MICRO FOCUS

PlateSpin® Protect 11.2 SP1
ユーザガイド

2017 年 12 月

保証と著作権

保証と著作権、商標、免責事項、保証、輸出およびその他の使用制限、米国政府の規制による権利、特許ポリシー、および FIPS コンプライアンスの詳細については、https://www.microfocus.com/about/legal/ を参照してください。

ライセンスの許諾

PlateSpin Protect 11 以降のバージョン用に購入したライセンスを PlateSpin Protect 10.3 以前のバージョン用に使用することはできません。

目次

このガイドについて

この『*ユーザガイド*』では、PlateSpin Protect の使用方法について説明します。このガイドでは、概念に関する情報とユーザインタフェースの概要、および一般的なタスクを手順を追って説明します。また、用語についても定義し、トラブルシューティング情報も含まれています。

本書の読者

このドキュメントは、継続的なワークロード保護および障害復旧ソリューションで PlateSpin Protect を使用するデータセンター管理者およびオペレータを対象としてます。

その他のマニュアル

このガイドの最新バージョンおよびその他の PlateSpin Protect ドキュメントリソースについては、PlateSpin Protect (https://www.netiq.com/documentation/platespin-protect/) マニュアルの Web サイトを参照してください。

オンラインマニュアルは、英語のほかに、簡体字中国語、繁体字中国語、フランス語、ドイツ語、日本語、およびスペイン語でご利用いただけます。

連絡先情報

本書またはこの製品に付属するその他のドキュメントについて、お客様のご意見やご提案をお待ちしています。オンラインヘルプのページ下部にある**このトピックのコメント**リンクを使用するか、または Documentation-Feedback@microfocus.com に電子メールを送信してください。

特定の製品の問題については、Micro Focus ご注文と配送 (https://www.microfocus.com/support-and-services/) にお問い合せください。

計画

PlateSpin Protect は、仮想化テクノロジを使用して物理的および仮想的ワークロード (オペレーティングシステム、ミドルウェア、およびデータ) を保護するビジネスコンティニュイティおよび障害復旧ソフトウェアです。運用サーバの停止時や障害発生時には、ターゲット*コンテナ* (VM ホスト) 内でワークロードの仮想化されたレプリカを直ちにパワーオンすることができ、運用環境が復元されるまで通常どおり実行し続けることができます。

PlateSpin Protect では、次のことが可能です。

- 障害時に迅速にワークロードを回復
- 複数のワークロードを同時に保護
- 運用環境に影響を与えずにフェールオーバーワークロードをテスト
- 元のインフラまたは完全に新しいインフラ (物理または仮想) にフェールオーバーワークロードをフェールバック
- SAN などの既存の外部ストレージソリューションの利用

- 13 ページの第 1 章「PlateSpin 環境の計画」
- 39 ページの第 2 章「ワークロードの保護と回復の基本ワークフロー」

1 PlateSpin 環境の計画

この項の情報を使用して、PlateSpin 保護および回復環境を計画します。

1.1 サポートされる構成

PlateSpin Protect では、Microsoft Windows、SUSE Linux Enterprise Server、および Red Hat Enterprise Linux の各オペレーティングシステムのほとんどのメジャーバージョンがサポートされています。また、Novell Open Enterprise Server、Oracle Enterprise Linux、および CentOS の各オペレーティングシステムの一部のバージョンを保護します。

この項では、PlateSpin Protect でサポートされるすべてのプラットフォーム構成と、ワークロードの保護と回復に必要なソフトウェア、ハードウェア、および仮想化環境について説明します。記載されているとおり、一部の構成ではワークロードの設定および回復用の特別な処理が必要です。ワークロードの設定を試みる前に、オンラインヘルプの別の場所で参照されている情報やナレッジベースの記事を確認してください。

注：ここで取り上げられていない構成はサポートされていませんが、PlateSpin Protect に対して行う改善の多くは、お客様から直接ご提案頂いたものです。弊社の製品がお客様のニーズをすべて満たすことができるよう、お客様のご協力をお願いいたします。記載されていないプラットフォーム構成に関心がある場合は、テクニカルサポートにお問い合わせください。貴重なご意見をぜひお寄せください。

1.1.1 サポートされる Windows のワークロード

PlateSpin Protect では、表 1-1 に一覧表示されている Microsoft Windows オペレーティングシステムバージョンのワークロードがサポートされています。

ファイルレベルのレプリケーションとブロックレベルのレプリケーションの両方がサポートされていますが、いくつか制約があります。詳細については、24 ページのセクション 1.2「サポートされるデータ転送方法」を参照してください。

注 : デスクトップ (ワークステーション) ワークロードの保護はサポートしていません。

表 1-1 *サポートされる Windows のワークロード*

オペレーティングシステム	備考
サーバ	
Windows Server 2016	Windows Server 2016 サーバの保護には VMware 6.0 以降が必要です。
Windows Server 2012 R2 Windows Server 2012	ドメインコントローラ (DC) および Small Business Server (SBS) エディションを含みます。 Active Directory ドメインコントローラの変換の詳細については、ナレッジベースの記事 7920501 (https://www.netiq.com/support/kb/doc.php?id=7920501) を参照してください。
Windows Server 2008 R2 (64 ビット) Windows Server 2008 (64 ビット) Windows Server 2008 最新 SP (32 ビット)	ドメインコントローラ (DC) および Small Business Server (SBS) エディションを含みます。 Active Directory ドメインコントローラの変換の詳細については、ナレッジベースの記事 7920501 (https://www.netiq.com/support/kb/doc.php?id=7920501) を参照してください。
Windows Server 2003 R2 (64 ビット) Windows Server 2003 R2 (32 ビット) Windows Server 2003 最新 SP (64 ビット) Windows Server 2003 最新 SP (32 ビット)	Windows 2003 では、ブロックベースレプリケーション用に SP1 以降が必要です。

オペレーティングシステム	備考
クラスタ	
Windows Server 2016 サーバベースの Microsoft フェールオーバークラスタ	Windows Server 2016 クラスタの保護には VMware 6.0 以降が必要です。 サポートされるモデル : 「ノードおよびディスクマジョリティのクォーラム」および「非マジョリティ : ディスク専用クォーラム」。 サポート対象には、クラスタの増分レプリケーションにおけるドライバ (ファイバチャネル SAN のみ) を使用するブロックベースデータ転送またはドライバを使用しないブロックベースデータ転送が含まれます。ファイルベースのレプリケーションはサポートされていません。 **警告 :** 共有 iSCSI ドライブを使用するクラスタでブロックベースドライバを使用しないでください。クラスタが使用不能になります。 詳細については、123 ページの 「Windows クラスタ保護の準備」を参照してください。
Windows Server 2012 R2 サーバベースの Microsoft フェールオーバークラスタ	
Windows Server 2008 R2 サーバベースの Microsoft フェールオーバークラスタ	
Windows Server 2003 R2 サーバベースの Windows クラスタサーバ	サポートされるモデル : 「シングルクォーラムデバイスクラスタ」。 サポート対象には、クラスタの増分レプリケーション用のドライバレスブロックベースのデータ転送のみが含まれます。ファイルベースのレプリケーションはサポートされていません。 詳細については、123 ページの 「Windows クラスタ保護の準備」を参照してください。
Hyper-V ホスト	
Windows Server 2012 R2 (Hyper-V 役割搭載) Windows Server 2012 (Hyper-V 役割搭載)	Hyper-V ホストとして機能している Windows サーバとそのボリュームを保護します。個々の VM を個別に保護します。

Windows 用の環境設定要件

Windows Update

最初の完全レプリケーションを実行する前に、ソースシステムで Windows Update を適用していることを確認してください。

ドメインコントローラとウィルス対策ソフトウェア

Windows マシンがドメインコントローラの場合、レプリケーション中はシステムでウィルス対策ソフトウェアを無効にしていることも確認してください。

1.1.2 サポートされる Linux のワークロード

PlateSpin Protect では、表 1-2 に一覧表示されている Linux オペレーティングシステムディストリビューションのワークロードがサポートされています。

保護されている Linux ワークロードのレプリケーションは、ブロックレベルでのみ実行されます。詳細については、18 ページの 「blkwatch ドライバの要件」を参照してください。

***表 1-2** サポートされる Linux のワークロード*

オペレーティングシステム	バージョン	備考
サーバ		
Red Hat Enterprise Linux (RHEL)	7.0 ～ 7.3 6.0 ～ 6.9 5.x 4.x	RHEL の各ディストリビューションでサポートされる Linux カーネルバージョンとアーキテクチャのリストについては、139 ページの「Protect によってサポートされている Linux ディストリビューション」を参照してください。 PlateSpin Protect では、RHEL 7.3 および RHEL 7.3 に基づくディストリビューション上の XFS バージョン 5 (v5) ファイルシステムがサポートされていません。 LVM ボリュームを持つ Red Hat Enterprise Linux 6.7、Oracle Linux 6.7、および CentOS 6.7 のワークロードについては、RHEL 6.7 ディストリビューション用の最新の使用可能なカーネル (バージョン 2.6.32-642.13.1.el6.x86_64) に対してのみ増分レプリケーションがサポートされます。これは、RHEL 6.8 ディストリビューションによって使用される同じカーネルです。
SUSE Linux Enterprise Server (SLES)	11 SP1 ～ 11 SP4 10.x 9.x	SLES の各ディストリビューションでサポートされる Linux カーネルバージョンとアーキテクチャのリストについては、139 ページの「Protect によってサポートされている Linux ディストリビューション」を参照してください。 SLES 11 SP3 のカーネルバージョン 3.0.13 はサポートされていません。ワークロードのインベントリを実行する前に、カーネルバージョン 3.0.27 以降にアップグレードしてください。

オペレーティングシステム	バージョン	備考
Open Enterprise Server (OES)	2015 SP1 11 SP1 ～ 11 SP3 2 SP3 詳細については、SUSE Linux Enterprise Server (SLES) を参照してください。	OES 2015 SP1 の場合、Protect では、最大サイズが 8 TB の NSS32 ビットプールがサポートされていますが、NSS64 ビットプールはサポートされていません。 SLES の各ディストリビューションでサポートされる Linux カーネルバージョンとアーキテクチャのリストについては、139 ページの「Protect によってサポートされている Linux ディストリビューション」を参照してください。 OES 11 SP2 のデフォルトのカーネルバージョン 3.0.13 はサポートされていません。ワークロードのインベントリを実行する前に、カーネルバージョン 3.0.27 以降にアップグレードしてください。
Oracle Linux (OL) (旧称 : Oracle Enterprise Linux (OEL))	詳細については、Red Hat Enterprise Linux (RHEL) を参照してください。	RHEL の各ディストリビューションでサポートされる Linux カーネルバージョンとアーキテクチャのリストについては、139 ページの「Protect によってサポートされている Linux ディストリビューション」を参照してください。 Blkwatch ドライバは、140 ページの 「ディストリビューションのリスト」に記載されているように、OEL 6 U7 以降の標準 Red Hat Compatible Kernel (RHCK) および Unbreakable Enterprise Kernel (UEK) で使用できます。 Unbreakable Enterprise Kernel を使用したワークロードは、PlateSpin Pro ect 11.2 以降ではサポートされません。 Oracle Linux 6 U7 の場合、カーネルバージョン 2.6.32-573 用の blkwatch ドライバでは、LVM ボリュームを持つワークロードに対する増分レプリケーションがサポートされていません。カーネルを更新して、カーネル 2.6.32-642 用の RHEL 6 U7 ドライバを使用してください。
CentOS	詳細については、Red Hat Enterprise Linux (RHEL) を参照してください。	RHEL の各ディストリビューションでサポートされる Linux カーネルバージョンとアーキテクチャのリストについては、139 ページの「Protect によってサポートされている Linux ディストリビューション」を参照してください。 CentOS 7.*x* では、VMware 5.5 以降が必要です。

Linux ワークロードの環境設定要件

blkwatch ドライバの要件

Linux ワークロードのデータのブロックベース転送には、保護対象である特定の Linux ディストリビューション用にコンパイルされた blkwatch ドライバが必要です。PlateSpin Protect ソフトウェアには、多数の非デバッグ Linux ディストリビューション (32 ビットおよび 64 ビット) 用に、事前コンパイルされたバージョンの blkwatch ドライバが付属しています。カスタムドライバを作成することもできます。詳細については、139 ページの 「Protect によってサポートされている Linux ディストリビューション」を参照してください。

1.1.3 サポートされる VM コンテナ

VM コンテナは、保護されたワークロードで定期的に更新されるブート可能な仮想レプリカのホストとして機能する保護インフラストラクチャです。

- 18 ページの 「サポートされる VMware プラットフォーム」
- 19 ページの 「コンテナとしての VMware DRS クラスタのサポート」
- 19 ページの 「VMware vCenter Site Recovery Manager 用サポート」
- 19 ページの 「VMware 上の保護のマルチテナンシのサポート」

サポートされる VMware プラットフォーム

サポートされている VMware プラットフォームのリストについては、表 1-3 を参照してください。プラットフォームは保護コンテナおよびフェールバックコンテナとしてサポートされています。

注 : ターゲット VM コンテナに対するワークロードの保護は、ホストベンダーによるターゲットホスト上のゲストオペレーティングシステムのサポート状況によって異なります。ターゲット VMware ホストについては、『*VMware 互換性ガイド* (http://www.vmware.com/resources/compatibility/)』を参照してください。

コンテナインフラストラクチャは、VMware ESXi Server または VMware DRS クラスタのいずれかにすることができます。VMware DRS クラスタ設定要件については、19 ページの 「コンテナとしての VMware DRS クラスタのサポート」を参照してください。

***表 1-3** VM コンテナとしてサポートされるプラットフォーム*

コンテナ	バージョン	備考
VMware vCenter または ESXi	6.5	VM コンテナとして、DRS クラスタは ESXi 6.5 サーバのみで構成されている必要があります。また、管理は vCenter 6.5 でのみ行うことができます。
VMware vCenter または ESXi	6.0 (GA2、U2、U3)	VM コンテナとして、DRS クラスタは ESXi 6.0 サーバのみで構成されている必要があります。また、管理は vCenter 6.0 でのみ行うことができます。

コンテナ	バージョン	備考
VMware vCenter または ESXi	5.5 (GA2、U2、U3)	VM コンテナとして、DRS クラスタは ESXi 5.5 サーバのみで構成されている必要があります。また、管理は vCenter 5.5 でのみ行うことができます。
VMware vCenter または ESXi	5.1 (GA2、U2、U3)	VM コンテナとして、DRS クラスタは ESXi 5.1 サーバのみで構成されている必要があります。また、管理は vCenter 5.1 でのみ行うことができます。
VMware vCenter または ESXi	4.1 (GA2、U3)	VM コンテナとして、DRS クラスタは ESXi 4.1 サーバのみで構成されている必要があります。また、管理は vCenter 4.1 でのみ行うことができます。

注 : VMware ESXi ホストには、購入したライセンスが必要です。これらのシステムが無償のライセンスで動作している場合、保護はサポートされません。

コンテナとしての VMware DRS クラスタのサポート

有効な保護ターゲットとするために、VMware DRS クラスタを VMware クラスタとしてコンテナのセット (インベントリ済み) に追加する必要があります。個々の ESX サーバのセットとして、DRS クラスタを追加しようとしないでください。詳細については、98 ページの 「コンテナ (保護ターゲット) の追加」を参照してください。

さらに、VMware DRS クラスタは次の構成要件を満たしている必要があります。

- DRS が有効になっていて、**一部自動**か**完全自動**に設定されている。(「手動」に設定されていてはならない。)
- 少なくとも 1 つのデータストアが、VMware クラスタのすべての VMware ホストで共有されている。
- 少なくとも 1 つの vSwitch および仮想ポートグループがある、また vNetwork Distributed Switch が、VMware クラスタのすべての VMware ホストに共通である。
- 各保護契約のフェールオーバーワークロード (VM) は、VMware クラスタのすべての VMware ホストで共有されているデータストア、vSwitch、および仮想ポートグループに排他的に配置される。

VMware vCenter Site Recovery Manager 用サポート

PlateSpin Protect では、VMware vCenter Site Recovery Manager (SRM) を使用した、リモート回復サイトへの複製された VM のコピーがサポートされています。詳細については、78 ページのセクション 6.7「VMware vCenter Site Recovery Manager 用サポートの設定」を参照してください。

VMware 上の保護のマルチテナンシのサポート

PlateSpin Protect では、VMware のマルチテナンシがサポートされています。複数の Protect サーバで同じ VMware クラスタバックエンドを共有できます。詳細については、59 ページの 「VMware での Protect のマルチテナンシの設定」を参照してください。

1.1.4 サポートされるワークロードアーキテクチャ

PlateSpin Protect では、次の x86 ベースのコンピュータアーキテクチャがサポートされています。

- 20 ページの 「プロセッサおよび OS アーキテクチャ」
- 20 ページの 「ターゲット VM 用のコア数とソケット数」
- 20 ページの 「ターゲット VM 用の仮想 CPU の数」
- 20 ページの 「UEFI および BIOS ファームウェア」

プロセッサおよび OS アーキテクチャ

PlateSpin Protect では、データセンターの物理および仮想ワークロードについて、x64 および x86 アーキテクチャの保護と回復がサポートされています。

- 64 ビット
- 32 ビット

ターゲット VM 用のコア数とソケット数

最小の VM ハードウェアレベル 8 で VMware 5.1 以降を使用する、サポート対象の VM コンテナの場合、PlateSpin Protect では、フェールオーバーワークロードに対し、ソケット数およびソケットあたりのコア数を指定することができます。合計コア数は自動的に計算されます。このパラメータは、初期レプリケーション設定である**完全**とともにワークロードの初期セットアップに適用されます。

注 : ワークロードが使用できるコアの最大数は、外部的な要因によって変わります。たとえば、ゲストオペレーティングシステム、VM のハードウェアバージョン、ESXi ホストの VMware ライセンス、vSphere の ESXi ホスト計算リソースの上限などです。「*ESXi/ESX 環境設定の上限*」(VMware ナレッジベース記事 1003497) (https://kb.vmware.com/kb/1003497) を参照してください。

ゲスト OS のディストリビューションによっては、コア数およびソケットあたりのコア数の設定が遵守されない場合があります。たとえば、SLES 10 SP4 および OES 2 SP3 を使用するゲスト OS では、インストールされている本来のコア数とソケットの設定が保持されます。一方、SLES、RHEL、および OES の他のディストリビューションでは、この設定が遵守されます。

ターゲット VM 用の仮想 CPU の数

VMware 4.1 を使用する VM コンテナの場合、PlateSpin Protect では、フェールオーバーワークロードに割り当てる必要がある vCPU (仮想 CPU) の数を指定することができます。このパラメータは、初期レプリケーション設定である**完全**とともにワークロードの初期セットアップに適用されます。各 vCPU は、VM コンテナ上のゲスト OS には、1 つのコア、1 つのソケットとして表示されます。

UEFI および BIOS ファームウェア

PlateSpin Protect では、Windows および Linux ワークロード用の UEFI および BIOS ファームウェアのインタフェースがサポートされています。

注 : UEFI ベースのワークロードを保護している場合、保護されているワークロードのライフサイクル全体で同じファームウェアブートモードを使用するには、vSphere 5.0 以降のコンテナをターゲットにする必要があります。

次に、UEFI システムと BIOS システムが保護されていて、同時にそれらのシステム間でフェールバックが行われたときの Protect の動作の例を示します。

- UEFIベースのワークロードをVMware vSphere 4*x*コンテナ(UEFIをサポートしていません)に転送すると、Protect は、フェールオーバー時のワークロードの UEFI ファームウェアを BIOS ファームウェアに遷移します。そして、UEFI ベースの物理マシンでフェールバックが選択されると、Protect は、ファームウェアを BIOS から UEFI に戻します。
- 保護されている Windows 2003 ワークロードを UEFI ベースの物理マシンにフェールバックしようとする場合、Protect は選択したものを分析し、有効でないことを通知します。つまり、Windows 2003 は UEFI ブートモードをサポートしていないため、BIOS から UEFI へのファームウェア遷移はサポートされません。
- BIOS ベースのターゲットで UEFI ベースのソースを保護している場合、Protect は、UEFI システムのブートディスク (GPT ディスク) を MBR ディスクにマイグレートします。この BIOS ワークロードを UEFI ベースの物理マシンにフェールバックすると、ブートディスクは GPT に変換されます。

Windows ワークロードでは、PlateSpin Protect は、UEFI または BIOS ベースの Windows ワークロードに対して、Microsoft と同様のサポートを提供します。Platespin Forge は、ソースからターゲットにワークロードを転送し、ソースとターゲットのそれぞれのオペレーティングシステムでサポートされているファームウェアを適用します。ブロックベースとファイルベースの両方の転送がサポートされています。物理マシンへのフェールバックでも同じ処理が行われます。UEFI システムと BIOS システムの間で遷移 (フェールオーバーとフェールバック) が開始されると、Protect では、遷移が分析され、その有効性に関するアラートが生成されます。

1.1.5 サポートされるストレージ

PlateSpin Protect では、Windows ワークロードおよび Linux ワークロードに対して以下のストレージ設定がサポートされています。

- 21 ページの 「ストレージディスク」
- 22 ページの 「パーティショニングスキーム」
- 22 ページの 「Windows ファイルシステム」
- 22 ページの 「Linux ファイルシステム」
- 22 ページの 「Linux ストレージの機能」

ストレージディスク

PlateSpin Protect では、ベーシックディスク、Windows ダイナミックディスク、LVM2、RAID、SAN など、さまざまなタイプのソースストレージディスクがサポートされています。

保護されている VM レプリカの仮想ディスクがシンプロビジョニングであるか、シックプロビジョニングであるかを指定できます。

注 : 以下の注意事項がストレージディスクに適用されます。

- **Windows ダイナミックディスク :** PlateSpin Protect では、ターゲットで Windows ダイナミックディスクがサポートされていません。

