Guide de l'utilisateur

Novell® PlateSpin® Protect

10.1

17 juin 2011

www.novell.com

Mentions légales

Novell, Inc. n'accorde aucune garantie, explicite ou implicite, quant au contenu de cette documentation, y compris toute garantie de bonne qualité marchande ou d'aptitude à un usage particulier. Novell se réserve en outre le droit de réviser cette publication à tout moment et sans préavis.

Par ailleurs, Novell exclut toute garantie relative à tout logiciel, notamment toute garantie, expresse ou implicite, que le logiciel présenterait des qualités spécifiques ou qu'il conviendrait à un usage particulier. Novell se réserve en outre le droit de modifier à tout moment tout ou partie des logiciels Novell, sans notification préalable de ces modifications à quiconque.

Tous les produits ou informations techniques fournis dans le cadre de ce contrat peuvent être soumis à des contrôles d'exportation aux États-Unis et à la législation commerciale d'autres pays. Vous vous engagez à respecter toutes les réglementations de contrôle des exportations et à vous procurer les licences et classifications nécessaires pour exporter, réexporter ou importer des produits livrables. Vous acceptez de ne pas procéder à des exportations ou à des réexportations vers des entités figurant sur les listes noires d'exportation en vigueur aux États-Unis ou vers des pays terroristes ou soumis à un embargo par la législation américaine en matière d'exportations. Vous acceptez de ne pas utiliser les produits livrables pour le développement prohibé d'armes nucléaires, de missiles ou chimiques et biologiques. Reportez-vous à la page Web des services de commerce international de Novell (http://www.novell.com/info/exports/) pour plus d'informations sur l'exportation des logiciels Novell. Novell décline toute responsabilité dans le cas où vous n'obtiendriez pas les autorisations d'exportation nécessaires.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
États-Unis
www.novell.com

Documentation en ligne : pour accéder à la documentation en ligne la plus récente de ce produit et des autres produits Novell ou pour obtenir des mises à jour, reportez-vous au site Web de documentation Novell (http://www.novell.com/documentation).

Marques de Novell

Pour connaître les marques commerciales de Novell, reportez-vous à la liste des marques commerciales et des marques de service de Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Éléments tiers

Toutes les marques commerciales de fabricants tiers appartiennent à leur propriétaire respectif.

Table des matières

À propos de ce Guide

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

Public

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

Commentaires

Nous souhaiterions connaître vos commentaires et suggestions sur ce Guide et les autres documentations fournies avec ce produit. Utilisez la fonction Commentaires au bas de chaque page de la documentation en ligne ou accédez au site Novell de commentaires sur la documentation (http://www.novell.com/documentation/feedback.html) pour entrer vos commentaires.

Documentation supplémentaire

Le présent guide fait partie de la documentation de PlateSpin Protect.

Pour obtenir une liste complète des publications relatives à cette version logicielle, visitez le site Web de documentation en ligne de PlateSpin Protect 10 (http://www.novell.com/documentation/platespin_protect_10).

Mises à jour de la documentation

La version la plus récente de ce guide est disponible sur le site Web de documentation en ligne de PlateSpin Protect 10 (http://www.novell.com/documentation/platespin_protect_10) :

Ressources supplémentaires

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

- Le forum des utilisateurs de Novell (http://forums.novell.com) : communauté Web traitant de divers sujets de discussion.
- La base de connaissances Novell (http://www.novell.com/support) : ensemble d'articles techniques détaillés.

Support technique

- Téléphone (Amérique du Nord) : +1-877-528-3774 (1 87 PlateSpin)
- Téléphone (international) : +1-416-203-4799
- Message électronique : support@platespin.com

Vous pouvez également visiter le site Web du support technique de PlateSpin (http://www.platespin.com/support).

Configuration de l'applicatif 1

1.1 Activation de la licence du produit

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

1.1.1 Obtention d'un code d'activation de licence

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

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

1.1.2 Activation en ligne de la licence

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

Remarque : les proxys HTTP peuvent être à l'origine d'échecs au cours de l'activation en ligne. L'activation hors ligne est recommandée pour les utilisateurs travaillant avec des proxys HTTP.

---

1 Dans le client Web PlateSpin Protect, cliquez sur *Paramètres* > *Licences* > *Ajouter une licence*. La page d'activation de la licence s'affiche.

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

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

1.1.3 Activation hors ligne de la licence

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

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

---

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

2 Sélectionnez *Activation hors ligne*.

3 Utilisez votre ID matériel pour créer un fichier de clé de licence sur le site Web d'activation des produits PlateSpin (http://www.platespin.com/productactivation/ActivateOrder.aspx). Pour ce faire, vous devez également entrer un nom d'utilisateur, un mot de passe, l'adresse électronique que vous avez spécifiée lorsque vous avez passé votre commande et le code d'activation que vous avez reçu.

4 Saisissez le chemin d'accès au fichier ou accédez à son emplacement et cliquez sur *Activer*.

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

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

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

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

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

- limiter l'accès aux applications à certains utilisateurs ;

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

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

- **Les administrateurs chargés de la protection des workloads :** ces utilisateurs bénéficient d'un accès illimité à toutes les fonctions de l'application. Un administrateur local appartient implicitement à ce groupe.
- **Les utilisateurs avec pouvoir chargés de la protection des workloads :** ces utilisateurs bénéficient d'un accès à un sous-ensemble limité de fonctions système, suffisant pour assurer un fonctionnement au quotidien.
- **Les opérateurs 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.

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. Si l'utilisateur est un administrateur local sur l'hôte du serveur PlateSpin Protect, ce compte est implicitement considéré comme celui d'un administrateur chargé de la protection de workload.

Tableau 1-1 *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

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

Par ailleurs, le logiciel PlateSpin Protect intègre un mécanisme basé sur des *groupes de sécurité* qui déterminent les utilisateurs de niveau OS devant avoir accès à des workloads spécifiques dans l'inventaire de workloads de PlateSpin Protect.

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

1. L'ajout d'utilisateurs de niveau OS aux groupes d'utilisateurs appropriés repris dans le Tableau 1-1.
2. La création de groupes de sécurité de niveau application qui associent ces utilisateurs à des workloads spécifiques.

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

- « Ajout d'utilisateurs PlateSpin Protect » page 12
- « Assignation d'un rôle de protection de workload à un utilisateur PlateSpin Protect » page 12

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 Protect, reportez-vous à la section « Assignation d'un rôle de protection de workload à un utilisateur PlateSpin Protect » page 12.

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

Vous pouvez maintenant assigner un rôle de protection de workload à l'utilisateur que vous venez de créer. Reportez-vous à la section « Assignation d'un rôle de protection de workload à un utilisateur PlateSpin Protect » page 12.

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 1-1, « Détails des rôles de protection de workload et des autorisations », page 11.

1. Sur l'hôte du serveur PlateSpin Protect, accédez à la console Utilisateurs et groupes locaux (*Démarrer* > *Exécuter* > `lusrmgr.msc` > *Entrée*).
2. Cliquez sur le noeud *Utilisateurs*, puis double-cliquez sur l'utilisateur souhaité dans le volet de droite.

3 Dans l'onglet *Membre de*, cliquez sur *Ajouter*, recherchez le groupe de protection de workload souhaité et assignez-le à l'utilisateur.

   Plusieurs minutes peuvent être nécessaires pour que le changement soit pris en compte. Pour tenter d'appliquer les modifications manuellement, redémarrez votre serveur. Reportez-vous à la section « Redémarrage du serveur PlateSpin Protect afin d'appliquer les modifications système » page 24.

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 13.

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

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

1 Assignez à un utilisateur PlateSpin Protect un rôle de protection de workload dont les autorisations sont les plus adaptées à ce rôle dans votre organisation. Reportez-vous à la section « Assignation d'un rôle de protection de workload à un utilisateur PlateSpin Protect » page 12.

2 Accédez à PlateSpin Protect en tant qu'administrateur à l'aide du client Web PlateSpin Protect, puis cliquez sur *Paramètres* > *Autorisations*.

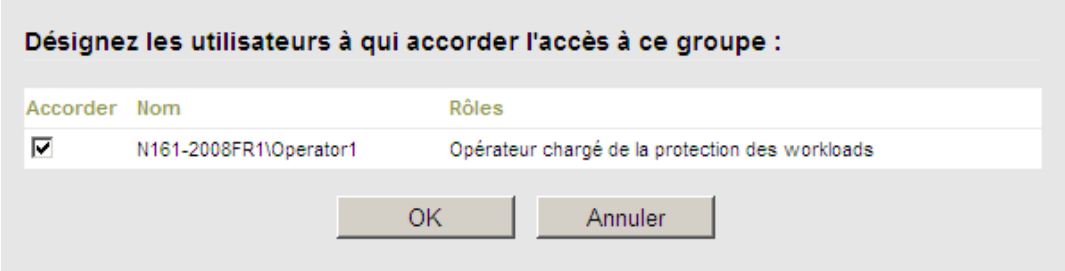
   La page Groupes de sécurité s'ouvre :

3 Cliquez sur *Créer un groupe de sécurité*.

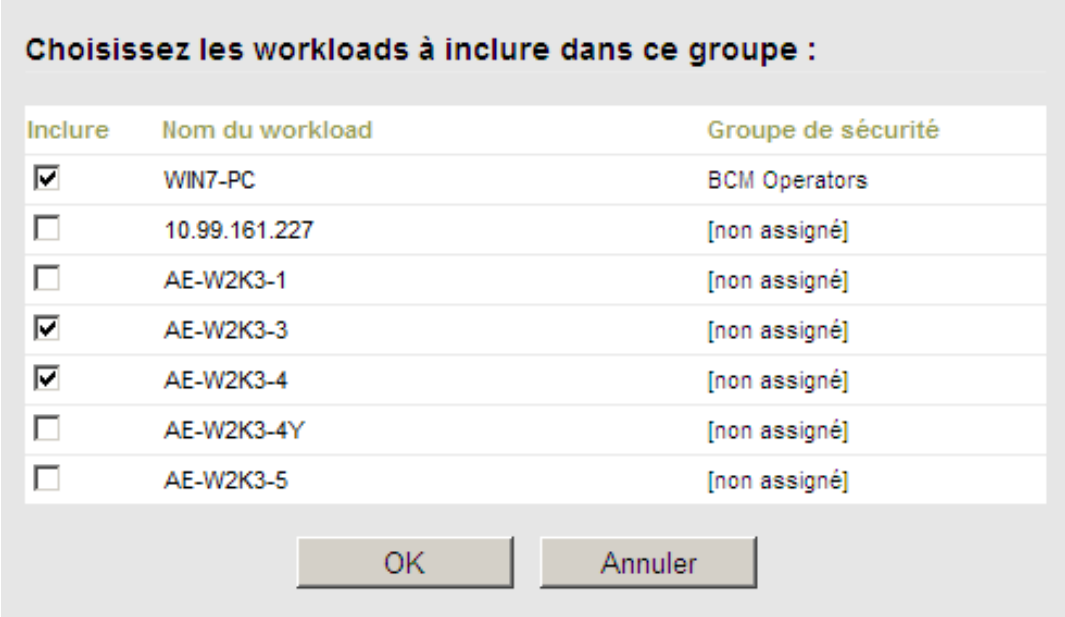
4 Dans le champ *Nom du groupe de sécurité*, saisissez un nom pour votre groupe de sécurité.

5 Cliquez sur *Ajouter des utilisateurs* et sélectionnez les utilisateurs que vous souhaitez ajouter à ce groupe de sécurité.

   Si vous voulez ajouter un utilisateur PlateSpin Protect récemment ajouté en tant qu'utilisateur de niveau OS à l'hôte PlateSpin Protect Server, il ne sera peut-être pas 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.

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

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

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

Tableau 1-2 *Conditions d'accès et de communication requises pour les workloads*

Type de workload	Conditions préalables	Ports requis
Tous les workloads	Fonctionnalité ping (demande et réponse d'écho ICMP).	

Type de workload	Conditions préalables	Ports requis
Tous les workloads Windows	.NET Framework version 2.0 ou ultérieure	

Windows 7 ;
 	
Windows Server 2008 ;
 	
Windows Vista
	◆ Compte `Administrateur` intégré ou références du compte d'administrateur de domaine (une simple appartenance au groupe Administrateurs local ne suffit pas). Sous Vista, le compte doit être activé (il est désactivé par défaut).
	◆ Pare-feu Windows configuré avec les règles entrantes ci-dessous 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)
	
	Ces paramètres de pare-feu sont configurés à l'aide de l'utilitaire Pare-feu Windows avec fonctions avancées de sécurité (`wf.msc`). Vous pouvez obtenir le même résultat par le biais de l'utilitaire de base Pare-feu Windows (`firewall.cpl`) : sélectionnez l'élément *Partage de fichiers et d'imprimantes* dans la liste des exceptions.
		TCP 3725
		
		NetBIOS 137 - 139
		
		SMB (TCP 139, 445 et UDP 137, 138)
		
		TCP 135/445

Type de workload	Conditions préalables	Ports requis
Windows Server 2000 ; Windows XP ; Windows NT 4	◆ Windows Management Instrumentation (WMI) installé WMI ne fait pas partie de l'installation par défaut de Windows NT Server. Procurez-vous le noyau WMI à partir du site Web de Microsoft. Si WMI n'est pas installé, la découverte du workload échoue. WMI (RPC/DCOM) peut utiliser les ports TCP 135 et 445 ainsi que les ports aléatoires ou assignés dynamiquement supérieurs à 1024. Si vous rencontrez des problèmes lors du processus de découverte, envisagez de placer momentanément le workload dans une zone démilitarisée ou d'ouvrir temporairement les ports protégés par pare-feu uniquement pendant ce processus. Pour plus d'informations, telles que des conseils pour la limitation de la plage de ports pour DCOM et RPC, reportez-vous aux articles techniques Microsoft suivants. ◆ Utilisation de DCOM avec des pare-feux (http://msdn.microsoft.com/en-us/library/ms809327.aspx) ◆ Configuration de l'allocation dynamique de port RPC en vue de son fonctionnement avec des pare-feux (http://support.microsoft.com/default.aspx?scid=kb;en-us;154596) ◆ Configuration de DCOM pour fonctionner sur un pare-feu NAT (http://support.microsoft.com/kb/248809)	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 et UDP 137, 138) TCP 135/445
Tous les workloads Linux	Serveur Secure Shell (SSH)	TCP 22, 3725

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

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

Tableau 1-3 *Conditions d'accès et de communication requises pour les conteneurs*

Système	Conditions préalables	Ports requis
Tous les conteneurs	Fonctionnalité ping (demande et réponse d'écho ICMP).	
VMware ESX Server 3.5, 4, 4.1 ESXi ; vCenter Server	◆ Compte VMware avec rôle d'administrateur ◆ API de gestion de fichiers et API de services Web VMware	HTTPS TCP 443

1.3.3 Exigences de port ouvert pour les hôtes du serveur PlateSpin Protect

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

Tableau 1-4 *Exigences de port ouvert pour les hôtes du serveur PlateSpin Protect*

Port	Remarques
TCP 80	Pour la communication HTTP
TCP 443	Pour la communication HTTP sécurisée (si SSL est activé)

1.3.4 Protection sur des réseaux publics et privés via NAT

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

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

- **Serveur PlateSpin Protect :** dans le fichier de configuration `web.config` de votre serveur, inscrivez les adresses IP supplémentaires assignées à cet hôte. Reportez-vous à la section « Paramètres des adresses IP de serveur PlateSpin Protect supplémentaires (paramètres NAT) » page 24.
- **Workload source :** prise en charge uniquement pour le rétablissement, quand vous pouvez spécifier une adresse IP alternative pour le workload de récupération dans la section Détails du rétablissement (Workload sur VM) (page 53).
- **Conteneur cible :** lorsque vous essayez de découvrir un conteneur (tel que VMware ESX), spécifiez l'adresse IP publique (ou externe) de cet hôte dans les paramètres de découverte.
- **Cible de rétablissement :** lorsque vous essayez d'enregistrer une cible de rétablissement, spécifiez l'adresse IP publique (ou externe) dans les paramètres de découverte/ d'enregistrement.

1.4 Configuration des options par défaut de PlateSpin Protect

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

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

- « Configuration SMTP » page 18
- « Configuration des notifications automatiques des événements par message électronique » page 18
- « Configuration des rapports de réplication automatiques par message électronique » page 20

Configuration SMTP

Utilisez le client Web PlateSpin Protect pour configurer les paramètres SMTP (Simple Mail Transfer Protocol) du serveur utilisé pour envoyer des notifications des événements et rapports de réplication par message électronique.

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

Pour configurer les paramètres SMTP :

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

Configuration des notifications automatiques des événements par message électronique

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

5. Cliquez sur *Enregistrer*.

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

Les événements suivants déclenchent des notifications par message électronique :

Événement	Remarques
`Détection de workload en ligne`	Généré lorsque le système détecte qu'un workload précédemment hors ligne est désormais en ligne. S'applique aux workloads dont l'état de planification de la protection n'est pas *Suspendu*.
`Détection de workload hors ligne`	Généré lorsque le système détecte qu'un workload précédemment en ligne est désormais hors ligne. S'applique aux workloads dont l'état de planification de la protection n'est pas *Suspendu*.
`Échec de la réplication incrémentielle`	
`Échec de la réplication complète`	
`Test de basculement effectué`	Généré lors du marquage manuel d'une opération de test de basculement comme réussie ou échouée.
`Basculement effectué`	
`Préparation du basculement effectuée`	
`Échec de la préparation du basculement`	
`Échec du basculement`	
`Réplication incrémentielle manquée`	Généré 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.
`Réplication complète manquée`	Similaire à l'événement `Réplication incrémentielle manquée` ci-dessus.

Configuration des rapports de réplication automatiques par message électronique

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

1. Configurez le serveur SMTP que PlateSpin Protect doit utiliser. Reportez-vous à la section Configuration SMTP.
2. Dans le client Web PlateSpin Protect, cliquez sur *Paramètres* > *Adresse électronique* > *Paramètres des rapports de réplication*.
3. Sélectionnez l'option *Activer les rapports de réplication*.
4. Dans la section *Signaler la récurrence*, cliquez sur *Configurer* et spécifiez le schéma de récurrence souhaité pour les rapports.
5. Dans la section *Destinataires*, cliquez sur *Éditer les destinataires*, entrez les adresses électroniques souhaitées en les séparant par des virgules, puis cliquez sur *OK*.
6. (Facultatif) Dans la section *Protéger l'URL d'accès*, spécifiez une URL autre que celle par défaut pour votre serveur PlateSpin Protect (par exemple, quand l'hôte du serveur PlateSpin Protect 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 à travers des hyperliens 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 41.

