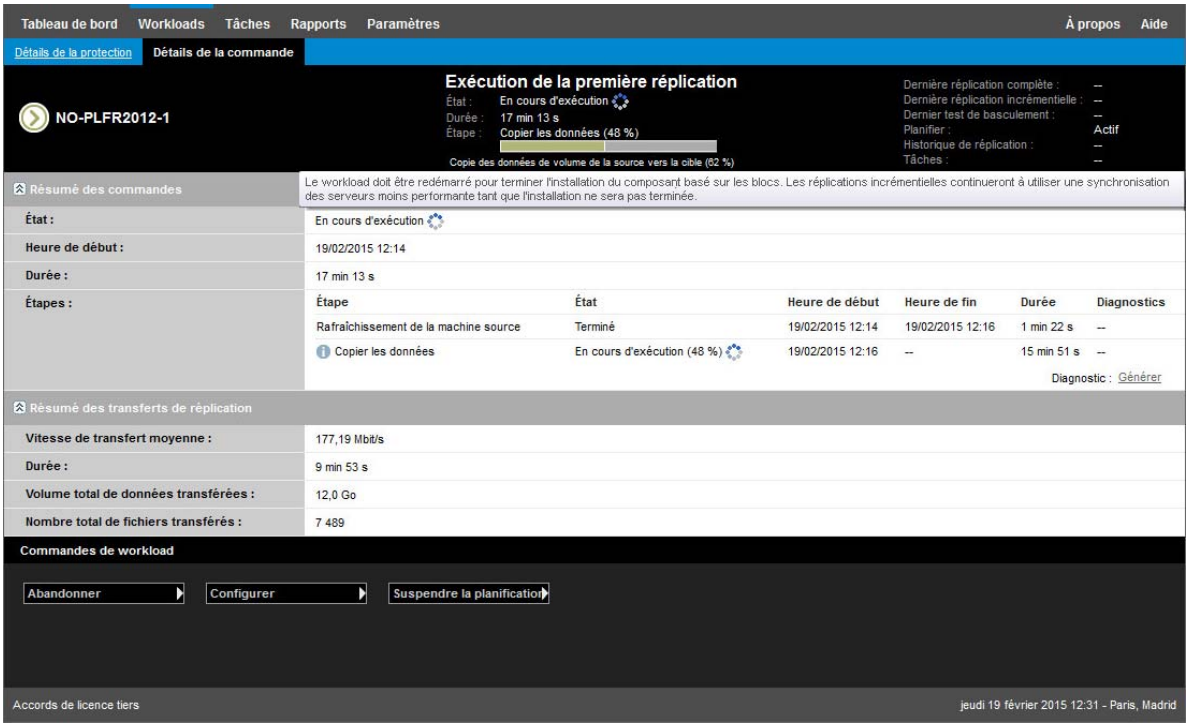
PlateSpin crée une tâche pour avertir l'utilisateur qu'un redémarrage est nécessaire pour terminer l'installation ou la mise à niveau du pilote. La notification apparaît dans la liste Tâches (Figure D-1).

Figure D-1 *Tâche de notification de redémarrage*



Au cours de la réplication, la notification apparaît dans la page Détails de la commande (Figure D-2).

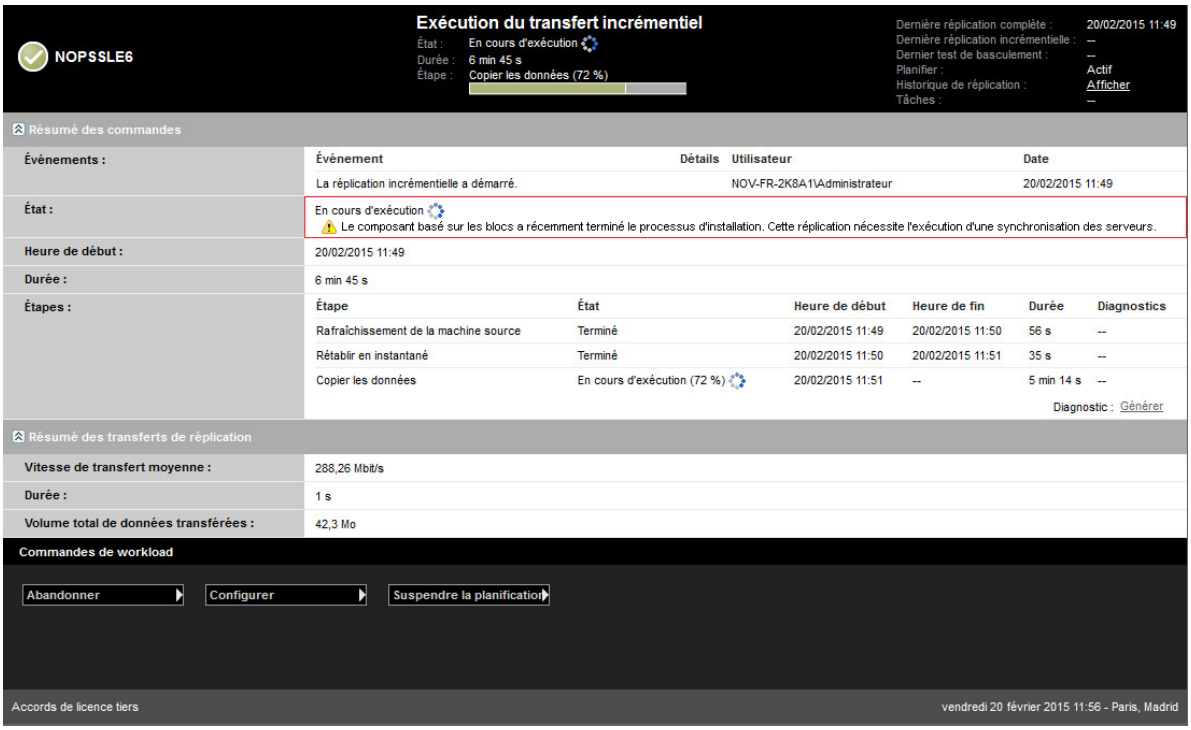
Figure D-2 *Notification de redémarrage pendant la réplication*



Le redémarrage de la machine source applique et démarre les pilotes installés ou mis à niveau. Si le pilote a été installé récemment, une réplication complète ou une réplication de synchronisation des serveurs est requise après le redémarrage afin de s'assurer que toutes les modifications d'une

source sont prises en compte. Cette réplication de synchronisation des serveurs sera présentée à l'utilisateur dans le champ État sous la forme d'un avertissement, comme le montre la Figure D-3. Les réplications incrémentielles suivantes s'exécuteront comme prévu, sans générer d'avertissement.

Figure D-3 *Notification de synchronisation des serveurs requise*



IV Protection des workloads

Une fois les cibles et les workloads découverts, vous pouvez préparer la protection en configurant des contrats de protection pour vos workloads.

15 Protection et reprise des charges de travail

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 le *workload de basculement*, est une machine virtuelle gérée par PlateSpin Protect qui reprend la fonction métier de votre workload de production en cas de perturbation au niveau du site de production.

15.1 Conditions préalables à la protection des workloads

Préparez vos conteneurs et workloads en vue de la protection. Reportez-vous à la Partie III, « Préparation des sources et des cibles de protection », page 93.

Dans un domaine Active Directory, suivez ces meilleures pratiques avant d'exécuter la première réplication complète :

- Veillez à mettre à jour Windows (exécutez Windows Update) sur votre workload source avant d'effectuer la première réplication complète.
- Veillez à configurer votre logiciel antivirus avec les exclusions de fichier et de dossier recommandées comme expliqué dans l'*article 822158 de la base de connaissances Microsoft : Recommandations d'analyse antivirus pour les ordinateurs d'entreprise qui exécutent des versions de Windows prises en charge* (https://support.microsoft.com/en-us/kb/822158).
- Si la machine Windows est un contrôleur de domaine, veillez à désactiver le logiciel antivirus sur le système pendant la réplication.

15.2 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 (Ajout d'un inventaire, Réplications initiales et en cours, Basculement, Rétablissement et Reprotection), le système lit les paramètres pertinents dans les

détails de protection. Reportez-vous à la « Workflow de base pour la protection et la récupération de workload » page 37. Cet ensemble de paramètres activés relatifs au cycle de vie complet de protection d'un workload est appelé *contrat de protection* du workload.

Pour configurer les détails de protection de votre workload :

1. Ajoutez un conteneur. Reportez-vous à la section « Ajout de conteneurs (cibles de protection) » page 96.
2. Ajoutez un workload. Reportez-vous à la section « Ajout de workloads (sources de protection) » page 100.
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 168.
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 168.

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

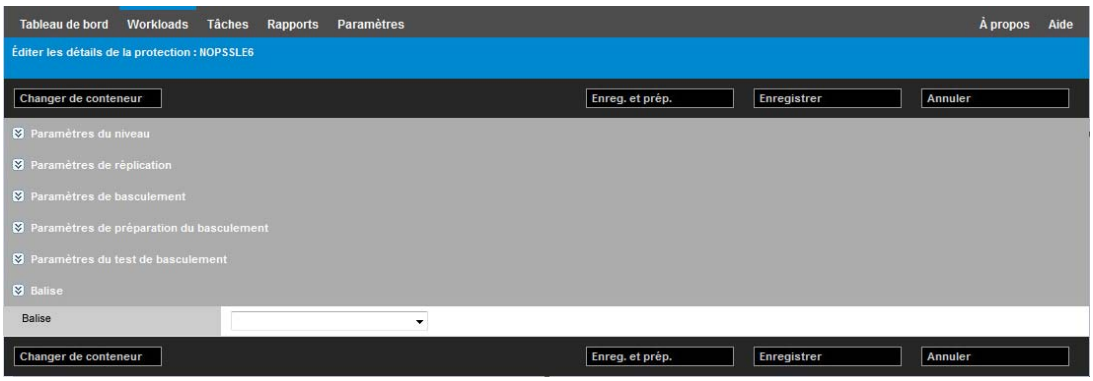
   ---
6. Configurez les détails de la protection dans chaque ensemble de paramètres en fonction de vos besoins en matière de continuité des opérations. Reportez-vous à la section « Détails de protection de workload » page 153.
7. Corrigez les erreurs de validation qu'affiche éventuellement l'interface Web PlateSpin Protect.
8. Cliquez sur **Save** (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 de prenne fin. Une fois terminé, un événement **La configuration du workload est terminée** s'affiche dans le tableau de bord.