  ダイナミックディスクの場合、ストレージでは［ソースと同じ］マッピング戦略が実行されません。シンプルダイナミックボリュームとスパニングされたダイナミックボリュームは両方とも、ターゲットワークロード上にシンプルベーシックボリュームディスクとして配置されます。ダイナミックボリュームの各メンバーディスクの合計サイズが MBR パーティションのサイズ制限を超える場合に、ターゲットディスクは GPT としてパーティショニングされます。詳細については、「*Microsoft TechNet: Windows ストレージの 2 TB 制限について* (https://blogs.technet.microsoft.com/askcore/2010/02/18/understanding-the-2-tb-limit-in-windows-storage/)」を参照してください。

- **Linux ソフトウェア RAID:** PlateSpin Protect は、ソフトウェア RAID のボリュームの Linux ワークロードをサポートしていません。

パーティショニングスキーム

PlateSpin Protect では、Windows ワークロードおよび Linux ワークロード向けに、MBR (マスタブートレコード) および GPT (GUID パーティションテーブル) パーティショニングスキームがサポートされています。保護用のワークロードとストレージは、MBR または GPT でパーティショニングされたディスク上で設定する必要があります。GPT ではディスク 1 台あたり最大 128 個のパーティションを使用できますが、PlateSpin Protect でサポートされる GPT パーティションはディスクあたり 57 個以下に限られます。

Windows ファイルシステム

PlateSpin Protect は、サポートされる任意の Windows システムで NTFS ファイルシステムのみサポートします。

Linux ファイルシステム

PlateSpin Protect では、EXT2、EXT3、EXT4、REISERFS、XFS、および NSS (Open Enterprise Server のみ) の各ファイルシステムでブロックベース転送のみがサポートされています。

注 : XFS v5 ファイルシステムは、Red Hat Enterprise Linux 7.3 およびこのバージョンに基づくディストリビューションではサポートされていません。

注 : ソース上のワークロードの暗号化ボリュームは、フェールオーバー VM で復号化されます。

Linux ストレージの機能

Linux のワークロードでは、PlateSpin Protect は以下の追加のストレージサポートを提供しています。

- ソースワークロードに関連付けられたスワップパーティションなどの非ボリュームストレージが、フェールオーバーワークロードに複製されます。

- ボリュームグループと論理ボリュームのレイアウトが保存されるので、フェールバック時にそれらを再作成できます。
- LVM RAW ディスクボリュームは、Linux ワークロードの［ソースと同じ］設定でサポートされています。
- (OES 11) ソースワークロードの NLVM (Novell Linux Volume Management) レイアウトは、VM コンテナで保持および再作成されます。NSS プールはソースから回復 VM にコピーされます。
- (OES 2) ソースワークロードの EVMS レイアウトは、VM コンテナで保持および再作成されます。NSS プールはソースから回復 VM にコピーされます。

1.1.6 サポートされる国際言語

英語のほかに、PlateSpin Protect では、次の国際言語用に設定されたマシンでインストールおよび使用するための各国語サポート (NLS) が提供されています。

- 簡体字中国語 (zh-cn)
- 繁体字中国語 (zn-tw)
- フランス語 (fr)
- ドイツ語 (de)
- 日本語 (ja)

ヒント : 他の国際バージョンのサポートは限定的であり、先に示した言語以外では、システムファイルの更新が影響を受ける可能性があります。

「ローカライズ済みオンラインドキュメント」には上記の各言語のほか、スペイン語も用意されています。

これらの言語のいずれかで Web インタフェースを使用する方法については、67 ページの 「国際バージョンの言語設定の設定」を参照してください。

1.1.7 サポートされる Web ブラウザ

製品の操作のほとんどは、ブラウザベースの Web インタフェースを介して行います。

サポートされているブラウザを次に示します。

- *Google Chrome* バージョン 34.0 以上
- *Microsoft Internet Explorer* バージョン 11.0 以上
- *Mozilla Firefox* バージョン 29.0 以上

注 : JavaScript (アクティブスクリプト) がブラウザで有効になっている必要があります。

サポートされる国際言語のいずれかで PlateSpin Protect Web インタフェースを使用する方法については、67 ページの 「国際バージョンの言語設定の設定」を参照してください。

1.2 サポートされるデータ転送方法

データ転送方法とは、データがソースワークロードからターゲットワークロードへ複製される方法を表したものです。PlateSpin Protect では、保護ワークロードのオペレーティングシステムに応じて、次の異なるデータ転送機能を提供しています。

- 24 ページのセクション 1.2.1「Windows ワークロードの場合のサポートされる転送方法」
- 24 ページのセクション 1.2.2「Linux ワークロードの場合のサポートされる転送方法」

1.2.1 Windows ワークロードの場合のサポートされる転送方法

Windows ワークロードの場合、PlateSpin Protect は、ブロックレベルまたはファイルレベルでワークロードボリュームデータを転送するメカニズムを提供します。

- **Windows のファイルレベルのレプリケーション** (Windows のみ) データはファイルごとに複製されます。
- **Windows のブロックレベルのレプリケーション** データはボリュームのブロックレベルでレプリケーションされます。この転送方法では、PlateSpin Protect は、継続性に対する影響とパフォーマンスが異なる 2 つのメカニズムを提供します。必要に応じて、これらのメカニズムを切り替えることができます。
  - **ブロックベースコンポーネントを使用したレプリケーション** このオプションでは、ブロックレベルデータ転送に専用のソフトウェアコンポーネントを使用します。これは、Microsoft ボリュームスナップショットサービス (VSS)、および VSS をサポートするアプリケーションとサービスを活用します。保護されたワークロード上でのコンポーネントのインストールは自動的に行われます。

    注 : ブロックベースコンポーネントのインストールおよびアンインストールでは、保護されたワークロードの再起動が必要です。ブロックレベルのデータ転送で Windows クラスタを保護している場合、再起動は必要ありません。ワークロード保護の詳細を設定する際、後でコンポーネントをインストールすることを選択できます (この場合、必要な再起動は、最初のレプリケーションが行われるまで延期されます)。

  - **ブロックベースコンポーネントを使用しないレプリケーション** このオプションでは、内部の「ハッシング」メカニズムと Microsoft VSS を組み合わせて使用して、保護されたボリューム上の変更を追跡します。レプリケーション時にディスク上の各ブロックを比較し、変更部分のみをコピーします。

    このオプションでは、再起動は必要ありませんが、ブロックベースコンポーネントよりもパフォーマンスが低下します。

1.2.2 Linux ワークロードの場合のサポートされる転送方法

Linux ワークロードの場合、PlateSpin Protect では、block-watch (blkwatch) ドライバを使用したブロックベースのデータ転送のみがサポートされています。

注 : blkwatch ドライバの展開または削除は、透過的に行われ、継続性に影響はなく、再起動が必要ありません。

PlateSpin Protect のディストリビューションには、サポート対象の Linux ディストリビューションの非デバッグ標準カーネルが動作するワークロードに対応した、事前コンパイル済みの blkwatch ドライバが付属します。詳細については、140 ページのセクション B.2「Linux ディストリビューション用に事前コンパイルされた blkwatch ドライバ」を参照してください。

ワークロードが非標準カーネル、カスタマイズされたカーネル、または新しいカーネルを使用している場合は、その特定のカーネルに対応したカスタム blkwatch ドライバをビルドできます。ナレッジベースの記事 7005873「*カスタムのブロックベース Linux カーネルドライバをビルドする方法* (https://www.netiq.com/support/kb/doc.php?id=7005873)」を参照してください。

1.3 セキュリティとプライバシー

PlateSpin Protect には、データを守り、セキュリティを向上させるために役立つ機能が用意されています。

- 25 ページのセクション 1.3.1「転送におけるデータの暗号化」
- 25 ページのセクション 1.3.2「クライアント / サーバ通信のセキュリティ」
- 26 ページのセクション 1.3.3「資格情報のセキュリティ」
- 26 ページのセクション 1.3.4「ユーザ権限および認証」
- 26 ページのセクション 1.3.5「Microsoft SQL Server データベースの Windows 認証」
- 26 ページのセクション 1.3.6「ポート設定とファイアウォール」

1.3.1 転送におけるデータの暗号化

転送の暗号化により、ワークロードレプリケーション時に、より安全にワークロードデータを転送できます。暗号化が有効な場合、ソースからターゲットへのネットワーク上のデータ転送は、AES(高度暗号化標準) を使用して暗号化されます。

注 : データ暗号化は、パフォーマンスに影響を及ぼし、データ転送率を大幅に (最大 30%) スローダウンさせる可能性があります。

データ転送の暗号化オプションを選択することで、ワークロードごとに個別に暗号化を有効または無効にできます。詳細については、154 ページの 「ワークロード保護の詳細」を参照してください。

1.3.2 クライアント / サーバ通信のセキュリティ

PlateSpin Server では、PlateSpin Server ホストで SSL が有効にされるので、Web ブラウザと PlateSpin Server の間の安全なデータ転送は HTTPS (Hypertext Transfer Protocol Secure) で実現されます。また、有効な証明書が見つからない場合は、自己署名証明書が追加されます。

1.3.3 資格情報のセキュリティ

PlateSpin Protect では、通信に SSL 接続を使用して資格情報が保護されており、パスワードの暗号化には Windows 暗号ライブラリが使用されています。

種々のシステム (ワークロードやフェールバックターゲットなど) にアクセスするために使用する資格情報は、PlateSpin データベースに保管され、したがって、PlateSpin Protect Server ホストに対して持つものと同じセキュリティセーフガードの対象とはなりません。

さらに、資格情報は診断情報の中に含まれます。診断情報は、認定されたユーザがアクセスすることができます。ワークロード保護プロジェクトは、許可を受けたスタッフにより取り扱われるように保証する必要があります。

1.3.4 ユーザ権限および認証

PlateSpin Protect は包括的で、ユーザの役割に基づく安全なユーザ認定と認証メカニズムを備え、ユーザが実行できるアプリケーションのアクセスと操作を制御します。55 ページの 「ユーザ権限および認証の設定」を参照してください。

1.3.5 Microsoft SQL Server データベースの Windows 認証

PlateSpin Protect には、Windows 認証を使用して Microsoft SQL Server データベースにアクセスする機能があります。詳細については、35 ページの 「Microsoft SQL Server データベースに対する Windows 認証の要件」を参照してください。

1.3.6 ポート設定とファイアウォール

表 1-4 は、PlateSpin Protect によって使用されているデフォルトポートを示しています。カスタムポートを設定する場合は、そのポートを代わりに開く必要があります。PlateSpin Server、およびそのサーバで管理するソースマシンとターゲットマシンの通信用に、これらの間にあるファイアウォールの適切なポートも開いてください。通信用のトラフィックは双方向 (着信と発信) です。31 ページの 「保護ネットワークにわたるアクセスおよび通信の要件」も参照してください。

表 1-4 *PlateSpin Protect によって使用されるデフォルトポート*

ポート番号	プロトコル	機能	Details (詳細)
80	TCP	HTTP	(安全ではない) PlateSpin Server ホスト、およびそのホストで管理するソースマシンとターゲットマシンとの間の HTTP 通信で使用されます。 このポートを PlateSpin Server ホスト、ソースワークロードとターゲットワークロード、および VMware ESXi ホストで開きます。
443	TCP	HTTPS	(安全) SSL が PlateSpin Server ホストとソースマシンおよびターゲットマシンとの間で有効な場合、HTTPS 通信で使用されます。 このポートを PlateSpin Server ホスト、ソースワークロードとターゲットワークロード、VMware ESXi ホスト、および vCenter ホストサーバで開きます。

ポート番号	プロトコル	機能	Details (詳細)
3725	TCP	データ転送	ファイルベース転送とブロックベース転送を含む、ソースマシンとターゲットマシンの間のデータ転送で使用されます。 このポートを、すべてのワークロードのソースマシンとターゲットマシンで開きます。ソースとそのターゲット間のファイアウォールで TCP ポート 3725 を許可する必要もあります。詳細については、13 ページの「サポートされる構成」を参照してください。
135 445	TCP	RPC/DCOM	検出プロセスの実行時に、Windows マシン上での RPC/DCOM 通信に、およびソースマシンの制御の取得と再起動に使用されます。 これらのポートを、すべての Windows ワークロードのソースマシンとターゲットマシンの通信用に開きます。詳細については、14 ページの「サポートされる Windows のワークロード」を参照してください。
137 138 139	TCP	NetBIOS	NetBIOS 通信用 (名前サービス、データグラムサービスおよびセッションサービス) に使用されます。 これらのポートを、すべての Windows ワークロードのソースマシンとターゲットマシンの通信用に開きます。詳細については、14 ページの「サポートされる Windows のワークロード」を参照してください。
137 138	UDP	SMB	PlateSpin Server からソースマシンへのファイル転送で、［制御取得］フォルダとそのファイルの SMB 通信に使用されます。 これらのポートを PlateSpin Server ホストおよびソースワークロードで開きます。
139 445	TCP	SMB	
22	TCP		検出プロセスの実行時に、Linux マシン上での SSH 通信と SCP 通信に使用されます。 このポートを、すべての Linux ワークロードのソースマシンとターゲットマシンで開きます。詳細については、16 ページの「サポートされる Linux のワークロード」を参照してください。
25	TCP	SMTP	電子メール通知が有効な場合、SMTP トラフィック用に使用されます。 このポートを、PlateSpin Server ホストとメールリレーホストで開きます。
25	UDP	SMTP	
1433	TCP	SQL	リモート SQL Server での認証とデータ交換用に、Microsoft SQL Server 通信に使用されます。 これらの SQL ポートを、PlateSpin Server ホストとリモート SQL Server ホスト、およびその間にあるファイアウォールで開きます。 SQL Server ポートの要件の詳細については、Microsoft Developers Network の「*Configure the Firewall to Allow Server Access*」を参照してください。

ポート番号	プロトコル	機能	Details (詳細)
1434	TCP	SQL	Microsoft SQL Server 専用の管理者接続に使用されます。
1434	UDP	SQL	Microsoft SQL Server の名前付きインスタンスに使用されます。 このポートは、リモート SQL Server で名前付きインスタンスを使用する際に必要な場合があります。
49152 から 65535	TCP	SQL	Microsoft SQL Server、または LSA、SAM、Netlogon の RPC に使用されます。 特定の TCP ポートを使用するように Microsoft SQL Server を設定した場合、ファイアウォールでそのポートを開く必要があります。 35 ページの 「Microsoft SQL Server データベースに対する Windows 認証の要件」を参照してください。

1.4 パフォーマンス

1.4.1 製品パフォーマンスの特性

PlateSpin Protect 製品のパフォーマンス特性は、多くの要因に依存します。次のような要因があります。

- ソースワークロードのハードウェアおよびソフトウェアのプロファイル
- ターゲットコンテナのハードウェアおよびソフトウェアのプロファイル
- PlateSpin Server ホストのハードウェアおよびソフトウェアのプロファイル
- ネットワークの帯域幅、構成、および条件の詳細
- 保護されたワークロードの数
- 保護されていないボリュームの数
- 保護されていないボリュームのサイズ
- ソースワークロードのボリューム上のファイル密度 (容量の単位ごとのファイルの数)
- ソースの I/O レベル (ワークロードがどの程度取り込んでいるか)
- 同時使用レプリケーションの数

- データ暗号化が有効か無効か
- データ圧縮が有効か無効か

大規模ワークロード保護プランの場合、一般的なワークロードのテスト保護を実施し、一部のレプリケーションを実行し、ベンチマークとして結果を使用し、プロジェクトを通して定期的にメトリックスを微調整します。

1.4.2 RPO、RTO、および TTO の仕様

保護環境では、さまざまなワークロードに必要な復旧ポイントと復旧時間について、期待値はそれぞれ異なります。

- **目標復旧時点 (RPO):** RPO 設定は、大規模な停電時における時間で測定されるデータ紛失の許容量について記述します。RPO は、保護されたワークロードの増分レプリケーション間の設定可能な時間間隔で定義されます。

  RPO は、PlateSpin Protect の現在の使用率レベル、ワークロードの変更の頻度と範囲、ネットワーク速度、および選択したレプリケーションスケジュールによって影響されます。
- **目標復旧時間 (RTO):** RTO 設定は、フェールオーバー操作が完了するまでにかかる時間で測定されるワークロードの許容可能なダウンタイムを記述します。フェールオーバー操作は、フェールオーバーワークロードをオンラインにし、保護されている運用ワークロードを一時的に置き換えます。

  RTO は、フェールオーバー操作の設定および実行にかかる時間 (10 ～ 45 分) に影響されます。159 ページの 「フェールオーバー」を参照してください。
- **目標テスト時間 (TTO):** TTO 設定は、サービス復旧についてある程度の自信を持てるまで障害復旧テストを行うのに必要な時間について記述します。これは RTO に似ていますが、ユーザがフェールオーバーワークロードをテストするのに必要な時間を含んでいます。

  フェールオーバーのテスト機能を使用して異なるシナリオを実行し、ベンチマークデータを生成します。詳細については、160 ページの 「フェールオーバー機能のテストの使用」を参照してください。

RPO、RTO、および TTO に影響を及ぼす要因の 1 つに、必要な同時フェールオーバー操作の数があります。単一のフェールオーバーワークロードは、基礎となるインフラストラクチャのリソースを共有している複数のフェールオーバーワークロードよりも多くの使用可能なメモリリソースおよび CPU リソースを所有します。

フェールオーバー応答をテストする場合は、設定した RPO、RTO、および TTO に関連付けられている実際の値に注意する必要があります。

- **実際の復旧時点 (RPA):** RPA とは、時間で測定され、保護されるワークロードの増分レプリケーション (フェールオーバーテストの実行中に発生する) 間の実際に測定された間隔によって定義される、実際のデータ紛失のことです。RPA は「実際の目標復旧時点」(実際の RPO) としても知られています。
- **実際の復旧時間 (RTA):** RTA とはフェールオーバーの操作が終了するまでにかかる時間によって定義される、ワークロードの実際のダウンダイムを示す尺度のことです。RTA は「実際の目標復旧時間」(実際の RTO) としても知られています。
- **実際のテスト時間 (TTA):** TTA とは障害復旧計画をテストできる実時間の尺度のことです。これは実際の RTO に似ていますが、ユーザがフェールオーバーワークロードをテストするのに必要な時間を含んでいます。TTA は「実際の目標テスト時間」(実際の TTO) としても知られています。

さまざまな状況でフェールオーバーを実施することで、環境内のワークロードの平均的なフェールオーバー時間を判別し、それらを全体的なデータ回復計画におけるベンチマークデータとして使用してください。詳細については、180 ページの 「ワークロードとワークロード保護のレポートの作成」を参照してください。

1.4.3 データ圧縮

必要に応じて、PlateSpin Protect はネットワーク上で送信する前に、ワークロードのデータを圧縮できます。これにより、レプリケーション中に送信されるデータの全体的な量を減らすことができます。

圧縮率はソースワークロードのボリュームのファイルのタイプに応じて異なり、約 0.9 (100MB のデータが 90MB に圧縮) から約 0.5 (100MB のデータが 50MB に圧縮) まで変動する場合があります。

注 : データ圧縮はソースワークロードのプロセッサパワーを利用します。

データ圧縮は各ワークロードまたは保護ティアごとに別々に設定することができます。168 ページの 「保護ティア」を参照してください。

1.4.4 帯域幅制限

PlateSpin Protect は、ワークロード保護の過程で、直接の送信元 - 対 - 送信先の通信を可能にすることにより、消費されるネットワーク帯域幅の量を制御できるようにします。各保護コントラクトのスループット量を指定できます。これは、マイグレーショントラフィックでの生産ネットワークの輻輳の回避を可能にし、PlateSpin Server の全体的な負荷を軽減します。

帯域幅制限は各ワークロードまたは保護ティアごとに別々に設定することができます。168 ページの 「保護ティア」を参照してください。

1.4.5 スケーラビリティ

スケーラビリティは、次のような PlateSpin Protect 製品の主要特性を含みます (また依存します)。

- **サーバごとのワークロード :** PlateSpin Server ごとのワークロードの数は、RPO 要件とサーバホストのハードウェア特性を含むいくつかの要素に応じて、10 ～ 50 の間で変動します。

- **コンテナごとの保護 :** コンテナごとの保護の最大数は、ESXi ホストごとにサポートされる VM の最大数に関連する VM 仕様に関連しています (ただし、同じではありません)。追加の要素には、回復統計 (同時レプリケーションとフェールオーバーを含む) とハードウェアベンダの仕様が含まれます。

テストを実施し、容量の数値を増分調整し、スケーラビリティの上限を決める際にそれらを使用します。

1.4.6 データベースサーバ

PlateSpin Protect には、Microsoft SQL Server Express Edition が付属します。SQL Server Express の機能は、最大 50 ワークロードを保護する単一の PlateSpin Server には十分です (30 ページのセクション 1.4.5「スケーラビリティ」を参照)。

注 : Microsoft SQL Server Express のデータベースサイズ制限は 10 GB であり、一度に 1 つの CPU コアのみを使用できます。SQL Server Express の要件と制限の詳細については、Microsoft SQL Server 2014 Express マニュアル (https://www.microsoft.com/en-us/download/details.aspx?id=42299) を参照してください。

PlateSpin Server データベースインスタンスは、スケジュールされる増分レプリケーションの数によって、ワークロードあたり毎月最大 0.5GB まで拡張できます。新しいレポーティングデータに対するスペースを確保するため、過去のレポーティングデータを定期的に保管するか破棄することをお勧めします。

VMware DRS クラスタでは、最適なパフォーマンスのためにクラスタ内の複数のホスト間で保護ターゲットを分散させてください。

以下の環境で既存の Microsoft SQL Server Standard Edition または Enterprise Edition データベースサーバ上のデータベースインスタンスを使用するように PlateSpin Server を設定することをお勧めします。