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

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

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

1. Accédez à la configuration des langues dans votre navigateur Web :
   - **Internet Explorer :** cliquez sur *Outils* > *Options Internet* > *onglet Général* > *Langues*.
   - **Firefox :** cliquez sur *Outils* > *Options* > *onglet Contenu* > *Langues*.
2. Ajoutez la langue souhaitée et déplacez-la vers le haut de la liste.
3. Enregistrez les paramètres, puis démarrez l'application client en vous connectant à votre serveur PlateSpin Protect. Reportez-vous à la section « Lancement du client Web PlateSpin Protect » page 31.

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

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

1. Accédez à l'hôte du serveur PlateSpin Protect.
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.

1.4.3 Configuration du comportement du produit via les paramètres de configuration XML

Certains aspects du comportement de votre serveur PlateSpin Protect dépendent des paramètres de configuration définis dans les fichiers `*.config` sur l'hôte du serveur PlateSpin Protect.

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

Pour modifier et appliquer des paramètres `*.config`, procédez comme suit :

1. Sur l'hôte du serveur PlateSpin Protect, accédez au répertoire indiqué.
2. Utilisez un éditeur de texte pour ouvrir le fichier `*.config`.
3. Recherchez le paramètre souhaité dans le fichier `*.config` et modifiez sa valeur, laquelle est entre guillemets (""). Ne supprimez pas les guillemets. Utilisez des valeurs acceptables telles que décrites dans cette section ou suivant les recommandations du support PlateSpin.
4. Enregistrez, puis fermez le fichier `*.config`.
5. Redémarrez le serveur PlateSpin Protect. Reportez-vous à la section « Redémarrage du serveur PlateSpin Protect afin d'appliquer les modifications système » page 24.

Les sections suivantes contiennent des informations sur les fichiers de configuration couramment utilisés et sur les valeurs qui influent sur le comportement de votre serveur PlateSpin Protect.

- « Paramètres permettant d'optimiser les transferts sur des connexions WAN » page 22
- « Paramètres d'activation de la communication SSL » page 23
- « Paramètres permettant d'imposer une fenêtre d'interdiction de réplication » page 23
- « Paramètres des adresses IP de serveur PlateSpin Protect supplémentaires (paramètres NAT) » page 24

Paramètres permettant d'optimiser les transferts sur des connexions WAN

Utilisez ces paramètres pour optimiser les transferts sur des réseaux WAN. Ces paramètres sont globaux et affectent l'ensemble des réplications basées sur les fichiers et VSS.

- **Fichier de configuration :** `productinternal.config`
- **Emplacement :** `\Program Files\PlateSpin Protect Server\Web`

Pour plus d'informations sur la procédure de mise à jour, reportez-vous à la section « Configuration du comportement du produit via les paramètres de configuration XML » page 21.

Remarque : la modification de ces valeurs peut avoir un impact négatif sur les vitesses de réplication Gigabit LAN locale.

Le Tableau 1-5 liste les paramètres de configuration avec les valeurs par défaut et les valeurs recommandées pour un fonctionnement optimal dans un environnement WAN à latence élevée.

Tableau 1-5 *Paramètres de configuration par défaut et optimaux dans* `productinternal.config`

Paramètre	Valeur par défaut	Valeur optimale
`fileTransferThreadcount` Contrôle le nombre de connexions TCP ouvertes pour le transfert des données basé sur les fichiers.	2	de 4 à 6
`fileTransferMinCompressionLimit` Spécifie en octets le seuil de compression au niveau des paquets.	0 (désactivé)	65 536 max (64 Ko)
`fileTransferCompressionThreadsCount` Contrôle le nombre de threads utilisés pour la compression des données au niveau des paquets. Ce paramètre est ignoré si la compression est désactivée. Étant donné que la compression fait appel à l'UC, ce paramètre peut avoir un impact sur les performances.	2	S/O

Paramètre	Valeur par défaut	Valeur optimale

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

Paramètres d'activation de la communication SSL

Utilisez ces paramètres pour activer la communication SSL entre le client Web PlateSpin Protect et le serveur sur lequel vous avez activé SSL *après* l'installation du produit. Si SSL était déjà activé sur l'hôte du serveur au moment de l'installation, cette procédure n'est pas nécessaire.

- **Fichier de configuration :** `Platespin.Config`
- **Emplacement :** `\Program Files\PlateSpin Protect Server\Configs`
- **Valeur :** remplacez

  ```
  <add key="PowerConvertURL" value="http://localhost:80/PlateSpinMigrate" />
  ```

  par

  ```
  <add key="PowerConvertURL" value="https://localhost:443/PlateSpinMigrate" />
  ```

Pour plus d'informations sur la procédure de mise à jour, reportez-vous à la section « Configuration du comportement du produit via les paramètres de configuration XML » page 21.

Paramètres permettant d'imposer une fenêtre d'interdiction de réplication

- **Fichier de configuration :** `PlateSpin.Protection.Scheduler.Service.dll.config`
- **Emplacement :** `\Program Files\PlateSpin Protect Server\services\PlateSpinService\Plugins`
- **Valeurs :** ce paramètre comporte deux valeurs :
  - `Workload_Scheduling_Blackout_Window_Start` : définit l'heure du début de l'interruption. Utilisez le format suivant :

    `HH:MM:SS (HH 00-23, MM 00-59, SS 00-59)`

- `Workload_Scheduling_Blackout_Window_Length` : définit la durée de l'interruption. Utilisez le format suivant :

  `HH:MM:SS (HH 00-23, MM 00-59, SS 00-59)`

Pour plus d'informations sur la procédure de mise à jour, reportez-vous à la section « Configuration du comportement du produit via les paramètres de configuration XML » page 21.

Paramètres des adresses IP de serveur PlateSpin Protect supplémentaires (paramètres NAT)

Utilisez ces paramètres pour enregistrer des adresses IP supplémentaires de votre serveur PlateSpin Protect pour la communication dans des environnements avec NAT activé :

- **Fichier de configuration :** `Web.config`
- **Emplacement :** `\Program Files\PlateSpin Protect Server\Web`
- **Valeurs :** `<add key="AlternateServerAddresses" value="" />`

  Ajoutez les adresses IP supplémentaires en les séparant par un point-virgule (;), par exemple :

  `<add key="AlternateServerAddresses" value="10.99.106.108;10.99.106.109" />`

1.4.4 Redémarrage du serveur PlateSpin Protect afin d'appliquer les modifications système

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

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

Présentation du produit 2

2.1 À propos de PlateSpin Protect

PlateSpin Protect est un logiciel qui réplique et récupère rapidement des workloads (systèmes d'exploitation, intergiciels et données). En cas de sinistre ou de panne du serveur de production, les workloads peuvent être rapidement activés et exécutés normalement jusqu'à ce que l'environnement de production soit restauré.

PlateSpin Protect propose deux mécanismes différents de protection des workloads :

- **Virtualisation :** ce mécanisme permet de récupérer rapidement un workload mais implique de disposer d'un hôte de VM existant (un *conteneur* de VM).

  Dans ce scénario, PlateSpin Protect crée un workload de basculement (une réplique virtuelle de votre workload de production) qu'il met à jour régulièrement à des intervalles configurables. Si votre workload de production se retrouve hors ligne, vous pouvez basculer vers la réplique de VM, qui assure alors les services du workload défectueux. Vous pouvez ensuite rétablir ce workload sur son infrastructure initiale ou sur une toute nouvelle, physique ou virtuelle.
- **Création d'image :** ce mécanisme permet de récupérer un workload à l'aide d'une image protégée de ses volumes. Cette méthode nécessite plus de temps que la récupération à partir d'une réplique virtuelle. Néanmoins, elle ne requiert pas d'hôte de VM ; une image du workload est capturée, stockée et régulièrement mise à jour sur pratiquement n'importe quel hôte que vous désignez comme serveur d'images. Si votre workload de production se retrouve hors ligne, vous pouvez déployer l'image capturée pour l'exécuter sur du matériel physique ou, si nécessaire et disponible, sur un hôte de VM.

2.2 Configurations prises en charge

2.2.1 Workloads pris en charge dans les conteneurs de VM

PlateSpin Protect prend en charge les workloads Windows et Linux.

Tableau 2-1 *Charges de travail Windows prises en charge*

Système d'exploitation	Remarques
Windows 7	
Windows Server 2008 R2	Y compris les systèmes DC (contrôleur de domaine) et les versions SBS (Small Business Server)
Windows Server 2008	Y compris les systèmes DC (contrôleur de domaine) et les versions SBS (Small Business Server)
Windows Vista	Éditions professionnelle, entreprise et intégrale ; SP1 et versions ultérieures
Windows Server 2003	Y compris les systèmes DC (contrôleur de domaine) et les versions SBS (Small Business Server)
Windows XP Professionnel	
Windows Server 2000	
Grappes (clusters) Windows	Prise en charge uniquement pour les cibles sur VMware ESX 3.0.2 et versions ultérieures. Reportez-vous à la section « Protection des grappes Windows » page 55.

Versions internationales prises en charge (Windows) : français, allemand, japonais, chinois traditionnel et chinois simplifié

Tableau 2-2 *Workloads Linux pris en charge*

Système d'exploitation
Open Enterprise Server 2, SP2 et SP3
SUSE Linux Enterprise Server (SLES) 9, 10, 11
Red Hat Enterprise Linux (RHEL) 4 ou 5

Versions internationales prises en charge (Linux) : toutes les versions internationales de ces systèmes Linux sont prises en charge.

2.2.2 Workloads pris en charge dans les conteneurs d'images

Systèmes d'exploitation :

- Windows Server 2008 (DC et SBS inclus)
- Windows Server 2008 R2
- Windows Vista
- Windows Server 2003 (DC et SBS inclus)
- Windows 2000
- Windows XP

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

2.2.3 Hôtes de conteneur d'images pris en charge

Tableau 2-3 *Hôtes de conteneur d'images pris en charge*

Configuration requise	Détails
Système d'exploitation	N'importe lequel des éléments suivants. ◆ Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 ◆ Microsoft Windows Vista ◆ Microsoft Windows Server 2003, Microsoft Windows Server 2003 R2 ◆ Microsoft Windows 2000
Espace disque	100 Mo minimum pour le logiciel du contrôleur de base. La quantité d'espace supplémentaire requise dépend du nombre et de la taille des images de workload que vous souhaitez enregistrer sur un serveur d'images donné.
Logiciel	◆ Microsoft .NET Framework 2.0 ou ultérieur ◆ Service d'accès à distance au Registre activé et exécuté

2.2.4 Conteneurs de VM pris en charge

Les plates-formes de virtualisation suivantes sont prises en charge en tant que conteneurs de VM :

- VMware vCenter 4.1
- Grappe VMware DRS dans vSphere 4.1
- VMware ESX 4
- VMware ESX 4i
- VMware ESX 3.5.*x*
- VMware ESX 3i

Remarque : les versions 3i et 4i d'ESX doivent avoir une licence payante ; la protection n'est pas prise en charge pour ces systèmes s'ils fonctionnent avec une licence gratuite.

2.3 Sécurité et confidentialité

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

- Section 2.3.1, « Sécurité des données de workload lors d'une transmission », page 28
- Section 2.3.2, « Sécurité des communications client/serveur », page 28
- Section 2.3.3, « Sécurité des références », page 28
- Section 2.3.4, « Authentification et autorisation utilisateur », page 28

2.3.1 Sécurité des données de workload lors d'une transmission

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

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

Vous pouvez activer ou désactiver le codage pour chaque protection de workload, le codage étant un paramètre des détails de protection de workload. Reportez-vous à la section « Détails de protection de workload » page 46.

2.3.2 Sécurité des communications client/serveur

La transmission de données entre le serveur PlateSpin Protect et le client Web PlateSpin Protect peut être configurée pour utiliser le protocole HTTP (par défaut) ou HTTPS (protocole sécurisé).

Pour sécuriser la transmission de données entre le client et le serveur, activez SSL sur l'hôte du serveur PlateSpin Protect, mettez à jour la configuration du serveur pour qu'elle intègre la modification (voir la section « Paramètres d'activation de la communication SSL » page 23) et utilisez le protocole HTTPS lorsque vous spécifiez le serveur URL.

2.3.3 Sécurité des références

Les références que vous utilisez pour accéder à divers systèmes (tels que les workloads et les cibles de rétablissement) sont stockées dans la base de données PlateSpin Protect. 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.

2.3.4 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 1.2, « Configuration de l'authentification et de l'autorisation utilisateur », page 10.

2.4 Performances

2.4.1 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 Protect ;
- 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 codage 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.

2.4.2 Compression des données

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

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

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

La compression des données peut être configurée par protection ou par niveau de protection. Reportez-vous à la section « Niveaux de protection » page 77.

2.4.3 Limitation de la bande passante

PlateSpin Protect permet de contrôler la consommation de la bande passante disponible grâce à une communication source-cible directe pendant une protection de workload ; vous pouvez définir un débit pour chaque planification 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 Protect.

La limitation de la bande passante est un paramètre du niveau de protection du contact de protection d'un workload. Reportez-vous à la section « Niveaux de protection » page 77.

2.4.4 Spécifications RPO, RTO et TTO

- **Perte de données maximale admissible (PDMA ou RPO – Recovery Point Objective) :** décrit la quantité acceptable de perte de données, mesurée dans le temps. La PDMA est déterminée par l'intervalle de temps entre les réplications incrémentielles d'un workload protégé et dépend des niveaux d'utilisation actuels de PlateSpin Protect, du taux et de l'ampleur des modifications sur le workload ainsi que de la vitesse de votre réseau.
- **Délai maximal d'interruption admissible (DMIA ou RTO – Recovery Time Objective) :** décrit le temps requis pour une opération de basculement (mise en ligne d'une réplique de workload pour remplacer temporairement un workload de production protégé).

  Le DMIA pour le basculement d'un workload sur sa réplique virtuelle dépend du temps nécessaire à la configuration et à l'exécution de l'opération de basculement (10 à 45 minutes). Reportez-vous à la section « Basculement » page 49.

  Le DMIA pour le déploiement d'une image protégée en tant que workload démarrable dépend de l'infrastructure cible (physique ou virtuelle) et du temps nécessaire au déploiement de l'image correspondante. Reportez-vous à la section « Déploiement d'une image de workload » page 62.
- **Délai maximal de test admissible (DMTA ou TTO – Test Time Objective) :** décrit le temps nécessaire au test de la reprise après sinistre avec un niveau de confiance pour la restauration du service.

  Utilisez la fonction *Test de basculement* pour passer en revue les différents scénarios et générer des données d'évaluation des performances.

Le nombre d'opérations de basculement simultanées nécessaires fait partie des facteurs ayant un impact sur la PDMA, le DMIA et le DMTA. En effet, un seul workload de basculement dispose de davantage de mémoire et de ressources d'UC que plusieurs workloads de basculement, lesquels partagent les ressources de leur infrastructure sous-jacente.

Pour obtenir un délai moyen de basculement pour les workloads de votre environnement, effectuez des tests de basculement à différents moments, puis utilisez-les en tant que données de référence dans vos plans généraux de récupération de données. Reportez-vous à la section « Génération de rapports sur les workloads et leur protection » page 41.

2.4.5 Évolutivité

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

- **Workloads par serveur :** nombre de workloads par serveur PlateSpin Protect. Peut être compris entre 5 et 50, en fonction de plusieurs 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 VM prises en charge par l'hôte ESX. D'autres facteurs comprennent les statistiques de récupération (dont les basculements et les réplications 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.

Fonctionnement

3

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

3.1 Lancement du client Web PlateSpin Protect

La plupart des interactions avec PlateSpin Protect s'effectuent via le client Web PlateSpin Protect basé sur un navigateur.

Les navigateurs pris en charge sont les suivants :

- Microsoft Internet Explorer 7, 8, 9
- Mozilla Firefox (sous Windows) 3.6, 4

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

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

Pour utiliser le client Web PlateSpin Protect et l'aide intégrée dans une des langues prises en charge, reportez-vous à la Section 1.4.2, « Configuration de la langue pour les versions internationales de PlateSpin Protect », page 20.

Pour lancer le client Web PlateSpin Protect :

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

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

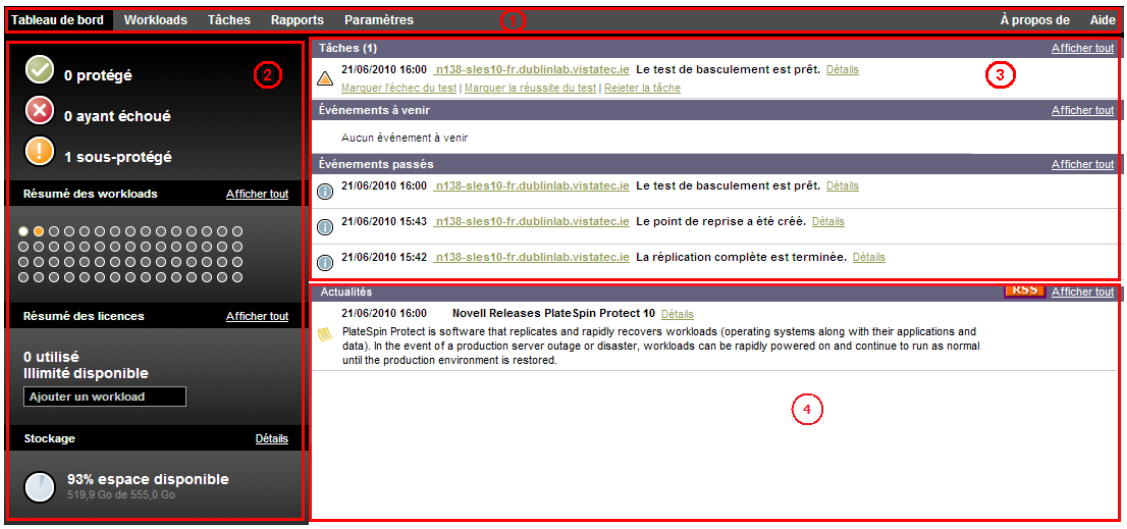
   Remplacez *<nom_hôte | adresse_IP>* par le nom d'hôte et l'adresse IP de l'hôte du serveur PlateSpin Protect.

   Si SSL est activé, utilisez le protocole `https` dans l'URL.

3.2 Éléments du client Web PlateSpin Protect

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

Figure 3-1 *Page Tableau de bord par défaut du client Web PlateSpin Protect*



La page Tableau de bord comprend les éléments suivants :

- **Barre de navigation :** figure sur la plupart des pages du client Web PlateSpin Protect.
- **Panneau de résumé visuel :** fournit une vue d'ensemble de l'état global de l'inventaire des workloads de PlateSpin Protect.
- **Panneau des tâches et événements :** fournit des informations sur les événements et les tâches nécessitant l'attention de l'utilisateur.
- **Panneau Actualités :** fournit des informations sur les produits et les mises à jour associées par le biais de flux RSS. Pour vous abonner au flux d'actualités PlateSpin Protect, cliquez sur *RSS*.