15.2.1 Détails de protection de workload

Les détails de protection de workload sont représentés par cinq ensembles de paramètres, comme décrit dans le Tableau 15-1 :



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

Tableau 15-1 *Détails de protection de workload*

Réglages des paramètres	Détails
Paramètres du niveau	
Niveau de protection	Indiquez le niveau de protection assuré par la protection actuelle. Reportez-vous à la section « Niveaux de protection » page 166.
Paramètres de réplication	
Méthode de transfert	(Windows) Sélectionnez un mécanisme de transfert des données par fichier ou par bloc. Pour plus d'informations sur la réplication par bloc avec ou sans composants basés sur les blocs, reportez-vous à la section « Méthodes de transfert des données prises en charge » page 23. Pour activer le chiffrement, sélectionnez l'option **Chiffrer le transfert des données**. Reportez-vous à la section « Chiffrement des données lors d'une transmission » page 25.
Codage du transfert	(Linux) Pour activer le chiffrement, sélectionnez l'option **Coder le transfert des données.** Reportez-vous à la section « Chiffrement des données lors d'une transmission » page 25.
Références de la source	Indiquez les références requises pour accéder au workload. Reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 165.

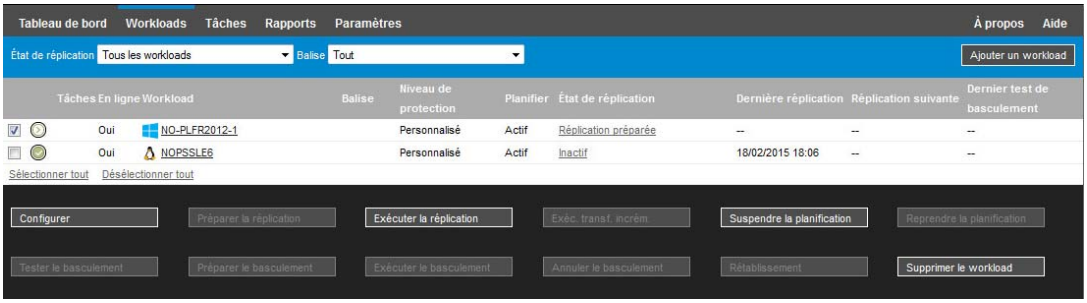
Réglages des paramètres	Détails
UC	(Conteneurs de machine virtuelle utilisant VMware 5.1, 5.5 et 6.0 avec un matériel de machine virtuelle de niveau 8 minimum) Indiquez le nombre de sockets, ainsi que le nombre de coeurs par socket pour le workload de basculement. Elle calcule automatiquement le nombre total de coeurs. Ce paramètre s'applique à la configuration initiale d'un workload avec une réplication initiale définie sur **Complète**. **REMARQUE :** le nombre maximal de coeurs que le workload peut utiliser est soumis à des facteurs externes tels que le système d'exploitation invité, la version du matériel de machine virtuelle, la licence VMware pour l'hôte ESXi et les ressources informatiques maximales de l'hôte ESXi pour vSphere (reportez-vous à la section *vSphere 5.1 Configuration Maximums (Configurations maximales pour vSphere 5.1)* (http://www.vmware.com/pdf/vsphere5/r51/vsphere-51-configuration-maximums.pdf)). Certaines distributions d'un système d'exploitation invité risquent de ne pas respecter la configuration des noyaux et des noyaux par socket. Par exemple, les systèmes d'exploitation invités SLES 10 SP4 et OES 2 SP3 conservent leurs paramètres de noyaux et de sockets d'origine, tels qu'installés, tandis que d'autres distributions SLES, RHEL et OES respectent la configuration.
Nombre de processeurs	(Conteneurs de machine virtuelle utilisant VMware 4.1) Spécifiez le nombre requis de vCPU (UC virtuelles) à assigner au workload de basculement. Ce paramètre s'applique à la configuration initiale d'un workload avec une réplication initiale définie sur **Complète**. Chaque vCPU est présentée au système d'exploitation invité sur le conteneur de machine virtuelle en tant que coeur unique, socket unique.
Réseau de réplication	Scindez le trafic de réplication en fonction des réseaux virtuels définis sur votre conteneur de machines virtuelles. Reportez-vous à la section « Réseautique » page 172. Pour ce paramètre, vous pouvez également spécifier une valeur MTU qui sera utilisée par le réseau de réplication LRD (Linux RAM Disk) PlateSpin Protect. La définition de cette valeur permet également d'éviter le phénomène de jabotage sur les réseaux (un VPN, par exemple) dont la valeur MTU est plus faible. La valeur par défaut est une chaîne vide (rien n'est indiqué dans la zone de texte). Lorsque la mise en réseau est configurée sur le disque LRD, cela permet au périphérique réseau de définir sa propre valeur par défaut (qui est généralement de 1500). Si vous saisissez une valeur, PlateSpin Protect ajuste la valeur MTU tout en configurant l'interface réseau.
Réseaux autorisés	Indiquez une ou plusieurs interfaces réseau (adresse IP ou de carte réseau) sur la source à utiliser pour le trafic de réplication.
Réserve de ressources pour la machine virtuelle cible	(Le conteneur de machines virtuelles fait partie d'une grappe DRS) Indiquez l'emplacement de la réserve de ressources dans laquelle la machine virtuelle de basculement doit être créée.
Dossier MV pour la machine virtuelle cible	(Le conteneur de machines virtuelles fait partie d'une grappe DRS) Indiquez l'emplacement du dossier de machines virtuelles dans lequel la machine virtuelle de basculement doit être créée.
Banque de données des fichiers de configuration	Sélectionnez une banque de données associée à votre conteneur de machines virtuelles pour stocker les fichiers de configuration des machines virtuelles. Reportez-vous à la section « Points de reprise » page 167.

Réglages des paramètres	Détails
Volumes protégés	Sélectionnez des volumes à protéger et assignez leurs répliques à des banques de données spécifiques de votre conteneur de machines virtuelles.
Disque léger	Sélectionnez cette option pour activer 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.
Volumes logiques protégés	(Linux) Indiquez un ou plusieurs volumes logiques LVM à protéger pour un workload Linux ou les réserves NSS sur un workload OES (Open Enterprise Server).
Stockage hors volume	(Linux) Indiquez une zone de stockage (telle qu'une partition d'échange) associée au workload source. Ce stockage est recréé dans le workload de basculement.
Groupes de volumes	(Linux) Indiquez les groupes de volumes LVM à protéger avec les volumes logiques LVM répertoriés dans la section Volumes logiques protégés des paramètres.
Services/daemons à arrêter pendant la réplication	Sélectionnez 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 169.
Paramètres de basculement	
Mémoire de la machine virtuelle	Indiquez la quantité de mémoire allouée au workload de basculement.
Hostname and Domain/Workgroup affiliation (Nom d'hôte et affiliation au domaine/groupe de travail)	Indiquez 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	Indiquez les paramètres LAN du workload de basculement. Reportez-vous à la section « Réseautique » page 172.
Serveurs DNS	Indiquez l'adresse IP du serveur DNS primaire ainsi qu'un autre serveur DNS (facultatif).
Services/Daemon States to Change (États des services/ daemons à modifier)	Indiquez 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 169.
Paramètres de préparation du basculement	
Réseau de basculement temporaire	Spécifiez les paramètres LAN temporaires du workload de basculement pendant l'opération facultative Préparer le basculement. Reportez-vous à la section « Réseautique » page 172.
Paramètres du test de basculement	
Mémoire de la machine virtuelle	Assignez la quantité de mémoire virtuelle requise au workload temporaire.
Nom d'hôte	Assignez un nom d'hôte au workload temporaire.
Domaine/groupe de travail	Affiliez 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	Indiquez les paramètres LAN du workload temporaire. Reportez-vous à la section « Réseautique » page 172.

Réglages des paramètres	Détails
Serveurs DNS	Indiquez l'adresse IP du serveur DNS primaire ainsi qu'un autre serveur DNS (facultatif).
Services/Daemon States to Change (États des services/ daemons à modifier)	Indiquez 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 169.
Balises	
Balise	(Facultatif) Assignez une balise à ce workload. Reportez-vous à la section « Ajout de balises à des workloads » page 101.

15.3 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 suivant les besoins ;
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.

15.4 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, telle que **Exécution du transfert incrémentiel**.

   L'interface Web affiche la page Détails de la commande correspondante :

3. Cliquez sur **Abandonner**.

15.5 Basculement

Lors d'une opération de *basculement*, le workload de basculement présent dans un conteneur de machines virtuelles PlateSpin Protect reprend la fonction métier d'un workload de production défaillant.

15.5.1 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 du niveau de protection de workload. Reportez-vous à la ligne « Paramètres du niveau » dans la section « Détails de protection de workload » page 153.

Si des notifications sont configurées avec des paramètres SMTP, PlateSpin Forge envoie simultanément une notification par message électronique aux destinataires spécifiés. Reportez-vous à la section « Configuration des services de notification par message électronique pour les événements et les rapports de réplication » page 67.

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 157), puis appliquez la commande **Exécuter le basculement**. Reportez-vous à la section « Exécution d'un basculement » page 158.

La Figure 15-1 représente la page Tableau de bord de l'interface Web de lorsqu'un échec de workload est détecté. Les tâches applicables s'affichent dans le volet des tâches et des événements.

Figure 15-1 *Page Tableau de bord en cas de détection d'un échec de workload (Workload hors ligne)*

15.5.2 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-vous au point « Paramètres de basculement » dans la section « Détails de protection de workload » page 153.

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 15-1.
- 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 167). 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 158.

15.5.3 Utilisation de la fonction Tester le basculement

PlateSpin Protect permet de tester la fonctionnalité de basculement et l'intégrité du workload de basculement. Pour ce faire, utilisez la commande **Tester le basculement**, laquelle démarre le workload de basculement dans un environnement réseau isolé pour tester la fonctionnalité du basculement et vérifier l'intégrité du workload de basculement.

Lorsque vous exécutez la commande, PlateSpin Protect applique au workload de basculement les paramètres du test de basculement tels qu'ils sont enregistrés dans les détails de protection de workload. Reportez-vous au point « Paramètres du test de basculement » dans la section « Détails de protection de workload » page 153.

Pour utiliser la fonction de test de basculement :

1. Définissez une fenêtre de temps appropriée pour les tests et assurez-vous 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 167), 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.

15.6 Rétablissement

Une opération de *rétablissement* permet de restaurer la fonction métier d'un workload de production défaillant dans son environnement d'origine, lorsque la fonction métier d'un workload de basculement temporaire n'est plus nécessaire. Le rétablissement constitue l'étape logique suivante après un basculement. Cette opération 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 Microsoft Hyper-V.