- 同じリモート Microsoft SQL Server データベースサーバのデータベースインスタンスに対して使用する複数の PlateSpin Server の展開
- レポーティングデータの履歴をすべて保持することが重要になる展開

複数の PlateSpin Server で同じリモートデータベースサーバを使用できますが、各サーバには個別のデータベースインスタンスが必要です。

PlateSpin Server に対してリモートデータベースインスタンスを設定するには、『*PlateSpin Protect インストールおよびアップグレードガイド*』の「リモート Microsoft SQL Server のデータベースサーバの設定」を参照してください。

1.5 保護ネットワークにわたるアクセスおよび通信の要件

保護および回復用のワークロードを設定する前に、この項で説明するアクセスおよび通信の設定を使用してネットワークを設定します。

- 32 ページのセクション 1.5.1「PlateSpin Server ホストの Web インタフェースのネットワーク要件」
- 32 ページのセクション 1.5.2「コンテナのネットワーク要件」

- 33 ページのセクション 1.5.3「ワークロードのネットワーク要件」
- 35 ページのセクション 1.5.4「Microsoft SQL Server データベースに対する Windows 認証の要件」
- 36 ページのセクション 1.5.5「NAT を通じたパブリックおよびプライベートネットワーク経由の保護の要件」
- 37 ページのセクション 1.5.6「PlateSpin Server が NAT 全体で機能するための要件」
- 37 ページのセクション 1.5.7「デフォルトの bash シェルを上書きして Linux ワークロードに対してコマンドを実行する」

1.5.1 PlateSpin Server ホストの Web インタフェースのネットワーク要件

表 1-5 は、Web インタフェースにアクセスできるようにするために PlateSpin Server ホストで開く必要があるポートについて説明しています。

表 1-5 *PlateSpin Server ホスト用に開くポートの要件*

ポート (デフォルト)	備考
TCP 80	HTTP 通信の場合
TCP 443	HTTPS 通信の場合 (SSL が有効の場合)

1.5.2 コンテナのネットワーク要件

表 1-6 は、サポートされるワークロードコンテナのソフトウェア、ネットワーク、およびファイアウォールの要件について説明しています。

表 1-6 *コンテナに関するアクセスおよび通信の要件*

システム	前提条件	必要なポート (デフォルト)
すべてのコンテナ	ping (ICMP エコー要求と応答) 機能。	
すべての VMware コンテナ。詳細については、18 ページの 「サポートされる VM コンテナ」を参照してください。	• 管理者の役割を持つ VMware アカウント • VMware Web サービス API およびファイル管理 API	HTTPS (TCP 443)
vCenter サーバ	アクセス権を持つユーザに適切な役割と許可が割り当てられている必要があります。詳細については、VMware の関連リリースのマニュアルを参照してください。	HTTPS (TCP 443)

1.5.3 ワークロードのネットワーク要件

表 1-7 は、PlateSpin Protect を使用して保護する、ワークロードのソフトウェア、ネットワーク、およびファイアウォールの要件について説明しています。

表 1-7 *ワークロードに関するアクセスおよび通信の要件*

ワークロードタイプ	前提条件	必要なポート (デフォルト)
すべてのワークロード	ping (ICMP エコー要求と応答) のサポート	
Windows のすべてのワークロード。詳細については、14 ページの「サポートされる Windows のワークロード」を参照してください。	◆ Microsoft .NET Framework 3.5 Service Pack 1 ◆ Microsoft .NET Framework 4.0 検出については、ソースワークロードが Microsoft .NET Framework 2 SP2 以降を実行している必要があります。	
すべての Windows Server クラスタのワークロード。14 ページの「サポートされる Windows のワークロード」のクラスタを参照してください。	PlateSpin Server で、Windows Server クラスタとクラスタノードの IP アドレスの DNS 前方向検索および DNS 後方向検索を解決できることを確認してください。DNS サーバをアップデートするか、PlateSpin Server ホスト上のローカル hosts ファイル (%systemroot%\system32\drivers\etc\hosts) をアップデートできます。	

ワークロードタイプ	前提条件	必要なポート (デフォルト)
Windows のすべてのワークロード。詳細については、14 ページの「サポートされる Windows のワークロード」を参照してください。	◆ ビルトイン Administrator またはドメインの管理者アカウント資格情報 (ローカル管理者グループ内のメンバーシップのみでは不十分です)。 ◆ **ファイルおよびプリンタ共有**が許可に設定された Windows ファイアウォール。次のいずれかのオプションを使用します。 ◆ **オプション 1。Windows ファイアウォールの使用 :** 基本的な **Windows ファイアウォール**コントロールパネル項目 (firewall.cpl) を使用し、例外のリストで**ファイルとプリンタの共有**を選択します。 - または - ◆ **オプション 2。セキュリティが強化された Windows ファイアウォールの使用 :** 次の受信規則が有効で「**許可**」に設定されたセキュリティが強化された Windows ファイアウォールユーティリティ (wf.msc) を使用します。 ◆ **ファイルおよびプリンタ共有 (エコー要求 - ICMPv4In)** ◆ **ファイルおよびプリンタ共有 (エコー要求 - ICMPv6In)** ◆ **ファイルおよびプリンタ共有 (NB データグラム受信)** ◆ **ファイルおよびプリンタ共有 (NB 名受信)** ◆ **ファイルおよびプリンタ共有 (NB セッション受信)** ◆ **ファイルおよびプリンタ共有 (SMB 受信)** ◆ **ファイルおよびプリンタ共有(スプーラサービス - RPC)** ◆ **ファイルおよびプリンタ共有(スプーラサービス - RPC-EPMAP)**	TCP 3725 NetBIOS (TCP 137 - 139) SMB (TCP 139、445 および UDP 137、138) RPC (TCP 135、445)
Windows Server 2003 (SP1 Standard、SP2 Enterprise、および R2 SP2 Enterprise を含む).	**注 :** 必要なポートを有効にした後、サーバプロンプトで次のコマンドを実行して、PlateSpin のリモート管理を有効にします。 netsh firewall set service RemoteAdmin enable netsh の詳細については、Microsoft TechNet の記事 (*The Netsh Command Line Utility* (http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx)) を参照してください。	TCP 3725、135、139、445 UDP 137、138、139

ワークロードタイプ	前提条件	必要なポート (デフォルト)
Linux のすべてのワークロード . 詳細については、16 ページの 「サポートされる Linux のワークロード」を参照してください。	Secure Shell (SSH) サーバ	TCP 22、3725

1.5.4 Microsoft SQL Server データベースに対する Windows 認証の要件

PlateSpin Protect には、Windows 認証を使用して Microsoft SQL Server データベースにアクセスする機能があります。Active Directory 設定を設定し、ファイアウォールでポートを開いて認証を有効にする必要があります。

SQL データベースに対する Windows 認証を有効化するには :

1. TCP/IP 接続と名前付きパイプ接続の両方が有効になるように、Microsoft SQL Server を設定していることを確認します。
2. (条件に応じて実行)Windows 認証を使用して Microsoft SQL Server データベースにアクセスする場合は、Active Directory で次のように設定する必要があります。
   - 該当のドメインに Microsoft SQL Server データベースサーバを追加する必要があります。
   - PlateSpin Protect のインストールでは、次に挙げる 2 つのドメインユーザアカウントが必要です。
     - **sysadmin 役割を設定したドメインユーザ :** SQL 管理者の権利を持つこのユーザは、データベース、テーブル、およびその他のスキーマオブジェクトを作成するために必要です。
     - **PlateSpin Service ユーザ :** ドメインの中で低い特権を持つドメインユーザをサービスユーザとすることもできますが、そのユーザは、PlateSpin Protect Server でローカル管理者になっていること、およびインストールの前にその特権を与えられていることが必要です。

       Windows ユーザのパスワードを変更した場合は、PlateSpin Service ユーザと IIS App Pool のパスワードもそれぞれ更新する必要があります。このような状況を避けるには、パスワードが失効しない Windows ユーザの使用を検討します。

   注 : Windows 認証を使用する場合、PlateSpin Server をアップグレードまたはアップデートする際に、SQL 管理者の権利を持つドメインユーザとしてログインする必要があります。
3. SQL Server に対する認証をサポートするために、ファイアウォール上で次の各ポートを開きます。
   - **ポート 49152 ～ 65535/TCP:** LSA、SAM、Netlogon の RPC トラフィックを許可します。
   - **ポート 1433/TCP:** Microsoft SQL Server のトラフィックを許可します。
   - **カスタムポート :** カスタム TCP ポートを使用するように SQL Server を設定する場合は、そのポートをファイアウォール上で開く必要があります。

注 : ダイナミックポートを使用しない場合は、**データベースサーバ**フィールドで専用ポートを指定する必要があります。

4 (条件に応じて実行)PlateSpin Protect で専用ポートを使用する場合は、そのポートをファイアウォール上で開く必要があります。

4a データベースサーバ上で、開く必要があるポートを判断します。

4a1 SQL Server 構成マネージャで、**Protocols for SQLExpress (SQL Express のプロトコル) > TCP/IP** の順に選択し、右クリックして**プロパティ**を選択します。

4a2 表示されたダイアログで **IP アドレス**タブを選択します。

4a3 **IPAll**(または目的のプロトコル) で **TCP ポート**または **TCP 動的ポート**が 0 以外の値に設定されている場合は、指定のポートをファイアウォール上で開きます。これらのポートが、SQL Server との接続で使用するポートです。

たとえば、**TCP 動的ポート**フィールドが 60664、**TCP ポート**フィールドが 1555 にそれぞれ設定されている場合は、SQL Server に対するファイアウォールルールでポート 60664 と 1555 を有効にします。

4b これらのポートをファイアウォール上で開きます。

注 : ダイナミックポートの値を設定している場合は、**参照**をクリックしても、そのサーバが SQL Server のリストに表示されないことがあります。その場合は、PlateSpin Protect のインストールで表示される**データベースサーバ**入力フィールドで、そのサーバを手動で指定する必要があります。

たとえば、使用しているサーバの名前が MYSQLSERVER、データベースインスタンス名が SQLEXPRESS、ダイナミックポートに設定している専用ポートが 60664 である場合は、次のテキストを入力し、目的の認証タイプを選択します。

MYSQLSERVER\SQLEXPRESS,60664

これらのポートをファイアウォール上で開く必要があります。

1.5.5 NAT を通じたパブリックおよびプライベートネットワーク経由の保護の要件

場合によっては、ソース、ターゲットまたは PlateSpin Protect 自身は、NAT (ネットワークアドレストランスレータ) の背後にある社内 (プライベート) ネットワーク上にあり、保護中に相手先と通信できません。

PlateSpin Protect は、次のホストのうちのどれが NAT デバイスの背後にあるかに応じて、ユーザがこの問題に対応することができるようにします。

- **PlateSpin Server:** サーバの PlateSpin 環境設定ツールを使用して、PlateSpin Server ホストに割り当てられた追加の IP アドレスを記録します。詳細については、37 ページの 「PlateSpin Server が NAT 全体で機能するための要件」を参照してください。
- **ターゲットコンテナ :** コンテナ (VMware ESX など) を検出するときは、検出パラメータでそのホストのパブリック (外部) IP アドレスを指定します。
- **ワークロード :** ワークロードを追加するときに、検出パラメータでそのワークロードのパブリック (外部) IP アドレスを指定します。

- **フェールオーバー VM:** フェールバック時に、(163 ページ) フェールバック詳細 (ワークロードを VM へ) のフェールオーバーワークロードに対して代替 IP アドレスを指定することができます。
- **フェールバックターゲット :** フェールバックターゲットを登録するとき、PlateSpin Server の IP アドレスを入力するよう要求されたら、PlateSpin Server ホストのローカルアドレスまたはサーバの PlateSpin 環境設定データベースに記録されているパブリック (外部) アドレスのいずれかを指定してください。詳細については、37 ページの 「PlateSpin Server が NAT 全体で機能するための要件」を参照してください。

1.5.6 PlateSpin Server が NAT 全体で機能するための要件

ネットワークアドレス変換を有効にした環境全体で機能するには、PlateSpin Server で追加の IP アドレスが必要です。詳細については、37 ページの 「PlateSpin Server が NAT 全体で機能するための要件」を参照してください。

1.5.7 デフォルトの bash シェルを上書きして Linux ワークロードに対してコマンドを実行する

デフォルトでは、Linux ソースのワークロードに対してコマンドを実行する場合、PlateSpin サーバは /bin/bash シェルを使用します。

必要に応じて、PlateSpin サーバの対応するレジストリキーを変更することで、デフォルトのシェルを上書きできます。ナレッジベースの記事 7010676「*Linux のデフォルトシェルのオーバーライド手順* (https://www.netiq.com/support/kb/doc.php?id=7010676)」を参照してください。

2 ワークロードの保護と回復の基本ワークフロー

PlateSpin Protect は、ワークロード保護と回復の次のワークフローを定義します。これらのステップのほとんどは、［ワークロード］ページのワークロードコマンドとして提示されます。詳細については、47 ページの 「ワークロードの保護と回復のコマンド」を参照してください。

表 2-1 保護と回復のライフサイクル

タスク	アクション	備考
準備 ワークロード、コンテナ、および環境が必要な基準を満たしていることを確認します。		
	1. PlateSpin Protect がご使用のワークロードをサポートしていることを確認します。	詳細については、13 ページの 「サポートされる構成」を参照してください。
	2. ご使用のワークロードと VM コンテナがアクセスおよびネットワークの前提条件を満たしていることを確認します。	詳細については、31 ページの 「保護ネットワークにわたるアクセスおよび通信の要件」を参照してください。
インベントリ 保護対象のワークロードと、フェールオーバーワークロードをホストするコンテナは、適切なインベントリを実行する必要があります。これらのワークロードとコンテナは任意の順序で追加できますが、各保護スケジュールでは、PlateSpin Server によって、定義済みのワークロードとコンテナのインベントリを実行する必要があります。		
	3. ターゲットコンテナを PlateSpin Server に追加します。	詳細については、98 ページの 「コンテナ (保護ターゲット) の追加」を参照してください。
	4. ソースワークロードを PlateSpin Server に追加します。	詳細については、102 ページの 「ワークロード (保護ソース) の追加」を参照してください。
	5. 物理的な保護ターゲットについて、デバイスドライバを準備します。	詳細については、107 ページの第 11 章「物理フェールバックターゲットのデバイスドライバの準備」を参照してください。
	6. Linux ワークロードについて、ワークロード保護を準備します。	詳細については、119 ページの第 12 章「保護用の Linux ワークロードの準備」を参照してください。
	7. Windows Server クラスタワークロードについて、クラスタワークロード保護を準備します。	詳細については、123 ページの第 13 章「Windows クラスタ保護の準備」を参照してください。

タスク	アクション	備考
保護コントラクトの定義		
	8. 保護コントラクトの詳細および仕様を定義します。	詳細については、153 ページの 「保護詳細の設定およびレプリケーションの準備」を参照してください。
	9. レプリケーションを準備します。	
保護の開始		
	10. 要件に従って保護コントラクトを開始します。	詳細については、158 ページの 「ワークロード保護の開始」を参照してください。
保護ライフサイクルタスク (オプション)		
これらのステップは、自動レプリケーションスケジュールには含まれていませんが、多くの場合、さまざまな状況で役に立ちます。または、ビジネスの継続性戦略によって決まる場合があります。		
	11. *手動での増分実行*: 増分レプリケーションをワークロード保護コントラクト外で、手動で実行できます。	ワークロードを選択し、**増分の実行**をクリックします。
	12. *テスト*. 制御された方法および環境で、フェールオーバー機能をテストできます。	フェールオーバー機能のテストの使用を参照してください。
フェールオーバー		
	13. このステップでは、保護されたワークロードを、VM コンテナ内で実行されているそのレプリカにフェールオーバーします。	詳細については、159 ページの 「フェールオーバー」を参照してください。
フェールバック		
	14. このステップは、運用ワークロードに関するすべての問題に対処した後の業務復旧フェーズに対応します。	詳細については、161 ページの 「フェールバック」を参照してください。
再保護		
	15. このステップでは、ワークロードの元の保護コントラクトを再定義できるようにします。	詳細については、166 ページの 「ワークロードの再保護」を参照してください。 **再保護**コマンドは、フェールバック操作が正常に終了すると利用可能になります。

PlateSpin Server の管理

この項では、PlateSpin Protect ライセンスをアクティブ化し、環境用に PlateSpin 製品をカスタマイズするために必要な情報を提供します。PlateSpin ツールと設定オプションに精通してください。ライセンスまたはユーザを管理したり、設定をカスタマイズしたりする必要があるときにはいつでもこの項に戻ることができます。

3 PlateSpin ツールの使用

製品の操作のほとんどは、ブラウザベースの Web インタフェースを介して行います。Web ベースの PlateSpin 環境設定ページを使用して、PlateSpin Server アプリケーションのグローバルパラメータを設定することもできます。

3.1 Web インタフェースの起動

1. (オプション) PlateSpin Server および使用する Web ブラウザが、英語ではなく、サポートされる国際言語のいずれかを使用するように設定します。詳細については、67 ページの 「国際バージョンの言語設定の設定」を参照してください。
2. サポートされる Web ブラウザを開き、次のページにアクセスします。

   https://*Your_PlateSpin_Server*/Protect

   Your_PlateSpin_Server を PlateSpin Server ホストの DNS ホスト名または IP アドレスで置き換えます。

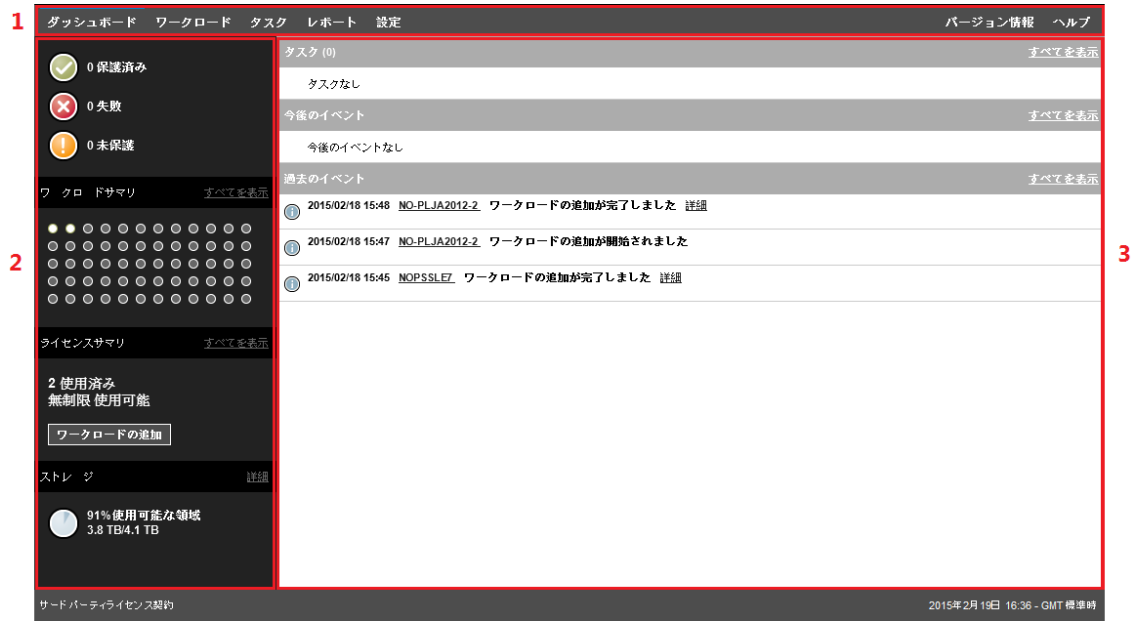
   SSL が有効でない場合は、URL に http を使用します。
3. PlateSpin Server ホストのローカル管理者ユーザの資格情報を使用してログインします。

   PlateSpin の追加ユーザの設定については、55 ページの第 5 章「ユーザ権限および認証の設定」を参照してください。

3.2 ダッシュボードの概要

PlateSpin Protect Web インタフェースの［ダッシュボード］ページには、インタフェースの別の機能領域に移動したり、ワークロード保護操作および回復操作を実行したりするための要素が含まれます。

図 3-1 PlateSpin Protect Web インタフェースのデフォルトのダッシュボードページ



［ダッシュボード］ページは次の要素で構成されています。

1. **ナビゲーションバー：** PlateSpin Protect Web インタフェースのほとんどのページ上に表示されます。
2. **ビジュアルサマリパネル：** PlateSpin Protect ワークロードインベントリの全体的な状態の概要レベルのビューが表示されます。
3. **タスクおよびイベントパネル：** ユーザによる介入が必要なイベントおよびタスクについての情報が表示されます。

次の各項目では、詳細が表示されます。

- 45 ページのセクション 3.2.1「ナビゲーションバー」
- 45 ページのセクション 3.2.2「ビジュアルサマリパネル」
- 46 ページのセクション 3.2.3「タスクおよびイベントパネル」

注： Web インタフェースの特定の要素を組織のブランディングに一致するように変更できます。詳細については、89 ページの 「PlateSpin Protect Web インタフェースのブランディングの変更」を参照してください。