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

- Section 3.2.1, « Barre de navigation », page 33
- Section 3.2.2, « Panneau de résumé visuel », page 33
- Section 3.2.3, « Panneau des tâches et événements », page 34

3.2.1 Barre de navigation

La barre de navigation fournit les liens suivants :

- **Tableau de bord :** affiche la page Tableau de bord par défaut.
- **Workloads :** affiche la page Workloads. Reportez-vous à la section « Workloads et commandes de workload » page 34.
- **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 41.
- **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 77.
  - **Autorisations :** reportez-vous à la section « Configuration de l'authentification et de l'autorisation utilisateur » page 10.
  - **Conteneurs :** reportez-vous à la section « Ajout de conteneurs » page 40.
  - **Adresse électronique/SMTP :** reportez-vous à la section « Configuration des notifications automatiques des événements et rapports par message électronique » page 18.
  - **Licences/Désignations des licences :** reportez-vous à la section « Activation de la licence du produit » page 9.

3.2.2 Panneau de résumé visuel

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

Les workloads inventoriés sont classés en trois catégories :

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

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

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

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

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

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

3.2.3 Panneau des tâches et événements

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

Des événements sont consignés à chaque fois que quelque chose de particulier en rapport avec le système ou le workload se produit. Par exemple, l'ajout d'un nouveau workload protégé, la réplication d'un workload en cours de démarrage ou en état d'échec, ou encore la détection d'un échec de workload protégé constituent des événements. Certains événements génèrent des notifications automatiques par message électronique si SMTP est configuré. Reportez-vous à la section « Configuration des notifications automatiques des événements et rapports par message électronique » page 18.

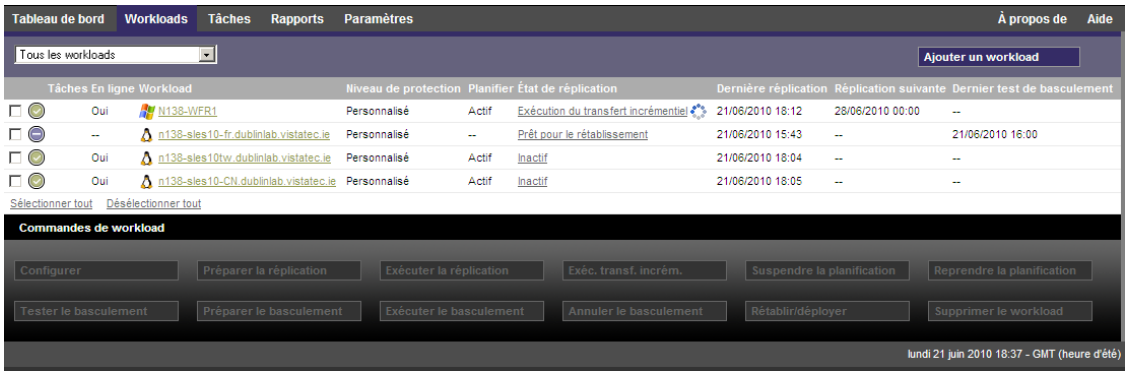
Les tâches sont des commandes spéciales qui sont liées à des événements exigeant l'intervention de l'utilisateur. Par exemple, à la fin de l'exécution d'une commande Tester le basculement, le système génère un événement associé à deux tâches : `Marquer le test comme réussi` et `Marquer le test comme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

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

3.3 Workloads et commandes de workload

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

Figure 3-2 *La page Workloads*

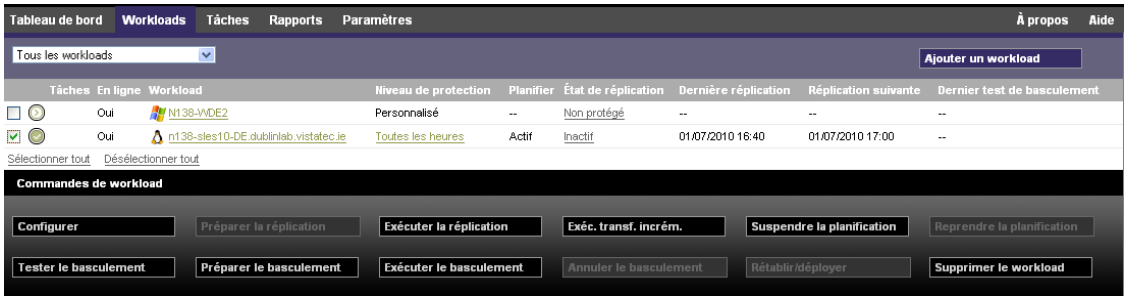


Remarque : tous les tampons horaires reflètent le fuseau horaire de l'hôte du serveur PlateSpin Protect, lequel peut être différent du fuseau horaire du workload protégé ou de celui de l'hôte sur lequel vous exécutez le client Web PlateSpin Protect. La date et l'heure du serveur s'affichent en bas en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

3.3.1 Commandes de protection et de récupération de workload

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

Figure 3-3 *Commandes de workload*



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

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

Commande de workload	Description
Configurer	Démarre la configuration de protection de workload à l'aide des paramètres applicables à un workload inventorié.
Préparer la réplication	Installe le logiciel de transfert de données requis sur la source et crée une VM de basculement en vue de la réplication de workload.
Exécuter la réplication	Démarre la réplication du workload source conformément aux paramètres spécifiés.
Exécuter le transfert incrémentiel	Effectue un transfert séparé des données modifiées à partir de la source vers la cible, hors de la planification de protection des workloads.
Suspendre la planification	Suspend la protection ainsi que le transfert des données du workload protégé.
Reprendre la planification	Reprend la protection en fonction des paramètres de protection enregistrés.
Tester le basculement	Met le workload de récupération en ligne dans un environnement isolé au sein du conteneur, afin de réaliser un test.
Préparer le basculement	Démarre le workload de récupération en vue d'une opération de basculement.

Commande de workload	Description
Exécuter le basculement	Démarre et configure le workload de récupération qui reprend les services métier d'un workload ayant échoué.
Annuler le basculement	Abandonne le processus de basculement.
Rétablir/déployer	À la suite d'une opération de basculement, rétablit le workload de récupération dans son infrastructure initiale ou dans une nouvelle infrastructure (virtuelle ou physique).
Supprimer le workload	Supprime un workload de l'inventaire.

3.4 Résumé des modifications de l'expérience utilisateur par rapport au client Portability Suite

Le tableau suivant contient une référence rapide aux utilisateurs du client Portability Suite discontinué.

Tableau 3-3 *Différences d'expérience utilisateur entre le client Portability Suite et le client Web*

Fonction	Client Portability Suite (ancien)	Client Web (nouveau)
Démarrage du client	*Démarrer* > *Programmes* > *PlateSpin Portability Suite Client*	Démarrer le navigateur > Accéder à `http://<accueil_serveur>/protect`
Réseau Portability Suite	Option d'interface utilisateur dans les paramètres de connexion du serveur	Discontinué
Découverte (sources)	Vue *Serveurs* > Clic avec le bouton droit de la souris dans un espace blanc > *Détails de découverte*	Tableau de bord > *Commande Ajouter un workload*
Découverte (cibles)	Vue *Serveurs* > Clic avec le bouton droit de la souris dans un espace blanc > *Détails de découverte*	*Paramètres* > *Conteneurs* > *Ajouter un conteneur*
Sélection d'étendue de transfert (synchronisation complète ou des serveurs)	Démarrez une tâche de migration et sélectionnez *Synchronisation des serveurs (modifications uniquement)* comme étendue du transfert.	Commencez à configurer l'opération appropriée (comme *Ajouter un workload* ou *Rétablissement*) puis, pour la méthode de *Réplication initiale*, choisissez *Incrémentielle*.
Affichage des listes de tâches	Vue *Tâches* spécifique	*Rapports* > *Événements*

Fonction	Client Portability Suite (ancien)	Client Web (nouveau)
Mise à jour des références de workload	Commande *Enregistrer* dans la boîte de dialogue *Détails de découverte* ou *Rafraîchir*.	◆ **Conteneurs :** *Paramètres* > *Conteneurs* > Cliquez sur *<nom_conteneur>*. ◆ **Workloads :** Modification des détails de protection (cliquez sur le nom du workload découvert)

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

Vous pouvez utiliser la fonctionnalité de protection de workload à l'aide d'un programme, via l'API `protection.webservices` inhérente à vos applications. Vous pouvez utiliser n'importe quel langage de script ou de programmation prenant en charge les services Web.

`http://`*<nom_hôte | adresse_IP>*`/protection.webservices`

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

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.

3.6 Gestion de plusieurs instances de PlateSpin Protect

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

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

- Section 3.6.1, « Utilisation de la console de gestion de PlateSpin Protect », page 37
- Section 3.6.2, « À propos des cartes de la console de gestion de PlateSpin Protect », page 38
- Section 3.6.3, « Ajout d'instances de PlateSpin Protect à la console de gestion », page 39
- Section 3.6.4, « Gestion des cartes sur la console de gestion », page 39

3.6.1 Utilisation de la console de gestion de PlateSpin Protect

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

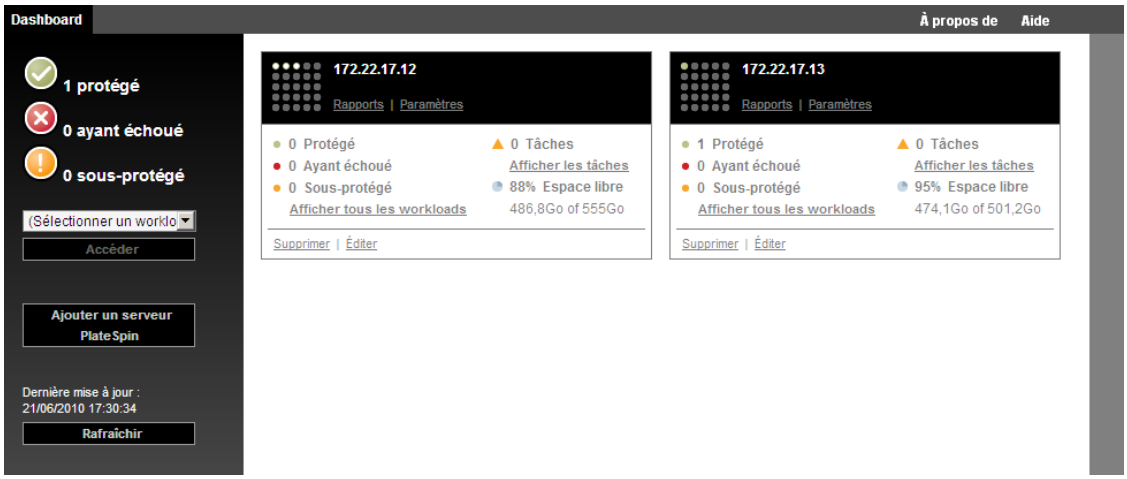
   `http://`*<adresse_IP | nom_hôte>*`/console`

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

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

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

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



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

Lorsqu'une instance de PlateSpin Protect est ajoutée à la console de gestion, elle est représentée par une carte.

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

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

- l'adresse IP/le nom d'hôte ;
- l'emplacement ;
- le numéro de version ;
- le nombre de workloads ;

- l'état des workloads ;
- la capacité de stockage ;
- l'espace libre disponible.

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

3.6.3 Ajout d'instances de PlateSpin Protect à la console de gestion

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

Remarque : lorsque vous vous loguez à la console de gestion sur une instance PlateSpin Protect, cette dernière n'est pas automatiquement ajoutée à la console. L'ajout doit se faire manuellement.

Pour ajouter une instance PlateSpin Protect à la console :

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

   La page *Ajouter/éditer* s'affiche.
2. Spécifiez l'URL de l'hôte du serveur PlateSpin Protect. Les protocoles HTTP et HTTPS sont tous deux pris en charge.
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 que vous ajoutez. Dans le champ *Mot de passe*, saisissez le mot de passe adéquat.
5. (Facultatif) Spécifiez un *nom d'affichage* identifiant ou descriptif (maximum 15 caractères), un *emplacement* (maximum 20 caractères) et les éventuelles *remarques* que vous souhaitez ajouter (maximum 400 caractères).
6. Cliquez sur *Ajouter/enregistrer*.

   Une nouvelle carte est ajoutée au tableau de bord.

3.6.4 Gestion des cartes sur la console de gestion

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

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

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

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

Pour supprimer une carte PlateSpin Protect de la console de gestion :

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

Une invite de confirmation s'affiche.

2 Cliquez sur *OK*.

Cette carte est supprimée du tableau de bord.

3.7 Ajout de conteneurs

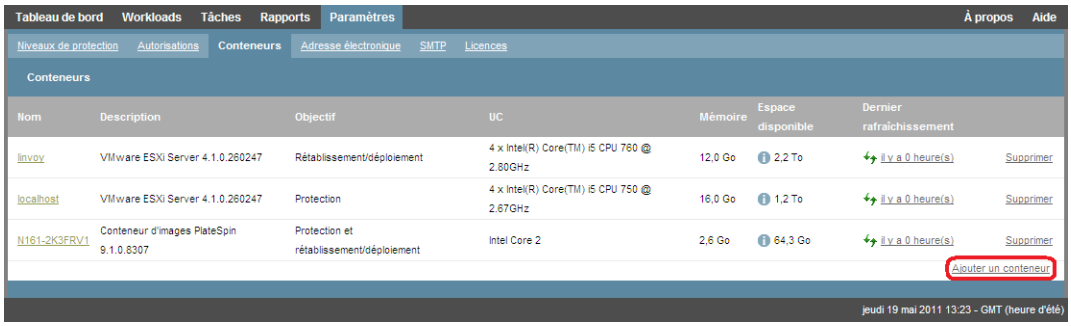
Un conteneur est une infrastructure de protection opérant en tant qu'hôte d'une réplique régulièrement mise à jour d'un workload protégé. Il existe deux catégories d'infrastructure de protection : la virtualisation et la création d'image.

Technologie de virtualisation	VMware ESX Server
	Grappe VMware DRS
Technologie de création d'image	Serveur d'images PlateSpin

Pour pouvoir protéger un workload, vous devez ajouter un conteneur soit à l'avance, soit durant la procédure d'ajout du workload à protéger.

Pour ajouter un conteneur :

1 Dans le client Web PlateSpin Protect, cliquez sur *Paramètres* > *Conteneurs* > *Ajouter un conteneur*.



2 Spécifiez les paramètres suivants :

- **Type :** sélectionnez le type de conteneur (*VMware ESX Server*, *Grappe DRS VMware* ou *Serveur d'images PlateSpin*). Assurez-vous que le conteneur sélectionné est pris en charge. Pour plus d'informations, reportez-vous aux sections suivantes :
  - « Conteneurs de VM pris en charge » page 27
  - « Hôtes de conteneur d'images pris en charge » page 27
- **Nom d'hôte ou adresse IP :** saisissez le nom d'hôte ou l'adresse IP du conteneur.
- **Nom d'hôte vCenter ou adresse IP :** (grappes DRS uniquement) entrez le nom d'hôte ou l'adresse IP du serveur vCenter.
- **Nom de la grappe :** (grappes DRS uniquement) entrez le nom de la grappe DRS souhaitée.

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

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

- **Nom d'utilisateur/mot de passe :** indiquez des références de niveau admin pour accéder à l'hôte requis. Reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 75
- **Objectif :** (conteneurs de VM uniquement) sélectionnez l'élément requis (*Protection*, *Rétablissement/déploiement* ou les deux). Si vous sélectionnez les deux éléments (*Protection* et *Rétablissement/déploiement*, le conteneur peut être sélectionné en tant que cible pour les opérations de protection et de rétablissement/déploiement.

3 Cliquez sur *Ajouter*.

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

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

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

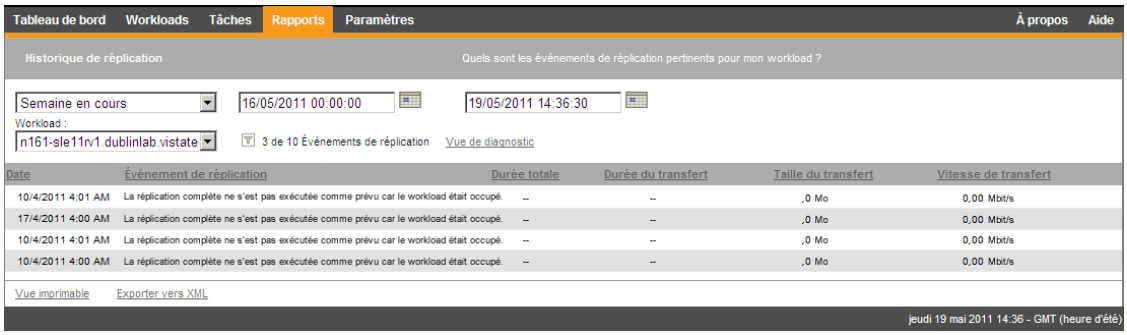
3.8 Génération de rapports sur les workloads et leur protection

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

Les types de rapport suivants sont pris en charge :

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

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



Pour générer un rapport :

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

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

Protection de workload

4

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

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

Outre la protection de workload à l'aide de la fonctionnalité de virtualisation, PlateSpin Protect permet également de protéger les images de workload par le biais d'une fonctionnalité de création d'image de volume. Reportez-vous à la section « Protection de l'image de workload » page 61.

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

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

1 Étape préparatoire :

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

Reportez-vous à la section « Configurations prises en charge » page 25.

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

Reportez-vous à la section « Conditions d'accès et de communication requises sur votre réseau de protection » page 14.

1c (Linux uniquement)

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

  Reportez-vous à l'article de la base de connaissances n° 7005873 (http://www.novell.com/support/viewContent.do?externalId=7005873).

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

  Reportez-vous à l'article de la base de connaissances n° 7005872 (http://www.novell.com/support/viewContent.do?externalId=7005872).

- (Facultatif) Définissez et préparez les scripts personnalisés que vous souhaitez exécuter sur votre workload source lors de chaque réplication.

  Reportez-vous à la section « Utilisation des scripts freeze et thaw pour chaque réplication (Linux) » page 80.

2. Ajoutez un conteneur.

   Reportez-vous à la section « Ajout de conteneurs » page 40.

3. Ajoutez un workload.

   Reportez-vous à la section « Ajout d'un workload à protéger » page 44.

4. Configurez les détails de protection et préparez la réplication.

   Reportez-vous à la section « Configuration des détails de protection et préparation de la réplication » page 46.