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

- Section 15.6.1, « Rétablissement automatisé sur une plate-forme VM », page 160
- Section 15.6.2, « Rétablissement semi-automatisé sur une machine physique », page 163
- Section 15.6.3, « Rétablissement semi-automatisé sur une machine virtuelle », page 163

15.6.1 Rétablissement automatisé sur une plate-forme VM

PlateSpin Protect prend en charge le rétablissement automatisé pour les conteneurs de rétablissement sur une grappe VMware DRS ou un serveur VMware ESXi pris en charge. Reportez-vous à la section « Conteneurs de VM pris en charge » page 17.

Pour effectuer un rétablissement automatisé d'un workload de basculement sur un conteneur VMware cible :

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

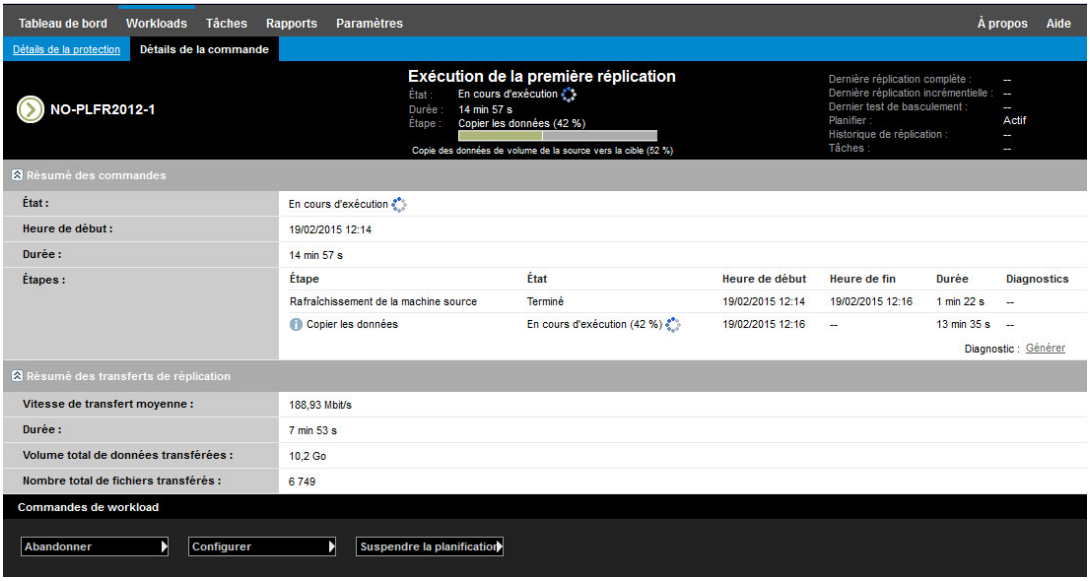
   Le système vous invite à effectuer les sélections suivantes :

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 165.
   - **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 168.
     - **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 161.
5. Cliquez sur **Enregistrer et rétablir** et surveillez la progression sur la page Détails de la commande. Reportez-vous à la Figure 15-2.

   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 .

Figure 15-2 *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. Reportez-vous au Tableau 15-2 pour plus d'informations sur les réglages des paramètres.

Tableau 15-2 *Détails du rétablissement (Workload sur VM)*

Réglages des paramètres	Détails
Paramètres de rétablissement	
Méthode de transfert	Sélectionnez un mécanisme de transfert des données ainsi qu'une sécurité par le biais du chiffrement. Reportez-vous à la section « Chiffrement des données lors d'une transmission » page 25.
Réseau de rétablissement	Indiquez le réseau à utiliser pour le trafic de rétablissement. Il s'agit d'un réseau spécifique basé sur les réseaux virtuels définis sur votre conteneur de machines virtuelles. Reportez-vous à la section « Réseautique » page 172.
Banque de données de VM	Sélectionnez une banque de données associée à votre conteneur de rétablissement pour le workload cible.
Assignation de volume	Si la méthode de réplication initiale est définie comme « Incrémentiel », sélectionnez des volumes sources et assignez-les à des volumes sur la cible de rétablissement en vue de la synchronisation.
Services/daemons à arrêter	Indiquez les services d'application (Windows) ou daemons (Linux) à arrêter automatiquement pendant le rétablissement. Reportez-vous à la section « Contrôle des services et des daemons » page 169.
Adresse alternative pour la source	Indiquez une adresse IP supplémentaire pour la machine virtuelle basculée, le cas échéant. Reportez-vous à la section « Exigences pour la protection sur des réseaux publics et privés via NAT » page 35.
Paramètres du workload	

Réglages des paramètres	Détails
UC	(Conteneurs de machine virtuelle utilisant VMware 5.1, 5.5 et 6.0 avec un matériel de machine virtuelle de niveau 8 minimum) Indiquez le nombre de sockets, ainsi que le nombre de coeurs par socket pour le rétablissement sur le workload virtuel. Elle calcule automatiquement le nombre total de coeurs. Ce paramètre s'applique à la configuration initiale d'un workload avec une réplication initiale définie sur **Complète**. **REMARQUE :** le nombre maximal de coeurs que le workload peut utiliser est soumis à des facteurs externes tels que le système d'exploitation invité, la version du matériel de machine virtuelle, la licence VMware pour l'hôte ESXi et les ressources informatiques maximales de l'hôte ESXi pour vSphere (reportez-vous à la section *vSphere 5.1 Configuration Maximums (Configurations maximales pour vSphere 5.1)* (http://www.vmware.com/pdf/vsphere5/r51/vsphere-51-configuration-maximums.pdf)). Certaines distributions d'un système d'exploitation invité risquent de ne pas respecter la configuration des noyaux et des noyaux par socket. Par exemple, les systèmes d'exploitation invités SLES 10 SP4 et OES 2 SP3 conservent leurs paramètres de noyaux et de sockets d'origine, tels qu'installés, tandis que d'autres distributions SLES, RHEL et OES respectent la configuration.
Nombre de processeurs	(Conteneurs de machine virtuelle utilisant VMware 4.1) Spécifiez le nombre requis de vCPU (UC virtuelles) à assigner au rétablissement sur le workload virtuel. Ce paramètre s'applique à la configuration initiale d'un workload avec une réplication initiale définie sur **Complète**. Chaque vCPU est présentée au système d'exploitation invité sur le conteneur de machine virtuelle en tant que coeur unique, socket unique.
Mémoire de la machine virtuelle	Assignez la quantité de mémoire virtuelle requise au workload cible.
Nom d'hôte, Domaine/groupe de travail	Spécifiez l'identité du workload cible et son affiliation à un domaine/groupe de travail. Pour l'affiliation au domaine, les références de l'administrateur du domaine sont requises.
Connexions réseau	Indiquez l'assignation réseau du workload cible sur la base des réseaux virtuels du conteneur de machines virtuelles sous-jacent.
États des services à modifier	Indiquez 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 169.
Paramètres de post-rétablissement	
Reprotéger le workload	Sélectionnez cette option si vous envisagez de recréer le contrat de protection pour le workload cible après le déploiement. Cette option 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 rétablissement terminé, une commande de **reprotection** est disponible dans l'interface Web de pour le workload basculé.
Aucune reprotection	Sélectionnez cette option si vous ne prévoyez pas 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.

15.6.2 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 172.
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 « Préparation des pilotes de périphérique pour les cibles de rétablissement physiques » page 105.
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 165).
   - **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 168.
     - **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.

15.6.3 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.

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

Vous pouvez également effectuer un rétablissement semi-automatisé pour les plates-formes de machine virtuelle cibles sur les hôtes Microsoft Hyper-V Server 2012.

Pour démarrer les machines virtuelles Hyper-V lors du basculement :

1. Dans un éditeur de texte, modifiez chaque fichier `/etc/vmware/config` de l'hôte Hyper-V en ajoutant la ligne suivante :

   ```
   vhv.allow = "TRUE"
   ```

2 Dans vSphere Web Client, modifiez les paramètres de machine virtuelle de basculement pour le processeur :

   2a Sous l'onglet **Virtual Hardware** (Matériel virtuel), sélectionnez **CPU** (UC).

   2b Dans **Hardware virtualization** (Virtualisation matérielle), sélectionnez **Expose hardware assisted virtualization to guest OS** (Exposer la virtualisation assistée du matériel au SE client).

3 Dans vSphere Web Client, modifiez les paramètres de machine virtuelle de basculement pour l'ID de processeur :

   3a Sous l'onglet **VM Options** (Options de machine virtuelle), développez **Advanced** (Avancé), puis sélectionnez **Edit configuration parameters** (Modifier les paramètres de configuration).

   3b Vérifiez le paramètre suivant :

   ```
   hypervisor.cpuid.v0 = FALSE
   ```

15.7 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 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 rétablissement. Reportez-vous à la section « Rétablissement » page 159.

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.

16 Notions fondamentales concernant la protection de workload

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

16.1 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 16-1 *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	Pour les machines membres du domaine : *autorité\principal*

À découvrir	Références	Remarques
Tous les workloads Linux	Nom d'utilisateur et mot de passe de niveau racine	Les comptes non root ne sont pas correctement configurés pour utiliser sudo. Reportez-vous à l'article 7920711 de la base de connaissances (https://www.netiq.com/support/kb/doc.php?id=7920711).
Hôte VMware ESX ou ESXi	Compte VMware avec configuration de rôle appropriée. Pour définir des rôles pour la mutualisation de la protection, reportez-vous à la section « Définition de rôles VMware pour la mutualisation » page 57.	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. Pour définir des rôles pour la mutualisation de la protection, reportez-vous à la section « Définition de rôles VMware pour la mutualisation » page 57.	

16.2 Niveaux de protection

Un niveau de protection est une collection personnalisée 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.

Pour créer des niveaux de protection personnalisés à l'avance :

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

Paramètre	Opération
Nom	Saisissez le nom que vous souhaitez utiliser pour le niveau.

Paramètre	Opération
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 29. 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 30. 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 167.
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.

16.3 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.

16.4 Méthode de réplication initiale (totale et incrémentielle)

La *réplication initiale* consiste en la création d'une copie de base initiale d'un workload de production sur le workload de basculement (réplique virtuelle) dans le cadre d'une opération de protection, ou d'un workload de basculement sur son infrastructure physique ou virtuelle d'origine en vue d'une opération de rétablissement pour le workload de production.

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.