3.2.1 ナビゲーションバー

ナビゲーションバーには次のリンクが含まれています。

- **ダッシュボード :** デフォルトの［ダッシュボード］ページを表示します。
- **ワークロード :**［ワークロード］ページを表示します。46 ページの 「ワークロードの概要」を参照してください。
- **タスク :** ユーザによる操作が必要な項目を一覧表示する［タスク］ページを表示します。
- **レポート :**［レポート］ページを表示します。180 ページの 「ワークロードとワークロード保護のレポートの作成」を参照してください。
- **設定 :** 次の設定オプションにアクセスできる［設定］ページを表示します。
  - **保護ティア :** 168 ページの 「保護ティア」を参照してください。
  - **Workload Tags (ワークロードタグ):** 81 ページの 「ワークロードタグの作成と管理」を参照してください。
  - **許可 :** 55 ページの 「ユーザ権限および認証の設定」を参照してください。
  - **コンテナ :** 98 ページの 「コンテナ (保護ターゲット) の追加」を参照してください。
  - **通知設定 :** 69 ページの 「イベント通知の有効化」.
  - **レプリケーションレポートの設定 :** 71 ページの 「レプリケーションレポートの有効化」
  - **SMTP:** 詳細については、69 ページの 「電子メール通知サービス用の SMTP の設定」を参照してください。
  - **ライセンス :** 詳細については、51 ページの 「製品ライセンスの有効化」を参照してください。

3.2.2 ビジュアルサマリパネル

［ビジュアルサマリ］パネルには、インベントリ済みワークロードの概要レベルの保護ステータス、ライセンス済みの各ワークロードの状態、ライセンス使用状況のサマリ、および使用可能なストレージの量が表示されます。

保護ステータス

インベントリ済みワークロードの全体的な保護ステータスは次の 3 つのカテゴリで表されます。

- **保護 :** アクティブな保護を受けているワークロードの数を示します。
- **失敗 :** ワークロードの保護ティアに従って失敗したとシステムが表示した保護ワークロードの数を示します。
- **保護不足 :** ユーザによる介入が必要な保護ワークロードの数を示します。

Workload Summary (ワークロードサマリ)

［Workload Summary (ワークロードサマリ)］には、［ワークロード］ページにリストされた各ライセンス済みワークロードのヘルス状態が表示されます。ワークロードの状態を示すドットアイコンの最大数は、PlateSpin Server にインストールされたワークロードライセンスの数と一致します。無制限ライセンスの場合は、96 個のドットアイコンがサマリに表示されます。表 3-1 は、ドットアイコンによって表されるワークロードのさまざまな状態について説明しています。

アイコンは、ワークロード名に従ってアルファベット順にワークロードを表します。ドットアイコンにマウスのカーソルを合わせるとワークロード名が表示され、アイコンをクリックすると対応する［ワークロードの詳細］ページが表示されます。

表 3-1 ドットアイコンによるワークロードの表示

● 保護	● 未保護
● 失敗	○ 未保護 – エラー
● 保護下	● 有効期限切れ
	● 未使用

License Summary (ライセンスサマリ)

[License Summary (ライセンスサマリ)] には、インストールされているライセンスの数、および現在ワークロードによって使用されているライセンスの数が表示されます。

ストレージ

ストレージには、PlateSpin Protect で使用可能なコンテナストレージ領域の合計量、および現在使用中の領域の量が表示されます。

3.2.3 タスクおよびイベントパネル

タスクおよびイベントパネルには、最近のタスク、最近の過去のイベント、および次の今後のイベントが表示されます。

システムまたはワークロードに関連して何かが発生すると、イベントがログ記録されます。たとえば、保護されたワークロードの新規追加、開始中または失敗中のワークロードのレプリケーション、保護されたワークロードの障害の検出などが、イベントとして挙げられます。イベントによっては、電子メールによる自動通知を生成するものもあります (SMTP が設定されている場合)。68 ページの 「イベントおよびレプリケーションレポートの電子メール通知サービスの設定」を参照してください。

タスクは、ユーザによる操作が必要なイベントに関連付けられている特別なコマンドです。たとえば、[フェールオーバーのテスト] コマンドを完了すると、[テストを成功としてマーク] および [テストを失敗としてマーク] という 2 つのタスクに関連するイベントがシステムによって生成されます。いずれかのタスクをクリックすると、[フェールオーバーのテスト] 操作はキャンセルされ、対応するイベントが履歴に書き込まれます。別の例としては、[完全レプリケーションに失敗しました] イベントが挙げられます。このイベントは、[完全処理の開始] タスクとともに表示されます。現在のタスクの完全なリストは、タスクタブで表示できます。

ダッシュボードのタスクおよびイベントパネルでは、各カテゴリに最大 3 つのエントリが表示されます。すべてのタスクを表示する、または過去および今後のイベントを表示するには、適切なセクションのすべてを表示をクリックします。

3.3 ワークロードの概要

[ワークロード] ページには、インベントリされたワークロードごとに割り当てられた行を含むテーブルが表示されます。ワークロードに関する設定とその状態を表示または編集するために [ワークロードの詳細] ページを表示するには、ワークロード名をクリックします。[ワークロード] リストには、ワークロードの可用性 (オンラインまたはオフライン)、タグ、保護階層、レプリケーションステータスおよび実行時間、および前回のテストフェールオーバー時間に関する情報が表示されます。

図 3-2　［ワークロード］ページ

注 : すべてのタイムスタンプは、PlateSpin Server ホストのタイムゾーンを反映しています。これは、保護ワークロードのタイムゾーンまたは Web インタフェースを実行しているホストのタイムゾーンとは異なる可能性があります。クライアントウィンドウの右下にサーバの日時が表示されます。

3.4　ワークロードの保護と回復のコマンド

コマンドには、ワークロード保護および回復のワークフローが反映されています。ワークロードにコマンドを実行するには、左側の該当するチェックボックスをオンにします。適切なコマンドは、ワークロードの現在の状態に依存します。

図 3-3　ワークロードコマンド

表 3-2 は、ワークロードのコマンドをその機能の説明と共にまとめたものです。

表 3-2　ワークロードの保護と回復のコマンド

ワークロードコマンド	説明
設定	インベントリされたワークロードに適したパラメータを使用してワークロード保護の設定を開始します。
レプリケーションの準備	必要なデータ転送ソフトウェアをソースにインストールし、ワークロードレプリケーションに備えてフェールオーバーワークロード (仮想マシン) を作成します。
レプリケーションの実行	指定されたパラメータに従って、ワークロードのレプリケーションを開始します (完全レプリケーション)。

ワークロードコマンド	説明
増分の実行	ワークロード保護コントラクト以外で、ソースからターゲットに変更されたデータの増分転送を実行します。
スケジュールの一時停止	保護を中断します。スケジュールされているすべてのレプリケーションは、スケジュールが再開されるまで一時停止します。
スケジュールの再開	保存された保護設定に従って保護を再開します。
フェールオーバーのテスト	テストの目的で、フェールオーバーワークロードをコンテナ内の隔離された環境で起動および設定します。
フェールオーバーの準備	フェールオーバー操作の準備としてフェールオーバーワークロードを起動します。
フェールオーバーの実行	失敗したワークロードのビジネスサービスを引き継ぐフェールオーバーワークロードを起動および設定します。
フェールオーバーのキャンセル	フェールオーバープロセスを中止します。
フェールバック	フェールオーバー操作に引き続き、フェールオーバーワークロードを元のインフラストラクチャか新しいインフラストラクチャ (仮想または物理) にフェールバックします。
再保護	フェールバック操作が正常に終了すると、［再保護］オプションが使用可能になります。
ワークロードの削除	インベントリからワークロードを削除します。

3.5 その他の PlateSpin Server 管理ツール

3.5.1 PlateSpin 設定

PlateSpin Server の動作の一部は、PlateSpin Server ホストの環境設定 Web ページで設定されている環境設定パラメータによって制御されます。このページは次の場所にあります。

https://*Your_PlateSpin_Server*/platespinconfiguration/

注 : 通常の状況では、PlateSpin Support が推奨しない限り、これらの設定を変更しないでください。

環境設定パラメータを変更して適用するには :

1. 任意の Web ブラウザから、次を開きます。

   https://*Your_PlateSpin_Server*/platespinconfiguration/
2. 検索して必要なサーバパラメータを見つけて、その値を変更します。

3 設定を保存し、ページを閉じます。

PlateSpin サービスの再起動または再開は、変更を適用するため必要とされません。

次の項目では、PlateSpin 環境設定パラメータを使用して製品動作を変更する必要が生じる可能性のある特定の状況について説明します。

- 37 ページの 「PlateSpin Server が NAT 全体で機能するための要件」
- 72 ページの 「WAN 接続を使用したデータ転送の最適化」
- 76 ページの 「レプリケーション環境の最適化」
- 77 ページの 「設定サービスに対する再起動方法の設定」
- 78 ページの 「VMware vCenter Site Recovery Manager 用サポートの設定」
- 89 ページの 「環境設定パラメータによる Web インタフェースの再ブランディング」
- 129 ページの 「Windows アクティブノードの検出の設定」
- 182 ページの 「設定サービスのトラブルシューティング」

3.5.2 Protect Agent ユーティリティ

Protect Agent ユーティリティ (ProtectAgent.cli.exe) は、ブロックベース転送ドライバのインストール、アップグレード、クエリ、またはアンインストールを実行するために使用できるコマンドラインユーティリティです。ドライバをインストール、アンインストール、またはアップグレードしたときは常に再起動が必要ですが、Protect Agent ユーティリティを使用すると、これらの操作を実行するタイミングを柔軟に制御できるため、サーバが再起動されるタイミングも柔軟に制御できます。たとえば、このユーティリティを使用して、最初のレプリケーション時ではなくスケジュールされたダウンタイム時にドライバをインストールできます。詳細については、145 ページの付録 D 「Protect Agent ユーティリティ」を参照してください。

3.5.3 VMware Role ツール

VMware Role ツール (PlateSpin.VMwareRoleTool.exe) は、マルチテナンシをサポートする際に、VMware データセンターで固有のユーザ役割を作成するために使用できるコマンドラインユーティリティです。この役割により、非管理 VMware ユーザ (つまり「有効化されたユーザ」) は、VMware 環境で保護ライフサイクル操作を実行できるようになります。詳細については、59 ページのセクション 5.4「VMware での Protect のマルチテナンシの設定」を参照してください。

4 ライセンスの管理

製品の特定のライセンスをアクティブ化した後は、ワークロードライセンスの可用性の監視、新しいライセンスの追加、および失効したライセンスの削除を行えます。

4.1 製品ライセンスの有効化

PlateSpin Protect 製品ライセンスでは、ワークロードライセンス契約を通して保護用に特定または無制限の数のワークロードを使用する権利が与えられます。

PlateSpin Protect 製品のライセンスには、ライセンスのアクティベーションコードが必要です。ライセンスのアクティベーションコードがない場合、カスタマーセンター (http://www.netiq.com/customercenter/) を通じて要求してください。ご注文と配送の担当者からユーザに、ライセンスアクティベーションコードが通知されます。

注 : PlateSpin の既存のお客様で、カスタマーセンターのアカウントをお持ちでない場合は、発注書に記載されているものと同じ電子メールアドレスを使用して、まずそのアカウントを作成する必要があります。「アカウントの作成 (https://www.netiq.com/selfreg/jsp/createAccount.jsp)」を参照してください。

製品ライセンスを有効にするには、オンラインとオフラインの 2 つのオプションがあります。

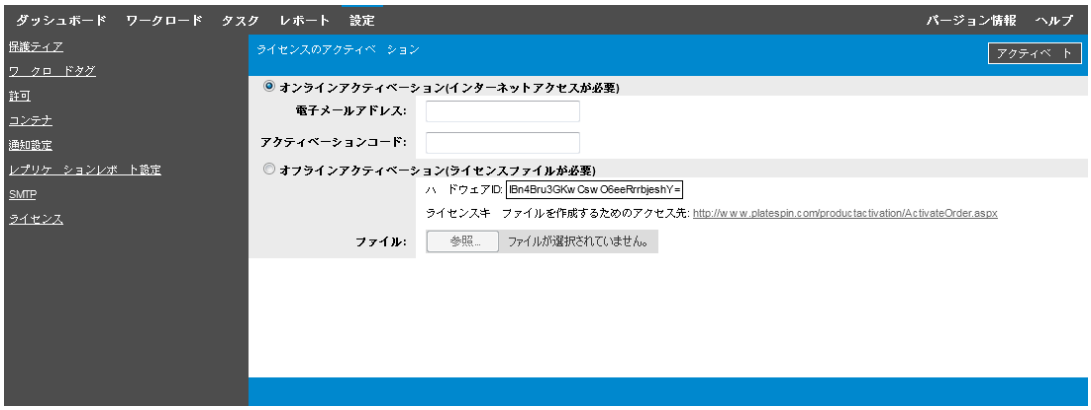
4.1.1 オンラインでのライセンスのアクティベーション

オンラインでアクティベーションするには、PlateSpin Protect がインターネットにアクセスできる必要があります。

注 : HTTP プロキシは、オンラインアクティベーション中に失敗する可能性があります。HTTP プロキシを使用する環境のユーザに対しては、オフラインアクティベーションをお勧めします。

オンラインライセンスアクティベーションを設定するには :

1 Web インタフェースで、**設定** > **ライセンス** > **ライセンスを追加**の順に選択します。



2 **オンラインアクティベーション**を選択します。

3 注文時に指定した電子メールアドレスと受け取ったアクティベーションコードを指定して、**有効にする**をクリックします。

システムはインターネット経由で必要なライセンスを取得し、製品を有効にします。

4.1.2 オフラインでのライセンスのアクティベーション

オフラインアクティベーションでは、インターネットにアクセスできるコンピュータを使用して、PlateSpin Protect のライセンスキーを取得します。

1 Web インタフェースで、**設定 > ライセンス** > **ライセンスを追加**の順に選択します。

2 **オフラインアクティベーション**を選択し、表示されたハードウェア ID をコピーします。

3 インターネットにアクセスできるコンピュータ上で Web ブラウザを使用して、PlateSpin Product Activation Web サイト (http://www.platespin.com/productactivation/ActivateOrder.aspx) に移動します。カスタマーセンターのユーザ名とパスワードを使用してログインします。

4 ハードウェア ID を使用して、ライセンスキーファイルを作成します。この処理には次の情報が必要です。

- 受け取ったアクティベーションコード
- 注文時に指定した電子メールアドレス
- ステップ 2 でコピーしたハードウェア ID

5 生成されたライセンスキーファイルを保存し、これをインターネット接続されていない製品ホストに転送し、このファイルを使用して製品を有効にします。

6 Web インタフェースの［License Activation (ライセンスアクティベーション)］ページで、ファイルへのパスを入力するか、ファイルの場所を参照して、**有効にする**をクリックします。

ライセンスキーファイルが保存され、このファイルに基づいて製品が有効化されます。

4.2 ワークロードライセンスの使用について

PlateSpin Protect 製品ライセンスでは、ワークロードライセンス契約を通して保護用に特定または無制限の数のワークロードを使用する権利が与えられます。保護用のワークロードを追加するたびに、システムではライセンスプールからワークロードライセンスを 1 つ消費します。ワークロードを削除した場合は、最大 5 回まで消費したライセンスを回復できます。

PlateSpin Protect Web インタフェースの［ダッシュボード］ページでは、［ライセンスサマリ］にインストール済みのライセンスと使用されているライセンスの現在の個数が表示されます。

［ライセンス］ページ (**設定** > **ライセンス**) に、使用するワークロードライセンスの現在の個数やこれらのライセンスで使用可能な再割り当ての残存数とともに、各インストール済みのライセンスが一覧表示されます。このページには、PlateSpin Server の残りの未使用ワークロードライセンスの合計数も表示されます。

図 4-1 *ライセンス数と再割り当ての残存数*

4.3 ライセンス情報の表示

製品ダッシュボードでは、インストール済みライセンスの合計数と、使用するライセンスの現在の個数が表示されるライセンスサマリが提供されます。

［ライセンス］ページでは、PlateSpin Server にインストールされたワークロードライセンスに関する情報が表示されます。ライセンスごとに、使用済みワークロードライセンスの現在の個数と、使用済みライセンスで使用可能な再割り当ての現在の残存数を表示できます。

ライセンス情報を表示するには :

1 Web インタフェースで、**設定 > ライセンス**の順に選択します。

2 ライセンス情報を表示します。
- アクティベーションコード
- 有効期限
- ワークロード
- 再割り当ての残存数

3 使用可能な未使用ライセンス数については、**残りのワークロード**を参照してください。

4.4 ライセンスの追加

新しいライセンスを追加するプロセスは、最初にライセンスをアクティブ化するのと同じプロセスを使用します。情報については、以下を参照してください。

- 51 ページのセクション 4.1.1「オンラインでのライセンスのアクティベーション」
- 52 ページのセクション 4.1.2「オフラインでのライセンスのアクティベーション」

4.5 ライセンスの削除

［ライセンス］ページで有効期限切れになったライセンスを削除できます。

1. Web インタフェースで、**設定 > ライセンス**の順に選択します。
2. ライセンス情報を表示します。
3. 期限切れになったライセンスの横の**削除**をクリックし、削除を確認します。

4.6 テクニカルサポート用のライセンスレポートの生成

ライセンスに問題がある場合は、テクニカルサポートによりライセンスレポートの生成を要求される場合があります。この診断レポートには、PlateSpin Server でアクティブ化したライセンスに関するエンコードされた製品情報が含まれます。

1. Web インタフェースで、**設定 > ライセンス**の順に選択します。
2. ライセンスのリストの下で、**ライセンスレポートの表示**をクリックします。

   ブラウザ設定に応じて、LicenseReport.txt ファイルが新しいブラウザタブまたはウィンドウで開きます。
3. LicenseReport.txt ファイルをローカルコンピュータ上に LicenseReport.psl として保存します。

5 ユーザ権限および認証の設定

このセクションには、次の情報が含まれています。

5.1 PlateSpin Protect の役割ベースのアクセスについて

PlateSpin Protect のユーザ権限および認証のメカニズムは、ユーザの役割に基づいており、ユーザが実行できるアプリケーションへのアクセスやその他の操作を制御します。このメカニズムは、Integrated Windows Authentication (IWA) とその Internet Information Services (IIS) との相互作用に基づきます。

役割ベースのアクセスメカニズムを使用すると、次のようないくつかの方法でユーザ権限の付与および認証を実行できるようになります。

- アプリケーションへのアクセスを特定のユーザに制限する
- 特定の操作のみを特定のユーザに許可する
- 割り当てられた役割によって定義された操作を実行するために、ユーザごとに特定のワークロードへのアクセスを許可する

すべての PlateSpin Protect インスタンスには、関連する機能の役割を定義する、次のような一連のオペレーティングシステムレベルのユーザグループが含まれています。

- **ワークロード保護の管理者：**アプリケーションのすべての機能に無制限にアクセスできます。ローカル管理者は、暗黙的にこのグループに含まれます。
- **ワークロード保護のパワーユーザ：**アプリケーションのほとんどの機能にアクセスできますが、ライセンスおよびセキュリティに関するシステム設定を変更する権限の制限など多少の制限があります。
- **ワークロード保護のオペレータ：**システムの機能のうち、日常的な操作を行うのに十分な一部の機能にのみアクセスできます。

ユーザが PlateSpin Protect に接続しようとすると、ブラウザを介して提供される資格情報が IIS によって検証されます。ユーザがワークロード保護の役割のメンバーに含まれない場合は、接続が拒否されます。

表 5-1 *ワークロード保護の役割および権限の詳細*

ワークロード保護の役割の詳細	管理者	パワーユーザ	オペレータ
ワークロードの追加	許可	許可	拒否

ワークロード保護の役割の詳細	管理者	パワーユーザ	オペレータ
ワークロードの削除	許可	許可	拒否
保護の設定	許可	許可	拒否
レプリケーションの準備	許可	許可	拒否
レプリケーション (完全) の実行	許可	許可	許可
増分の実行	許可	許可	許可
スケジュールの一時停止 / 再開	許可	許可	許可
テストフェールオーバー	許可	許可	許可
フェールオーバー	許可	許可	許可
フェールオーバーのキャンセル	許可	許可	許可
中止	許可	許可	許可
廃棄 (タスク)	許可	許可	許可
設定 (すべて)	許可	拒否	拒否
レポート / 診断の実行	許可	許可	許可
フェールバック	許可	拒否	拒否
再保護	許可	許可	拒否

さらに、PlateSpin Protect ソフトウェアでは、どのユーザが *PlateSpin Protect* ワークロードインベントリ内のどのワークロードにアクセスできるようにするかを定義するセキュリティグループに基づいたメカニズムも提供されます。

PlateSpin Protect への適切な役割ベースのアクセスを設定するには :

1. 表 5-1 で詳細が説明されている必要なユーザグループに、ユーザを追加します。Windows のマニュアルを参照してください。
2. それらのユーザを特定のワークロードに関連付けるアプリケーションレベルのセキュリティグループを作成します。詳細については、58 ページの 「PlateSpin Protect セキュリティグループおよびワークロードの権限の管理」を参照してください。

5.2 PlateSpin Protect のアクセスおよび権限の管理

次の各項で、詳細について説明します。

5.2.1 PlateSpin Protect ユーザの追加

この項の手順に従って、新しい PlateSpin Protect ユーザを追加します。

PlateSpin Server ホスト上の既存のユーザに特定の役割権限を付与したい場合は、57 ページの「PlateSpin Protect ユーザへのワークロード保護の役割の割り当て」を参照してください。

1. PlateSpin Server ホスト上で、システムのローカルユーザとグループのコンソールにアクセスします (**スタート** > **ファイル名を指定して実行**の順に選択して「lusrmgr.msc」と入力し、**<Enter>** を押します)。
2. **ユーザ**ノードを右クリックし、**New User (新規ユーザ)** を選択します。
3. 必要な詳細を指定して、**作成**をクリックします。

これで、新しく作成されたユーザにワークロード保護の役割を割り当てることができます。57 ページの 「PlateSpin Protect ユーザへのワークロード保護の役割の割り当て」を参照してください。

5.2.2 PlateSpin Protect ユーザへのワークロード保護の役割の割り当て

ユーザに役割を割り当てる前に、そのユーザに最適な権限のコレクションを決定します。55 ページの 表 5-1 「ワークロード保護の役割および権限の詳細」を参照してください。