5. Lancez la planification de protection de workload.

   Reportez-vous à la section « Démarrage de la protection du workload » page 48.

6. (Facultatif) Effectuez manuellement un transfert incrémentiel.

7. (Facultatif) Testez la fonctionnalité de basculement.

   Reportez-vous à la section Test du workload de récupération et de la fonctionnalité de basculement.

8. Exécutez un basculement.

   Reportez-vous à la section « Basculement » page 49.

9. Exécutez un rétablissement.

   Reportez-vous à la section « Rétablissement » page 51.

10. (Facultatif) Protégez à nouveau un workload après rétablissement.

À l'exception des étapes 1, 8 et 9, ces étapes correspondent à des commandes de workload sur la page Workloads. Reportez-vous à la section « Workloads et commandes de workload » page 34.

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

4.2 Ajout d'un workload à protéger

1. Suivez les étapes préparatoires requises.

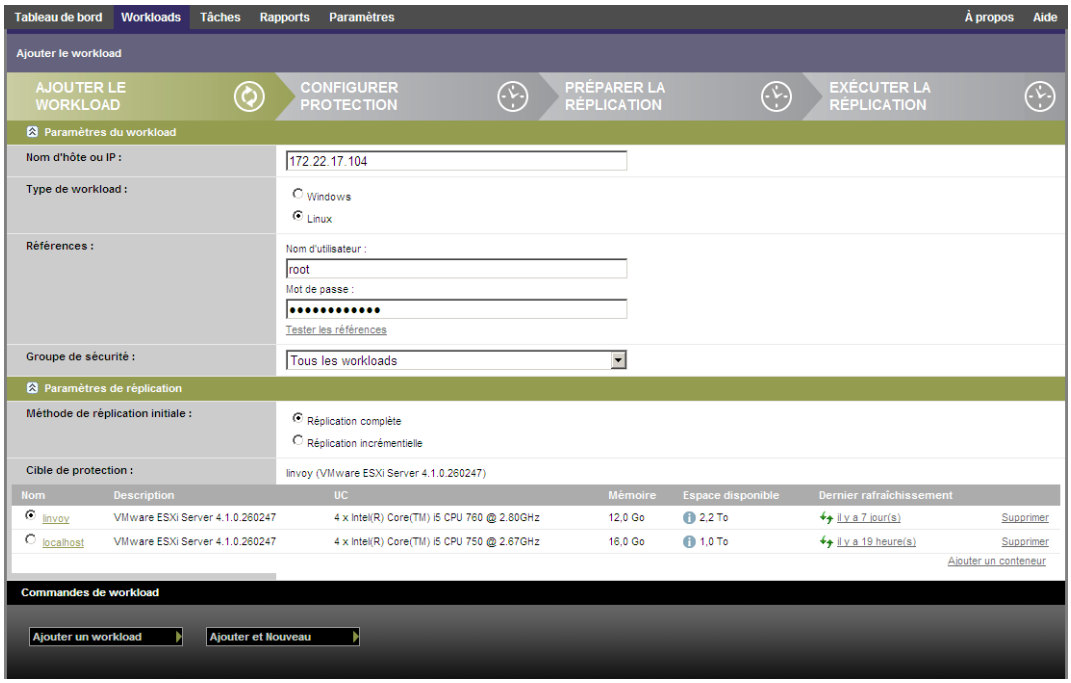
   Reportez-vous à l'Étape 1 de la section « Workflow de base pour la protection et la récupération de workload » page 43.

2. Ajoutez un conteneur de VM.

   Reportez-vous à la section « Ajout de conteneurs » page 40.

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

   Le client Web PlateSpin Protect affiche la page Ajouter le workload.



4 Spécifiez les détails de workload requis.

- **Paramètres du workload :** spécifiez le nom d'hôte de votre workload ou l'adresse IP, le système d'exploitation, les références de niveau d'administration et un groupe de sécurité à assigner au workload. Reportez-vous à la section « Gestion des groupes de sécurité et des autorisations de workload de PlateSpin Protect » page 13.

  Utilisez le format requis pour les références. Reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 75.

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

- **Paramètres de réplication :** sélectionnez les paramètres de réplication requis. Reportez-vous à la section « Méthode de réplication initiale (totale et incrémentielle) » page 79.

- **Cible de protection :** sélectionnez la cible de protection requise. Il s'agit soit du conteneur cible, soit d'un workload préparé si vous avez sélectionné *Réplication incrémentielle* comme méthode de réplication initiale. Reportez-vous à la section « Méthode de réplication initiale (totale et incrémentielle) » page 79.

5 Cliquez sur *Ajouter un workload*.

PlateSpin Protect recharge la page Workloads et affiche un indicateur de processus pour le workload en cours d'ajout. Attendez que le processus se termine. Une fois terminé, un événement *Workload ajouté* s'affiche dans le tableau de bord.

4.3 Configuration des détails de protection et préparation de la réplication

Les détails de protection contrôlent les paramètres de protection et de récupération de workload, ainsi que le comportement d'un workload protégé durant tout son cycle de vie. À chaque phase du workflow de protection et de récupération (voir la section « Workflow de base pour la protection et la récupération de workload » page 43), les paramètres pertinents sont lus à partir des détails de protection.

Pour configurer les détails de protection de votre workload :

1. Ajoutez un workload. Reportez-vous à la section « Ajout d'un workload à protéger » page 44.
2. Sur la page Workloads, sélectionnez le workload souhaité, puis cliquez sur *Configurer*.

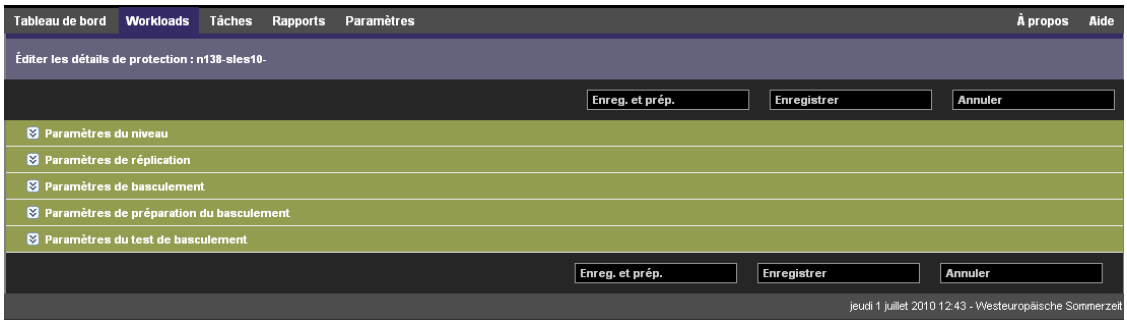
   Le client Web PlateSpin Protect affiche la page des détails de protection du workload.
3. Configurez les détails de la protection dans chaque ensemble de paramètres en fonction de vos besoins en matière de continuité des opérations. Reportez-vous à la section « Détails de protection de workload » page 46.
4. Corrigez les erreurs de validation éventuelles.
5. Cliquez sur *Enregistrer*.

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

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

4.3.1 Détails de protection de workload

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



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

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

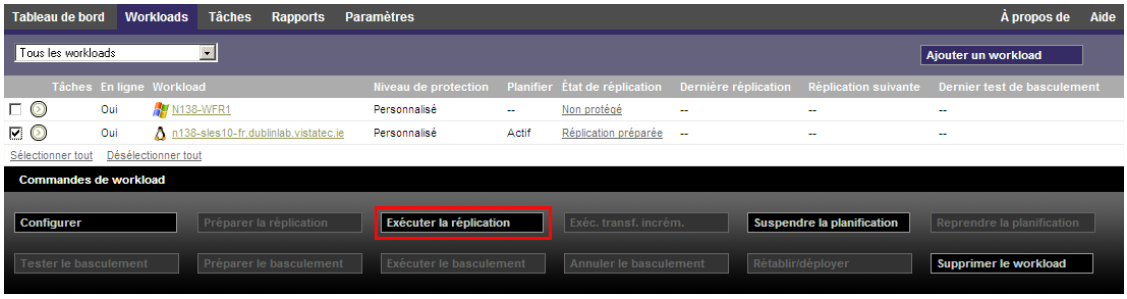
Tableau 4-1 *Détails de protection du workload*

Ensemble de paramètres (paramètres)	Détails
Niveau	Indique le niveau de protection assuré par la protection actuelle. Reportez-vous à la section « Niveaux de protection » page 77.
Réplication	**Codage du transfert :** pour activer le codage, sélectionnez l'option *Coder le transfert des données*. Reportez-vous à la section « Sécurité et confidentialité » page 27. **Méthode de transfert :** (Windows) permet de sélectionner un mécanisme de transfert des données ainsi qu'une sécurité par le biais du codage. Reportez-vous à la section « Méthodes de transfert » page 76. **Références sources :** requises pour accéder au workload. Reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 75. **Nombre d'UC :** permet de spécifier le nombre requis d'UC assigné au workload de récupération. **Réseau de réplication :** permet de scinder le trafic de réplication en fonction des réseaux virtuels définis sur votre conteneur de VM. Reportez-vous à la section « Réseautique » page 82. **Banque de données des points de reprise :** permet de sélectionner une banque de données associée à votre conteneur de VM pour stocker les points de reprise. Reportez-vous à la section « Points de reprise » page 78. **Volumes protégés :** ces options permettent de sélectionner des volumes à protéger et d'assigner leurs répliques à des banques de données spécifiques de votre conteneur de VM. Vous pouvez également sélectionner pour la protection : ◆ Workloads Linux : volumes logiques et groupes de volumes ◆ Workloads OES 2 : volumes EVMS Reportez-vous à la section « Volumes » page 81. **Option de disque léger :** active la fonction de disque virtuel alloué dynamiquement, un disque virtuel qui se présente à la VM avec une taille définie, mais qui ne consomme que l'espace disque nécessaire à ce disque. **Services/daemons à arrêter pendant la réplication :** permet de sélectionner les services Windows ou les daemons Linux à arrêter automatiquement pendant la réplication. Reportez-vous à la section « Contrôle des services et des daemons » page 80.

Ensemble de paramètres (paramètres)	Détails
Basculement	**Mémoire de la machine virtuelle :** permet de spécifier la quantité de mémoire allouée à la machine virtuelle de basculement. **Nom d'hôte et affiliation au domaine/groupe de travail :** ces options permettent de contrôler l'identité et l'affiliation à un domaine/groupe de travail du workload de basculement lorsqu'il est actif. Pour l'affiliation au domaine, les références de l'administrateur du domaine sont requises. **Connexions réseau :** ces options permettent de contrôler les paramètres LAN du workload de basculement. Reportez-vous à la section « Réseautique » page 82. **États des services/daemons à modifier :** permet de contrôler l'état de démarrage de services d'application (Windows) ou de daemons (Linux) spécifiques. Reportez-vous à la section « Contrôle des services et des daemons » page 80.
Préparer le basculement	Permet de contrôler les paramètres réseau temporaires du workload de basculement pendant l'opération facultative Préparer le basculement. Reportez-vous à la section « Réseautique » page 82.
Test de basculement	**Mémoire de la machine virtuelle :** permet d'assigner la quantité de mémoire virtuelle requise au workload temporaire. **Nom d'hôte :** permet d'assigner un nom d'hôte au workload temporaire. **Domaine/groupe de travail :** permet d'affilier le workload temporaire à un domaine ou groupe de travail. Pour l'affiliation au domaine, les références de l'administrateur du domaine sont requises. **Connexions réseau :** contrôle les paramètres LAN du workload temporaire. Reportez-vous à la section « Réseautique » page 82. **États des services/daemons à modifier :** permet de contrôler l'état de démarrage de services d'application (Windows) ou de daemons (Linux) spécifiques. Reportez-vous à la section « Contrôle des services et des daemons » page 80.

4.4 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 l'établissement d'un contact de protection :

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

4.5 Basculement

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

- Section 4.5.1, « Détection de dysfonctionnements », page 49
- Section 4.5.2, « Exécution d'un basculement », page 50
- Section 4.5.3, « Test du workload de récupération et de la fonctionnalité de basculement », page 51

4.5.1 Détection de dysfonctionnements

Si une tentative de détection d'un workload échoue un certain nombre de fois, PlateSpin Protect génère un événement *Le workload est hors ligne*. Les critères qui déterminent et consignent les échecs de workload font partie des paramètres de niveau de protection de workload (reportez-vous à la ligne Niveau dans la section « Détails de protection de workload » page 46).

Si des notifications sont configurées avec des paramètres SMTP, PlateSpin Protect envoie simultanément une notification par message électronique aux destinataires spécifiés. Reportez-vous à la section « Configuration des notifications automatiques des événements et rapports par message électronique » page 18.

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, puis exécutez la commande *Exécuter le basculement*. Reportez-vous à la section « Exécution d'un basculement » page 50.

La figure ci-dessous montre comment se présente la page Tableau de bord du client Web PlateSpin Protect lorsqu'un échec de workload est détecté. Les tâches applicables s'affichent dans le volet des tâches et des événements.

Figure 4-1 *Page Tableau de bord en cas de détection d'un échec de workload*

4.5.2 Exécution d'un basculement

Les paramètres de basculement, dont les paramètres LAN et d'identité réseau du workload de récupération, sont enregistrés avec les détails de protection du workload au moment de la configuration. Reportez à la ligne Basculement dans la section « Détails de protection de workload » page 46.

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

- Sélectionnez le workload souhaité sur la page Workloads et cliquez sur *Exécuter le basculement*. Vous pouvez utiliser la commande facultative *Préparer le basculement* pour appliquer vos paramètres de basculement enregistrés au workload de récupération et le redémarrer en vue d'un basculement complet. Pensez à effectuer une opération *Préparer le basculement* distincte afin de vous assurer que votre workload de production a bel et bien échoué. Cela vous permet de gagner du temps lorsque vous exécutez une commande de *basculement* complet.
- Cliquez sur le lien hypertexte de commande adéquat de l'événement *Le workload est hors ligne* dans le volet des tâches et des événements. Reportez-vous à la Figure 4-1.
- Démarrez manuellement le workload de récupération à l'aide du client VMware vSphere. Si vous utilisez cette méthode, sélectionnez un instantané (point de reprise) à l'aide du gestionnaire d'instantanés du client vSphere.

  Reportez-vous à la documentation relative à votre produit VMware.

  Remarque : lorsque vous effectuez un basculement manuel, le système applique les paramètres de basculement tels qu'enregistrés lors de la réplication du workload.

Utilisez l'une de ces méthodes pour démarrer le processus de basculement et sélectionnez un point de reprise à appliquer au workload de récupération (reportez-vous à la section « Points de reprise » page 78). 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 de récupération ou le processus de basculement dans le cadre d'un exercice planifié de reprise après sinistre, reportez-vous à la section « Test du workload de récupération et de la fonctionnalité de basculement » page 51.

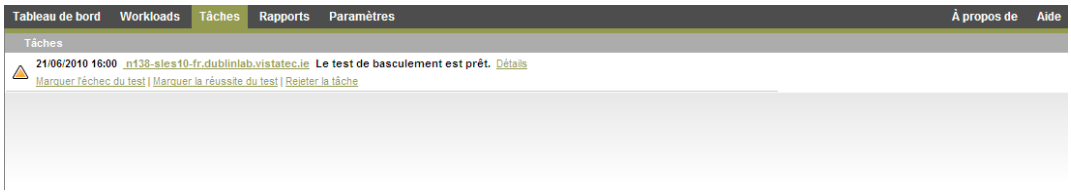
4.5.3 Test du workload de récupération et de la fonctionnalité de basculement

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

Lorsque vous exécutez la commande, PlateSpin Protect applique au workload de récupération les paramètres du test de basculement tels qu'enregistrés dans les détails de protection de workload (reportez-vous à la ligne Test de basculement dans la section « Détails de protection de workload » page 46).

1. Définissez une fenêtre de temps appropriée pour les tests et vérifiez qu'aucune réplication n'est en cours. L'état de réplication du workload doit être *Inactif*.
2. Sur la page Workloads, sélectionnez le workload requis, cliquez sur *Tester le basculement*, sélectionnez un point de reprise (voir la section « Points de reprise » page 78), 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 récupération. Utilisez le client VMware vSphere pour accéder au workload de récupération dans le conteneur de VM.
4. Indiquez si le test a réussi ou échoué. 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. 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 récupération et la protection reprend son état d'avant le test.

4.6 Rétablissement

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

Les méthodes de rétablissement varient en fonction du type d'infrastructure cible et du niveau d'automatisation du processus de rétablissement.

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

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

- Section 4.6.1, « Rétablissement automatisé sur une machine virtuelle », page 52
- Section 4.6.2, « Rétablissement semi-automatisé sur une machine physique », page 54
- Section 4.6.3, « Rétablissement semi-automatisé sur une machine virtuelle », page 55

4.6.1 Rétablissement automatisé sur une machine virtuelle

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

Les conteneurs suivants sont pris en charge en tant que cibles de rétablissement automatisées : VMware ESX 3i, 3.5.x, 4, 4i, 4.1.

1. Après un basculement, sélectionnez le workload sur la page Workloads, puis cliquez sur *Rétablir/déployer*.
2. Spécifiez les ensembles de paramètres suivants :
   - **Paramètres du workload :** spécifiez le nom d'hôte ou l'adresse IP du workload de récupération et entrez des références de niveau admin. Utilisez le format requis pour les références (reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 75).
   - **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 une cible. Reportez-vous à la section « Méthode de réplication initiale (totale et incrémentielle) » page 79.
     - **Type de cible :** sélectionnez *Cibles virtuelles*. Si vous ne disposez pas encore d'un conteneur de rétablissement, cliquez sur *Ajouter un conteneur* et désignez un hôte de VM pris en charge à l'aide de références de niveau root.
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 53.

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

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

Figure 4-2 *Détails de la commande Rétablissement*

Détails du rétablissement (Workload sur VM)

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

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

Ensemble de paramètres (paramètres)	Détails
Rétablissement	**Méthode de transfert :** (Windows) permet de sélectionner un mécanisme de transfert des données ainsi qu'une sécurité par le biais du codage. Reportez-vous à la section « Méthodes de transfert » page 76. **Réseau de rétablissement :** permet de diriger le trafic de rétablissement sur un réseau dédié, sur la base des réseaux virtuels définis sur votre conteneur de VM. Reportez-vous à la section « Réseautique » page 82. **Banque de données de VM :** permet de sélectionner une banque de données associée à votre conteneur de rétablissement pour le workload cible. **Volumes à copier :** permet de sélectionner les volumes à récréer sur la cible et à assigner à une banque de données spécifique. **Services/daemons à arrêter :** permet de sélectionner les services Windows ou daemons Linux à arrêter automatiquement pendant le rétablissement. Reportez-vous à la section « Contrôle des services et des daemons » page 80. **Adresse alternative pour la source :** accepte la saisie d'une adresse IP supplémentaire pour le workload source, le cas échéant. Reportez-vous à la section « Protection sur des réseaux publics et privés via NAT » page 17.