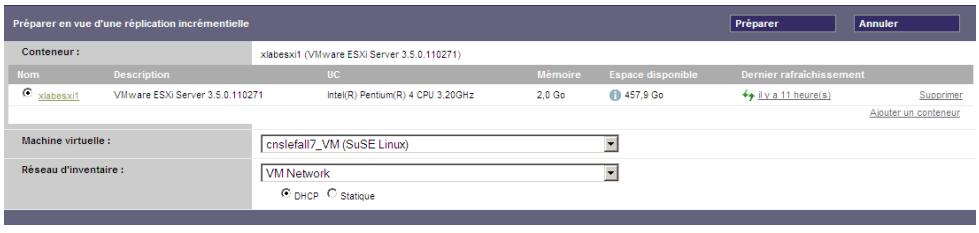
- **Complète :** l'ensemble des données du workload sont transférées.
- **Incrémentielle :** seules les différences sont transférées depuis une source vers sa cible, à condition qu'elles aient un système d'exploitation et des profils de volume similaires.
  - **Au cours de la protection :** le workload 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.
  - **Au cours du rétablissement vers une machine virtuelle :** le workload de basculement est comparé à une machine virtuelle existante 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 (voir la section « Rétablissement semi-automatisé sur une machine physique » page 163).

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.

Pour configurer la méthode de réplication initiale :

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 affiche la page Préparer en vue d'une réplication incrémentielle.



4. Sélectionnez le conteneur requis, la machine virtuelle et le réseau 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 pour 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.

16.5 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 119.
- **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.

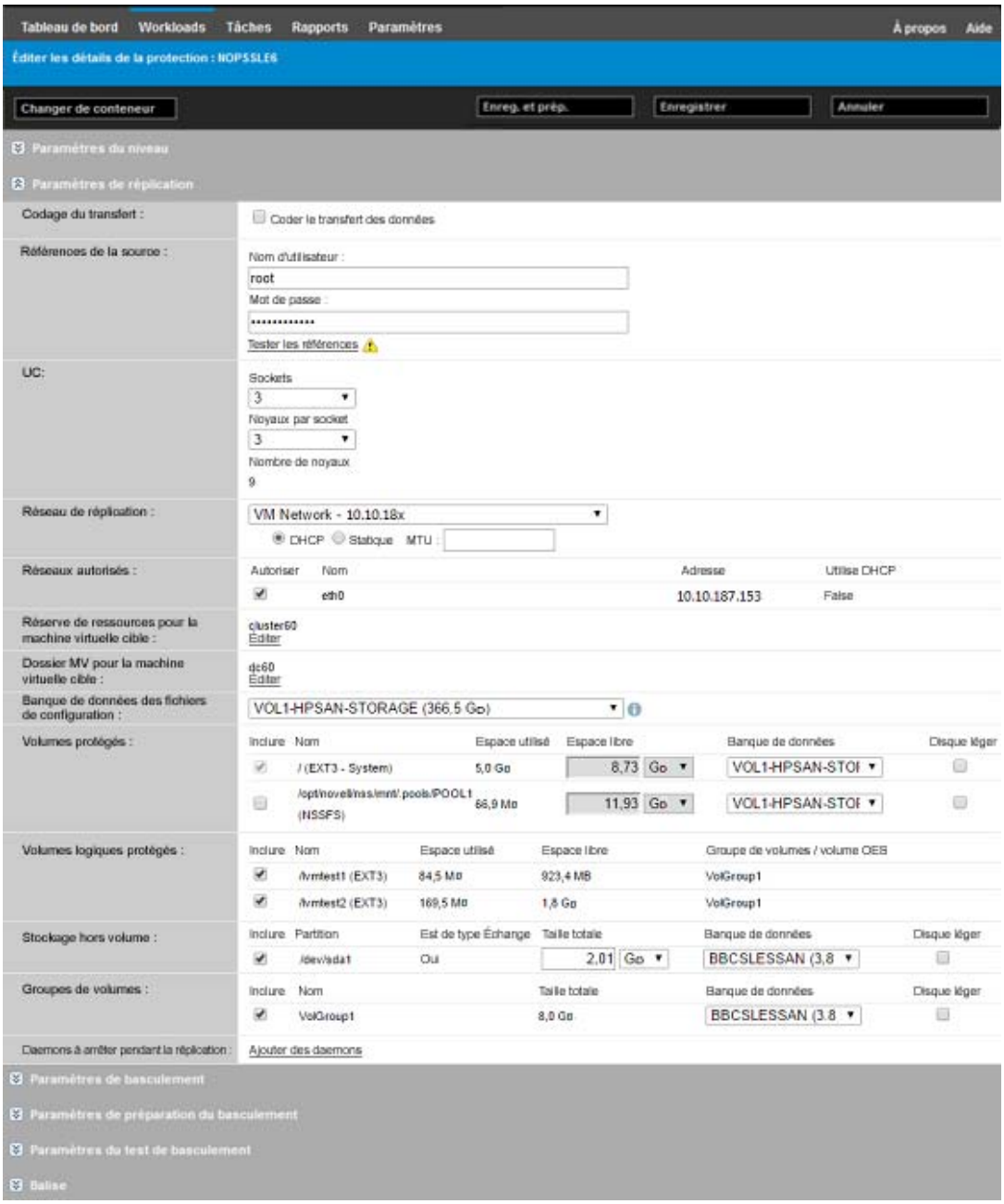
  Les services courants auxquels vous souhaiterez peut-être assigner un état de démarrage `désactivé` sont des services spécifiques au fournisseur liés à leur infrastructure physique sous-jacente et qui ne sont pas requis dans une machine virtuelle.

16.6 Stockage des volumes

Lors de l'ajout d'un workload à protéger, établit l'inventaire du support de stockage de votre workload source et configure automatiquement les options dans l'interface Web de PlateSpin Protect pour vous permettre de spécifier les volumes nécessitant une protection. Pour plus d'informations, reportez-vous à la Section 1.1.5, « Stockage pris en charge », page 21.

La Figure 16-1 affiche l'ensemble des paramètres de réplication pour un workload Linux avec plusieurs volumes et deux volumes logiques dans un groupe de volumes.

Figure 16-1 *Volumes, volumes logiques et groupes de volumes d'un workload Linux protégé*



La Figure 16-2 affiche les options de protection de volume d'un workload OES 11 avec des options indiquant que la disposition du volume LVM2 et de la réserve NSS doit être préservée et recréée pour le workload de basculement :

Figure 16-2 *Paramètres de réplication, options de volume (workload OES 11)*

La Figure 16-3 affiche les options de protection de volume d'un workload OES 2 avec des options indiquant que la disposition des réserves EVMS et NSS doit être préservée et recréée pour le workload de basculement :

Figure 16-3 *Paramètres de réplication, options de volume (workload OES 2)*

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

16.8 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 OFX de démarrage PlateSpin.

- Section 16.8.1, « Téléchargement de l'image ISO OFX de démarrage PlateSpin », page 172
- Section 16.8.2, « Insertion de pilotes de périphérique supplémentaires dans l'image ISO de démarrage », page 173
- Section 16.8.3, « Enregistrement de machines physiques en tant que cibles de rétablissement avec PlateSpin Protect », page 174

16.8.1 Téléchargement de l'image ISO OFX de démarrage PlateSpin

Vous pouvez télécharger les images ISO OFX de démarrage PlateSpin (`bootofx.x2p.iso` pour les cibles basées sur le microprogramme BIOS et celles basées sur le microprogramme UEFI) à partir de la page de téléchargement du logiciel PlateSpin Protect.

1. Accédez au site de téléchargement Micro Focus (https://www.microfocus.com/support-and-services/download/).
2. Sélectionnez PlateSpin Protect dans la liste **Parcourir par produit**, ou saisissez le nom du produit dans le champ **Parcourir par produit** pour rechercher le produit, puis sélectionnez-le.
3. Sur la page de présentation du téléchargement, cliquez sur **proceed to download** (Lancer le téléchargement), puis connectez-vous à l'aide de vos références de compte client.
4. Cliquez sur **accept** (Accepter) pour confirmer que vous acceptez la législation et la réglementation américaines en matière d'exportation.
5. Sur la page de téléchargement, cliquez sur **download** (Télécharger) en regard du fichier `bootofx.x2p.iso`, puis enregistrez-le.

16.8.2 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.

Pour utiliser cet utilitaire :

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 n° 7005990 de la base de connaissances (https://www.netiq.com/support/kb/doc.php?id=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`	Employée 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.

Argument	Description
`-c <chemin>`	<*chemin*> indique l'emplacement où réside un fichier `ConfigureTakeControl.xml`.

`-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
  ```

16.8.3 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
   ```

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 invité 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.

16.9 Protection des grappes Windows

PlateSpin Protect prend en charge la protection des services métiers d'un cluster Microsoft Windows Server. Pour plus d'informations sur la configuration requise et les options de protection des noeuds d'un cluster Windows Server, reportez-vous au Chapitre 13, « Préparation de la protection des clusters Windows », page 121.

16.9.1 Basculement PlateSpin

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

Pour effectuer le basculement PlateSpin (ou tester le basculement PlateSpin) sur un cluster Windows, celui-ci 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).

16.9.2 Rétablissement PlateSpin

Une opération de rétablissement PlateSpin nécessite une réplication complète pour les workloads de cluster Windows.

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

- Assignez tous les disques de la grappe PlateSpin virtuelle à un noeud 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 PlateSpin afin de restaurer le volume système de la machine de basculement sur le `Disque 1` et les autres disques de la machine de 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.

Après la fin d'un rétablissement PlateSpin, vous devez rattacher le stockage partagé et recréer l'environnement de grappe avant de pouvoir joindre à nouveau des noeuds supplémentaires à la grappe nouvellement restaurée.

REMARQUE : lorsque la grappe est dans la phase **Prêt pour la reprotection**, assurez-vous de commencer par reconstruire et restaurer la cible de rétablissement afin qu'elle soit découverte en tant que grappe. Vous devez désinstaller manuellement le pilote de grappe PlateSpin grappe au cours du processus de reconstruction.

Pour plus d'informations sur la reconstruction de l'environnement de grappe après un basculement et un rétablissement de PlateSpin, reportez-vous aux ressources suivantes :

- **Cluster de basculement Windows Server 2012 R2 (rétablissement vers une reconstruction physique ou virtuelle) :** reportez-vous à l'article 7016770 de la base de connaissances (http://www.netiq.com/support/kb/doc.php?id=7016770).
- **Cluster de basculement Windows Server 2008 R2 (rétablissement vers une reconstruction physique ou virtuelle) :** reportez-vous à l'article n° 7015576 de la base de connaissances (http://www.netiq.com/support/kb/doc.php?id=7015576).