1. PlateSpin Server ホスト上で、システムのローカルユーザとグループのコンソールにアクセスします (**スタート** > **ファイル名を指定して実行**の順に選択して「lusrmgr.msc」と入力し、**<Enter>** を押します)。
2. [**ユーザ**] ノードをクリックし、右側のペインの必要なユーザをダブルクリックします。
3. **メンバー :** タブで、**追加**をクリックします。
4. 必要なワークロード保護グループを見つけ、それをユーザに割り当てます。

変更が有効になるには数分かかる場合があります。変更を手動で適用するには、RestartPlateSpinServer.exe 実行可能ファイルを使用してサーバを再起動します。

PlateSpin Server を再起動するには :

1. PlateSpin Server の再起動を試みる前に、すべてのコントラクトを一時停止するか、進行中のレプリケーション、フェールオーバー、またはフェールバックがないことを確認します。すべてのワークロードがアイドル状態になるまで、次の手順に進まないでください。
2. PlateSpin Server ホストで、..\bin\RestartPlateSpinServer サブディレクトリに移動します。
3. RestartPlateSpinServer.exe 実行可能ファイルをダブルクリックします。

   確認を求めるコマンドプロンプトウィンドウが開きます。
4. 「Y」と入力し、<Enter> キーを押します。

ユーザを PlateSpin Protect セキュリティグループに追加し、特定のワークロードのコレクションを関連付けることができるようになりました。58 ページの 「PlateSpin Protect セキュリティグループおよびワークロードの権限の管理」を参照してください。

5.3 PlateSpin Protect セキュリティグループおよびワークロードの権限の管理

PlateSpin Protect は、特定のユーザが特定のワークロードに対して特定のワークロード保護タスクを実行できるようにする、きめ細かいアプリケーションレベルのアクセスメカニズムを備えています。これは、「セキュリティグループ」を設定することで実現します。

1 ユーザの権限が組織内における役割に最適になるようなワークロード保護の役割を PlateSpin Protect ユーザに割り当てます。57 ページの 「PlateSpin Protect ユーザへのワークロード保護の役割の割り当て」を参照してください。

2 PlateSpin Protect Web インタフェースを使用して管理者として PlateSpin Protect にアクセスし、**設定** > **許可**の順にクリックします。

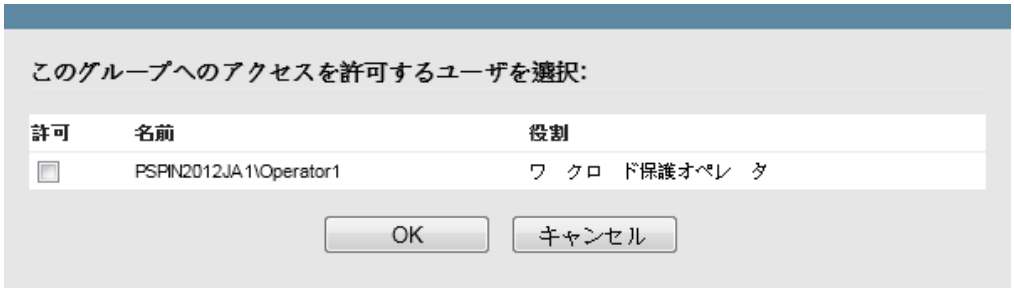
［セキュリティグループ］ページが開きます。

3 **セキュリティグループの作成**をクリックします。

4 **セキュリティグループ名**フィールドにセキュリティグループ名を入力します。

5 **ユーザの追加**をクリックし、このセキュリティグループに必要なユーザを選択します。

PlateSpin Server ホストに最近追加された PlateSpin Protect ユーザを追加する場合、ユーザインタフェースですぐに使用できない可能性があります。この場合、まず**ユーザアカウントの更新**をクリックします。



6 **ワークロードの追加**をクリックし、必要なワークロードを選択します。

このセキュリティグループに含まれるユーザのみが選択したワークロードにアクセスできます。

7 作成をクリックします。

ページが再ロードされ、セキュリティグループのリスト内に新しいグループが表示されます。

セキュリティグループを編集するには、セキュリティグループのリストの中からグループ名をクリックします。

5.4 VMware での Protect のマルチテナンシの設定

PlateSpin Protect には、VMware の非管理ユーザ (つまり、「有効化されたユーザ」) が VMware 環境で Protect ライフサイクル操作を実行するのを可能にする、固有のユーザ役割が含まれます (VMware データセンターでユーザ役割を作成するためのツールも含まれます)。この役割を使用することにより、ユーザはサービスプロバイダとして、VMware クラスタをセグメント化し、マルチテナンシを実装できます。マルチテナンシでは、データセンター内で複数の Protect コンテナをインスタンス化することで、Protect の複数の顧客 (つまり、「テナント」) のデータを格納します。これらのテナントは、データセンターを使用する他の顧客がアクセスできないように、自分のデータとその所在の痕跡を分離することを求めています。

このセクションでは、次の情報を紹介します。

- 59 ページのセクション 5.4.1「マルチテナンシに対する VMware の役割の定義」
- 62 ページのセクション 5.4.2「vCenter での役割の割り当て」

5.4.1 マルチテナンシに対する VMware の役割の定義

PlateSpin Protect では、VMware Infrastructure (つまり、VMware の「コンテナ」) でのタスクのアクセスと実行、およびその環境での Protect ワークフローと機能の実行を可能にする特定の権限が必要です。PlateSpinRole.xml ファイルでは、必要な最低限の権限を定義し、3 つの VMware カスタム役割にそれぞれ集められます。

- PlateSpin Virtual Machine Manager
- PlateSpin Infrastructure Manager
- PlateSpin User

このファイルは、PlateSpin Protect Server インストールに含まれています。付属している実行可能ファイル (PlateSpin.VMwareRoleTool.exe) は、定義ファイルにアクセスすることで、これらのカスタム PlateSpin 役割をターゲット vCenter 環境内に作成します。

デフォルトでは、役割定義ファイル (PlateSpinRole.xml) および役割定義ツール (PlateSpin.VMwareRoleTool.exe) は、VMwareRolesTool フォルダに配置されています。

<*install-directory*>\PlateSpin Protect Server\bin\VMwareRolesTool

このセクションでは、次の情報を紹介します。

- 60 ページの 「基本的なコマンドライン構文」
- 60 ページの 「その他のコマンドラインパラメータおよびフラグ」
- 60 ページの 「ツールの利用例」
- 61 ページの 「(オプション) vCenter での PlateSpin 役割の手動定義」
- 61 ページの 「vCenter を使用した PlateSpin カスタム役割の権限の表示」

基本的なコマンドライン構文

役割ツールのインストール先で、次の基本的な構文を使用して、このツールをコマンドラインで実行します。

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

ここで、PlateSpinRole.xml は役割定義ファイル名です。

注 : デフォルトでは、役割定義ファイルは、役割定義ツールと同じフォルダにあります。

その他のコマンドラインパラメータおよびフラグ

PlateSpin.VMwareRoleTool.exe を使用して vCenter の役割を作成または更新する際には、必要に応じて次のパラメータを適用します。

パラメータ

/ 作成	(必須) /role パラメータによって定義された役割を作成します
/get_all_prvileges	サーバによって定義された権限をすべて表示します
/get_compatible_roles	/role によって定義される役割と互換性のあるすべての役割を表示します
/check_role=[*role name*]	指定された役割について、/role によって定義された役割との互換性の有無を確認します

オプションのフラグ

/interactive	個々の役割の作成、役割の互換性のチェック、または互換性のあるすべての役割の一覧表示を選択できる対話型オプションを指定して、ツールを実行します。 インタラクティブなモードでツールを使用する方法については、「*VMware Role ツールを使用した役割許可の確認* (KB 7018547) (https://www.netiq.com/support/kb/doc.php?id=7018547)」を参照してください。
/password=[password]	VMware パスワードを示します (パスワードプロンプトを迂回します)
/verbose	詳細情報を表示する

ツールの利用例

「使用法」: PlateSpin.VMware.Role.Tool.exe /host=houston_sales /user=pedrom /role=PlateSpinRole.xml /create

結果としてのアクション:

1. 役割定義ツールは、管理者のユーザ名が pedrom の houston_sales vCenter サーバで実行されます。
2. /password パラメータを指定しないと、ツールによってユーザパスワードの入力を求めるプロンプトが表示されます。このパスワードを入力します。

3. ツールの実行可能ファイルと同じディレクトリにある (そのパスをさらに詳細に定義する必要はない) 役割定義ファイル (PlateSpinRole.xml) が、ツールによってアクセスされます。
4. 定義ファイルが見つかり次第、そのファイル内で定義されている役割を vCenter 環境に作成 (/create) するように指示されます。
5. ツールが定義ファイルにアクセスし、vCenter 内に新しい役割 (定義されている限定的なアクセス用の最低限の権限を含む) を作成します

   新しいカスタム役割は、vCenter で後でユーザに割り当てられます。

(オプション) vCenter での PlateSpin 役割の手動定義

PlateSpin カスタム役割を手動で作成して割り当てるには、vCenter クライアントを使用します。これには、PlateSpinRole.xml で定義され列挙されている、役割を作成することが関係しています。手動で作成する場合は、役割名に関する制限がありません。唯一の制限は、定義ファイル内の役割と同等の作成済みの役割名に、適切な最低限の権限を定義ファイルからすべて付与する必要があることです。

vCenter でカスタム役割を作成する方法の詳細については、VMware テクニカルリソースセンターの「*VMWare VirtualCenter の役割と権限の管理* (http://www.vmware.com/pdf/vi3_vc_roles.pdf)」を参照してください。

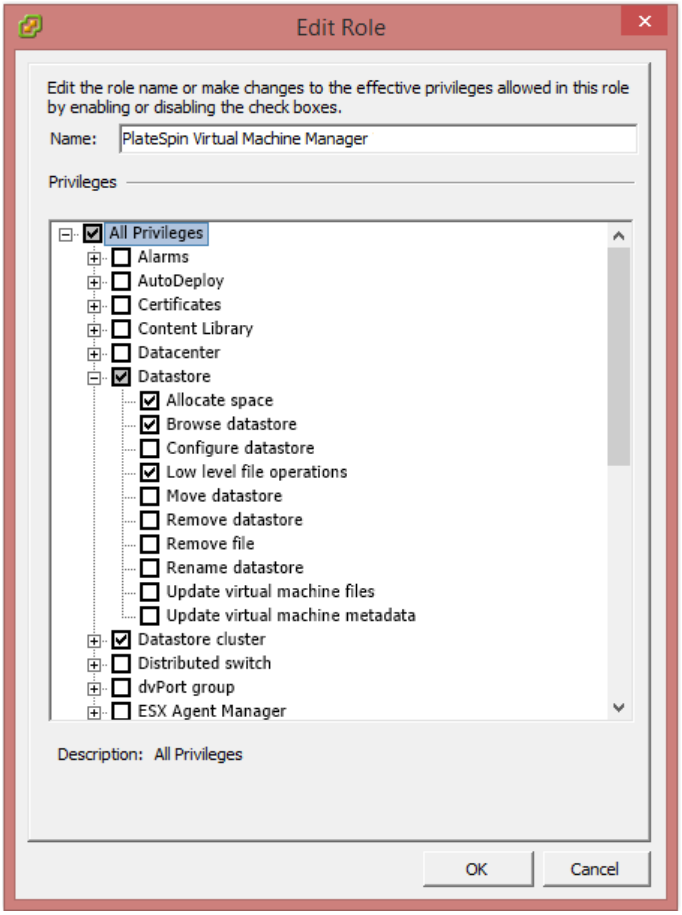
vCenter を使用した PlateSpin カスタム役割の権限の表示

vCenter クライアントを使用すると、PlateSpin カスタム役割に対して設定された最小権限を表示することができます。

1 vCenter で、カスタム役割を選択します。
- PlateSpin Virtual Machine Manager
- PlateSpin Infrastructure Manager
- PlateSpin User

2 **編集**をクリックして、［Edit Role (役割の編集)］ダイアログで権限の設定を表示します。

たとえば、以下の図には、PlateSpin Virtual Machine Manager 役割に対して設定された権限の一部が示されています。



5.4.2 vCenter での役割の割り当て

マルチテナンシ環境を設定する際には、顧客またはテナントごとに単一の Protect サーバをプロビジョニングする必要があります。この Protect サーバに、特別な Protect VMware 役割を持つ有効化されたユーザを割り当てます。この有効化されたユーザは、Protect コンテナを作成します。サービスプロバイダは、このユーザの資格情報を保持して、テナント顧客には公開しません。

次の表は、有効化されたユーザに対して定義する必要がある役割を一覧表示しています。この役割の用途に関する説明も示します。

役割割り当て用の vCenter コンテナ	役割割り当ての詳細	プロパゲート手順	説明
vCenter インベントリツリーのルート。	有効化されたユーザに、*PlateSpin Infrastructure Manager* (またはそれと同等の) 役割を割り当てます。	セキュリティ上の理由から、プロパゲートしないように権限を定義します。	この役割は、Protect ソフトウェアによって実行されているタスクを監視したり、失効した VMware セッションを終了するために必要です。

役割割り当て用の vCenter コンテナ	役割割り当ての詳細	プロパゲート手順	説明
有効化されたユーザがアクセスする必要のあるすべてのデータセンターオブジェクト。	有効化されたユーザに、*PlateSpin Infrastructure Manager* (またはそれと同等の) 役割を割り当てます。	セキュリティ上の理由から、プロパゲートしないように権限を定義します。	この役割は、ファイルのアップロード / ダウンロード用にデータセンターのデータストアへのアクセスを許可するために必要です。 プロパゲートしないように権限を定義します。
コンテナとして Protect に追加される各クラスタ、およびクラスタ内の各ホスト	有効化されたユーザに、*PlateSpin Infrastructure Manager* (またはそれと同等の) 役割を割り当てます。	プロパゲーションは、VMware 管理者の判断で行われます。	ホストに割り当てるには、クラスタオブジェクトから権限をプロパゲートするか、クラスタホストごとに追加権限を作成します。 クラスタオブジェクトに割り当てた役割をプロパゲートした場合は、クラスタに新しいホストを追加した後、これ以上の変更は必要ありません。ただし、この権限のプロパゲートは、セキュリティに影響を与えます。
有効化されたユーザがアクセスする必要のある各リソースプール。	有効化されたユーザに、*PlateSpin Virtual Machine Manager* (またはそれと同等の) 役割を割り当てます。	プロパゲーションは、VMware 管理者の判断で行われます。	ツリー内の任意の場所にある任意の数のリソースプールに対するアクセスを割り当てることができますが、有効化されたユーザには、この役割を割り当ててから、少なくとも 1 つのリソースプールに対するアクセスを付与する必要があります。
有効化されたユーザがアクセスする必要のある各 VM フォルダ。	有効化されたユーザに、*PlateSpin Virtual Machine Manager* (またはそれと同等の) 役割を割り当てます。	プロパゲーションは、VMware 管理者の判断で行われます。	ツリー内の任意の場所にある任意の数の VM フォルダに対するアクセスを割り当てることができますが、有効化されたユーザには、この役割を割り当ててから、少なくとも 1 つのフォルダに対するアクセスを付与する必要があります。

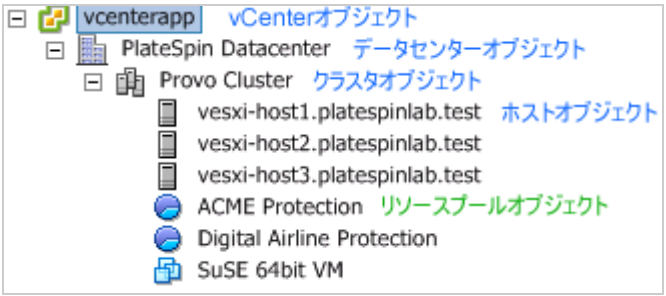
役割割り当て用の vCenter コンテナ	役割割り当ての詳細	プロパゲート手順	説明
有効化されたユーザがアクセスする必要のある各ネットワーク。 dvSwitch および dvPortgroup が使用可能な分散仮想ネットワーク。	有効化されたユーザに、*PlateSpin Virtual Machine Manager* (またはそれと同等の) 役割を割り当てます。	プロパゲーションは、VMware 管理者の判断で行われます。	ツリー内の任意の場所にある任意の数のネットワークに対するアクセスを割り当てることができますが、有効化されたユーザには、この役割を割り当ててから、少なくとも 1 つのフォルダに対するアクセスを付与する必要があります。 ◆ dvSwitch に適切な役割を割り当てるには、データセンターで役割をプロパゲートするか (役割を受け取るオブジェクトが増える)、dvSwitch をフォルダに配置してそのフォルダに役割を割り当てます。 ◆ 標準的なポートグループが、使用可能なネットワークとして Protect UI に一覧表示されるようにするには、クラスタ内の各ホストでポートグループの定義を作成します。
有効化されたユーザがアクセスする必要のある各データストアおよびデータストアクラスタ。	有効化されたユーザに、*PlateSpin Virtual Machine Manager* (またはそれと同等の) 役割を割り当てます。	プロパゲーションは、VMware 管理者の判断で行われます。	有効化されたユーザには、この役割を割り当ててから、少なくとも 1 つのデータストアまたはデータストアクラスタに対するアクセスを付与する必要があります。 データストアクラスタの場合、含まれているデータストアに対して権限をプロパゲートする必要があります。クラスタの個々のメンバーに対するアクセスが許可されないと、レプリケーションの準備と完全レプリケーションが両方とも失敗します。.

次の表は、顧客またはテナントユーザに割り当てることができる役割を示しています。

役割割り当て用の vCenter コンテナ	役割割り当ての詳細	プロパゲート手順	説明
顧客の VM の作成先であるリソースプールおよびフォルダ。	テナントユーザに、*PlateSpin User* (またはそれと同等の) 役割を割り当てます。	プロパゲーションは、VMware 管理者の判断で行われます。	このテナントは、PlateSpin Protect サーバ上の PlateSpin 管理者グループのメンバーであり、vCenter サーバ上にも存在します。 テナントに、VM によって使用されるリソース (つまり、ネットワーク、ISO イメージなど) を変更する許可を付与するには、このユーザにそれらのリソースに対する必要な権限を付与します。たとえば、顧客が自分の VM の接続先ネットワークを変更できるようにするには、このユーザに対してそのネットワークへの読み込み専用の役割を割り当てるか、(より優れた方法として) 顧客がアクセスできるすべてのネットワークへの読み込み専用の役割を割り当てます。

次の図は、vCenter コンソールの Virtual Infrastructure を示しています。青色でラベル付けされている vCenter、データセンター、クラスタ、およびホストオブジェクトには、Infrastructure Manager 役割が割り当てられます。緑色でラベル付けされているリソースプールオブジェクトには、Virtual Machine Manager 役割が割り当てられます。ツリーには、VM フォルダ、ネットワーク、およびデータストアが表示されていません。これらのオブジェクトには、*PlateSpin Virtual Machine Manager* 役割が割り当てられます。

***図 5-1** vCenter に割り当てられている役割*



VMware の役割を割り当てることによるセキュリティへの影響

PlateSpin ソフトウェアでは、保護ライフサイクルの操作を実行する場合にのみ、有効化されたユーザを使用します。サービスプロバイダであるユーザの観点からすると、有効化されたユーザの資格情報に対するアクセス権はエンドユーザに付与されず、VMware リソースの同じセットにもアクセスできないように思えます。複数の Protect サーバが同一の vCenter 環境を使用するように設定された環境では、Protect により、クロスクライアントアクセスの可能性が防止されます。主なセキュリティへの影響は次のとおりです。

- vCenter オブジェクトに *PlateSpin Infrastructure Manager* 役割を割り当てることにより、すべての有効化されたユーザが、他のユーザが実行したタスクを確認できるようになります (それらのタスクに影響を与えることはできない)。

- データストアのフォルダまたはサブフォルダに対して権限を設定することはできないため、データストアへの権限を持つすべての有効化されたユーザは、そのデータストアに格納されている他のすべての有効化されたユーザのディスクに対するアクセス権を持っています。
- クラスタオブジェクトに *PlateSpin Infrastructure Manager* 役割を割り当てると、すべての有効化されたユーザが、クラスタ全体の HA または DRS のオン / オフを切り替えられるようになります。
- ストレージクラスタオブジェクトに *PlateSpin User* 役割を割り当てると、すべての有効化されたユーザが、クラスタ全体の SDRS のオン / オフを切り替えられるようになります。
- DRS クラスタオブジェクトに *PlateSpin Infrastructure Manager 役割*を設定してからこの役割をプロパゲートすると、有効化されたユーザが、デフォルトのリソースプールまたはデフォルトの VM フォルダ (あるいはその両方) にあるすべての VM を確認できるようになります。また、プロパゲーションでは、アクセスすべきではないすべてのリソースプール /VM フォルダに対する「アクセス不可」役割が付与されるように、管理者は有効化されたユーザに明示的に設定する必要があります。
- vCenter オブジェクトに *PlateSpin Infrastructure Manager 役割*を設定すると、有効化されたユーザが、vCenter に接続している他のユーザのセッションを終了できるようになります。

注 : これらのシナリオでは、有効化された各ユーザが、実際には PlateSpin ソフトウェアの各インスタンスを表していることを明記してください。

---

6 PlateSpin Server アプリケーションの設定

この項では、PlateSpin Protect の環境設定要件とセットアップについて説明します。

6.1 国際バージョンの言語設定の設定

PlateSpin Protect は、英語のほかに、次の国際言語の各国語サポート (NLS) を提供します。

- 簡体字中国語
- 繁体字中国語
- フランス語
- ドイツ語
- 日本語

PlateSpin Server をこれらのサポートされる言語のいずれかで管理するには、PlateSpin Server ホストおよびご使用の Web ブラウザで、オペレーティングシステムの言語コードを設定します。