Ensemble de paramètres (paramètres)	Détails
Workload	***Nombre d'UC :*** permet de spécifier le nombre requis d'UC assignées au workload cible. **Mémoire de la machine virtuelle :** permet d'assigner la quantité de mémoire virtuelle requise au workload cible. **Nom d'hôte, Domaine/groupe de travail :** utilisez ces options pour contrôler l'identité du workload cible et vérifiez son appartenance à un domaine/groupe de travail. Pour l'affiliation au domaine, les références de l'administrateur du domaine sont requises. **Connexions réseau :** utilisez ces options pour spécifier l'assignation réseau du workload cible sur la base des réseaux virtuels du conteneur de VM sous-jacent. **États des services à modifier :** permet de contrôler l'état de démarrage de services d'application (Windows) ou de daemons (Linux) spécifiques. Reportez-vous à la section « Contrôle des services et des daemons » page 80.
Post-rétablissement	**Reprotéger le workload :** utilisez cette option si vous envisagez de recréer le contrat de protection pour le workload cible après le déploiement. Cela permet de conserver un historique continu des événements pour le workload et d'assigner ou de désigner automatiquement une licence de workload. ◆ ***Protéger à nouveau après rétablissement :*** sélectionnez cette option si vous prévoyez de recréer un contrat de protection pour le workload cible. ◆ ***Aucune reprotection :*** sélectionnez cette option si vous n'avez pas l'intention de recréer un contrat de protection pour le workload cible.

4.6.2 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 Protect. Reportez-vous à la section « Enregistrement de machines physiques auprès de PlateSpin Protect en vue du rétablissement » page 83.
2. (Facultatif : plates-formes Windows) Exécutez l'outil PS Analyzer pour vérifier si des pilotes sont manquants. Reportez-vous à la section « Analyse des workloads avec PlateSpin Analyzer (Windows) » page 69.
3. Si PS Analyzer signale que des pilotes sont incompatibles ou manquants, téléchargez les pilotes requis dans la base de données des pilotes de périphérique de PlateSpin Protect. Reportez-vous à la section « Gestion des pilotes de périphérique » page 70.
4. Après un basculement, sélectionnez le workload sur la page Workloads, puis cliquez sur *Rétablir/déployer*.
5. Spécifiez les ensembles de paramètres suivants :
   - **Paramètres du workload :** spécifiez le nom d'hôte ou l'adresse IP du workload de récupération et entrez des références de niveau admin. Utilisez le format requis pour les références (reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 75).

- **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 79.
  - ***Type de cible :*** sélectionnez l'option *Cible physique*, puis la machine physique que vous avez enregistrée à l'Étape 1.

6 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.

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

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

4.6.3 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.

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

- Xen sous SLES 10, 11
- Microsoft Hyper-V

4.7 Sections sur la protection de workload avancée

4.7.1 Protection des grappes Windows

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

- Serveur de clusters Windows basé sur Windows 2003 Server (modèle *Single-Quorum Device Cluster* (Cluster de serveurs à périphérique quorum unique))
- Cluster de basculement Microsoft basé sur Windows 2008 Server (modèles *Nœud et disque majoritaires* et *Pas de majorité : disque uniquement*)

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

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

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

Si un basculement de noeud se produit entre les réplications incrémentielles d'une grappe protégée, PlateSpin Protect génère un événement de protection. Si le profil du nouveau noeud actif est similaire à celui qui a échoué, la planification de protection se poursuit. Dans le cas contraire, la commande échoue. Les profils des noeuds de grappe sont considérés similaires si :

- ils ont le même nombre de volumes ;
- chaque volume a exactement la même taille sur chaque noeud ;
- ils ont un nombre identique de connexions réseau.

Pour protéger une grappe Windows, suivez le workflow de protection du workload normal (reportez-vous à la section « Workflow de base pour la protection et la récupération de workload » page 43).

Lors du rétablissement, PlateSpin Protect fournit une validation qui permet de vérifier si les dispositions de volumes partagés sont préservées sur la cible. Veillez à assigner les volumes correctement.

4.7.2 Rétablissement de Linux vers une VM paravirtualisée sur Xen sous SLES

Vous pouvez effectuer un rétablissement vers une VM paravirtualisée sur Xen sous SLES (version 10 uniquement). Cela se fait indirectement, à travers un processus en deux étapes. La VM paravirtualisée doit d'abord être transformée en VM entièrement virtualisée, puis retransformée en VM paravirtualisée. L'utilitaire (`xmps`), compris dans votre image ISO de démarrage PlateSpin, permet de transformer la VM.

La procédure varie légèrement, selon que la cible est une nouvelle VM paravirtualisée ou une VM paravirtualisée existante.

- « Rétablissement de Linux vers une nouvelle VM paravirtualisée » page 56
- « Migration de Linux vers une VM paravirtualisée existante » page 58

Rétablissement de Linux vers une nouvelle VM paravirtualisée

1. Copiez l'image ISO de démarrage PlateSpin Linux vers le serveur Xen/SLES cible. Reportez-vous au Tableau 7-2, « Images de démarrage ISO pour des machines physiques cibles », page 83.
2. Lancez le gestionnaire de machines virtuelles et créez une VM entièrement virtualisée :
   - **2a** Sélectionnez l'option *Je dois installer un système d'exploitation*.

2b Choisissez une taille d'image disque adéquate (la taille de disque doit être égale ou supérieure à celle de la machine source).

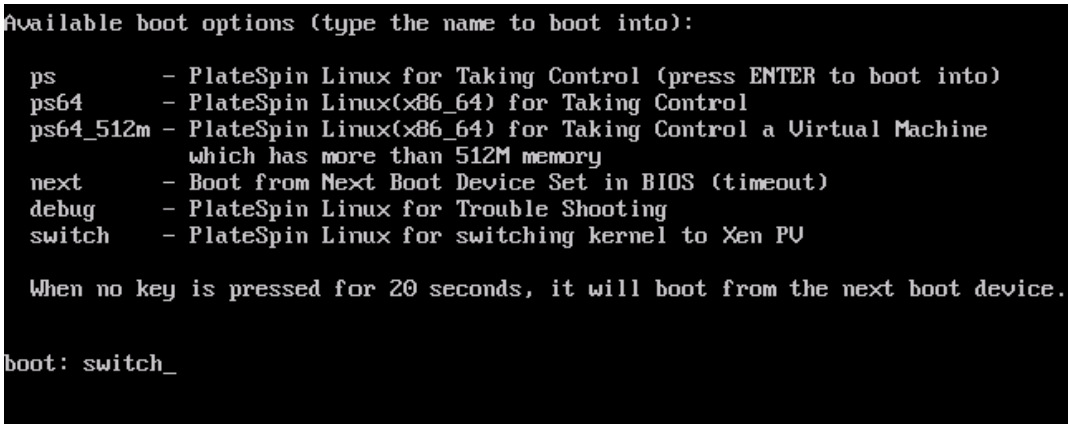
2c Sélectionnez l'image ISO de démarrage comme source d'installation.

La VM démarre dans l'environnement système PlateSpin, utilisé dans les paramètres de *rétablissement sur machine physique*.

3 Suivez la procédure de rétablissement. Reportez-vous à la section « Rétablissement semi-automatisé sur une machine physique » page 54.

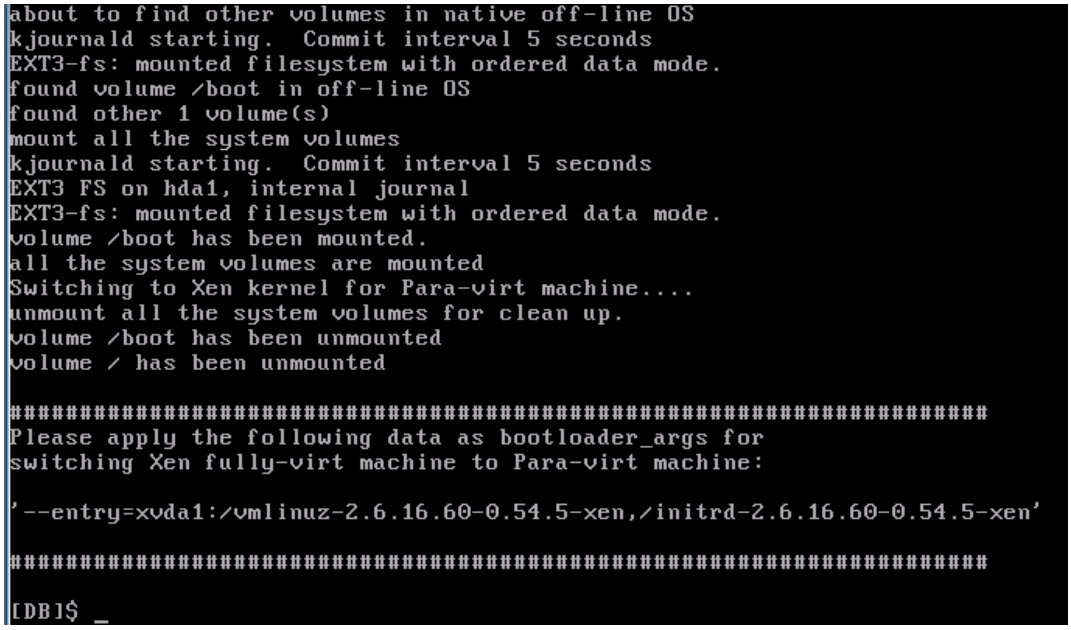
À la fin du processus, la VM devrait être complètement fonctionnelle en tant que machine entièrement virtualisée.

4 Redémarrez la VM et assurez-vous qu'elle démarre toujours dans l'environnement système PlateSpin.



5 À l'invite `boot:`, tapez `switch` et appuyez sur Entrée.

Le système d'exploitation va être reconfiguré pour être démarrable en tant que machine paravirtualisée. Une fois le processus terminé, le résultat devrait se présenter comme suit :



Notez les arguments du chargeur de démarrage dans le dernier segment du résultat :

```
Please apply the following data as bootloader_args for
switching Xen fully-virt machine to Para-virt machine:

'-entry=xvda1:/vmlinuz-2.6.16.60-0.54.5-xen, /initrd-2.6.16.60-0.54.5-
xen'
```

Ils sont utilisés par l'utilitaire `xmps` pour configurer l'emplacement du kernel et l'image `initrd` à partir d'où la machine paravirtualisée démarre.

6 Mettez la machine virtuelle hors tension :

```
[DB]$ poweroff
```

7 Connectez-vous au serveur XEN/SLES en tant que `root` et montez l'image ISO de démarrage PlateSpin Linux (l'exemple de commande part du principe que l'ISO a été copiée dans le répertoire `/root`) :

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

8 Exécutez l'utilitaire `xmps` pour créer une VM paravirtualisée basée sur la configuration de la VM entièrement virtualisée :

```
# /mnt/ps/tools/xmps --pv --vm_name=SLES10-FV --new_vm_name=SLES10-PV --
bootloader_args="--entry=xvda1:/vmlinuz-2.6.16.60-0.54.5-xen, /initrd-
2.6.16.60-0.54.5-xen"
```

L'utilitaire utilise en entrée :

- le nom de la VM entièrement virtualisée sur laquelle la configuration de la machine paravirtualisée sera basée (`SLES10-FV`) ;
- le nom de la machine virtuelle à créer (`SLES10-PV`) ;
- les arguments du chargeur de démarrage de la machine paravirtualisée `"--bootloader_args"` (indiqués à l'Étape 5).

S'il existe déjà une VM du même nom que celui transmis `nouveau_nom_vm`, l'utilitaire `xmps` échoue.

La nouvelle VM paravirtualisée (`SLES10-PV`) doit maintenant être disponible dans le gestionnaire de machines virtuelles, prête à être activée. La machine entièrement virtualisée correspondante est retirée et ne peut pas démarrer. Cette VM peut être supprimée en toute sécurité (seule la configuration de VM sera supprimée).

9 Démontez l'image ISO de démarrage de PlateSpin Linux :

```
# umount /mnt/ps
```

Migration de Linux vers une VM paravirtualisée existante

1 Copiez l'image ISO de démarrage PlateSpin Linux vers le serveur Xen/SLES cible. Reportez-vous au Tableau 7-2, « Images de démarrage ISO pour des machines physiques cibles », page 83.

2 Connectez-vous au serveur XEN/SLES en tant que `root` et montez l'image ISO de démarrage PlateSpin Linux :

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

3 Exécutez l'utilitaire `xmps` pour créer une VM entièrement virtualisée basée sur la configuration de la VM paravirtualisée (la cible de rétablissement visée) :

```
# /mnt/ps/tools/xmps --fv --vm_name=SLES10-PV  --new_vm_name=SLES10-FV --
bootiso=/root/linuxfailback.iso
```

L'utilitaire utilise en entrée :

- le nom de la machine paravirtualisée existante (`SLES10-PV`), qui est la cible de rétablissement visée ;
- le nom de la machine entièrement virtualisée temporaire (`SLES10-FV`) à créer pour l'opération de rétablissement en deux étapes ;
- le chemin d'accès complet de l'image ISO de démarrage (en partant du principe que le fichier ISO se trouve sur `/root: /root/booxofxx2p.iso`).

S'il existe déjà une VM du même nom que celui transmis `nouveau_nom_vm`, l'utilitaire `xmps` échoue.

La nouvelle machine entièrement virtualisée (`SLES10-FV`) doit maintenant être disponible dans le gestionnaire de machines virtuelles.

4 Activez la nouvelle machine entièrement virtualisée (`SLES10-FV`).

La VM démarre dans l'environnement système PlateSpin, utilisé dans les paramètres de *rétablissement sur machine physique*.

5 Suivez la procédure de rétablissement. Reportez-vous à la section « Rétablissement semi-automatisé sur une machine physique » page 54.

6 Redémarrez la VM, exécutez `switch` et reconfigurez le workload comme décrit à la section « Rétablissement de Linux vers une nouvelle VM paravirtualisée » page 56 (de l'Étape 4 à l'Étape 9 uniquement).

Protection de l'image de workload 5

La création d'image est l'une des deux infrastructures de protection de workload de PlateSpin Protect. Pour plus d'informations sur l'infrastructure de virtualisation, reportez-vous à la section « Protection de workload » page 43.

Une image PlateSpin est une copie stockée statique de l'état d'une machine physique ou virtuelle (notamment les données de volume et les détails de configuration du profil matériel, du système d'exploitation et de l'identité réseau du workload), capturée à un moment spécifique et régulièrement mise à jour aux intervalles que vous spécifiez dans les paramètres de protection du workload.

Lors de l'échec du workload protégé, vous pouvez déployer l'image capturée pour qu'elle s'exécute sur le matériel physique ou sur un hôte de VM.

Tout comme la fonctionnalité de protection de workload avec la virtualisation, le déploiement d'images propose des options de configuration de workload clés, comme les options de gestion de la disposition du disque du workload, les tailles des volumes, l'identité du réseau et l'affiliation à un domaine ou à un groupe de travail.

5.1 Protection d'une image de workload

Cette section contient des informations sur la protection d'image de workload.

5.1.1 Ajout d'un workload pour la protection d'images

La protection d'une image de workload capture les données de volume du workload spécifié au format d'une image flexible PlateSpin et met en place une protection continue de l'image à l'aide de mises à jour incrémentielles aux intervalles spécifiés.

1. Vérifiez que votre workload est pris en charge pour la protection des images.

   Reportez-vous à la section « Workloads pris en charge dans les conteneurs d'images » page 26.
2. Ajoutez un conteneur d'images.

   Reportez-vous à la section « Ajout de conteneurs » page 40.
3. Dans le client Web PlateSpin Protect, cliquez sur *Ajouter le workload*.
4. Spécifiez les informations requises concernant le workload.

   Reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 75.
5. Sélectionnez le serveur d'images requis en tant que cible de protection.

6 Cliquez sur *Ajouter un workload*.

PlateSpin Protect recharge la page Workloads et affiche un indicateur de processus pour le workload en cours d'ajout  . Attendez que le processus se termine. Une fois terminé, un événement *Workload ajouté* s'affiche dans le tableau de bord.

5.1.2 Configuration des détails de protection d'image de workload

Les paramètres de protection d'image déterminent la fréquence de synchronisation de l'image d'un workload avec les modifications des volumes de ce dernier, le type de mécanisme de transfert utilisé lors des réplications et les volumes du workload sélectionnés en vue d'être protégés.

1 Ajoutez un workload dont l'image doit être protégée. Reportez-vous à la section « Ajout d'un workload pour la protection d'images » page 61.

2 Sur la page Workloads, sélectionnez le workload souhaité, puis cliquez sur *Configurer*.

3 Configurez les paramètres de niveau de protection requis. Reportez-vous à la section « Niveaux de protection » page 77.

4 Configurez les paramètres de réplication d'image :

- **Méthode de transfert et codage :** reportez-vous à la section « Méthodes de transfert » page 76.
- **Références sources :** spécifiez des références de niveau admin pour le workload source. Reportez-vous à la section « Directives relatives aux références de workload et de conteneur » page 75.
- **Volumes protégés :** sélectionnez les volumes du workload dont vous souhaitez protéger l'image.
- **Banque de données :** sélectionnez la banque de données pour les données d'image du workload.
- **Services à arrêter pendant la réplication :** reportez-vous à la section « Contrôle des services et des daemons » page 80.

5 Cliquez sur *Enregistrer*.

6 Pour démarrer l'opération, cliquez sur *Exécuter la réplication*, puis confirmez en cliquant sur *Exécuter*.

PlateSpin Protect recharge la page Workloads et affiche un indicateur de processus pour le workload en cours de réplication  .

5.2 Déploiement d'une image de workload

En cas d'erreur ou d'échec de workload associé à une image protégée, vous pouvez déployer l'image protégée stockée sur votre serveur d'images sur une infrastructure physique ou virtuelle en tant que workload démarrable. Les critères qui déterminent et consignent les échecs de workload font partie des paramètres de niveau du contrat de protection d'image de workload (reportez-vous à la section « Niveaux de protection » page 77).

Si des notifications sont configurées avec des paramètres SMTP, PlateSpin Protect envoie simultanément une notification par message électronique aux destinataires spécifiés. Reportez-vous à la section « Configuration des notifications automatiques des événements et rapports par message électronique » page 18.

5.2.1 Déploiement d'une image sur une cible virtuelle

Utilisez la procédure suivante pour déployer une image sur une machine virtuelle, en tant que workload démarrable.