---

17 Création de rapports

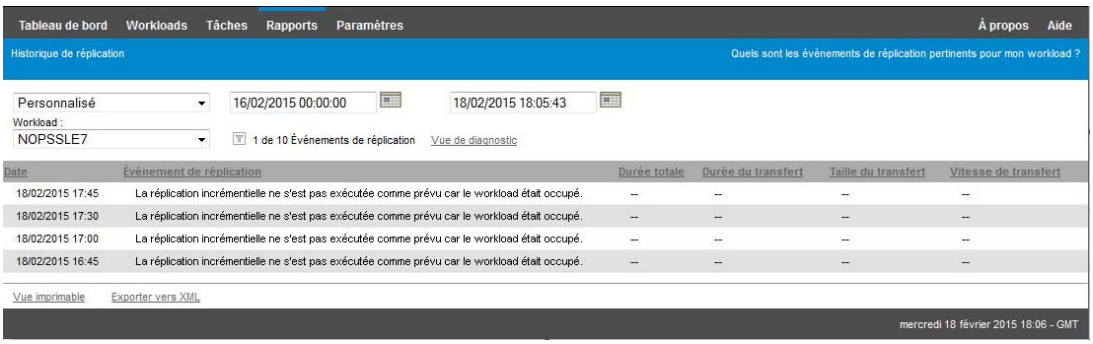
L'interface Web de PlateSpin permet de générer des rapports à propos des workloads découverts et des contrats de protection de workload. Pour plus d'informations sur la génération d'un rapport sur les licences, reportez-vous à la Section 4.6, « Génération d'un rapport sur les licences pour le support technique », page 52.

17.1 À propos des rapports PlateSpin Protect

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

- **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 17-1 *Options d'un rapport de type Historique de réplication*



17.2 Génération de rapports sur les workloads et leur protection

Pour générer un rapport :

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

   Une liste des types de rapport s'affiche.
2. Cliquez sur le nom du type de rapport souhaité.
3. Sélectionnez un ou plusieurs workloads pour lesquels vous souhaitez créer le rapport.
4. Configurez la période pour laquelle vous souhaitez afficher le rapport.
5. Spécifiez les paramètres appropriés pour le rapport.
6. effectuez l'une des opérations suivantes :
   - Cliquez sur **Vue imprimable** pour afficher le rapport dans votre navigateur Web.
   - Cliquez sur **Exporter vers XML**, puis enregistrez le fichier XML sur votre ordinateur.

17.3 Génération 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** en bas à droite du panneau.

   La page se rafraîchit après quelques instants et propose un lien **Télécharger** au-dessus du lien **Générer**.
2. Cliquez sur **Télécharger**.

   Un fichier `.zip` contient des informations de diagnostic complètes sur la commande en cours.
3. Enregistrez le fichier, puis extrayez les diagnostics pour les consulter.
4. Préparez le fichier `.zip` si vous avez besoin de contacter le support technique.

18 Dépannage de la protection et de la récupération des workloads

Cette section peut vous aider à résoudre les problèmes courants survenant lors de la protection et de la récupération des workloads.

Pour les problèmes de découverte et d'inventaire des workloads sources et des hôtes cibles, reportez-vous au Chapitre 14, « Dépannage de la découverte et de l'inventaire de workloads », page 131.

18.1 Optimisation du débit d'une connexion

Si le débit est lent, vous pouvez effectuer des tests pour identifier les éventuels problèmes de connexion ou de bande passante et les résoudre. Reportez-vous à la section Annexe F, « Emploi de l'outil de test réseau iPerf pour optimiser le débit réseau des produits PlateSpin », page 199.

18.2 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 n° 7005495 de la base de connaissances (https://www.netiq.com/support/kb/doc.php?id=7005495).

18.3 Dépannage du service de configuration

Après un test de basculement ou un basculement proprement dit, une erreur se produit sur la machine virtuelle cible en raison de problèmes non spécifiques liés au service de configuration. Le message d'erreur est généralement le suivant :

```
Le service de configuration de la machine cible ne semble pas avoir démarré.
```

Les conseils de dépannage de cette section expliquent les problèmes courants liés au service de configuration et certaines solutions permettant de les résoudre.

18.3.1 Compréhension de l'origine du problème

L'erreur associée au service de configuration indique que le serveur PlateSpin ne parvient pas à communiquer avec le service de configuration sur la machine virtuelle cible. Analysez votre système pour déterminer la cause initiale potentielle du problème.

Échec du démarrage de la machine virtuelle cible

Le système d'exploitation doit être chargé dans la machine virtuelle cible pour que le service de configuration puisse démarrer normalement. Un échec de démarrage indique un éventuel conflit de pilote, une erreur du chargeur de démarrage ou une altération possible du disque.

Nous vous recommandons d'ouvrir un ticket de service auprès du service clients Micro Focus si le système d'exploitation ne parvient pas à démarrer sur la machine virtuelle cible.

Le réseau n'est pas correctement configuré

Le réseau doit être correctement configuré pour que le service de configuration sur le workload cible puisse communiquer avec le serveur PlateSpin.

Vérifiez que vous avez configuré votre réseau de manière à permettre la communication entre le workload cible et le serveur PlateSpin. Voir Section 1.5, « Conditions d'accès et de communication requises sur votre réseau de protection », page 31.

Impossible de lire ou d'écrire des messages d'état sur les lecteurs de disquette

Le service de configuration doit pouvoir communiquer avec les lecteurs de disquette pour les machines virtuelles VMware afin de pouvoir lire et écrire des messages d'état pour le serveur PlateSpin.

Sur la machine virtuelle cible, vérifiez que l'ordinateur est en mesure de communiquer avec les lecteurs de disquette :

1. Sur la machine virtuelle, ouvrez le fichier journal (`C:\windows\platespin\configuration\data\log.txt`).
2. Un des messages suivants peut constituer une indication selon laquelle que la disquette n'est pas accessible :

   ```
   Failed (5) to write to file \\?\Volume{<numéro-guid>}\log.zip ([5] échecs d'écriture
   dans le fichier \\?\Volume{<numéro-guid>}\log.zip ) CopyFile \\?\Volume{<numéro-
   guid>}\windows\platespin\configuration\data\result.txt to \\?\Volume{<guid-
   number>}\result.txt failed (La copie du fichier \\?\Volume{<numéro-
   guid>}\windows\platespin\configuration\data\result.txt to \\?\Volume{<numéro-
   guid>}\result.txt a échoué) The output floppy was not accessible after the timeout
   period (La disquette de sortie n'était pas accessible après le timeout.)
   ```

18.3.2 Solutions envisageables pour résoudre le problème

Pour résoudre une erreur du service de configuration, vous pouvez essayer l'une des solutions de cette section.

- « Ignorer les optimisations de redémarrage de la machine virtuelle cible » page 181
- « Réduction du trafic en lecture-écriture pour les lecteurs de disquette » page 182
- « Modification du type de démarrage pour augmenter le délai » page 183
- « Configuration de la non-exécution automatique au démarrage des services en conflit » page 184

Ignorer les optimisations de redémarrage de la machine virtuelle cible

PlateSpin Protect tente de réduire le nombre de redémarrages sur la machine virtuelle cible par défaut afin d'accélérer le processus de basculement. Cela dit, il se peut que le fait d'autoriser les redémarrages supplémentaires améliore la capacité de la machine cible à communiquer avec le serveur PlateSpin.

Pour ignorer les optimisations de redémarrage, procédez comme suit :

1. Connectez-vous au serveur PlateSpin, puis ouvrez la page de configuration du serveur PlateSpin à l'adresse :

   `https://Votre_serveur_PlateSpin/platespinconfiguration/`
2. Recherchez le paramètre **ConfigurationServiceValues**.
3. Modifiez le paramètre **ConfigurationServiceValues** et définissez l'option **SkipRebootOptimization** sur la valeur `true`.
4. Cliquez sur **Enregistrer**.
5. Exécutez une réplication incrémentielle ou complète.

   La réplication propage également les paramètres de configuration modifiés à la machine virtuelle cible.
6. Réexécutez le test de basculement ou le basculement proprement dit pour les workloads affectés.

Réduction du trafic en lecture-écriture pour les lecteurs de disquette

Vous pouvez réduire le nombre de tentatives de lecture et d'écriture sur les lecteurs de disquette VMware d'entrée ou de sortie par le serveur PlateSpin si le journal de diagnostic affiche l'erreur suivante :

`Information:1:Attempting floppy download` (Information :1 : tentative de téléchargement sur la disquette)

suivi de

`Verbose:1:Failed to copy file from remote URL` (Verbeux : 1 : impossible de copier un fichier à partir d'une URL distante)

-ou-

`Exception: The remote server returned an error: (500) Internal Server Error` (Exception : le serveur distant a renvoyé une erreur : erreur de serveur interne [500])

Cette erreur survient en raison du verrouillage de la ressource par VMware. Cela indique que le serveur PlateSpin détache, puis rattache la disquette lors de chaque vérification de l'état. Le verrouillage peut empêcher la machine virtuelle de lire et d'écrire sur le lecteur de disquette. Reportez-vous à l'article de la base de connaissances VMware *Using the VMware vCenter Server 4.x,5.x and 6.0 Datastore Browser to Download or Copy a Powered-On Virtual Machine's .vmx and .nvram Files Fails (1019286)* (https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1019286) (Échec de l'utilisation du navigateur de la banque de données du serveur VMware vCenter 4.x, 5.x et 6.0 pour télécharger ou copier des fichiers .vmx et .nvram d'une machine virtuelle sous tension [1019286]).

Si vous rencontrez des problèmes de verrouillage du lecteur de disquette, vous pouvez augmenter les valeurs des paramètres d'interrogation du service de configuration sur le serveur PlateSpin :

vmwareConfigServicePollStartDelay

Ce paramètre détermine le délai d'attente avant que le serveur PlateSpin commence à se renseigner sur l'état du workload cible. La valeur par défaut est 120 secondes (2 minutes).

vmwareConfigServicePollIntervalInMilliseconds

Ce paramètre détermine la fréquence à laquelle le serveur PlateSpin tente de communiquer avec le workload cible et de lire ou écrire sur les lecteurs de disquette VMware. La valeur par défaut de l'intervalle d'interrogation est de 30 000 ms (30 secondes).

vmwareConfigServicePollStartTimeout

Ce paramètre détermine le délai pendant lequel le serveur PlateSpin patiente après le démarrage de la machine virtuelle cible avant d'afficher une erreur dans l'interface Web. La valeur par défaut est 420 secondes (7 minutes).

vmwareConfigServicePollUpdateTimeout

Ce paramètre détermine le délai pendant lequel le serveur PlateSpin patiente après chaque intervalle d'interrogation avant d'afficher une erreur dans l'interface Web. La valeur par défaut est 300 secondes (5 minutes).