6.1.1 オペレーティングシステムの言語の設定

PlateSpin Server によって生成されるごく一部のシステムメッセージの言語は、ご使用の PlateSpin Server ホストで選択されているオペレーティングシステムのインタフェース言語に依存します。

オペレーティングシステムの言語を変更するには :

1. ご使用の PlateSpin Server ホストにアクセスします。
2. ［地域と言語のオプション］アプレットを開始し (**［スタート］>［ファイル名を指定して実行］** をクリックし、「intl.cpl」と入力して <Enter> キーを押す)、**Languages (言語)**(Windows Server 2003) または **Keybords and Languages (キーボードと言語)**(Windows Server 2008) タブで該当するほうをクリックします。

3 インストールされていない場合は、必要な言語パックをインストールします。OS のインストールメディアを使用する必要がある場合もあります。

4 必要な言語をオペレーティングシステムのインタフェース言語として選択します。メッセージが表示されたら、ログアウトするか、システムを再起動してください。

6.1.2 Web ブラウザでの言語の設定

PlateSpin Protect Web インタフェースをこれらの言語のいずれかで使用するには、該当する言語を Web ブラウザに追加して、優先順位の最上位にする必要があります。

1 Web ブラウザの言語設定にアクセスします。

- **Chrome:**
  1. Chrome メニューから**設定**をクリックし、スクロールして**詳細設定を表示**をクリックします。
  2. **Languages (言語)** までスクロールし、**Language and input settings (言語と入力の設定)** をクリックします。
- **Firefox:**
  1. **ツール**メニューから**オプション**を選択して、**Content (コンテンツ)** タブを選択します。
  2. **Languages (言語)** で **Choose (選択)** をクリックします。
- **Internet Explorer:**
  1. **ツール**メニューから**インターネットオプション**を選択して、**全般**タブを選択します。
  2. **Appearance (デザイン)** で、**Languages (言語)** をクリックします。

2 必要な言語を追加し、それをリストの最上部に移動させます。

3 設定を保存し、PlateSpin Server に接続してクライアントアプリケーションを開始します。詳細については、43 ページの 「Web インタフェースの起動」を参照してください。

注 : (簡体字中国語および繁体字中国語をご使用のユーザの場合) 特定のバージョンの中国語が追加されていないブラウザを使用して PlateSpin Server に接続しようとすると、Web サーバエラーが発生することあります。適切に動作するようにするには、ブラウザの環境設定を使用して特定の中国語 (たとえば、Chinese [zh-cn] または Chinese [zh-tw]) を追加します。文化的な区別のない Chinese [zh] という言語は使用しないでください。

6.2 イベントおよびレプリケーションレポートの電子メール通知サービスの設定

適切な受信者を指定した電子メールアドレスにイベントやレプリケーションレポートの通知を自動的に送信するように、PlateSpin Protect を設定することができます。この機能では、最初に使用する PlateSpin Protect の有効な SMTP サーバを指定することが必要です。

6.2.1 電子メール通知サービス用の SMTP の設定

イベントおよびレプリケーションレポートの電子メール通知を配信するために使用されるサーバ用の SMTP (シンプルメール転送プロトコル) 設定を実行するには、PlateSpin Protect Web インタフェースを使用します。

図 6-1 SMTP (シンプルメール転送プロトコル) の設定

SMTP 設定を行うには :

1. PlateSpin Protect Web インタフェースで、**設定 > SMTP** の順にクリックします。
2. 電子メールイベントおよび進捗通知を受信するための SMTP サーバ設定を指定します。
   - **アドレス**
   - **ポート** (デフォルトは 25 です)
   - **返信アドレス**
3. ユーザ名およびパスワードを入力して、そのパスワードを確認します。
4. [**保存**] をクリックします。

6.2.2 イベント通知の有効化

イベントは必ず、警告、エラー、および情報のログエントリタイプに従って、システムアプリケーションイベントログに追加されます。適切な受信者にイベント通知を自動的に送信するように通知を有効にすることもできます。

1. 使用する PlateSpin Protect の SMTP サーバをセットアップします。

   詳細については、69 ページの 「電子メール通知サービス用の SMTP の設定」を参照してください。
2. PlateSpin Protect Web インタフェースで、**設定 > 通知設定**の順にクリックします。
3. **通知を有効にする**オプションを選択します。
4. **受信者の編集**をクリックし、必要な電子メールアドレスをカンマで区切って入力し、**OK** をクリックします。

5 **保存**をクリックします。

一覧表示された電子メールアドレスを削除するには、そのアドレスの隣の**削除**をクリックします。

イベント通知が有効化されている場合、表 6-1 に示すイベントタイプで電子メール通知をトリガできます。

注 : イベントログエントリには一意の ID が付いていますが、これらの ID が今後のリリースでも同じままであることは保証されていません。

表 6-1 *ログエントリタイプ別のイベントタイプ*

イベントの種類	備考
ログエントリタイプ : 警告	
FullReplicationMissed	［増分レプリケーションが実行されませんでした］イベントに類似しています。
IncrementalReplicationMissed	次のいずれかの場合に生成されます。 ◆ スケジュールされた増分レプリケーションの期限中に、レプリケーションを手動で一時停止した。 ◆ 手動でトリガしたレプリケーションの実行中に、スケジュールされた増分レプリケーションの実行をシステムが試みた。 ◆ 十分な空きディスク容量がターゲットにないと、システムが判断した。
WorkloadOfflineDetected	以前にオンラインであったワークロードが現在はオフラインになっていることをシステムが検出した場合に生成されます。 保護コントラクトの状態が**一時停止中**ではないワークロードに適用されます。
ログエントリタイプ : エラー	
FailoverFailed	

イベントの種類	備考
FullReplicationFailed	
IncrementalReplicationFailed	
PrepareFailoverFailed	
ログエントリタイプ : 情報	
FailoverCompleted	
FullReplicationCompleted	
IncrementalReplicationCompleted	
PrepareFailoverCompleted	
TestFailoverCompleted	［フェールオーバーのテスト］操作を成功または失敗として手動でマークした場合に生成されます。
WorkloadOnlineDetected	以前にオフラインであったワークロードが現在はオンラインになっていることをシステムが検出した場合に生成されます。 保護コントラクトの状態が**一時停止中**ではないワークロードに適用されます。

6.2.3 レプリケーションレポートの有効化

適切な受信者にレポートを自動的に送信するようにレプリケーションレポートを有効にすることができます。

1. 使用する PlateSpin Protect の SMTP サーバをセットアップします。

   詳細については、69 ページの 「電子メール通知サービス用の SMTP の設定」を参照してください。
2. PlateSpin Protect Web インタフェースで、**設定 > レプリケーションレポートの設定**の順にクリックします。
3. **レプリケーションレポートの有効化**オプションを選択します。
4. **レポートの繰り返し**セクションで、**Edit (編集)** をクリックし、レポートに適した繰り返しパターンを指定します。**Close (閉じる)** をクリックすると、このセクションを縮小できます。
5. **受信者**セクションの**受信者の編集**をクリックし、適切な電子メールアドレスをカンマで区切って入力し、**OK** をクリックします。電子メールアドレスの横にある**削除**をクリックして、リストから受信者を削除できます。

6 (オプション) **アクセス URL の保護 :** の項で、PlateSpin Server のデフォルト以外の URL (例 : PlateSpin Server ホストに複数の NIC がある場合、または NAT サーバの背後にある場合) を指定します。URL はレポートのタイトル、および電子メールで送信されたレポート内のハイパーリンクを通じてサーバの関連コンテンツにアクセスする機能に影響を与えます。

7 **保存**をクリックします。

オンデマンドで生成したり表示できるレポートのその他のタイプについては、180 ページの 「ワークロードとワークロード保護のレポートの作成」を参照してください。

6.3 PlateSpin Server の代替 IP アドレスの設定

NAT 対応環境全体で PlateSpin Server が機能できるように、PlateSpin 環境設定の AlternateServerAddresses パラメータに代替 IP アドレスを追加できます。

PlateSpin Server に代替 IP アドレスを追加するには :

1 任意の Web ブラウザから、次を開きます。

https://*Your_PlateSpin_Server*/platespinconfiguration/

2 検索して AlternateServerAddresses パラメータを見つけ、PlateSpin Server の IP アドレスを追加します。

3 設定を保存し、ページを閉じます。

PlateSpin サービスの再起動または再開は、変更を適用するために必要とされません。

6.4 WAN 接続を使用したデータ転送の最適化

WAN 接続用のデータ転送のパフォーマンスを最適化し、チューニングを行うことができます。これを実行するには、システムが、PlateSpin Server ホストにある環境設定ツールで行われている設定から読み取る環境設定パラメータを変更します。詳細については、48 ページのセクション 3.5.1 「PlateSpin 設定」を参照してください。

- 73 ページのセクション 6.4.1 「パラメータの微調整」
- 75 ページのセクション 6.4.2 「FileTransferSendReceiveBufferSize の微調整」

6.4.1 パラメータの微調整

ファイル転送環境設定パラメータの設定を使用すると、WAN でのデータ転送を最適化できます。これらの設定はグローバルなので、ファイルベースのレプリケーションおよび VSS レプリケーションのすべてに影響します。

注 : これらの値が変更されると、Gigabit Ethernet など高速ネットワーク上でのレプリケーション時間が遅くなるなどマイナスの影響を受ける可能性があります。これらのパラメータを変更する前に、まず PlateSpin Support に相談することを検討してください。

ファイル転送速度を制御する環境設定パラメータは、PlateSpin の環境設定ページ (https://*Your_PlateSpin_Server*/platespinconfiguration/) にあります。表 6-2 に、これらの環境設定パラメータのデフォルト値と最大値を示します。高レイテンシの WAN 環境での動作を最適化するために、試行錯誤を繰り返してこれらの値を変更できます。

***表 6-2** ファイル転送環境設定パラメータのデフォルト値と最適値*

パラメータ	デフォルト値	Maximum Value
AlwaysUseNonVSSFileTransferForWindows2003	False	
FileTransferCompressionThreadsCount パケットレベルのデータ圧縮に使用されるスレッド数を制御します。圧縮が無効の場合、この設定は無視されます。圧縮は CPU に依存するため、この設定はパフォーマンスに影響を与える可能性があります。	2	該当なし
FileTransferBufferThresholdPercentage 新しいネットワークパケットを作成して送信するためにバッファする必要があるデータの最小量を決定します。	10	
FileTransferKeepAliveTimeOutMilliSec TCP がタイムアウトした場合にキープアライブメッセージを送信するまでに待機する時間を指定します。	120000	
FileTransferLongerThan24HoursSupport	True	
FileTransferLowMemoryThresholdInBytes サーバが自身をメモリ不足であると見なすタイミングを決定します。メモリが不足すると、ネットワーキング動作の増加を引き起こします。	536870912	
FileTransferMaxBufferSizeForLowMemoryInBytes メモリ不足状態で使用する内部バッファサイズを指定します。	5242880	
FileTransferMaxBufferSizeInBytes パケットデータを保持する内部バッファサイズを指定します。	31457280	
FileTransferMaxPacketSizeInButes 送信する最大パケットサイズを決定します。	1048576	

パラメータ	デフォルト値	Maximum Value
FileTransferMinCompressionLimit パケットレベルの圧縮のしきい値をバイトで指定します。	0 (無効)	最大 65536 (64KB)
FileTransferPort	3725	
FileTransferSendReceiveBufferSize レプリケーションネットワークの TCP 接続の送受信バッファの最大サイズ (バイト単位) を定義します。バッファサイズは TCP 受信ウィンドウ (RWIN) のサイズに影響します。RWIN は、TCP 確認応答なしで送信できるバイト数を設定するものです。この設定はファイルベース転送とブロックベース転送の両方に関係があります。ネットワークの帯域幅とレイテンシに応じてバッファサイズを微調整することで、スループットが向上し、CPU 処理が軽減されます。 値を 0 (オフ) に設定すると、デフォルトの TCP ウィンドウサイズ (8KB) が使用されます。カスタムのサイズにするには、サイズをバイトで指定します。 次の式を使用して、適切な値を決定します。 ((リンク速度 (Mbps) ÷ 8) x 遅延 (秒))) x 1000 x 1024 たとえば、10 ミリ秒の遅延のある 100Mbps のリンクでは、適切なバッファサイズは次のようになります。 (100/8)*0.01 * 1024 * 1000 = 128000 バイト 微調整については、75 ページのセクション 6.4.2「FileTransferSendReceiveBufferSize の微調整」を参照してください。	0 (8192 バイト)	最大 5242880 (5MB)
FileTransferSendReceiveBufferSizeLinux Linux でのファイル転送接続の TCP/IP Receive Window (RWIN) サイズの設定を指定します。このパラメータは、TCP 受信確認なしで送信されるバイト数を制御します。 値が 0 (オフ) に設定されている場合、Linux の TCP/IP ウィンドウサイズ値は FileTransferSendReceiveBufferSize の設定に基づいて自動的に計算されます。どちらのパラメータも 0 (オフ) に設定されている場合、デフォルト値は 248KB です。カスタムのサイズにするには、サイズをバイトで指定します。 **注 :** 旧リリースのバージョンでは、このパラメータを希望する値の半分に設定する必要がありましたが、現在はその必要はありません。	0 (253952 バイト)	
FileTransferShutDownTimeOutInMinutes	1090	
FileTransferTCPTimeOutMilliSec TCP Send Timeout と TCP Receive Timeout の両方の値を設定します。	30000	
PostFileTransferActionsRequiredTimeInMinutes	60	

6.4.2 FileTransferSendReceiveBufferSize の微調整

FileTransferSendReceiveBufferSize パラメータは、レプリケーションネットワークの TCP 接続の送受信バッファの最大サイズ (バイト単位) を定義します。バッファサイズは TCP 受信ウィンドウ (RWIN) のサイズに影響します。RWIN は、TCP 確認応答なしで送信できるバイト数を設定するものです。この設定はファイルベース転送とブロックベース転送の両方に関係があります。ネットワークの帯域幅とレイテンシに応じてバッファサイズを微調整することで、スループットが向上し、CPU 処理が軽減されます。

FileTransferSendReceiveBufferSize パラメータを微調整することで、ご使用のレプリケーション環境におけるソースサーバからターゲットサーバへのブロックまたはファイルの転送を最適化できます。PlateSpin の環境設定ページ (https://*Your_PlateSpin_Server*/platespinconfiguration/) でパラメータを設定します。

最適なバッファサイズを計算するには :

1 ソースサーバとターゲットサーバとの間のレイテンシ (遅延) を判断します。

ここでの目的は、パケットサイズをできる限り MTU に近付けた場合に、レイテンシがどの程度かを確認することです。

1a 管理者ユーザとしてソースサーバにログインします。

1b コマンドプロンプトで次のコマンドを入力します。

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

通常、ping の -l オプションは、*target-server-ip-address* に対して指定したペイロードのヘッダに 28 バイトを追加します。したがって、MTU から 28 を引いたバイト数のサイズの値を最初に試してみることをお勧めします。

1c 次のメッセージが表示されるまで、ペイロードを変更してステップ 1b のコマンドを再入力する操作を繰り返します。

パケットの断片化が必要です。

1d レイテンシを秒単位に変換してメモします。

たとえば、レイテンシが 35ms (ミリ秒) の場合、0.035 をレイテンシとしてメモします。

2 初期バッファサイズのバイト値を計算します。

バッファサイズ = (帯域幅 (Mbps) ÷ 8) x レイテンシ (秒) x 1000 x 1024

ネットワーク帯域幅にはバイナリ値を使用します。つまり、10Gbps の場合は 10240Mbps、1Gbps の場合は 1024Mbps を使用します。

たとえば、10Gbps ネットワークでレイテンシが 35ms の場合、次のような計算になります。

バッファサイズ = (10240 ÷ 8) x 0.035 x 1000 x 1024 = 45875200 バイト

3 (オプション) 最適なバッファサイズを計算します。端数は最大セグメントサイズ (MSS) の倍数になるように切り上げます。

3a MSS を判断します。

MSS = MTU サイズ (バイト) - (IP ヘッダサイズ + TCP ヘッダサイズ)

IP ヘッダサイズは 20 バイトです。TCP ヘッダサイズは、20 バイトにタイムスタンプなどのオプションのバイト数を足した値になります。

たとえば、MTU サイズが 1470 の場合、MSS は通常 1430 になります。

MSS = 1470 バイト – (20 バイト + 20 バイト) = 1430 バイト

3b 最適なバッファサイズを計算します。

最適なバッファサイズ = (roundup(バッファサイズ ÷ MSS)) x MSS

上の例で計算すると、次のようになります。

最適なバッファサイズ = (roundup(45875200 ÷ 1430)) x 1430 = 32081 x 1430 = 45875830

切り捨てではなく切り上げで計算してください。切り捨てで計算すると、バッファサイズ 45875200 より小さい MSS の倍数になります。

最適ではないバッファサイズ = 32080 x 1430 = 45874400

6.5 レプリケーション環境の最適化

制御の取得およびスナップショット環境設定パラメータの設定を使用して、レプリケーションパフォーマンスを最適化します。これらの設定はグローバルであり、すべてのレプリケーションに影響します。

表 6-3 に、PlateSpin 環境設定ページ (https://*Your_PlateSpin_Server*/platespinconfiguration/) の環境設定パラメータを示します。これらのパラメータは、レプリケーション環境をデフォルト値で制御します。

表 6-3 レプリケーション環境のデフォルト環境設定パラメータ

パラメータ	デフォルト値
TakeControlMemorySizeInMB レプリケーションを制御する際に設定するメモリサイズ (MB 単位)。	768
TakeControlCoresPerSocket ターゲットが LRD または bootofx.iso で起動する際に、制御するために使用するソケットあたりの仮想コア数。	1
TakeControlSockets ターゲットが LRD または bootofx.iso で起動する際に、制御するために使用する仮想ソケット数。	1
MaximumConcurrentReplications 同じ時間に実行できる同時レプリケーション数。	25
VssSnapshotCreationDelay レプリケーション中に VSS スナップショットを作成する際に再試行間で遅延する秒数。	120
VssSnapshotCreationRetryCount レプリケーション中にレプリケーションの試みが失敗するまでに VSS スナップショットを作成した最大回数。	5

6.6 設定サービスに対する再起動方法の設定

フェールオーバーアクション時に、環境設定サービスは、再起動の回数を最小化し、再起動のタイミングを制御することによって、再起動を最適化します。Windows ワークロードに対するフェールオーバーアクション時に環境設定サービスのハングが発生して、［Configuration Service Not Started (環境設定サービスが開始していません)］エラーが表示された場合、設定時の要求に従って再起動できるようにすることが必要になる可能性があります。再起動の最適化をスキップするように影響を受ける単一のワークロードを設定したり、すべての Windows ワークロードに対する再起動の最適化をスキップするように PlateSpin Server 上のグローバルな SkipRebootOptimization 設定を指定することができます。

単一の Windows ワークロードに対する再起動の最適化をスキップするには :

1. ソースワークロード上で管理者ユーザとしてログオンします。
2. PlateSpin.ConfigService.LegacyReboot と呼ばれるファイルをシステムドライブのルート (通常 C:) にファイル拡張子無しで追加します。コマンドプロンプトで、次のように入力します。

   ```
   echo $null >> %SYSTEMDRIVE%\PlateSpin.ConfigService.LegacyReboot
   ```

3. 失敗した［フェールオーバーのテスト］または［フェールオーバー］アクションを再度実行します。

すべての Windows ワークロードに対する再起動の最適化をスキップするには :

1. PlateSpin Server にログインして、次の PlateSpin Server 設定ページを開きます。

   https://*Your_PlateSpin_Server*/platespinconfiguration/

2. 設定パラメータ **ConfigurationServiceValues** を検索して、そのパラメータに対する**編集**をクリックします。
3. 設定 **SkipRebootOptimization** を false から true に変更します。
4. **保存**をクリックします。
5. 増分または完全レプリケーションを実行します。

   レプリケーションにより、変更された設定もターゲット VM にプロパゲートされます。

6. 影響を受ける Windows ワークロードに対して［フェールオーバーのテスト］または［フェールオーバー］を再度実行します。

6.7 VMware vCenter Site Recovery Manager 用サポートの設定

PlateSpin Protect を使用して、ワークロードをローカルで保護してから、いくつかの追加メソッドを使用して、これらのワークロードを SAN などのリモートの場所に複製する場合があります。たとえば、VMware vCenter Site Recovery Manager (SRM) を使用して、複製されたターゲット VM のデータストア全体をリモートサイトに複製する場合があります。この場合、ターゲット VM が複製され、リモートサイトでの稼働時に正しく動作するように、特定の設定手順が必要です。

PlateSpin Protect で複製され、VMware vCenter SRM で管理されるワークロードは、次の調整を行って SRM をサポートするように PlateSpin Protect を設定した場合、シームレスに動作できます。

- PlateSpin Protect ISO およびフロッピーが VMware .vmx ファイルおよび vmdk ファイルと同じデータストアに保持されるように設定します。
- VMwareツールがフェールオーバーターゲットにコピーされるようにPlateSpin Protect環境を準備します。これには、VMware ツールのインストールプロセスをより迅速にする環境設定を行うだけでなく、手動でファイルの作成とコピーを行うことが含まれています。
- 78 ページのセクション 6.7.1「同じデータストア上でのワークロードファイルのセットアップ」
- 78 ページのセクション 6.7.2「フェールオーバーターゲット用の VMware ツールのセットアップ」
- 80 ページのセクション 6.7.3「設定プロセスの促進」

6.7.1 同じデータストア上でのワークロードファイルのセットアップ

ワークロードファイルが同じデータストア上に保持されるようにするには :