1. Ajoutez un conteneur de rétablissement. Reportez-vous à la section « Ajout de conteneurs » page 40.
2. Dans le client Web PlateSpin Protect, sélectionnez le workload souhaité, puis cliquez sur *Rétablir/déployer*. Choisissez *Virtuelle* comme type de cible et sélectionnez votre conteneur de rétablissement en tant que cible.
3. Cliquez sur *Enregistrer et préparer*. Lorsque vous y êtes invité, spécifiez les paramètres complets de l'opération :

Ensemble de paramètres (paramètres)	Détails
Déploiement	**Méthode de transfert :** (Windows) permet de sélectionner un mécanisme de transfert des données ainsi qu'une sécurité par le biais du codage. Reportez-vous à la section « Méthodes de transfert » page 76.
	Réseau de rétablissement : permet de diriger le trafic de rétablissement sur un réseau dédié, sur la base des réseaux virtuels définis sur votre conteneur de VM. Reportez-vous à la section « Réseautique » page 82.
	Banque de données de VM : permet de sélectionner une banque de données associée à votre conteneur de rétablissement pour le workload cible.
	Volumes à copier : permet de sélectionner les volumes protégés à déployer sur la cible sélectionnée et de les assigner à des banques de données spécifiques.
Workload	**Nombre d'UC :** permet de spécifier le nombre requis d'UC assignées au workload cible.
	Mémoire de la machine virtuelle : permet d'assigner la quantité de mémoire virtuelle requise au workload cible.
	Nom d'hôte, Domaine/groupe de travail : utilisez ces options pour contrôler l'identité du workload cible et vérifiez son appartenance à un domaine/groupe de travail. Pour l'affiliation au domaine, les références de l'administrateur du domaine sont requises.
	Connexions réseau : utilisez ces options pour spécifier l'assignation réseau du workload cible sur la base des réseaux virtuels du conteneur de VM sous-jacent.
	États des services à modifier : permet de contrôler l'état de démarrage de services d'application spécifiques. Reportez-vous à la section « Contrôle des services et des daemons » page 80.

Ensemble de paramètres (paramètres)	Détails
Post-rétablissement	**Reprotéger le workload :** utilisez cette option si vous envisagez de recréer le contrat de protection d'image pour le workload cible après le déploiement. Cela permet de maintenir un historique d'événements continu pour le workload. ◆ *Arrêter le workload déployé* : si cette option est sélectionnée, la VM cible est mise hors tension une fois le déploiement terminé.

4 Cliquez sur *Exécuter le déploiement* et surveillez la progression.

Une fois l'opération terminée, PlateSpin Protect indique l'état de la commande en affichant le message *Le déploiement est terminé.*

5 Accédez à la machine physique cible et vérifiez sa fonctionnalité ainsi que son intégrité.

Détails de déploiement (Image sur VM)

Les détails du déploiement sont représentés par trois ensembles de paramètres que vous configurez lorsque vous déployez une image de workload sur une machine virtuelle.

5.2.2 Déploiement d'une image sur une cible physique

Utilisez la procédure suivante pour déployer une image sur une machine physique, en tant que workload démarrable.

1 Enregistrez la machine physique souhaitée auprès de votre serveur PlateSpin Protect.

Reportez-vous à la section « Enregistrement de machines physiques auprès de PlateSpin Protect en vue du rétablissement » page 83.

2 Exécutez l'outil PlateSpin Analyzer pour vérifier si des pilotes sont manquants.

Reportez-vous à la section « Analyse des workloads avec PlateSpin Analyzer (Windows) » page 69.

3 Si PlateSpin Analyzer signale que des pilotes sont incompatibles ou manquants, téléchargez les pilotes requis dans la base de données des pilotes de périphérique de PlateSpin Protect.

Reportez-vous à la section « Gestion des pilotes de périphérique » page 70.

4 Dans le client Web PlateSpin Protect, sélectionnez le workload souhaité, puis cliquez sur *Rétablir/déployer*. Choisissez *Physique* comme type de cible et sélectionnez votre machine physique en tant que cible.

5 Cliquez sur *Enregistrer et préparer*. Lorsque vous y êtes invité, spécifiez les paramètres complets de l'opération :

Ensemble de paramètres (paramètres)	Détails
Rétablissement	**Méthode de transfert :** (Windows) permet de sélectionner un mécanisme de transfert des données ainsi qu'une sécurité par le biais du codage. Reportez-vous à la section « Méthodes de transfert » page 76. **Volumes à copier :** permet de sélectionnez les volumes protégés à déployer sur la cible sélectionnée.

Ensemble de paramètres (paramètres)	Détails
Workload	**Nom d'hôte, Domaine/groupe de travail :** utilisez ces options pour contrôler l'identité du workload cible et vérifiez son appartenance à un domaine/groupe de travail. Pour l'affiliation au domaine, les références de l'administrateur du domaine sont requises. **Connexions réseau :** ces options permettent de spécifier les paramètres LAN du workload cible. **États des services à modifier :** permet de contrôler l'état de démarrage de services d'application spécifiques. Reportez-vous à la section « Contrôle des services et des daemons » page 80. **Partitions à conserver :** permet de conserver n'importe quelle partition existante sur la cible. **États des services à modifier :** permet de contrôler l'état de démarrage de services d'application spécifiques. Reportez-vous à la section « Contrôle des services et des daemons » page 80.
Post-rétablissement	**Reprotéger le workload :** utilisez cette option si vous envisagez de recréer le contrat de protection d'image pour le workload cible après le déploiement. Cela permet de maintenir un historique d'événements continu pour le workload. ◆ **Désactiver le workload déployé :** si cette option est sélectionnée, la VM cible est mise hors tension une fois le déploiement terminé.

6 Cliquez sur *Exécuter le déploiement* et surveillez la progression.

Une fois l'opération terminée, PlateSpin Protect indique l'état de la commande en affichant le message *Le déploiement est terminé.*

7 Accédez à la machine physique cible et vérifiez sa fonctionnalité ainsi que son intégrité.

Détails de déploiement (Image sur machine physique)

Les détails du déploiement sont représentés par trois ensembles de paramètres que vous configurez lorsque vous déployez une image de workload sur une machine physique.

5.3 Exploration et extraction de fichiers image

Dans le cadre d'une reprise après sinistre ou d'un exercice de continuité des opérations, vous pouvez restaurer de manière sélective des fichiers dans le système de fichiers de votre workload à l'aide des versions de sauvegarde de ces fichiers enregistrées en tant qu'images.

Pour ce faire, vous pouvez utiliser l'utilitaire Parcoureur d'images, qui permet de parcourir, de rechercher, de trier et d'extraire des fichiers à partir d'un fichier image ou d'un fichier d'incrément d'image spécifique.

Vous pouvez travailler avec des images de base ou des incréments d'image en chargeant l'un des deux types de fichier suivants :

- un fichier binaire correspondant à une image de base (*volume-x*`.pkg`) ou un fichier de configuration texte (*nom_image*`.xml`) ;
- un fichier binaire d'incrément d'image (*incrément_image*`.pkg`). Vous ne pouvez pas utiliser un fichier de configuration texte d'incrément (*nom_incrément_image*`.xml`).

L'utilitaire vous permet de travailler avec des fichiers image dans un environnement de type Explorateur Windows. Une version de ligne de commande vous permet d'extraire des fichiers en ligne de commande.

- Section 5.3.1, « Lancement du parcoureur d'images et chargement des fichiers image », page 66
- Section 5.3.2, « Tri et recherche d'éléments dans l'interface du parcoureur d'images », page 67
- Section 5.3.3, « Extraction d'éléments à partir d'une image », page 68
- Section 5.3.4, « Recherche et extraction de fichiers d'images via la ligne de commande », page 68

5.3.1 Lancement du parcoureur d'images et chargement des fichiers image

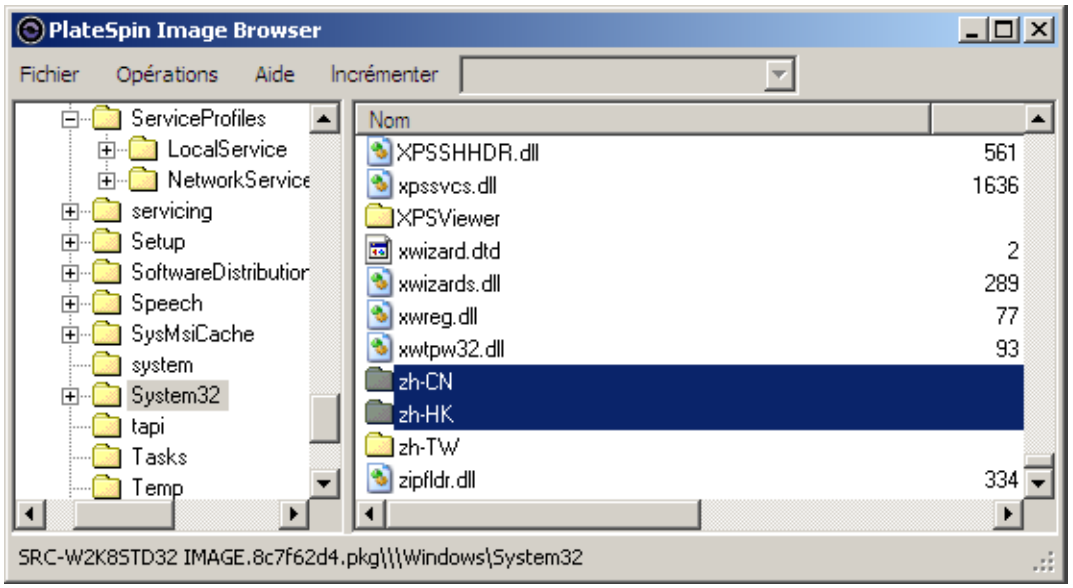
1. Démarrez le programme du parcoureur d'images (`ImageBrowser.exe`), situé sur l'hôte du serveur d'images, dans le répertoire suivant :

   ```
   \Program Files\PlateSpin Image Server\ImageOperations
   ```

   L'utilitaire démarre et affiche la boîte de dialogue Ouvrir. Après le démarrage initial du programme, vous pouvez à tout moment charger un fichier image en cliquant sur *Fichier* > *Ouvrir*.

2. Dans la boîte de dialogue Ouvrir, sélectionnez le type de fichier, accédez au fichier image ou d'incrément d'image souhaité, sélectionnez-le et cliquez sur *OK*.

   L'utilitaire charge le fichier souhaité et affiche son contenu dans une interface à deux volets.



Selon la taille de l'image, le chargement du fichier souhaité peut prendre un certain temps.

5.3.2 Tri et recherche d'éléments dans l'interface du parcoureur d'images

Vous pouvez trier le contenu d'un répertoire sélectionné en fonction du nom, de la taille, de la date de la dernière modification et de l'attribut de fichier. Pour trier des éléments dans un vue sélectionnée, cliquez sur la barre qui correspond en haut du volet de droite.

Vous pouvez rechercher un nom de répertoire ou de fichier spécifique. Vous pouvez utiliser des caractères alphanumériques, des caractères joker ou des expressions régulières. Les modèles de recherche d'expression régulière que vous spécifiez doivent être conformes aux exigences de syntaxe des expressions régulières de Microsoft .NET Framework. Reportez-vous à la page sur les expressions régulières de Microsoft .NET Framework sur MSDN (http://msdn.microsoft.com/en-us/library/hs600312.aspx).

Pour rechercher un élément :

1. Chargez l'image ou l'incrément d'image requis.
2. Dans le volet de gauche, sélectionnez un volume ou un sous-répertoire.
3. Dans le menu *Opérations*, cliquez sur *Rechercher*.

   Vous pouvez également cliquer avec le bouton droit sur le volume ou le sous-répertoire requis dans le volet de gauche et cliquer sur *Rechercher* dans le menu contextuel.

   La fenêtre Recherche du parcoureur d'images s'ouvre.
4. Spécifiez le nom du fichier que vous recherchez. Si vous utilisez une expression régulière, sélectionnez l'option correspondante.
5. Cliquez sur *Rechercher*.

   Les résultats s'affichent dans le volet de droite.

5.3.3 Extraction d'éléments à partir d'une image

1. Chargez l'image ou l'incrément d'image requis.
2. Localisez le fichier ou le répertoire requis et sélectionnez-le. Vous pouvez en sélectionner plusieurs dans le volet de droite.
3. Dans le menu *Opérations*, cliquez sur *Extraire*.

   Vous pouvez également cliquer avec le bouton droit sur l'élément requis, puis cliquer sur *Extraire* dans le menu contextuel.

   La fenêtre Rechercher le dossier s'ouvre.
4. Recherchez la destination souhaitée, puis cliquez sur *OK*.

   Les éléments sélectionnés sont extraits vers la destination spécifiée.

Remarque : les fichiers que vous décidez d'écraser sont supprimés si vous interrompez le processus d'extraction.

5.3.4 Recherche et extraction de fichiers d'images via la ligne de commande

Pour rechercher des fichiers et les extraire à partir d'images et d'incréments d'image via la ligne de commande, vous pouvez faire appel à l'utilitaire `ImageBrowser.Console`.

Pour démarrer cet utilitaire :

1. Sur l'hôte du serveur d'images flexibles, ouvrez un interpréteur de commandes (`cmd.exe`) et remplacez le répertoire actuel par `\Program Files\PlateSpin Image Server\ImageOperations`.
2. À l'invite de commande, saisissez `ImageBrowser.Console`, puis appuyez sur Entrée.

   Pour la syntaxe de la commande et les détails d'utilisation, saisissez `ImageBrowser.Console /help`, puis appuyez sur Entrée.

Outils auxiliaires pour l'utilisation de machines physiques

6

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

6.1 Analyse des workloads avec PlateSpin Analyzer (Windows)

Avant d'exécuter une opération de rétablissement de workload ou de déploiement d'image sur une machine physique, utilisez PlateSpin Analyzer pour identifier les éventuels problèmes de pilote et y remédier avant de poursuivre.

Remarque : à l'heure actuelle, PlateSpin Analyzer ne prend en charge que les workloads Windows.

1. Sur l'hôte du serveur PlateSpin Protect, démarrez le programme `Analyzer.Client.exe` situé dans le répertoire suivant :

   `\Program Files\PlateSpin Protect Server\PlateSpin Analyzer`

2. Assurez-vous que le réseau sélectionné est celui *par défaut*, puis choisissez la machine requise dans la liste déroulante *Toutes les machines*.
3. (Facultatif) Pour réduire le temps d'analyse, limitez l'étendue des machines à une langue spécifique.
4. Cliquez sur *Analyser*.

   L'analyse peut durer de quelques secondes à plusieurs minutes en fonction du nombre de workloads inventoriés sélectionnés.

Les serveurs sont listés dans le volet gauche. Sélectionnez un serveur pour afficher les résultats du test dans le volet droit. Les résultats du test peuvent combiner les valeurs suivantes :

Tableau 6-1 *Messages de statut dans les résultats des tests de PlateSpin Analyzer*

Résultat	Description
Réussi	La machine a réussi les tests de PlateSpin Analyzer.
Avertissement	Au moins un test a renvoyé des avertissements pour la machine, ce qui indique d'éventuels problèmes de migration. Cliquez sur le nom d'hôte pour afficher les détails.
Échec	Au moins un test a échoué pour cette machine. Cliquez sur le nom d'hôte pour afficher les détails et obtenir plus d'informations.

L'onglet *Résumé* fournit une liste indiquant le nombre de machines analysées et non vérifiées, ainsi que celles qui ont échoué au test, qui l'ont réussi ou qui ont reçu l'état d'avertissement.

L'onglet *Résultats du test* fournit les informations suivantes :

Tableau 6-2 *Onglet Résultats du test de PlateSpin Analyzer*

Section	Détails
Test du système	Vérifie que la machine répond à la configuration de système d'exploitation et matérielle minimale requise.
Prise en charge du matériel	Vérifie la compatibilité matérielle du workload.
Prise en charge du matériel cible	Vérifie la compatibilité du matériel à utiliser comme machine physique cible.
Test des logiciels	Recherche les applications qui doivent être arrêtées pour le transfert à chaud et les bases de données qui devraient l'être pendant le transfert à chaud pour garantir l'intégrité des transactions.
Test d'applications incompatibles	Vérifie que les applications reconnues comme perturbant le processus de migration ne sont pas installées sur le système. Ces applications sont stockées dans la base de données d'applications incompatibles. Pour ajouter, supprimer ou modifier des entrées dans la base de données, sélectionnez *Application incompatible* dans le menu *Outils*.

L'onglet *Propriétés* fournit des informations détaillées sur une machine sélectionnée.

6.2 Gestion des pilotes de périphérique

PlateSpin Protect est fourni avec une bibliothèque de pilotes de périphérique et installe automatiquement les pilotes adéquats sur les workloads cibles. Pour déterminer si les pilotes requis sont disponibles, utilisez l'utilitaire PlateSpin Analyzer. Reportez-vous à la section « Analyse des workloads avec PlateSpin Analyzer (Windows) » page 69.

Si PlateSpin Analyzer détecte des pilotes manquants ou incompatibles ou si vous avez besoin de pilotes spécifiques pour votre infrastructure cible, il est possible que vous deviez ajouter (télécharger) des pilotes dans la base de données des pilotes de PlateSpin Protect.

- Section 6.2.1, « Création d'un paquetage contenant les pilotes de périphérique pour les systèmes Windows », page 71
- Section 6.2.2, « Création d'un paquetage contenant les pilotes de périphérique pour les systèmes Linux », page 71
- Section 6.2.3, « Téléchargement de pilotes dans la base de données des pilotes de périphérique de PlateSpin Protect », page 72

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

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

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

Les pilotes sont à présent prêts à être téléchargés. Reportez-vous à la section « Téléchargement de pilotes dans la base de données des pilotes de périphérique de PlateSpin Protect » page 72.

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

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

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

Pour créer un paquetage de vos pilotes de périphérique Linux en vue de les télécharger dans la base de données des pilotes de PlateSpin Protect, vous pouvez employer un utilitaire personnalisé inclus dans votre image de démarrage ISO de prise de contrôle Linux. Reportez-vous au Tableau 7-2, « Images de démarrage ISO pour des machines physiques cibles », page 83.

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 supposant que l'image ISO a été copiée dans le répertoire `/root`, exécutez les commandes suivantes :

   ```
   # mkdir /mnt/ps
   # mount -o loop /root/linuxfailback.iso /mnt/ps
   ```
3. Dans le sous-répertoire `/tools` de l'image ISO montée, copiez l'archive `packageModules.tar.gz` dans un autre répertoire de travail et extrayez-la.