Des valeurs plus élevées pour ces paramètres réduisent la fréquence à laquelle le serveur PlateSpin tente de lire et d'écrire sur les lecteurs de disquette VMware sur les machines virtuelles cibles.

Pour réduire le trafic de lecture et d'écriture pour les lecteurs de disquette VMware, procédez comme suit :

1. Connectez-vous au serveur PlateSpin, puis ouvrez la page de configuration du serveur PlateSpin à l'adresse :

   `https://Votre_serveur_PlateSpin/platespinconfiguration/`

2. Recherchez les paramètres d'interrogation du service de configuration, modifiez leurs paramètres de manière appropriée, puis cliquez sur **Enregistrer**.

   Par exemple :

   ```
   vmwareConfigServicePollStartDelay = 180 (3 minutes)
   vmwareConfigServicePollIntervalInMilliseconds = 300000 (5 minutes)
   vmwareConfigServicePollStartTimeout = 1200 (20 minutes)
   vmwareConfigServicePollUpdateTimeout = 900 (15 minutes)
   ```

   ou

   ```
   vmwareConfigServicePollStartDelay = 300 (5 minutes)
   vmwareConfigServicePollIntervalInMilliseconds = 480000 (8 minutes)
   vmwareConfigServicePollStartTimeout = 1200 (20 minutes)
   vmwareConfigServicePollUpdateTimeout = 900 (15 minutes)
   ```

3. Exécutez une réplication incrémentielle ou complète.

   La réplication propage également les paramètres de configuration modifiés à la machine virtuelle cible.

4. Réexécutez le test de basculement ou le basculement proprement dit pour les workloads affectés.

Modification du type de démarrage pour augmenter le délai

Le service de configuration peut s'afficher avant que les ressources ne soient accessibles. Vous pouvez modifier le type de démarrage du service de configuration pour augmenter le délai.

Pour modifier le type de démarrage, procédez comme suit :

1. Connectez-vous au serveur PlateSpin, puis ouvrez la page de configuration du serveur PlateSpin à l'adresse :

   `https://Votre_serveur_PlateSpin/platespinconfiguration/`

2. Recherchez le paramètre **windowsConfigServiceStartType**.

3. Modifiez la valeur **windowsConfigServiceStartType** sur **AutoDelay**.

   Les options pour **windowsConfigServiceStartType** sont les suivantes :

   - **GroupDelay** est la valeur par défaut. Le service de configuration est ajouté à la fin de **ServiceGroupOrder** dans le registre.
   - **AutoDelay** optimise le délai pendant lequel le service patiente avant de démarrer (2 minutes après le démarrage). Modifiez également la valeur du paramètre **ServicesPipeTimeoutForWindowsConfigService** à l'Étape 4.
   - **NoDelay** est l'option la plus performante. Le service démarre dès que Windows le permet. Toutefois, cette option n'est pas recommandée en raison des problèmes potentiels de connexion aux ressources.

4 (AutoDelay) Modifiez la valeur du paramètre **ServicesPipeTimeoutForWindowsConfigService** sur 180 secondes pour prendre en compte les 120 secondes dont le service a besoin pour démarrer après l'amorçage lorsque l'option AutoDelay est définie sur **windowsConfigServiceStartType** à l'Étape 3.

5 Cliquez sur **Enregistrer**.

6 Exécutez une réplication incrémentielle ou complète.

   La réplication propage également les paramètres de configuration modifiés à la machine virtuelle cible.

7 Réexécutez le test de basculement ou le basculement proprement dit pour les workloads affectés.

Configuration de la non-exécution automatique au démarrage des services en conflit

Lors d'une opération de basculement, un service Windows interfère avec le montage des lecteurs de disquette.

Déterminez les services Windows configurés pour démarrer automatiquement lors d'un redémarrage. Certains services sont connus pour provoquer des interférences lorsque le service de configuration tente d'écrire sur une disquette, notamment la configuration sans fil et certains logiciels antivirus. Vous devez configurer ces services pour qu'ils ne s'exécutent pas automatiquement lors d'un test ou d'un basculement, puis réexécuter le test de basculement ou le basculement proprement dit.

Vous pouvez également essayer de désactiver tous les services non indispensables au test et au basculement sur la page de configuration, puis réexécuter le test ou le basculement proprement dit.

18.3.3 Conseils de dépannage supplémentaires

Si le service de configuration ne parvient pas à contacter le serveur PlateSpin, les diagnostics ne seront pas complets. Vous devez également obtenir les journaux de la machine virtuelle cible :

- **Workloads Windows :** les journaux du service de configuration se trouvent dans le dossier `C:\windows\platespin\configuration\data`.
  - Le fichier `log.txt` contient toutes les informations consignées, mais le fichier `Config.ini` permet de comprendre ce qui doit être configuré.
  - Le fichier `result.txt` contient l'état du service de configuration en cours d'exécution.
  - Si la machine virtuelle cible ne parvient pas à lire sur le lecteur de disquette d'entrée, elle ne disposera pas du fichier `Config.ini` fusionné susceptible de contenir des informations de configuration du réseau personnalisé pour l'environnement réseau du test de basculement.
  - Si le fichier `Config.ini` ne dispose d'aucune information relative au réseau (comme `[NIC0]`, l'adaptateur réseau de la machine virtuelle cible peut contenir des caractères spéciaux dans son nom.

    Il s'agit d'un problème connu selon lequel le fichier `Config.ini` risque de ne pas être correct tant qu'il n'a pas été fusionné avec celui du lecteur de disquette.
  - La machine virtuelle cible tente un redémarrage si elle ne peut pas se connecter à la disquette de sortie ou d'entrée (une seule fois). Un fichier `config.ini.floppyreboot` s'affichera dans ce cas.
- **Workloads Linux :** les journaux du service de configuration se trouvent dans le dossier `/tmp`.
  - Les fichiers journaux principaux sont au format `nom_fichier*.PlateSpin.FileLogger`.

Nous vous recommandons de passer en revue tous les dossiers de configuration dans le répertoire `/tmp`. Compressez les dossiers de configuration ainsi que le fichier `nom_fichier*.PlateSpin.FileLogger` pour les envoyer au service clients Micro Focus.

- Autres fichiers de configuration à passer en revue pour inclure ce qui suit :

  ```
  /tmp/Ofx.RunCommand.Output*
  /tmp/*DiskHelper*
  /tmp/*VmTools*
  ```

- Le fichier de configuration est `/usr/lib/psconfigservice/data/config.conf`.
- Le fichier journal contenant le résultat final est `/usr/lib/psconfigservice/data/result.txt`.

18.4 Dépannage de la préparation de la réplication des workloads (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 185.
Impossible de déterminer si .NET Framework est installé (avec exception d'`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. Voir également « Dépannage de la découverte pour les workloads Windows » page 131.

18.4.1 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 `gpupdate /force`.

18.4.2 Plusieurs volumes ont le même numéro de série

Problème : lorsque vous essayez de configurer une protection pour un serveur Windows, le message d'erreur suivant s'affiche :

```
[Source] Deux volumes ou plus ont le même numéro de série. Modifiez les numéros de série de sorte qu'ils soient uniques et redécouvrez la machine.
```

Solution : ce problème peut se produire si les numéros de série de plusieurs volumes sont identiques. PlateSpin Protect requiert des numéros de série uniques.

Pour résoudre ce problème, modifiez les numéros de série des volumes de données selon les besoins, puis redécouvrez la machine. Pour plus d'informations sur l'utilisation des outils natifs Windows pour modifier les numéros de série, reportez-vous à l'article de la base de connaissance n° 7921101.

18.5 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.
La réplication incrémentielle basée sur des fichiers ne se termine pas lorsque le chiffrement est activé	Une fois le codage activé pour un workload Windows configuré pour le transfert de données basé sur des fichiers, le récepteur Windows peut se bloquer à la fin du transfert pour les réplications incrémentielles. La suspension se produit si le dernier octet du transfert est mal défini par le processus de codage sur une valeur autre que zéro, ce qui indique que d'autres fichiers sont en cours de transfert et qu'il faut poursuivre la lecture à partir du flux. Vous pouvez utiliser le transfert de données par bloc pour les workloads Windows si vous souhaitez activer le chiffrement pour les transferts de données de réplication.
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.
La protection sur un réseau étendu (WAN) prend énormément de temps si le conteneur de machines virtuelles compte un nombre important de banques de données	Dans certains cas, le processus de localisation de l'image ISO appropriée pour le démarrage de la cible peut durer plus longtemps que prévu. Cela peut arriver lorsque votre serveur PlateSpin est connecté à un conteneur de machines virtuelles via un réseau étendu (WAN) et que ce conteneur compte de nombreuses banques de données.

Problèmes ou messages	Solutions
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.
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 71.

`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.
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. Reportez-vous à l'article 7920339 de la base de connaissances (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 7920862 de la base de connaissances (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 185.

Problèmes ou messages	Solutions
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* (http://msdn.microsoft.com/en-us/library/aa819132.aspx) (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`.

18.6 Dépannage du basculement ou du rétablissement des workloads

Problèmes ou messages	Solutions
Active Directory Domain Services n'est pas disponible à la suite d'un rétablissement (sous Windows)	Active Directory Domain Services peut ne plus être disponible après un basculement si des erreurs `chkdsk` se sont produites. Deux causes d'erreur `chkdsk` peuvent être évitées : ◆ Les fichiers journaux liés aux mises à jour Microsoft si les mises à jour ou correctifs Microsoft recommandés n'ont pas été appliqués à la machine source au moment de la première réplication complète. ◆ Les fichiers et dossiers système qui doivent être exclus de votre logiciel antivirus. Pour éviter ces problèmes, suivez les meilleures pratiques décrites dans la Section 15.1, « Conditions préalables à la protection des workloads », page 151 avant d'exécuter la première réplication complète.
Des cartes réseau incorrectes sont assignées lors du rétablissement et bloquent l'opération	Pour que le rétablissement s'exécute correctement, utilisez une des solutions suivantes : ◆ Faites basculer la configuration IP vers les assignations attendues afin que la cible soit correctement configurée. ◆ Redémarrez le matériel 'takecontrol' sur le disque LRD, puis répétez la procédure pour l'utiliser en tant que cible de rétablissement. Il est probable que la fois suivante, PlateSpin Protect assigne les volumes aux interfaces Ethernet correctes. ◆ Dans l'interface Web, si le rétablissement semble se bloquer alors que l'opération est presque terminée, il est probable que la cible du rétablissement ne puisse pas communiquer au serveur PlateSpin que le rétablissement est terminé. Branchez les câbles réseau à l'arrière de la cible du rétablissement de manière à placer la carte réseau adéquate sur les réseaux voulus. La cible de rétablissement pourra alors communiquer avec le serveur PlateSpin, et le rétablissement se terminera.