1. Web ブラウザから、https://*Your_PlateSpin_Server*/platespinconfiguration/ を開いて、環境設定 Web ページを表示します。
2. 環境設定 Web ページで、CreatePSFilesInVmDatastore サーバパラメータを見つけて、その値を true に変更します。

   注 : レプリケーション契約の設定担当者は、すべてのターゲット VM ディスクファイルに対して同じデータストアが指定されていることを確認する必要があります。
3. 設定を保存し、ページを閉じます。

6.7.2 フェールオーバーターゲット用の VMware ツールのセットアップ

VM のブート時に設定サービスによってインストールされるように、VMware ツールセットアップパッケージを、レプリケーション中にフェールオーバーターゲットにコピーできます。これは、フェールオーバーターゲットが PlateSpin Server に接続できる場合は自動的に行われます。これが自動的に行われない場合には、レプリケーション前に環境を準備する必要があります。

環境を準備するには :

1 ESX ホストから VMware ツールパッケージを取得します。

1a windows.iso イメージをアクセス可能な VMware ホスト上の /usr/lib/vmware/isoimages ディレクトリからローカル一時フォルダにセキュアコピーします (scp)。

1b ISO を開いて、そのセットアップパッケージを抽出し、それをアクセス可能な場所に保存します。

- **VMware 5.*x* 以降 :** セットアップパッケージは、setup.exe および setup64.exe です。
- **VMware 4.*x* からアップグレードする前に次の許可を持っているとします。**セットアップパッケージは、VMware Tools.msi および VMware Tools64.msi です。

2 抽出したセットアップパッケージから OFX パッケージを作成します。

2a 希望のパッケージを圧縮し、セットアップインストーラファイルが .zip アーカイブのルートにあることを確認します。

2b .zip アーカイブの名前を 1.package に変更し、OFX パッケージとして使用できるようにします。

注 : 複数のセットアップパッケージに対して 1 つの OFX パッケージを作成する場合は、各セットアップパッケージに独自の .zip アーカイブが必要であることを覚えておいてください。

各パッケージは同じ名前 (1.package) である必要があるため、OFX パッケージとして複数の .zip アーカイブを保存する場合は、それぞれのアーカイブを独自のサブディレクトリに保存する必要があります。

---

3 適切な OFX パッケージ (1.package) を PlateSpin Server 上の %ProgramFiles(x86)%\PlateSpin\Packages\%*GUID*% ディレクトリにコピーします。

%*GUID*% の値は、表 6-4 に示すように、VMware Server とその VMware Tools アーキテクチャのバージョンによって異なります。適切な GUID の値を使用して、パッケージを正しいディレクトリにコピー U ます。

表 6-4 *VMware Tools ディレクトリ名の GUID*

VMware Server バージョン	VMware ツールアーキテクチャ	GUID
6.5	x86	D61C0FCA-058B-42C3-9F02-898F568A3071
6.5	x64	5D3947B7-BE73-4A00-A549-B15E84B98803
6.0	x86	311E672E-05BA-4CAF-A948-B26DF0C6C5A6
6.0	x64	D7F55AED-DA64-423F-BBBE-F1215529AD03
5.5	x86	660C345A-7A91-458b-BC47-6A3914723EF7
5.5	x64	8546D4EF-8CA5-4a51-A3A3-6240171BE278
5.1	x86	34DD2CBE-183E-492f-9B36-7A8326080755
5.1	x64	AD4FDE1D-DE86-4d05-B147-071F4E1D0326
5.0	x86	AD4FDE1D-DE86-4d05-B147-071F4E1D0326

VMware Server バージョン	VMware ツールアーキテクチャ	GUID
5.0	x64	F7C9BC91-7733-4790-B7AF-62E074B73882
4.1	x86	F2957064-65D7-4bda-A52B-3F5859624602
4.1	x64	80B1C53C-6B43-4843-9D63-E9911E9A15D5
4.0	x86	D052CBAC-0A98-4880-8BCC-FE0608F0930F
4.0	x64	80B50267-B30C-4001-ABDF-EA288D1FD09C

6.7.3 設定プロセスの促進

フェールオーバーターゲットのブート後は、設定サービスが起動して、VM が使用に備えて準備されますが、このサービスは PlateSpin Server からのデータを待機したり、CD ROM 上の VMware ツールを検索したりするため、数分間非アクティブな状態になります。

この待機時間を短縮するには :

1. 環境設定 Web ページで、ConfigurationServiceValues 環境設定を見つけて、WaitForFloppyTimeoutInSecs サブ設定の値をゼロ (0) に変更します。
2. 環境設定 Web ページで、ForceInstallVMToolsCustomPackage を見つけて、その値を true に変更します。

これらの設定を行った後は、次の設定プロセスが 15 分以内で実行されます。ターゲットマシンが再起動し (最大 2 回)、VMware ツールがインストールされ、SRM によるツールへのアクセスによって、リモートサイトでのネットワーク設定が行われます。

7 PlateSpin Web インタフェースの設定

PlateSpin Web インタフェースでは、ワークロード間の論理的な関連付けの追跡に使用するタグを設定できます。また、複数ページの画面更新率を制御できます。この項の情報を使用して、Web インタフェースを制御します。

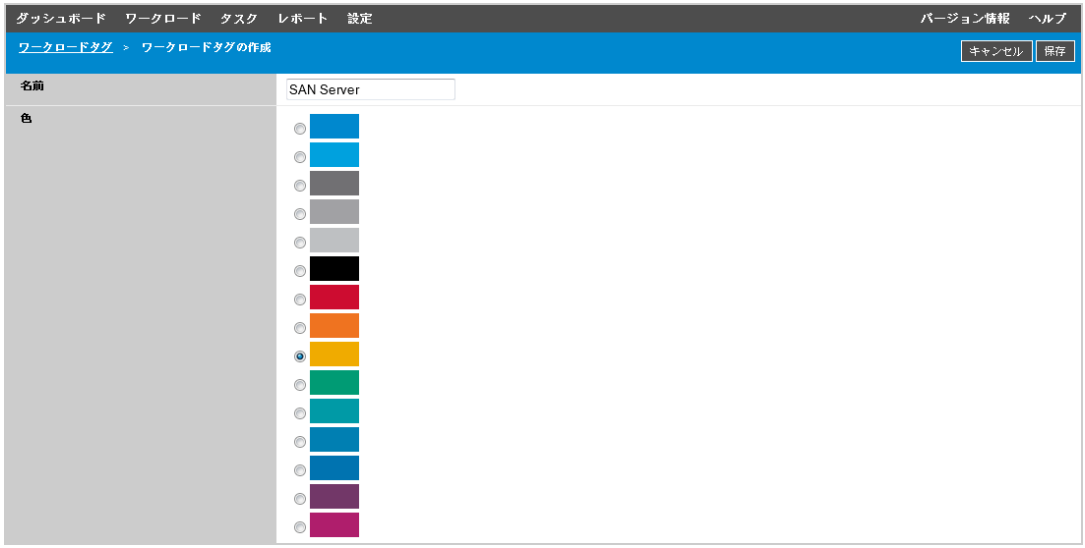
7.1 ワークロードタグの作成と管理

管理するワークロードが大量にある場合、リストをブラウズして類似するワークロードを選択し、同時に操作しようとすると、時間がかかる可能性があります。この場合、名前または機能でソートすると便利です。別の方法としては、タグを使用して、グループとして管理するワークロードにカスタム関連付けを設定します。[Tag (タグ)] 列でワークロードを容易にソートして、タグの付いた適切なワークロードを選択し、それらに対して実行可能な操作を同時に実行できます。

タグは、ユーザにとってわかりやすい、ワークロードの論理的または物理的な関連付けを表すことができます。各タグに固有の色と名前を関連付けます。固有タグは必要な数だけ作成できますが、固有色の選択肢は限られています。各ワークロードには 1 つのタグを関連付けることができます。ワークロードを新しいサーバにエクスポートする際、そのタグ設定は維持されます。

7.1.1 ワークロードタグの作成

1 PlateSpin Protect Web インタフェースで、**設定** >**Workload Tags (ワークロードタグ)**>**Create Workload Tag (ワークロードタグの作成)** の順にクリックします。



2 固有のタグ名 (最大 25 文字) を指定し、その説明に色を関連付けます。

3 **保存**をクリックすると、この新しいタグが［設定］ページの［Workload Tags (ワークロードタグ)］ビューの使用可能なワークロードタグのリストに追加されます。

7.1.2 ワークロードタグの編集

1 PlateSpin Protect Web インタフェースで、**設定** >**Workload Tags (ワークロードタグ)** の順にクリックします。

2 使用可能なタグを編集します。タグ名をクリックして、名前または関連付けられている色をクリックし、**保存**をクリックします。

7.1.3 ワークロードへのタグの追加

1 ワークロードリストでタグを付けるアクティブなワークロードを選択し、**設定**をクリックしてその環境設定ページを開きます。

2 **Tag (タグ)** セクションを展開して、**Tag (タグ)** ドロップダウンボックスを表示します。

3 ワークロードに関連付けるタグの名前を選択して、**保存**をクリックします。

7.1.4 ワークロードからのタグの削除

1 ワークロードリストでワークロードを選択し、**設定**をクリックしてその環境設定ページを開きます。

2 **Tag (タグ)** セクションを展開して、**Tag (タグ)** ドロップダウンボックスを表示します。

3 使用可能なタグ名のリストで「空」の行を選択し、**保存**をクリックします。

7.1.5 ワークロードタグの削除

不要になったタグは削除することができます。いずれかのワークロードに関連付けられているタグは削除できません。

1. PlateSpin Protect Web インタフェースで、**設定** >**Workload Tags (ワークロードタグ)** の順にクリックします。
2. ワークロードから目的のタグの関連付けを解除します。
3. タグの横にある **Delete (削除)** をクリックし、**OK** をクリックして確認します。

7.2 Web インタフェースの更新頻度の設定

Web インタフェースのいくつかのページについては、更新頻度を設定できます (表 7-1 を参照)。ご使用の PlateSpin 環境のニーズに合わせて、更新間隔を変更できます。

表 7-1 *Web インタフェースのデフォルト更新間隔*

Web インタフェースのパラメータ	デフォルトの更新間隔 (秒単位)
DashboardUpdateIntervalSeconds	60
WorkloadsUpdateIntervalSeconds	60
WorkloadTargetsUpdateIntervalSeconds	30
WorkloadDetailsUpdateIntervalSeconds	15
TasksUpdateIntervalSeconds	15

1. 次のファイルをテキストエディタで開きます。

   Program Files\PlateSpin ProtectServer\Platespin Forge\web\web.config

2. 次のうち任意の間隔設定を、ご使用の PlateSpin 環境に適した値に変更します。

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

3. ファイルを保存します。

   新しい設定は、次回の Web インタフェースセッションで適用されます。PlateSpin Server のサービスやサーバを再起動する必要はありません。

7.3 Web インタフェース用の UI のカスタマイズ

PlateSpin Web インタフェースの外観を、企業イメージのルックアンドフィールに一致するように変更できます。変更できるのは、色、ロゴ、製品名です。詳細については、89 ページの付録 A「PlateSpin Protect Web インタフェースのブランディングの変更」を参照してください。

8 管理コンソールでの複数の PlateSpin Server の管理

PlateSpin Protect には、Web ベースのクライアントアプリケーションである PlateSpin Protect 管理コンソールが含まれます。これにより、PlateSpin Protect および PlateSpin Forge の複数インスタンスに一元的にアクセスできます。

PlateSpin Protect と PlateSpin Forge の複数インスタンスが存在するデータセンターでは、インスタンスの 1 つをマネージャとして指定し、そこから管理コンソールを実行できます。マネージャの下に他のインスタンスを追加することで、制御と対話を一元的に行うことができます。

8.1 PlateSpin Protect 管理コンソールの使用

管理コンソールの使用を開始するには :

1. ご使用の PlateSpin Protect インスタンスにアクセスできるマシン上で Web ブラウザを開き、次の URL に移動します。

   https://*Your_PlateSpin_Server*/console

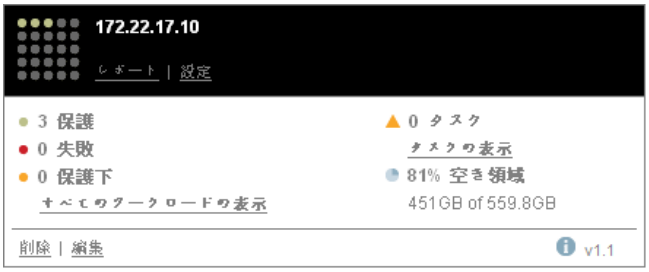
   Your_PlateSpin_Server の部分は、マネージャとして指定されている PlateSpin Server ホストの IP アドレスまたは DNS ホスト名で置き換えます。
2. ユーザ名とパスワードを使用してログインします。
3. (最初のログイン) ようこそページで、**PlateSpin Server の追加**をクリックし、87 ページのセクション 8.3「PlateSpin Protect および PlateSpin Forge のインスタンスの管理コンソールへの追加」で説明されるように PlateSpin Server インスタンスを設定します。

4 (後続のログオン) ダッシュボードを表示します。

8.2 PlateSpin Protect 管理コンソールについて

PlateSpin Protect および PlateSpin Forge の個別のインスタンスは、管理コンソールに追加されるとカードで表されます。

図 8-1 *PlateSpin Protect インスタンスカード*



1 枚のカードには、PlateSpin Protect および PlateSpin Forge の特定のインスタンスに関する次のような基本情報が表示されます。

- IP アドレス / ホスト名
- 場所
- バージョン番号
- ワークロードの数
- ワークロードの状態
- ストレージの容量
- 残りの空き領域

各カードのハイパーリンクを使用すると、特定のインスタンスのワークロード、レポート、設定、およびタスクのページに移動できます。カードの設定を編集したり、表示からカードを削除したりできるハイパーリンクもあります。

8.3 PlateSpin Protect および PlateSpin Forge のインスタンスの管理コンソールへの追加

PlateSpin Protect または PlateSpin Forge のインスタンスを管理コンソールに追加すると、管理コンソールのダッシュボードに新しいカードが追加されます。

注 : PlateSpin Protect または PlateSpin Forge のインスタンスで実行中の管理コンソールにログインしても、そのインスタンスはコンソールに自動的には追加されません。手動で追加する必要があります。

PlateSpin Protect または PlateSpin Forge のインスタンスをコンソールに追加するには :

1 コンソールのメインダッシュボードで、**PlateSpin Server の追加**をクリックします。

2 PlateSpin Server ホストまたは Forge VM の URL を指定します。HTTPS 通信を使用します (SSL が有効の場合)。

3 (オプション) **管理コンソールの資格情報の使用**チェックボックスをオンにし、コンソールが使用するのと同じ資格情報を使用します。これをオンにすると、コンソールによって自動的に **Domain\Username** フィールドに入力されます。

4 **Domain\Username** フィールドに、追加する PlateSpin Protect または PlateSpin Forge のインスタンスに対して有効なドメイン名とユーザ名を入力します。**パスワード**フィールドに、該当するパスワードを入力します。

5 (オプション) PlateSpin Server に対して、わかりやすい固有の **Display Name (表示名)** (最大 15 文字)、その **Location (場所)** (最大 20 文字)、および必要な **Notes (メモ)** (最大 400 文字) を指定します。

6 **追加**をクリックします。

新しいカードがダッシュボードに追加されます。

8.4 管理コンソールでのカードの編集

管理コンソールでカードの詳細を変更するには :

1 管理コンソールで、変更する PlateSpin Protect サーバまたは PlateSpin Forge サーバのカードインスタンスを見つけます。

2 カードの**編集**ハイパーリンクをクリックします。

コンソールの**追加 / 編集**ページが表示されます。

3 任意の変更を行い、**追加 / 保存**をクリックします。

更新されたコンソールダッシュボードが表示されます。

8.5 管理コンソールでのカードの削除

管理コンソールからカードを削除するには :

1 管理コンソールで、削除する PlateSpin Protect サーバまたは PlateSpin Forge サーバのカードインスタンスを見つけます。

2 カードの**削除**ハイパーリンクをクリックします。

確認のプロンプトが表示されます。

3 **OK** をクリックして、確認します。

カードインスタンスがダッシュボードから削除されます。

A PlateSpin Protect Web インタフェースのブランディングの変更

Web インタフェースの色、ロゴ、製品名などの外観を、企業イメージに一致するように変更できます。製品インタフェースの **About (バージョン情報)** タブと **Help (ヘルプ)** タブへのリンクを削除することもできます。

この項では、製品のブランディングの変更に役立つ情報について説明します。

- 89 ページのセクション A.1「環境設定パラメータによる Web インタフェースの再ブランディング」
- 92 ページのセクション A.2「Windows レジストリでの製品名ブランディングの変更」

A.1 環境設定パラメータによる Web インタフェースの再ブランディング

Web インタフェースの外観を、組織の専用 Web サイトに一致するように変更できます。Web インタフェースのブランディングをカスタマイズするには、PlateSpin Server ホストの環境設定パラメータを変更します。

Web インタフェースのブランディングパラメータを変更するには :

1. Web ブラウザから、https://*Your_PlateSpin_Server*/platespinconfiguration/ を開き、管理者としてログインします。
2. 必要なサーバパラメータを見つけて、**編集**をクリックし、その値を変更します。

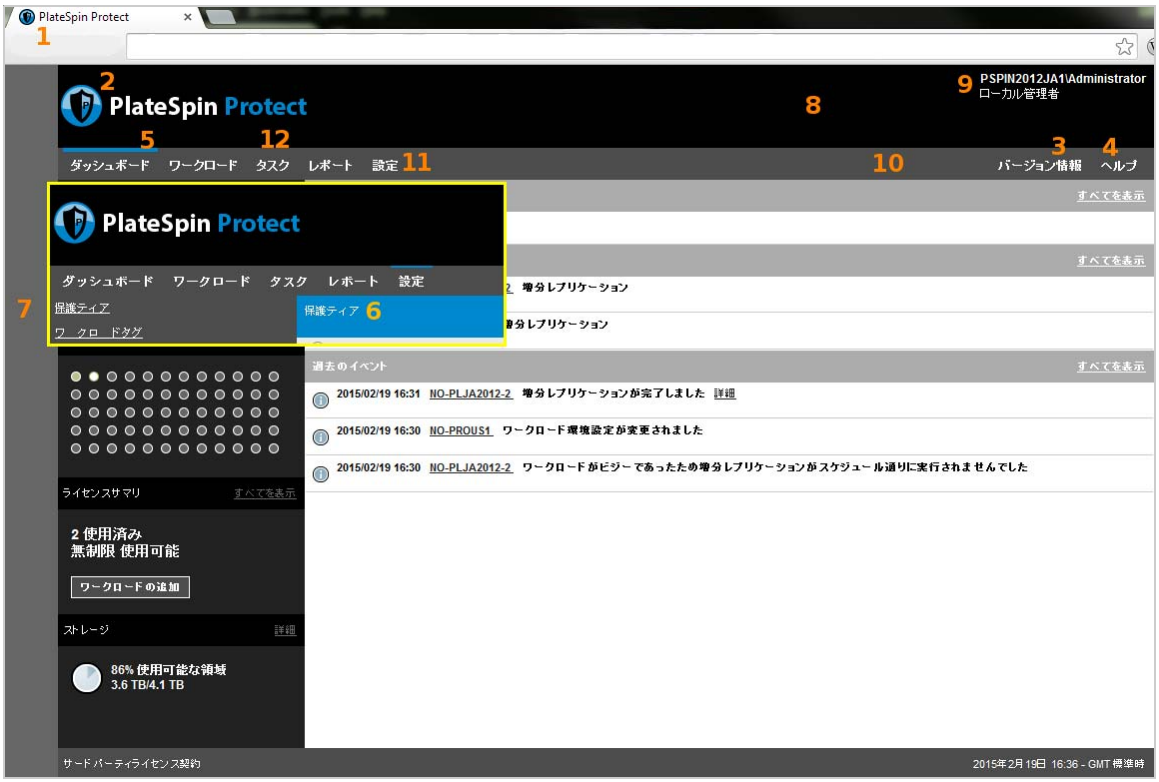
   UI で設定可能な要素を表示する方法の詳細については、図 A-1 を参照してください。設定可能な要素ごとに設定名、説明、およびデフォルト値を表示する方法については、表 A-1 を参照してください。
3. 設定を保存し、ページを閉じます。

   環境設定ツールで変更を行った後にサービスを再起動または再開する必要はありませんが、インタフェースに変更が反映されるまで、最大で 30 秒かかる可能性があります。

A.1.1 Web インタフェースの設定可能な要素

Web インタフェースのルックアンドフィールは全体を通して整合性があります。図 A-1 の PlateSpin Protect ダッシュボードの図に、変更可能要素を番号付きのコールアウトを使用して示します。埋め込みは、［設定］パネルの設定可能な要素を示しています。

図 A-1 *Protect Web インタフェースとラベル付きの設定可能要素*



A.1.2 Web インタフェースの設定可能パラメータ

次の表に、スクリーンショットで示されているインタフェース要素 (または「ID」)、設定名、説明、およびデフォルト値をリストします。PlateSpin Server の［Configuration Settings (環境設定)］ページを使用して、新しい「ルックアンドフィール」に従ってこれらの値を変更します (つまり、設定ページで設定値の**編集**をクリックします)。