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

   ```
   tar -xvzf packageModules.tar.gz
   ```
4. Entrez le répertoire de travail et exécutez la commande suivante :

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

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

Nompilote-versionpilote-dist-versionkernel-arch.pkg

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

Le paquetage est à présent prêt à être téléchargé. Reportez-vous à la section « Téléchargement de pilotes dans la base de données des pilotes de périphérique de PlateSpin Protect » page 72.

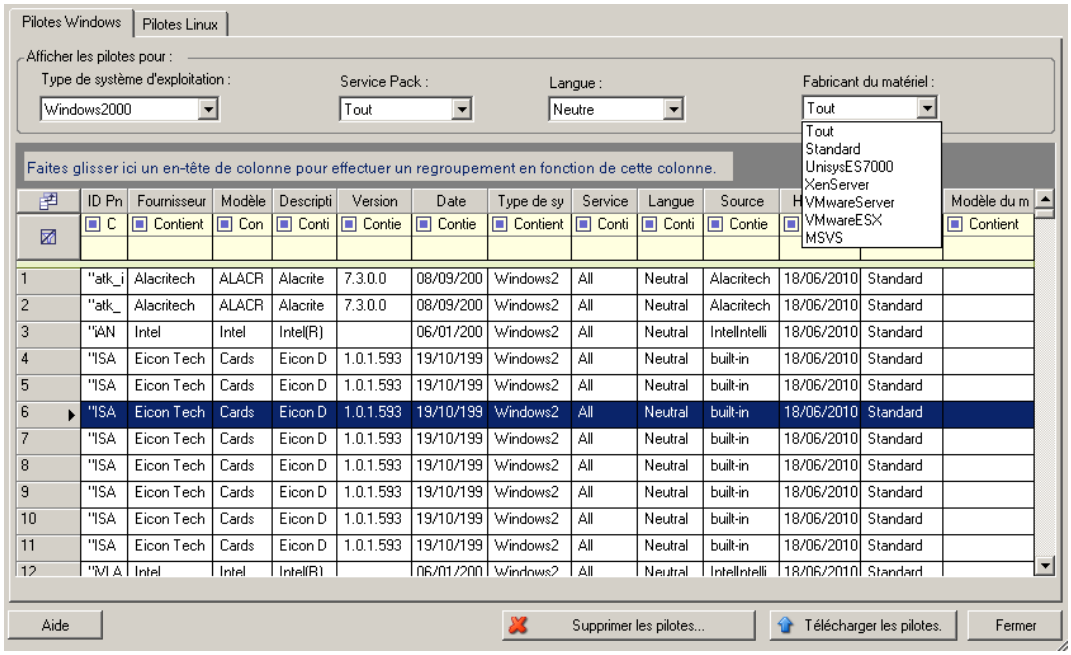
6.2.3 Téléchargement de pilotes dans la base de données des pilotes de périphérique de PlateSpin Protect

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

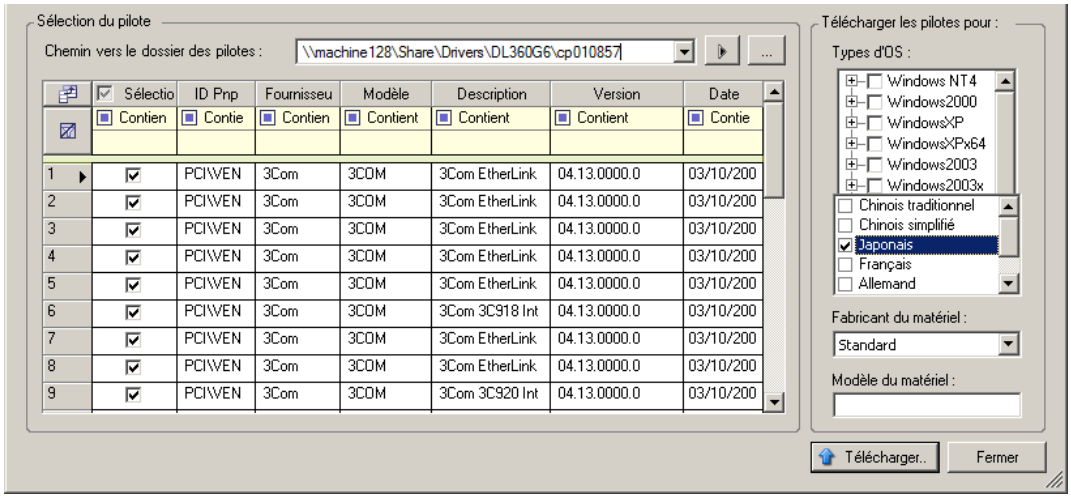
Remarque : lors du téléchargement, PlateSpin Protect ne valide pas les pilotes par rapport aux types de systèmes d'exploitation sélectionnés ou à leurs spécifications au niveau des bits. Veillez donc à télécharger uniquement des pilotes convenant à votre infrastructure cible.

Procédure de téléchargement de pilotes de périphérique (Windows)

1. Procurez-vous les pilotes de périphérique requis et préparez-les. Reportez-vous à la section Création d'un paquetage contenant les pilotes de périphérique pour les systèmes Windows.
2. Sur votre hôte PlateSpin Protect Server, sous `\Program Files\PlateSpin Protect Server\DriverManager`, démarrez le programme `DriverManager.exe`, puis cliquez sur l'onglet *Pilotes Windows*.



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



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

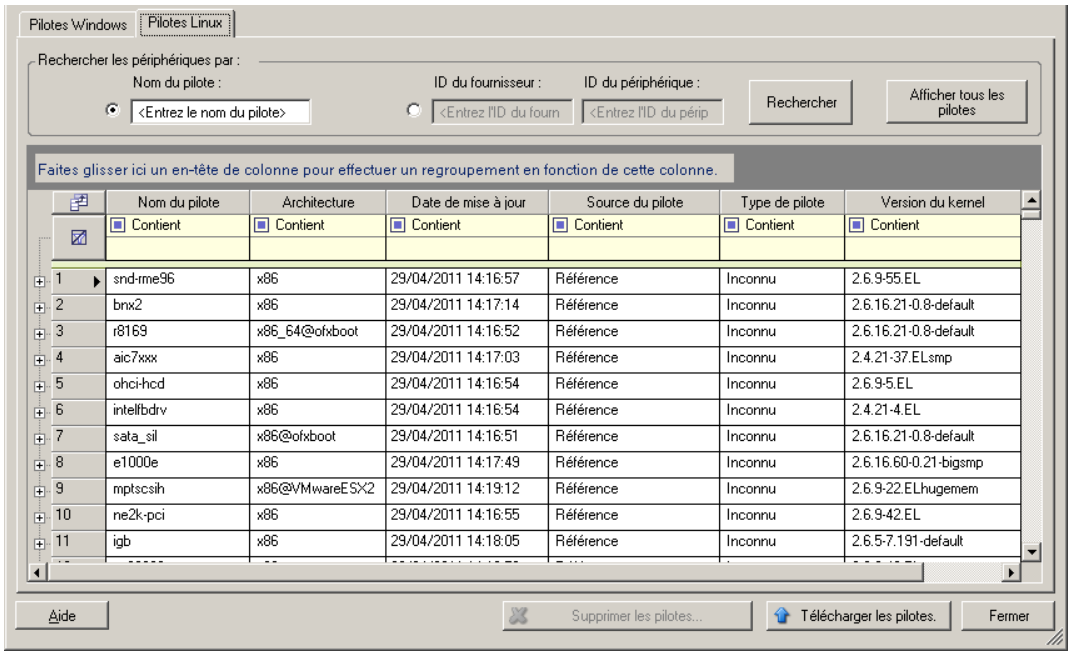
4 Cliquez sur *Télécharger* et confirmez vos sélections quand vous y êtes invité.

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

Procédure de téléchargement de pilotes de périphérique (Linux)

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

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



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

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

Notions fondamentales concernant la protection de workload

7

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

7.1 Directives relatives aux références de workload et de conteneur

PlateSpin Protect doit disposer d'un accès de niveau admin aux workloads et aux 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 7-1 *Références de workload et de conteneur*

À découvrir	Références	Remarques
Tous les workloads Windows Conteneurs de serveur d'images	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	Utilisez l'adresse IP virtuelle de la grappe Si vous utilisez l'adresse IP d'un noeud de grappe Windows individuel, ce noeud est découvert en tant que workload Windows ordinaire (ne prenant pas en charge les grappes).

À découvrir	Références	Remarques
Tous les workloads Linux	Nom d'utilisateur et mot de passe de niveau root	Les comptes non root ne sont pas correctement configurés pour utiliser `sudo`. Reportez-vous à l'article de la base de connaissances n° 7920711 (http://www.novell.com/support/viewContent.do?externalId=7920711).
Hôtes VMware ESX (4.0 et les versions antérieures)	Compte ESX avec rôle d'administrateur	
VMware ESX 4.1	Compte ESX avec rôle d'administrateur	Si ESX Server 4.1 est configuré pour l'authentification de domaine Windows, vous pouvez aussi utiliser vos références de domaine Windows.

7.2 Méthodes de transfert

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

- **Basée sur les blocs :** les données sont répliquées sur la base de blocs d'un volume. Pour cette méthode de transfert, PlateSpin Protect utilise un pilote pour surveiller les changements sur le workload source.
  - **Systèmes Windows :** pour les systèmes Windows, PlateSpin Protect utilise un composant basé sur les blocs qui tire parti du service d'instantanés de volume Microsoft avec des applications et des services prenant en charge ce service. L'installation automatique du composant basé sur les blocs nécessite le redémarrage du workload source (aucun redémarrage n'est requis lorsque vous protégez des grappes Windows avec le transfert de données par bloc). Lorsque vous configurez les détails de protection de workload, vous pouvez choisir le moment de l'installation du composant. De façon similaire, lors de la suppression d'un workload, la désinstallation du composant basé sur les blocs nécessite un redémarrage.
  - **Systèmes Linux :** pour le transfert par bloc des systèmes Linux, PlateSpin Protect utilise un composant de transfert de données par bloc qui exploite des instantanés LVM le cas échéant (option par défaut recommandée). Reportez-vous à l'article de la base de connaissances n° 7005872 (http://www.novell.com/support/viewContent.do?externalId=7005872).

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

    Le déploiement ou la suppression du composant sont transparents, n'ont pas d'impact sur la continuité et ne nécessitent aucune intervention.
- **Basée sur les fichiers :** les données sont répliquées fichier par fichier (Windows seulement). Cette méthode est prise en charge avec ou sans VSS.

  Dans le cadre des opérations de protection et de déploiement d'image, les données sont répliquées au niveau des fichiers sans devoir effectuer une sélection explicite.

Pour sécuriser davantage le transfert de données de workload, PlateSpin Protect permet de coder la réplication des données. Lorsque le codage est activé, le transfert de données sur le réseau depuis la source vers la cible est codé via la norme AES (Advanced Encryption Standard) ou 3DES si le codage compatible FIPS est activé.

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

7.3 Niveaux de protection

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

- la fréquence et le schéma de récurrence des réplications ;
- s'il faut 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 que le système applique pour considérer l'échec d'un workload.

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

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

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

Nom	Saisissez le nom que vous souhaitez utiliser pour le niveau.
Récurrence incrémentielle	Spécifiez la fréquence des réplications incrémentielles ainsi que le schéma de récurrence incrémentielle. Vous pouvez saisir les données directement dans le champ *Début de la récurrence* ou cliquer sur l'icône du calendrier pour sélectionner une date. Sélectionnez *Aucun* comme schéma de récurrence pour ne jamais utiliser la réplication incrémentielle.
Récurrence totale	Spécifiez la fréquence des réplications complètes ainsi que le schéma de récurrence totale.

Fenêtre d'interdiction	Ces paramètres permettent d'imposer une interdiction de réplication. Il est conseillé d'implémenter cette fonctionnalité pour suspendre les réplications programmées aux heures de pointe en termes d'utilisation du système ou pour éviter les conflits entre les applications Windows compatibles VSS et le composant de transfert de données par bloc VSS. 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 :** au début de la fenêtre d'interdiction, le système interrompt toutes les réplications qui ne sont pas terminées.
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 29. 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 78. La valeur `0` a pour effet de désactiver cette fonction.
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.

7.4 Points de reprise

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

Pour chaque workload protégé, vous pouvez conserver jusqu'à 32 points de reprise.

Pour chaque image protégée, vous pouvez conserver jusqu'à 100 points de reprise.

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

7.5 Méthode de réplication initiale (totale et incrémentielle)

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

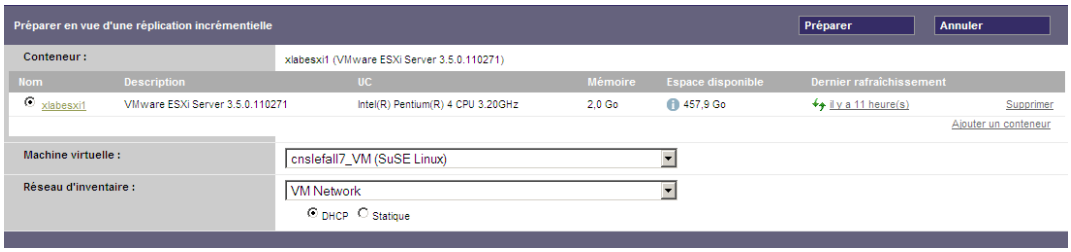
- **Complète :** un transfert de volumes complet a lieu entre un workload de production vers sa réplique (le workload de récupération) ou depuis un workload de basculement vers son infrastructure virtuelle ou physique d'origine.
- **Incrémentielle :** seules les différences sont transférées depuis une source d'opération sélectionnée vers sa cible, à condition qu'elles aient un système d'exploitation et un profil 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 à un site de récupération distant (pour VMware ESX 3.5 et versions suivantes uniquement).

      Pour plus de détails, reportez-vous à la documentation de VMware.
  - Au cours du rétablissement vers une machine virtuelle : le workload de basculement est comparé à une machine virtuelle dans un conteneur de rétablissement.
  - Au cours du rétablissement vers une machine physique : le workload de basculement est comparé à un workload sur la machine physique cible, si elle est enregistrée auprès de PlateSpin Protect (reportez-vous à la section « Rétablissement semi-automatisé sur une machine physique » page 54).

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

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

   Le client Web PlateSpin Protect affiche la page Préparer en vue d'une réplication incrémentielle.



4 Sélectionnez le conteneur requis, la machine virtuelle et le réseau d'inventaire à utiliser pour communiquer avec la machine virtuelle.

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 sont basées sur des données déjà interrogées par le composant basé sur les blocs pendant la surveillance d'une source.

7.6 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 source soit transféré vers le workload de récupération dans un état plus cohérent que si les services et daemons restaient 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 80.

- **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 le workload cible. 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.

7.7 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. `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 80). 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`

7.8 Volumes

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

PlateSpin Protect prend en charge plusieurs types de stockages, notamment les disques dynamiques Windows, LVM, RAID et SAN.

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

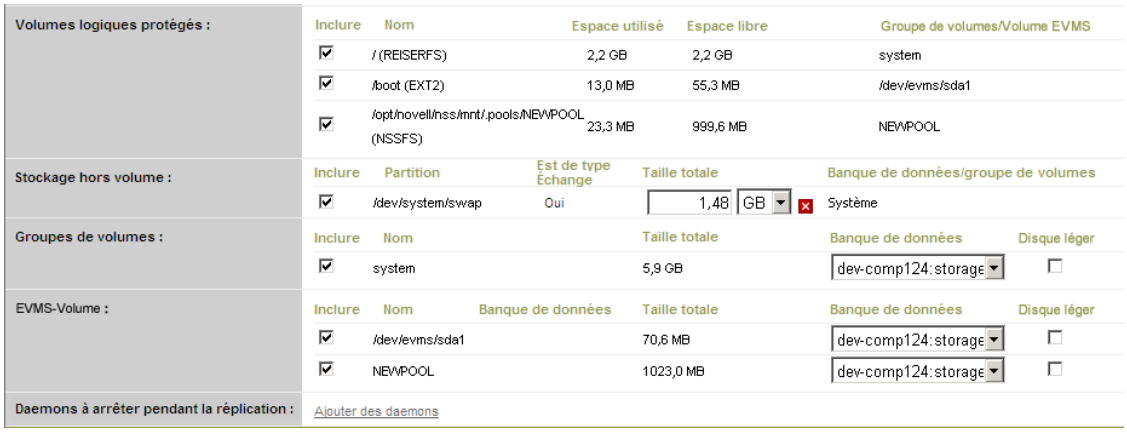
- Tout stockage, autre qu'un volume, associé au workload source est créé à nouveau et assigné au workload de récupération.
- La disposition des groupes de volumes et des volumes logiques est conservée pour vous permettre de la recréer pendant le rétablissement.
- (Workloads OES 2) Les dispositions EVMS de workloads sources sont conservées et recréées dans le conteneur de VM. Les réserves NSS sont copiées de la source vers la VM de récupération.

La figure suivante affiche l'ensemble des paramètres de réplication pour un workload Linux avec plusieurs volumes et deux volumes logiques dans un groupe de volumes.

Figure 7-1 *Volumes, volumes logiques et groupes de volumes d'un workload Linux protégé*

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

Figure 7-2 *Paramètres de réplication, options de volume (workload OES 2)*



7.9 Réseautique

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

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

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

7.10 Enregistrement de machines physiques auprès de PlateSpin Protect en vue du rétablissement

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

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

Pour utiliser une image ISO de démarrage, téléchargez-la depuis la section PlateSpin Protect du site Téléchargements Novell (http://download.novell.com/Download?buildid=IgohE3eAIVw). Utilisez l'image appropriée pour votre machine cible :

Tableau 7-2 *Images de démarrage ISO pour des machines physiques cibles*

Nom de fichier	Remarques
`WindowsFailback.zip` (contient `WindowsFailback.iso`)	Windows
`LinuxFailback.zip` (contient `LinuxFailback.iso`)	Systèmes Linux
`WindowsFailback-Cisco.zip` (contient `WindowsFailback-Cisco.iso`)	Systèmes Windows sur du matériel Cisco
`WindowsFailback-Dell.zip` (contient `WindowsFailback-Dell.iso`)	Systèmes Windows sur du matériel Dell
`WindowsFailback-Fujitsu.zip` (contient `WindowsFailback-Fujitsu.iso`)	Systèmes Windows sur du matériel Fujitsu

Après avoir téléchargé le fichier requis, dézippez le fichier ISO et enregistrez-le.

- Section 7.10.1, « Enregistrement des machines physiques cibles », page 84

7.10.1 Enregistrement des machines physiques cibles

1. Gravez l'image appropriée 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*.

   La version Windows de l'image du CD de démarrage ne prenant en charge que l'option *Duplex intégral - Négociation automatique*, vous assurez ainsi l'absence de conflit dans les paramètres de duplex.
3. Démarrez la machine physique cible à l'aide du CD de démarrage, puis attendez l'ouverture de la fenêtre d'invite de commande.