Problèmes ou messages	Solutions
Le rétablissement X2P de workloads Linux provoque une panne de l'interface graphique de X Server	Ce problème est provoqué par une reconfiguration de la machine virtuelle basculée lors de l'installation des outils VMware. Pour le résoudre, utilisez la commande suivante afin de rechercher les fichiers dont le nom comporte la chaîne `BeforeVMwareToolsInstall` : `find / -iname '*BeforeVMwareToolsInstall'` Une fois ces fichiers identifiés, replacez-les dans leur emplacement d'origine, puis redémarrez le workload pour réparer son interface X Server.

18.7 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 n° 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.

18.8 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.

- Section 18.8.1, « Nettoyage des workloads Windows », page 189
- Section 18.8.2, « Nettoyage des workloads Linux », page 190

18.8.1 Nettoyage des workloads Windows

Composant	Instructions de suppression
Composant de transfert par bloc PlateSpin	Reportez-vous à l'article n° 7005616 de la base de connaissances (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`..

Composant	Instructions de suppression
Logiciel d'inventaire de workloads	Dans le répertoire `Windows` du workload : ◆ Supprimez tous les fichiers nommés `machinediscovery*`. ◆ Supprimez le sous-répertoire nommé `platespin`.
Logiciel contrôleur	1. Ouvrez une invite de commande sur le workload source 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*`..

18.8.2 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 de 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*

Instantané NSS	Instantané NSS créé et utilisé par PlateSpin pour les réplications en cours. Le nom de l'instantané se termine par le suffixe `PSSNP`.
	
	Pour supprimer ces instantanés NSS :
	
	1. Générez une liste d'instantanés sur le workload requis à l'aide de l'une des méthodes suivantes :
	◆ Utilisez l'interface Web de pour générer un rapport pour la tâche ayant échoué. Le rapport doit contenir des informations sur les instantanés NSS et leurs noms.
	
	- OU -
	
	◆ Sur le workload Open Enterprise Server requis, entrez la commande suivante pour afficher une liste de tous les instantanés NSS :
	
	`# NLVM list snaps`
	
	- OU -
	
	◆ Sur le workload Open Enterprise Server requis, lancez l'utilitaire NSSMU et sélectionnez **Instantané** pour afficher une liste des instantanés.
	2. Notez le nom et l'emplacement des instantanés à supprimer.
	3. Sur le workload Open Enterprise Server, supprimez les instantanés appropriés en utilisant l'une des méthodes suivantes :
	◆ Saisissez la commande suivante :
	
	`NLVM delete snap <`*nom_instantané*`>`
	
	- OU -
	
	◆ Lancez l'utilitaire NSSMU, puis sélectionnez **Instantané**. Sélectionnez chaque instantané à supprimer, puis cliquez sur Supprimer.

Composant	Instructions de suppression
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`

V Outils PlateSpin

PlateSpin Protect inclut des outils supplémentaires permettant d'optimiser votre environnement de protection.

E Utilisation des fonctions de protection de workload à l'aide de l'API du serveur PlateSpin Protect

Vous pouvez utiliser les fonctions de protection de workload par programmation de PlateSpin Protect, via l'API (`protectionservices`) du serveur PlateSpin Protect, 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.

REMARQUE : l'API du serveur Protect est expérimentale. Les informations contenues dans cette section sont présentées à titre d'aperçu technologique.

E.1 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

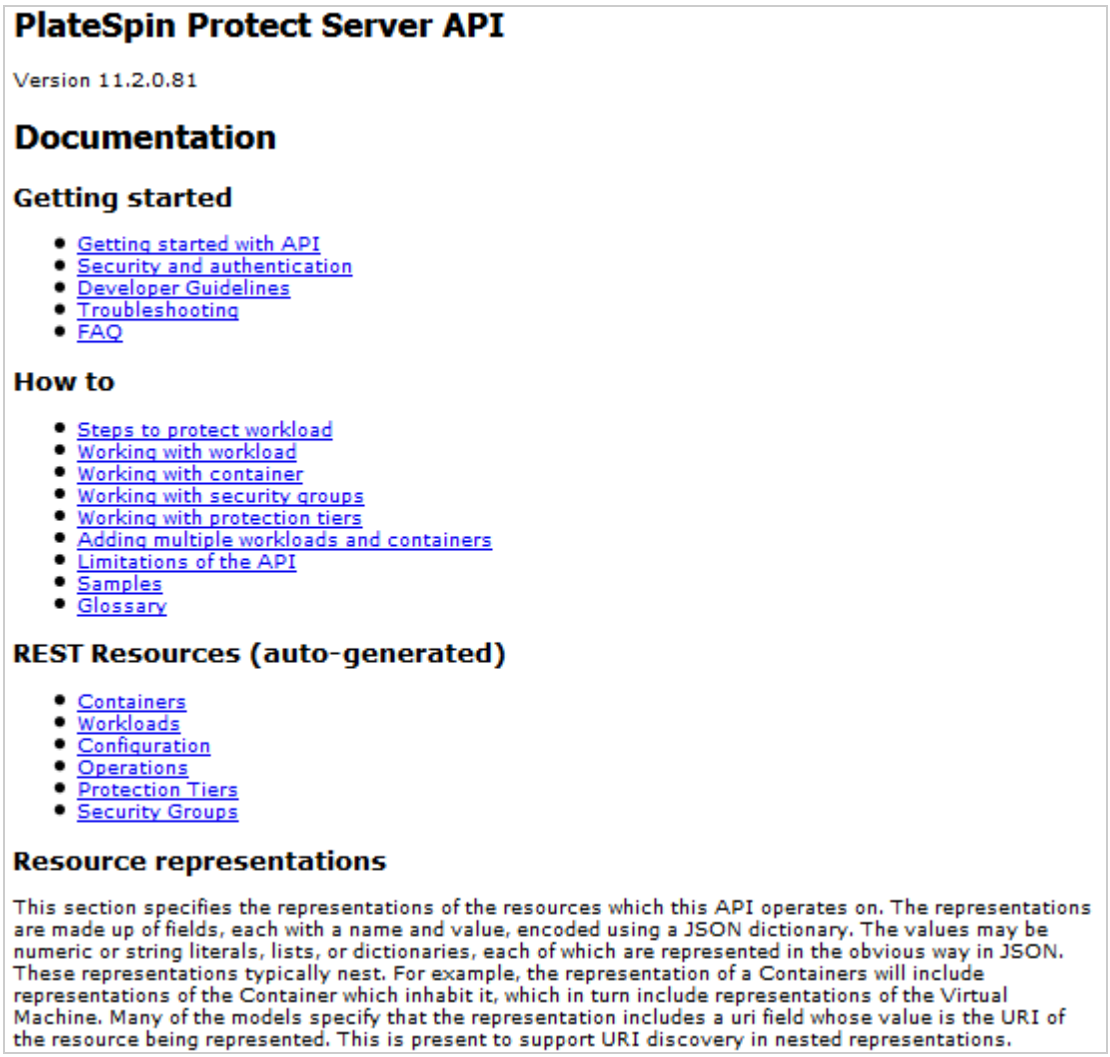
E.2 Documentation relative à l'API du serveur PlateSpin Protect

La page d'accueil de l'API du serveur PlateSpin Protect pour `protectionservices` fournit de la documentation et des exemples qui peuvent être utiles pour les développeurs et les administrateurs. Pour plus d'informations, accédez à l'emplacement suivant sur l'hôte du serveur PlateSpin :

`https://`*votre_serveur_PlateSpin*`/protectionservices`

Remplacez *votre_serveur_PlateSpin* par le nom d'hôte ou l'adresse IP de l'hôte de votre serveur PlateSpin. Si SSL n'est pas activé, utilisez le protocole `http` dans l'URI.

Figure E-1 *Page d'accueil de l'API du serveur Protect*



E.3 Exemples et autres références

Les administrateurs Protect peuvent générer un échantillon JScript à partir de la ligne de commande pour accéder au produit via l'API. Sur l'hôte du serveur PlateSpin, consultez l'exemple à l'adresse

https://localhost/protectionservices/Documentation/Samples/protect.js

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

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.

F Emploi de l'outil de test réseau iPerf pour optimiser le débit réseau des produits PlateSpin

Avant d'exécuter une réplication, veillez à tester la connexion pour vérifier l'éventuelle présence de problèmes de bande passante ou de connexion et, le cas échéant, veillez à les résoudre. Cette section décrit comment utiliser l'outil de test réseau iPerf Open Source pour optimiser le débit de la connexion.

F.1 Introduction

Pour aider les administrateurs PlateSpin à améliorer le débit réseau lors de l'utilisation des produits PlateSpin, l'outil de test réseau iPerf est fourni dans l'environnement de prise de contrôle du disque virtuel Linux PlateSpin LRD (Linux RAM Disk). Comme l'indique la documentation d'iPerf : « Le principal objectif d'iPerf est d'aider à ajuster au mieux les connexions TCP pour un chemin d'accès donné. Le problème de réglage le plus fondamental pour le protocole TCP est la taille de fenêtre TCP qui contrôle la quantité de données que peut héberger le réseau à un moment donné. »

L'objectif de ce fichier lisezmoi est de décrire une méthode de base de réglage réseau et de test, eu égard à l'utilisation des produits PlateSpin. Commencez par calculer une taille de fenêtre TCP qui serait optimale d'un point de vue théorique. Vous utilisez ensuite l'outil iPerf pour valider et affiner cette taille théorique et mesurer le débit obtenu dans la pratique. L'utilisation de cette méthode permet également de déterminer le débit réel pouvant être obtenu pour un réseau donné.

En réalité, l'outil iPerf et les produits PlateSpin utilisent la *taille de tampon d'envoi/réception TCP* pour affecter l'éventuel choix interne de *taille de fenêtre TCP*. À partir d'ici, ces termes seront utilisés indifféremment.

REMARQUE : plusieurs facteurs sont susceptibles d'affecter le débit réseau. Il existe de nombreuses informations sur Internet permettant de faciliter la compréhension. Citons notamment l'*outil de calcul du débit réseau* (http://wintelguy.com/wanperf.pl) qui peut aider à calculer le débit TCP maximal attendu en fonction des caractéristiques réseau applicables au client. Nous vous recommandons vivement d'utiliser que cet outil de calcul en ligne afin de définir correctement les attentes en matière de débit.

F.2 Calculs

Le réglage de la taille de fenêtre TCP est basé sur un certain nombre de facteurs, notamment la vitesse de liaison et la latence réseau. Pour nos besoins concernant les produits PlateSpin, le choix initial de taille de fenêtre TCP pour le réglage est basé sur des calculs standard (disponibles sur Internet et ailleurs) comme suit :

```
WinSizeInBytes=((LINK_SPEED(Mbit/s)/8)*DELAY(sec))*1 000*1 024
```

Par exemple, pour une liaison de 54 Mbit/s et une latence de 150 ms, la taille de fenêtre initiale appropriée est de :

```
(54/8)*0,15*1 000*1 024 = 1 036 800 octets
```

Par exemple, pour une liaison de 1000 Mbit/s et une latence de 10 ms, la taille de fenêtre initiale appropriée est de :

```
(1 000/8)*.01*1 000*1 024 = 1 280 000 octets
```

Pour obtenir une valeur de latence réseau, utilisez `ping` à partir de l'invite de commande (Windows) ou du terminal (Linux). Bien que le temps d'aller-retour (RTT) `ping` soit sans doute différent de la latence réelle, la valeur obtenue est suffisamment proche pour l'utiliser dans cette méthode.

L'exemple suivant est un résultat de commande `ping` Windows pour lequel la latence observée est en moyenne de 164 ms :

```
ping 10.10.10.232 -n 5

Pinging 10.10.10.232 with 32 bytes of data:
Reply from 10.10.10.232: bytes=32 time=154ms TTL=61
Reply from 10.10.10.232: bytes=32 time=157ms TTL=61
Reply from 10.10.10.232: bytes=32 time=204ms TTL=61
Reply from 10.10.10.232: bytes=32 time=153ms TTL=61
Reply from 10.10.10.232: bytes=32 time=153ms TTL=61

Ping statistics for 10.10.10.232:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 153ms, Maximum = 204ms, Average = 164ms
```

Voici un exemple de résultat d'une commande `ping` Linux pour laquelle la latence observée est en moyenne de 319 ms :

```
ping 10.10.10.232 -c 5

PING 10.10.10.232 (10.10.10.232) 56(84) bytes of data.
64 bytes from 10.10.10.232: icmp_seq=1 ttl=62 time=0.328 ms
64 bytes from 10.10.10.232: icmp_seq=2 ttl=62 time=0.280 ms
64 bytes from 10.10.10.232: icmp_seq=3 ttl=62 time=0.322 ms
64 bytes from 10.10.10.232: icmp_seq=4 ttl=62 time=0.349 ms
64 bytes from 10.10.10.232: icmp_seq=5 ttl=62 time=0.316 ms

--- 10.10.10.232 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.280/0.319/0.349/0.022 ms
```

Dans la pratique, vous devez utiliser l'option `-n` ou `-c` pour spécifier un nombre élevé de paquets ping afin de mieux mesurer la valeur de latence.

F.3 Installation

L'outil iPerf s'exécute en mode serveur ou client.

La syntaxe de base pour le mode de serveur `iperf` est la suivante :

```
iperf -s -w <win_size>
```

La syntaxe de base pour le mode client `iperf` est la suivante :

```
iperf -c <server_ip> -w <win_size>
```

Notre objectif est de mesurer et régler la vitesse réseau entre un workload source et cible. Dans de nombreux cas, il peut s'agir de la source et des cibles réellement en cours d'utilisation. Le test peut être effectué à l'aide d'un workload différent pour la source ou la cible, pour autant que le workload de remplacement ait les mêmes caractéristiques réseau que l'original, par exemple une carte d'interface, une connexion réseau etc.

REMARQUE : assurez-vous de ne pas tester le débit à partir du serveur PlateSpin sur la source ou la cible, dans la mesure où ce trafic est minime et ne représente pas bien le trafic lors d'une migration ou d'une réplication.

Bien qu'il soit possible d'utiliser un workload en direct (Windows ou Linux) en tant que serveur cible/iperf, les étapes suivantes fournissent l'environnement ressemblant le plus à ce qui se produit au moment de la migration/réplication et est dès lors vivement recommandé.

Pour configurer et exécuter `iperf` sur la cible, procédez comme suit :

1. Démarrez la cible à l'aide du disque virtuel Linux (LRD).
2. Dans la console LRD, utilisez le terminal du programme auxiliaire (accessible via Alt+F2) pour effectuer les opérations suivantes :
   - **2a** Configurez la mise en réseau à l'aide de l'option 5.
   - **2b** Montez le CD à l'aide de l'option 6.
3. Dans la console LRD, basculez vers le terminal de débogage (accessible via Alt+F7) pour accéder à l'emplacement de l'outil iPerf :

   ```
   cd /mnt/cdrom/LRDTools/iperf_2.0.X/linux
   ```

4. Exécutez l'outil iPerf en mode serveur. Entrez

   ```
   ./iperf -s -w <win_size>
   ```

Pour configurer et exécuter `iperf` sur la source, procédez comme suit :

1. Montez l'image ISO LRD à l'aide d'un logiciel ou d'un support physique.
2. Ouvrez une invite de commande (Windows) ou un terminal (Linux) et accédez à l'emplacement de l'outil iPerf :

   ```
   cd <media>/LRDTools/iperf_2.0.X/
   ```

3. En fonction de votre système d'exploitation source, accédez au sous-répertoire `windows` ou `linux` :

```
cd windows

-OR-

cd linux
```

4 Exécutez l'outil iPerf en mode client. Entrez

```
iperf -c <target_ip> -w <win_size>
```

REMARQUE : vous pouvez télécharger et utiliser `iperf3` pour effectuer les calculs, ce qui est utile dans certains cas pour lesquels `iperf2` ne parvient pas à générer des chiffres de débit exploitables. Bien que la syntaxe et le résultat de commande de `iperf3` diffèrent légèrement, il doit être relativement simple d'adapter et d'interpréter le nouveau résultat, au besoin.

F.4 Méthodologie

En partant de la taille `win_size` calculée dans la section Calculs, enregistrez le résultat de plusieurs itérations de l'outil iPerf à l'aide de la valeur calculée, ainsi que les valeurs légèrement plus élevées et moins élevées. Nous vous recommandons d'augmenter et de diminuer la taille `win_size` par incréments de 10 pour cent de la valeur d'origine.

Pour l'exemple de 1 280 000 octets ci-dessus, vous pouvez augmenter ou diminuer la taille `win_size` par incréments de 100 000 octets environ.

REMARQUE : l'option `-w` d'`iperf` permet de spécifier des unités K (pour kilo-octets) ou M (pour méga-octets).

En suivant le même exemple, vous pouvez utiliser des valeurs `-w` de `1,28M`, `1,38M`, `1,18M`, etc., comme taille `win_size` à l'étape 4. Bien entendu, nous partons du principe que seule l'étape d'exécution est répétée pour chaque itération de l'outil iPerf.

Un exemple de résultat d'une itération d'un client se présente comme suit :

```
iperf.exe -c 10.10.10.232 -w 1.1M

------------------------------------------------------------
Client connecting to 10.10.10.232, TCP port 5001
TCP window size: 1.10 MByte
------------------------------------------------------------
[296] local 10.10.10.224 port 64667 connected with 10.10.10.232 port 5001
[ ID] Interval       Transfer     Bandwidth
[296]  0.0-10.2 sec  11.3 MBytes  9.29 Mbits/sec
```

Un exemple de résultat du serveur cible référencé se présente comme suit :

```
./iperf -s -w .6M

------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 1.20 MByte (WARNING: requested 614 Kbyte)
------------------------------------------------------------
[  4] local 10.10.10.232 port 5001 connected with 10.10.10.224 port 64667
[  4] 0.0-10.2 sec  11.3 MBytes  9.29 Mbits/sec
```

REMARQUE :

- Le client se déconnecte du serveur après une seule itération, tandis que le serveur continue à écouter jusqu'à ce qu'il soit arrêté à l'aide de la commande Ctrl+C.
- La taille de fenêtre spécifiée pour un serveur Linux correspond à la moitié de la valeur souhaitée, car Linux double automatiquement la taille de tampon TCP demandée.

Utilisez plusieurs itérations pour déterminer la valeur optimale de la taille de fenêtre TCP. N'oubliez pas d'utiliser uniquement la moitié de la valeur désirée lorsque vous spécifiez l'option `-w` pour `iperf` sous Linux.

Un débit en augmentation indique que vous atteindrez bientôt une taille de fenêtre TCP optimale. Enfin, à mesure que vous vous rapprochez de la valeur optimale, utilisez des itérations plus longues afin de simuler au mieux les conditions réelles d'exécution. Pour obtenir une itération plus longue, utilisez l'option `-t <délai_en_secondes>` pour `iperf`. Cette option ne doit être spécifiée que du côté client.

Par exemple :

```
iperf.exe -c 10.10.10.232 -w 1.25M -t 60
```

Dès qu'une valeur optimale a été déterminée, configurez celle-ci comme paramètre `FileTransferSendReceiveBufferSize` pour le serveur PlateSpin approprié à l'emplacement :

https://<*mon_serveur_ps*>/PlatespinConfiguration/

Cette valeur globale s'applique à tous les workloads du serveur PlateSpin. Dès lors, soyez attentif aux workloads groupés et à leurs réseaux respectifs sur l'ensemble des serveurs PlateSpin disponibles.

F.5 Attentes

Dans certains cas, la modification indirecte de la taille de fenêtre TCP à l'aide de la taille du tampon d'envoi/réception TCP peut être une méthode très efficace pour augmenter le débit réseau. Cela permet parfois de double, tripler (et parfois même plus) le débit par rapport au débit initial. Toutefois, n'oubliez pas que les caractéristiques réseau peuvent (souvent) varier au fil du temps en raison de changements des modèles d'utilisation, de matériel, de logiciels ou de toute autre infrastructure.

Nous recommandons vivement d'utiliser cette méthode pour calculer la valeur optimale au même moment de la journée et en employant les mêmes modèles d'utilisation réseau que ceux que vous prévoyez d'utiliser pour réaliser les tâches de réplication ou de migration prévues. Nous vous recommandons également de recalculer le paramètre régulièrement pour prendre en compte les changements de conditions réseau.