   (Windows uniquement) Attendez l'ouverture des fenêtres d'entrée de commande *REGISTERMACHINE* et *Console de récupération*. Utilisez l'utilitaire de ligne de commande REGISTERMACHINE. Pour plus d'informations sur l'utilitaire Console de récupération, reportez-vous à la section « Utilisation de l'utilitaire de ligne de commande Outil de récupération (Windows) » page 84.
4. (Linux uniquement) Pour les systèmes 64 bits, à l'invite de démarrage initiale, tapez ce qui suit :
   - `ps64` (pour les systèmes ayant jusqu'à 512 Mo de RAM)
   - `ps64_512m` (pour les systèmes ayant plus de 512 Mo de RAM)
5. Appuyez sur Entrée.
6. À l'invite du système, entrez l'URL suivante :

   `http://<nom_hôte | adresse_IP>/platespinprotect`

   Remplacez *<nom_hôte | adresse_IP>* par le nom d'hôte et l'adresse IP de l'hôte du serveur PlateSpin Protect.
7. Fournissez vos références d'administrateur pour l'hôte du serveur PlateSpin Protect, 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. Entrez *Yes* si vous avez activé SSL, sinon indiquez *No*.

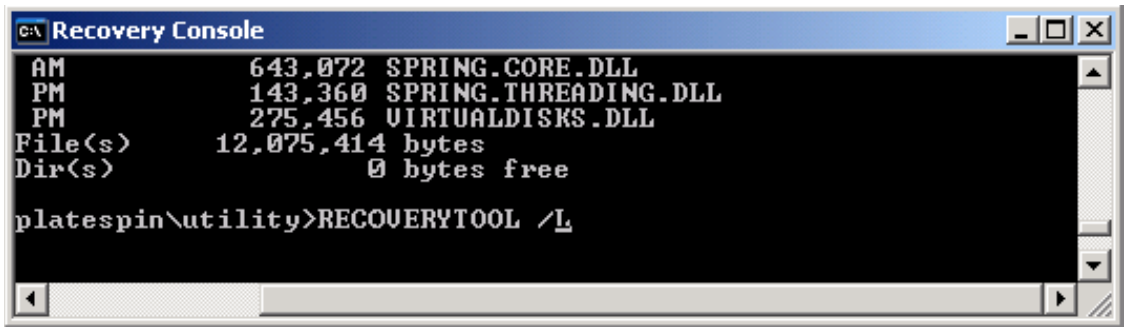
Après quelques instants, la machine physique doit être disponible dans les paramètres de déploiement d'image/de rétablissement du client Web PlateSpin Protect.

Utilisation de l'utilitaire de ligne de commande Outil de récupération (Windows)

L'utilitaire de ligne de commande Console de récupération permet d'ajouter dynamiquement des pilotes de périphérique Windows à la machine physique cible sans avoir à relancer tout le processus d'enregistrement de la cible physique.

L'utilitaire se charge dans une fenêtre d'entrée de commande secondaire à la tentative initiale de démarrage à partir de l'image de démarrage Windows (reportez-vous à l'Étape 3 page 84).

Pour utiliser l'outil de récupération, entrez son nom de commande, `RECOVERYTOOL`, suivi d'un paramètre applicable, dans la fenêtre Console de récupération.



Vous pouvez utiliser :

- `/L` - pour afficher la liste des services de pilotes installés sur l'OS cible ;
- `/J` - pour ajouter des pilotes à l'OS cible.

Vous pouvez spécifier si les pilotes doivent être téléchargés à partir du serveur PlateSpin Protect ou d'un chemin local. Si vous comptez utiliser un chemin local, regroupez les pilotes associés au même périphérique. Si vous téléchargez les pilotes à partir du serveur PlateSpin Protect, l'utilitaire vous invite à spécifier le pilote à utiliser (s'il y en a plusieurs).

Insertion de pilotes dans une image de démarrage PlateSpin (Linux)

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

1. Procurez-vous les fichiers de pilotes `*.ko` requis ou compilez-les.

   Important : assurez-vous que les pilotes sont valides pour le kernel inclus dans le fichier ISO (`2.6.16.21-0.8-default`) et conviennent à l'architecture cible.

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. Une fois 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 où vous avez enregistré le script `rebuildiso.sh`, exécutez la commande suivante en tant qu'utilisateur `root` :

   `./rebuildiso.sh –i <fichier_ISO> -d <répertoire_pilotes> -m i586|x86_64`

   Une fois l'opération terminée, le fichier ISO est mis à jour avec les pilotes supplémentaires.

Dépannage

8

8.1 Dépannage de l'inventaire de workload (Windows)

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

Problèmes ou messages	Solutions
`The domain in the credentials is invalid or blank`	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`
`Unable to connect to Windows server...Access is denied`	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 89. Si le test réussit, réessayez d'ajouter le workload. ◆ « Dépannage de la connectivité DCOM » page 89 ◆ « Dépannage de la connectivité du service RPC » page 89
`Unable to connect to Windows server...The network path was not found`	Échec de la connectivité réseau Effectuez les tests de la section « Exécution des tests de connectivité » page 88. En cas d'échec du test, vérifiez si PlateSpin Protect et le workload se trouvent sur le même réseau. Reconfigurez le réseau, puis réessayez.

Problèmes ou messages	Solutions
`“Discover Server Details {hostname}” Failed Progress: 0% Status: NotStarted`	Cette erreur peut se produire pour plusieurs raisons et chacune a sa propre solution : ◆ Pour les environnements qui utilisent un proxy local avec une authentification, ignorez le proxy ou ajoutez les autorisations appropriées. Pour plus de détails, reportez-vous à l'article de la base de connaissances 7920339 (http://www.novell.com/support/viewContent.do?externalId=7920339). ◆ Si des restrictions de stratégies locales ou de domaine nécessitaient des autorisations, suivez la procédure décrite dans l'article de la base de connaissances n°7920862 (http://www.novell.com/support/viewContent.do?externalId=7920862).

La découverte du workload échoue avec le message d'erreur
`Could not find file output.xml`
ou
`Network path not found`
ou (lors d'une tentative de découverte d'une grappe Windows)
`Inventory failed to discover. Inventory result returned nothing.`
	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 90.
	◆ 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 C$ et/ou Admin$ sur la source ne sont peut-être pas accessibles. Vérifiez que PlateSpin Protect peut accéder à ces partages. Reportez-vous à la section « Activation des autorisations et de l'accès aux fichiers/partages » page 90.
	◆ Changez l'état du drapeau `ForceMachineDiscoveryUsingService` sur `true` dans le fichier `web.config` du dossier `\Program Files\PlateSpin Portability Suite Server\Web`.
	◆ 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.

8.1.1 Exécution des tests de connectivité

- « Test de connectivité réseau » page 88
- « Test de connectivité WMI » page 89
- « Dépannage de la connectivité DCOM » page 89
- « Dépannage de la connectivité du service RPC » page 89

Test de connectivité réseau

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

1 Accédez à votre hôte de serveur PlateSpin Protect.

2 Ouvrez une invite de commande et effectuez un test ping sur votre workload :

```
ping workload_ip
```

Test de connectivité WMI

1 Accédez à votre hôte de serveur PlateSpin Protect.

2 Cliquez sur *Démarrer* > *Exécuter*, tapez `Wbemtest` et appuyez sur `Entrée`.

3 Cliquez sur *Connecter*.

4 Dans l'*espace de noms*, tapez le nom du workload que vous tentez de découvrir et ajoutez-y `\root\cimv2`. Par exemple, si le nom d'hôte est `win2k`, tapez :

```
\\win2k\root\cimv2
```

5 Entrez les références appropriées, en utilisant le format `nom_hôte\AdminLocal` ou `domaine\AdminDomaine`.

6 Cliquez sur *Connexion* pour tester la connexion WMI.

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

Dépannage de la connectivité DCOM

1 Loguez-vous au workload à protéger.

2 Cliquez sur *Démarrer* > *Exécuter*.

3 Saisissez `dcomcnfg` et appuyez sur Entrée.

4 Vérifiez la connectivité :

- Sur la machine d'un serveur Windows NT/2000, la boîte de dialogue Configuration DCOM s'affiche. Cliquez sur l'onglet *Propriétés par défaut* et vérifiez que l'option *Activer Distributed COM (DCOM) sur cet ordinateur* est sélectionnée.
- Pour Windows Server 2003, la fenêtre Services des 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.

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 matériel.

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

- Placez PlateSpin Protect et le workload du même côté du pare-feu.
- Ouverture de ports spécifiques entre PlateSpin Protect et le workload (reportez-vous à la section « Conditions d'accès et de communication requises sur votre réseau de protection » page 14).

8.1.2 Désactivation du logiciel anti-virus

Un logiciel anti-virus peut parfois bloquer certaines fonctionnalités de PlateSpin Protect liées à WMI et au registre à distance. Pour garantir la réussite de l'inventaire de workloads, il peut être nécessaire de commencer par désactiver le service anti-virus sur le 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.

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

Pour protéger un workload, PlateSpin Protect doit pouvoir déployer et installer le contrôleur OFX ainsi qu'un composant dédié basé sur les blocs, si une réplication par bloc est requise. Lors du déploiement de ces composants sur un workload, de même que pendant le processus Ajouter le workload, PlateSpin Protect utilise les partages administratifs du workload. Pour pouvoir fonctionner, PlateSpin Protect requiert un accès administratif 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 C$ et Admin$.

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

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

   Le répertoire s'ouvre vous permettant de le parcourir et de modifier son contenu.

4 Répétez le processus pour tous les partages à l'exception du partage IPC$.

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

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

8.2 Dépannage de l'inventaire de workload (Linux)

Problèmes ou messages	Solutions
`Impossible de se connecter ni au serveur SSH qui s'exécute sur <adresse_IP> ni aux services Web VMware Virtual Infrastructure à <adresse_ip>/sdk`	Les causes possibles pouvant avoir généré l'envoi de ce message sont les suivantes : ◆ le workload est inaccessible ; ◆ SSH ne s'exécute pas sur le workload ; ◆ le pare-feu est activé et les ports requis n'ont pas été ouverts ; ◆ le système d'exploitation spécifique du workload n'est pas pris en charge. Pour les conditions d'accès et de réseau d'un workload, reportez-vous à la section « Conditions d'accès et de communication requises sur votre réseau de protection » page 14.
`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 75.

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

Problèmes ou messages	Solutions
Erreur d'authentification lors de la vérification de la connexion du contrôleur pendant la configuration de ce dernier sur la source.	Le compte utilisé pour ajouter un workload doit être autorisé par cette stratégie. Reportez-vous à la section « Stratégie de groupe et droits utilisateur » page 92.
Impossible de déterminer si .NET Framework est installé (à l'exception de `Échec de la relation d'approbation entre le poste de travail et le domaine principal`).	Vérifiez si le service d'accès à distance au Registre est activé et exécuté. Reportez-vous également à la « Dépannage de l'inventaire de workload (Windows) » page 87.

8.3.1 Stratégie de groupe et droits utilisateur

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

8.4 Dépannage de la réplication de workload

Problèmes ou messages	Solutions
Un problème de workload nécessite une intervention de l'utilisateur. 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. La solution consiste à attendre la fin de la réplication.
Tous les workloads signalent des erreurs récupérables en raison de l'espace disque insuffisant.	Vérifiez l'espace disponible. Si vous avez besoin de plus d'espace, supprimez un workload.
Le réseau est très lent (vitesse inférieure à 1 Mo).	Vérifiez si le paramètre de duplex de la carte d'interface réseau de la machine source est activé et si le commutateur auquel elle est connectée dispose d'un paramètre correspondant. En effet, si le paramètre est configuré sur Automatique, la source ne peut pas être définie sur 100 Mo.

Problèmes ou messages	Solutions
Le réseau est très lent (vitesse supérieure à 1 Mo).	Mesurez le temps de réponse en exécutant la commande suivante à partir du workload source : `ping ip –t` (remplacez *ip* par l'adresse IP de votre hôte de serveur PlateSpin Protect). Autorisez-le à exécuter 50 itérations et la moyenne indique la latence. Reportez-vous également à la section « Paramètres permettant d'optimiser les transferts sur des connexions WAN » page 22.

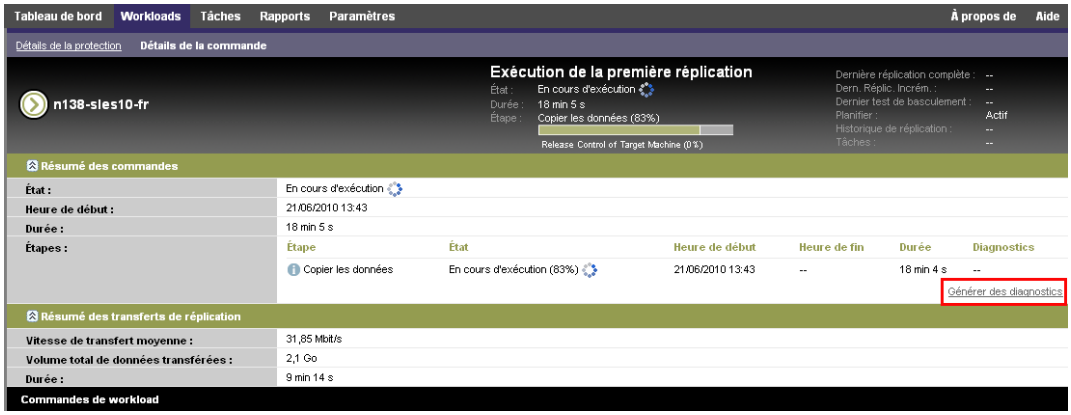
`The file transfer cannot begin - port 3725 is already in use`
 	
ou
 	
`3725 unable to connect`
	Assurez-vous que le port est ouvert et écoute :
	
	Exécutez `netstat -ano` sur le workload.
	
	Vérifiez le pare-feu.
	
	Réessayez la réplication.

`Controller connection not established` 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 Protect. Remplacez l'IP de réplication par un 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 Protect.
La tâche de réplication ne démarre pas (bloquée à 0 %)	Cette erreur peut se produire pour diverses raisons et chacune a sa propre solution : ◆ Pour les environnements qui utilisent un proxy local avec une authentification, ignorez le proxy ou ajoutez les autorisations appropriées pour résoudre ce problème. Pour plus de détails, reportez-vous à l'article de la base de connaissances n° 20339 (http://www.novell.com/support/viewContent.do?externalId=7920339). ◆ Si des restrictions de stratégies locales ou de domaine nécessitaient des autorisations, suivez la procédure décrite dans l'article de la base de connaissances n°7920862 (http://www.novell.com/support/viewContent.do?externalId=7920862). Il s'agit d'un problème courant lorsque l'hôte du serveur PlateSpin Protect 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 92.

8.5 Génération et affichage de rapports de diagnostic

Dans le client Web PlateSpin Protect, après avoir exécuté une commande, vous pouvez générer des rapports de diagnostic détaillés sur les détails de la commande.

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



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

2 Cliquez sur *Afficher*.

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

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

8.6 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.

8.6.1 Nettoyage des workloads Windows

Composant	Instructions de suppression
Composant de transfert par bloc PlateSpin	Reportez-vous à l'article de la base de connaissances n° 7005616 (http://www.novell.com/support/viewContent.do?externalId=7005616).

Composant	Instructions de suppression
Composant tiers de transfert par bloc (discontinué)	1. Utilisez l'applet Ajout/Suppression de programmes de Windows (exécutez le fichier `appwiz.cpl`) et supprimez le composant. Selon la source, vous pouvez disposer de l'une des versions suivantes : ◆ SteelEye Data Replication pour Windows v6 Update2 ◆ SteelEye DataKeeper pour Windows v7 2. Redémarrez la machine.
Composant de transfert basé sur les fichiers	Au niveau de la racine de chaque volume protégé, supprimez tous les fichiers nommés `PlateSpinCatalog*.dat`.
Logiciel d'inventaire de workloads	Dans le répertoire `Windows` du workload : ◆ Supprimez tous les fichiers nommés `machinediscovery*`. ◆ Supprimez le sous-répertoire nommé `platespin`.
Logiciel contrôleur	1. Ouvrez une invite de commande et remplacez le répertoire actuel par : ◆ `\Program Files\platespin*` (systèmes 32 bits) ◆ `\Program Files (x86)\platespin` (systèmes 64 bits) 2. Exécutez la commande suivante : `ofxcontroller.exe /uninstall` 3. Supprimez le répertoire `platespin*`.

8.6.2 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 source, supprimez le répertoire `/usr/lib/ofx` et son contenu.

Composant	Instructions de suppression

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/`*`[Kernel_Version]`*`/Platespin`
	5. Supprimez le fichier suivant :
	`/etc/blkwatch.conf`

Instantanés du gestionnaire de volumes logiques (LVM)	1. Dans la vue Tâches, générez un rapport de tâche pour la tâche qui a échoué, puis prenez note du nom de l'instantané. 2. Supprimez le périphérique d'instantané à l'aide de la commande suivante : `lvremove` *nom_instantané*
Fichiers Bitmap	À la racine de chaque volume protégé, supprimez le fichier `.blocks_bitmap` correspondant.
Outils	Sur le workload source, sous `/sbin`, supprimez les fichiers suivants : ◆ `bmaputil` ◆ `blkconfig`

8.6.3 Suppression de workloads

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

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

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

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

2 À la page Confirmation de commande, cliquez sur *Confirmer* pour exécuter la commande. Attendez que le processus se termine.

Glossaire

Conteneur
Soit un hôte de VM, soit un serveur d'images, à savoir les deux infrastructures de protection de workload que PlateSpin Protect prend en charge.

Déploiement
Commande de PlateSpin Protect qui à la suite d'un échec, récupère un workload en déployant son image protégée sur un serveur d'images, pour l'exécuter sur du matériel physique ou un conteneur de VM.

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

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

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

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

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

Préparer le basculement
Opération de PlateSpin Protect qui démarre le workload de récupération pour préparer une opération complète de basculement.

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

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

PDMA (Perte de données maximale admissible)
Perte de données tolérable mesurée en temps et définie par un intervalle configurable entre les réplications incrémentielles d'un workload protégé ou d'une image de workload protégée.

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

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

Réplication
1. Création d'une copie de base initiale d'un workload (*réplication initiale*).

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

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

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

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

Pour le déploiement d'une image, la source est l'image d'un workload sur un serveur d'images désigné.

Voir également Cible.

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

Pour le déploiement d'une image, la cible est l'infrastructure sur laquelle une image protégée est déployée pour démarrer.

Voir également Source.

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

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

Workload

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