表 A-1 Web インタフェースの環境設定パラメータとデフォルト値

ID	設定名と説明	デフォルト値
1	WebUIFaviconUrl 有効な .ico グラフィックファイルの場所。次のいずれかを指定します。 ◆ 別のマシン上の該当する .ico ファイルを参照する有効な URL。 例 : https://myserver.example.com/dir1/dir2/icons/mycompany_favicon.ico ◆ 該当する .ico ファイルをアップロードしたローカル Web サーバのルートからの相対パス。 たとえば、カスタムアイコングラフィックの保存場所として、Web サーバのルートに mycompany\images\icons というパスを作成した場合、次のように指定します。 ~/mycompany/images/icons/mycompany_favicon.ico この例では、ファイルが置かれる実際のファイルシステムパスは、C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\mycompany\images\icons\mycompany_favicon.ico になります。	~/doc/en/favicon.ico [1]
2	WebUILogoUrl 製品ロゴのグラフィックファイルの場所。次のいずれかを指定します。 ◆ 別のマシン上の該当するグラフィックファイルを参照する有効な URL。 例 : https://myserver.example.com/dir1/dir2/logos/mycompany_logo.png ◆ 該当するグラフィックスファイルをアップロードしたローカル Web サーバのルートからの相対パス。 たとえば、カスタムロゴ画像の保存場所として、Web サーバのルートに mycompany\images\logos というパスを作成した場合、次のように指定します。 ~/mycompany/images/logos/mycompany_logo.png この例では、ファイルが置かれる実際のファイルシステムパスは、C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\mycompany\images\logos\mycompany_logo.png になります。	~/Resources/protectLogo.png [2]
3	WebUIShowAboutTab **About (バージョン情報)** タブの表示 (**True**)/ 非表示 (**False**) をトグルします。	True

ID	設定名と説明	デフォルト値
4	WebUIShowHelpTab **Help (ヘルプ)** タブの表示 (**True**)/ 非表示 (**False**) をトグルします。	True
5	WebUISiteAccentColor 差し色 (RGB 16 進数値)	#0088CE
6	WebUISiteAccentFontColor Web UI で差し色で表示するフォント色 (RGB 16 進数値)	#FFFFFF
7	WebUISiteBackgroundColor サイト背景色 (RGB 16 進数値)	#666666
8	WebUISiteHeaderBackgroundColor サイトヘッダ背景色 (RGB 16 進数値)	#000000
9	WebUISiteHeaderFontColor Web UI のサイトヘッダのフォント色 (RGB 16 進数値)	#FFFFFF
10	WebUISiteNavigationBackgroundColor Web UI のサイトナビゲーション背景色 (RGB 16 進数値)	#4D4D4D
11	WebUISiteNavigationFontColor Web UI のサイトナビゲーションリンクのフォント色 (RGB 16 進数値)	#FFFFFF
12	WebUISiteNavigationLinkHoverBackgroundColor カーソルがポイントした状態のサイトナビゲーションリンクの背景色 (RGB 16 進数値)	#808080

[1] 実際のファイルパスは C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\doc\en\favicon.ico です。

[2] 実際のファイルパスは C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\Resources\protectLogo.png です。

A.2 Windows レジストリでの製品名ブランディングの変更

製品インタフェースの最上部にあるマストヘッドは、企業ロゴと製品自体の名前の両方を表示するスペースになります。環境設定パラメータを使用して、ロゴを変更できます。通常は、製品名も変更対象に含まれます。ブラウザタブの製品名を変更または削除するには、Windows レジストリを変更する必要があります。

製品名を変更するには :

1. PlateSpin Server で regedit を実行します。

2 Windows レジストリエディタで、次のレジストリキーに移動します。

HKEY_LOCAL_MACHINE\SOFTWARE\PlateSpin\ProtectServer\ProductName

---

注 : 場合によっては、このレジストリキーは次の場所にあります。

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PlateSpin\Protect

---

3 ProductName キーをダブルクリックし、必要に応じてキーの**値データ**を変更して **OK** をクリックします。

4 IIS サーバを再起動して、インタフェースの変更を反映します。

保護ターゲットとソースの準備

保護コントラクトを設定する前に、予定したターゲットコンテナとソースワークロードを識別する必要があります。インベントリプロセスからターゲットおよびワークロードに関する詳細を得ます。

9 コンテナ (保護ターゲット) の準備

このコンテナは保護されたワークロードで定期的に更新されるレプリカのホストとして機能する保護インフラストラクチャです。ターゲットコンテナを追加すると、PlateSpin Protect データベースにコンテナとそのリソースの詳細なインベントリ情報が入力されます。インベントリでは、コンテナの使用を決定し、ターゲットコンテナの 1 つ以上のワークロード保護コントラクトを正しく設定するために必要なデータが提供されます。

9.1 コンテナ (保護ターゲット) について

PlateSpin Web インタフェースは、サポートされているターゲットコンテナプラットフォームの自動化されたインベントリを提供します。

9.1.1 サポートされるコンテナ

コンテナを PlateSpin Server に追加する前に、VM コンテナバージョンがサポートされていることを確認します。詳細については、18 ページの 「サポートされる VM コンテナ」を参照してください。

9.1.2 コンテナのネットワークアクセス要件

インベントリ操作を開始する前に、PlateSpin Server がソースワークロードおよびターゲットと通信できることを確認します。詳細については、32 ページのセクション 1.5.2「コンテナのネットワーク要件」を参照してください。

9.1.3 コンテナのパラメータガイドライン

表 9-1 では、Web インタフェースを使用したターゲットホスト用インベントリパラメータのマシンタイプの選択、資格情報形式、構文に関するガイドラインを示します。

表 9-1 ターゲットコンテナの Web インタフェース検出パラメータのガイドライン

検出対象	ターゲットタイプ	資格情報
VMware vCenter クラスタ	VMware DRS クラスタ	VMware vCenter Web サービス資格情報 (ユーザ名およびパスワード)
VMware ESXi Server	VMware ESX サーバ	管理者の役割を持つ ESX アカウント または Windows ドメイン資格情報 (バージョン 4 と 4.1 のみ)

9.2 コンテナ (保護ターゲット) の追加

このコンテナは保護されたワークロードで定期的に更新されるレプリカのホストとして機能する保護インフラストラクチャです。インフラストラクチャは、VMware ESX Server または VMware DRS クラスタのどちらでも可能です。PlateSpin Protect では、保護およびフェールバックの両方でコンテナを使用できます。

ワークロードを保護するには、PlateSpin Server によってワークロードとコンテナのインベントリを実行する (または PlateSpin Server にワークロードとコンテナを*追加する*) 必要があります。

コンテナを追加するには :

1 Web インタフェースで、**設定**］>［**コンテナ**］>［**コンテナの追加**の順に選択します。

2 コンテナのタイプを指定します。
- **VMware ESX サーバ**
- **VMware DRS クラスタ**

3 前の手順で選択したターゲットのタイプに応じて、適切なアクセス情報を指定します。

表 9-2 VMware DRS クラスタターゲットのオプション

オプション	説明
vCenter ホスト名または IP	vCenter サーバのホスト名または IP アドレスを指定します。

オプション	説明
vCenter ホスト名または IP	vCenter サーバのホスト名または IP アドレスを指定します。

- **VMware DRS クラスタ**：詳細については、表 9-3 を参照してください。
- **VMware ESX サーバ**：詳細については、表 9-4 を参照してください。

表 9-3 VMware DRS クラスタターゲットのオプション

オプション	説明
vCenter ホスト名または IP	vCenter サーバのホスト名または IP アドレスを指定します。

オプション	説明
vCenter ホスト名または IP	vCenter サーバのホスト名または IP アドレスを指定します。

表 9-4 VMware ESX サーバターゲットのオプション

オプション	説明
ホスト名または IP	VMware ESX サーバのホスト名または IP アドレスを指定します。
ユーザ名とパスワード	ターゲットコンテナにアクセスするための管理者レベルの資格情報を指定します。 詳細については、167 ページの 「ワークロードおよびコンテナの資格情報向けのガイドライン」を参照してください。

4 テスト資格情報をクリックして、指定した資格情報の値を検証します。

5 VM コンテナの目的を選択します。

- 保護
- フェールバック
- Protection and Failback (保護とフェールバック)

保護とフェールバックの両方を選択すると、保護操作とフェールバック操作の両方でターゲットとしてコンテナが選択可能になります。

6 追加をクリックしてコンテナを追加し、その詳細を検出して、それを［コンテナ］ページに表示します。

PlateSpin Protect によって［コンテナ］ページがリロードされ、追加されるコンテナのプロセスインジケータが表示されます。終了したら、プロセスインジケータのアイコンがリフレッシュアイコンに変わります。

9.3 コンテナ詳細のリフレッシュ

保護コントラクトを設定または実施する前に、ターゲットコンテナに関する詳細を定期的にリフレッシュする必要があります。PlateSpin Web インタフェースでは、仮想ターゲットコンテナの検出されたリソースをリフレッシュすることができます。

ターゲットをリフレッシュすると、それに関連付けられているリソースも自動的に再検出され更新されます。一度に 1 つのコンテナをリフレッシュできます。

ターゲットコンテナの詳細をリフレッシュするには :

1. PlateSpin Web インタフェースで、**設定 > コンテナ**の順に選択します。
2. リフレッシュしたいコンテナの隣にある**リフレッシュ**アイコン をクリックします。

   これは、コンテナの再インベントリを実行します。
3. インベントリの変更に関する情報については、コンテナ詳細ページのパネルを展開します。

9.4 コンテナ (保護ターゲット) の削除

ターゲットコンテナのすべての保護コントラクトを削除する場合は、ターゲットコンテナを削除 (未検出に) することができます。使用されていないコンテナも削除できます。

重要 : 設定されたワークロード保護コントラクト用に使用中のターゲットコンテナを削除する前に、影響を受けるすべてのコントラクトが異なるターゲットコンテナでも削除または再設定されていることを確認する必要があります。

Web インタフェースからターゲットを削除するには :

1. PlateSpin Web インタフェースで、**設定 > コンテナ**の順に選択します。
2. ［コンテナ］ページで、Protect から削除するコンテナの横にある**削除**をクリックします。

10 ワークロード (保護ソース) の準備

保護コントラクトについては、ソースワークロードおよびターゲットコンテナが必要です。PlateSpin Protect Server にワークロードを追加すると、PlateSpin データベースにマシンに関する詳細なインベントリ情報が入力されます。この情報は、マシンの用途を判別し、保護コントラクトを適切に設定するために必要なデータを提供します。

10.1 ワークロード (保護ソース) について

PlateSpin Web インタフェースは、サポートされているソースワークロード設定の自動化されたインベントリを提供します。

10.1.1 サポートされるワークロード

ワークロードを PlateSpin Server に追加する前に、ワークロードオペレーティングシステムのバージョンとハードウェアがサポートされていることを確認します。13 ページのセクション 1.1「サポートされる構成」で以下の項を確認してください。

10.1.2 ソースワークロードのネットワークアクセス要件

Windows ワークロードおよび Linux ワークロードのインベントリのネットワークアクセス要件については、33 ページのセクション 1.5.3「ワークロードのネットワーク要件」を参照してください。

10.1.3 ソースワークロードのパラメータガイドライン

表 10-1 では、ワークロードのインベントリパラメータのマシンタイプの選択、資格情報形式、および構文に関するガイドラインを示します。

表 10-1 *ワークロードの検出パラメータのガイドライン*

検出対象	コンピュータのタイプ	資格情報	備考
Windows のすべてのワークロード	Windows	ローカルまたはドメインの管理者資格情報	ユーザ名には次のフォーマットを使用します。 ◆ ドメインメンバーのマシン用 : *authority\principal* ◆ ワークグループメンバーのマシン用 : *hostname*
Linux のすべてのワークロード	Linux	ルートレベルのユーザ名とパスワード	ルート以外のアカウントは、sudo を使用できるよう適切に設定する必要があります。ナレッジベースの記事 7920711 (https://www.netiq.com/support/kb/doc.php?id=7920711) を参照してください。

10.2 ワークロード (保護ソース) の追加

データストアにおける保護の基本的なオブジェクトであるワークロードは、基礎となる物理インフラまたは仮想インフラから切り離された、オペレーティングシステムとそのミドルウェアおよびデータです。

ワークロードを保護するには、PlateSpin Server によってワークロードとコンテナのインベントリを実行する (または PlateSpin Server にワークロードとコンテナを*追加する*) 必要があります。

ワークロードを追加するには :

1 準備のために必要な手順を実行します。

39 ページの 「ワークロードの保護と回復の基本ワークフロー」の準備を参照してください。

2 ［ダッシュボード］ページまたは［ワークロード］ページでワークロードの追加をクリックします。

Web インタフェースに［ワークロードの追加］ページが表示されます。

3 必要なワークロードの詳細を指定します。

- **ワークロードの設定：** ワークロードのホスト名または IP アドレス、オペレーティングシステム、および管理者レベルの資格情報を指定します。

  必要な資格情報のフォーマットを使用します (167 ページの 「ワークロードおよびコンテナの資格情報向けのガイドライン」を参照)。

  PlateSpin Protect がワークロードにアクセスできることを確認するには、**テスト資格情報**をクリックします。

4 **ワークロードの追加**をクリックします。

PlateSpin Protect によって［ワークロード］ページがリロードされ、追加されるワークロードのプロセスインジケータが表示されます。プロセスが終了するのを待ちます。完了すると、**ワークロードが追加されました**イベントがダッシュボードに表示され、［ワークロード］ページで新しいワークロードが使用できるようになります。

5 (条件付き) このワークロードで使用するコンテナをまだ追加していない場合は、ワークロードの保護の準備を行うためにコンテナを追加します。詳細については、97 ページの 「コンテナ (保護ターゲット) の準備」を参照してください。

6 153 ページの 「保護詳細の設定およびレプリケーションの準備」に進みます。

10.3 ワークロードのタグ付け

PlateSpin Web インタフェースの［ワークロード］ページには、ワークロードが一覧表示されていることがあります。これらのワークロードを検索して同様のワークロードに対する操作を管理しようとすると、時間がかかることがあります。この問題を解決するために、さまざまなワークロードカテゴリ、部門、または環境に適した他の論理的な関連付けに対してタグを作成できます。

ワークロードタグの作成、変更、または削除については、81 ページのセクション 7.1「ワークロードタグの作成と管理」を参照してください。

作成したタグは、［Edit Target Details (ターゲットの詳細の編集)］ページの下部に表示されます。ここで、適切なワークロードにタグを割り当てることができます。［ワークロード］ページの**タグ**列には、ワークロードに関連付けるタグが 1 つ表示されます。この列でソートして、同様のワークロードを一緒にグループ化することができます。これにより、タグ付けされたワークロードを簡単に見つけると同時に、このワークロードで操作を実行することができます。

注 : タグに新しいサーバが設定されたワークロードをエクスポートすると、タグ設定が保持されます。

保護の設定中にタグをワークロードに関連付けるには :

1. Protect Web インタフェースで、**ワークロード**をクリックします。
2. タグ付けするワークロードをワークロードリストから選択し、**保護の設定**をクリックします。
3. ワークロードを設定します。
4. ［Edit Target Details (ターゲットの詳細の編集)］ページの下部にある［タグ］セクションで、ワークロードに関連付けるタグ名を選択します。
5. ［**保存**］をクリックします。

設定されたワークロードに関連付けられているタグを追加または変更するには :

1. Protect Web インタフェースで、**ワークロード**をクリックします。
2. ワークロードリストで、タグ付けするワークロードをクリックして、［ターゲットの詳細］ページを開きます。
3. ［**編集**］をクリックします。
4. ［Edit Target Details (ターゲットの詳細の編集)］ページの下部にある［タグ］セクションで、ワークロードに関連付けるタグ名を選択します。
5. ［**保存**］をクリックします。

ワークロードからタグの関連付けを解除するには :

1. Protect Web インタフェースで、**ワークロード**をクリックします。
2. タグを削除するワークロードをワークロードリストから選択し、**保護の設定**をクリックします。
3. 環境設定ページの［タグ］セクションで空の文字列を選択し、**保存**をクリックします。

10.4 ワークロードの詳細のリフレッシュ

PlateSpin Web インタフェースでは、検出されたワークロードの詳細のリフレッシュがサポートされていません。検出されたワークロードに関する詳細を更新するには、ワークロードを削除してから、その詳細を再度追加して検出する必要があります。ワークロードを削除したときにワークロードが設定された状態の場合は、設定の詳細は失われています。保護ライセンスが使用中の場合は、ワークロードから削除され、ライセンスプールに戻されます。詳細については、105 ページのセクション 10.5「ワークロードを削除しています」を参照してください。

10.5 ワークロードを削除しています

場合によっては、ワークロードを Protect インベントリから削除し、それを後で追加し直すことが必要になる場合があります。

1 ［ワークロード］ページで、削除するワークロードを選択し、［**ワークロードの削除**］をクリックします。

2 (条件付き、Windows) ブロックレベルのレプリケーションで以前保護されていた Windows ワークロードに対して、Web インタフェースでは、ブロックベースのコンポーネントも削除するかどうかを指定するように求められます。次のとおり選択できます。

- **次のコンポーネントを削除しないでください：** コンポーネントは削除されません。
- **コンポーネントとは削除されますが、ワークロードは再起動されません：** コンポーネントは削除されます。ただし、ワークロードの再起動は、アンインストール処理を完了するために必要です。
- **コンポーネントを削除し、ワークロードを再起動します：** コンポーネントは削除され、ワークロードは自動的に再起動されます。スケジュールされたダウンタイム中にこの操作を実行するようにしてください。

3 ［コマンドの確認］ページで、**確認**をクリックして、コマンドを実行します。

プロセスが終了するのを待ちます。

4 (条件付き、Linux) Linux ワークロードの場合、ソースワークロードからブロックベースのドライバを手動でアンインストールします。Linux ワークロードのクリーンアップのブロックレベルのデータ転送ソフトウェアを参照してください。

11 物理フェールバックターゲットのデバイスドライバの準備

PlateSpin Protect では、物理マシンをフェールバックターゲットとして使用する場合は、必要とされるデバイスドライブのライブラリと PnP (プラグアンドプレイ) ID を提供しています。PlateSpin デバイスドライバツール (DeviceDriver.exe) を使用して、カスタムデバイスドライブと PnP ID マッピングを追加できます。

11.1 デバイスドライバの管理

PlateSpin Protect には、デバイスドライバのライブラリが付属しています。このライブラリは、ターゲットワークロードに適切なデバイスドライバを自動的にインストールします。物理フェールバックターゲットマシン上に一部のドライバがないか互換性がない場合、またはターゲットインフラストラクチャ用に特定のドライバを必要とする場合は、PlateSpin Protect ドライバデータベースにドライバを追加 (アップロード) する必要が生じる可能性があります。

11.1.1 Windows ワークロード用のデバイスドライバのパッケージ化

PlateSpin Protect ドライバデータベースへのアップロードに備えて、Windows デバイスドライバをパッケージ化する必要があります。

注 : 保護ジョブおよびターゲットワークロードを問題なく処理するために、次のシステム用に、デジタル署名されているドライバのみをパッケージ化してアップロードします。

- すべての 64 ビット Windows システム
- Windows Server 2008 システムの 32 ビットバージョン

Windows デバイスドライバをパッケージ化するには :

1. ターゲットインフラストラクチャおよびデバイス用に、依存関係のあるすべてのドライバファイル (*.sys、*.inf、*.dll など) を準備します。

   製造元固有のドライバを .zip アーカイブまたは実行可能ファイルとして取得した場合は、まず解凍します。
2. ドライバファイルを異なるフォルダ (デバイスごとに別個のフォルダ) に保存します。

これで、パッケージをアップロードする準備が整いました。108 ページの 「PlateSpin デバイスドライバデータベースへのドライバパッケージのアップロード」を参照してください。

11.1.2 Linux ワークロード用のデバイスドライバのパッケージ化

PlateSpin Protect ドライバデータベースへのアップロードに備えて、Linux デバイスドライバをパッケージ化する必要があります。この目的のカスタムユーティリティは、PlateSpin ISO ブートイメージ (bootofx.x2p.iso) に含まれています。

1. Linux ワークステーション上で、デバイスドライバファイル用のディレクトリを作成します。ディレクトリ内のすべてのドライバは、同じカーネルおよびアーキテクチャ用でなければなりません。
2. ブートイメージをダウンロードして、それをマウントします。

   たとえば、ISO が /root ディレクトリにコピーされていると仮定すると、BIOS ファームウェアベースのターゲットおよび UEFI ファームウェアベースのターゲットに次のコマンドを発行します。

   # mkdir /mnt/ps # mount -o loop /root/bootofx.x2p.iso /mnt/ps
3. マウントされた ISO イメージの /tools サブディレクトリから、packageModules.tar.gz アーカイブを別の作業ディレクトリにコピーし、それを抽出します。

   たとえば、現在の作業ディレクトリに .gz ファイルがある場合、次のコマンドを発行します。

   tar -xvzf packageModules.tar.gz
4. 作業ディレクトリを入力し、次のコマンドを実行します。

   ./PackageModules.sh –d< ドライバのディレクトリへのパス > -o< パッケージ名 >

   次の形式を使用して、< ドライバのディレクトリへのパス > をドライバファイルが保存されている実際のディレクトリに置き換え、< パッケージ名 > を実際のパッケージ名に置き換えます。

   Drivername-driverversion-dist-kernelversion-arch.pkg

   次に例を示します。

   bnx2x-1.48.107-RHEL4-2.6.9-11.EL-i686.pkg

これで、パッケージをアップロードする準備が整いました。詳細については、108 ページの「PlateSpin デバイスドライバデータベースへのドライバパッケージのアップロード」を参照してください。

11.1.3 PlateSpin デバイスドライバデータベースへのドライバパッケージのアップロード

PlateSpin Driver Manager ツールを使用して、デバイスドライバをドライバデータベースにアップロードします。

注 : アップロード時に PlateSpin Protect では、選択したオペレーティングシステムタイプまたはビット仕様についてドライバが検証されません。ターゲットインフラストラクチャ用に適切なドライバのみアップロードされていることを確認します。

- 109 ページの 「デバイスドライバのアップロード手順 (Windows)」
- 110 ページの 「デバイスドライバのアップロード手順 (Linux)」

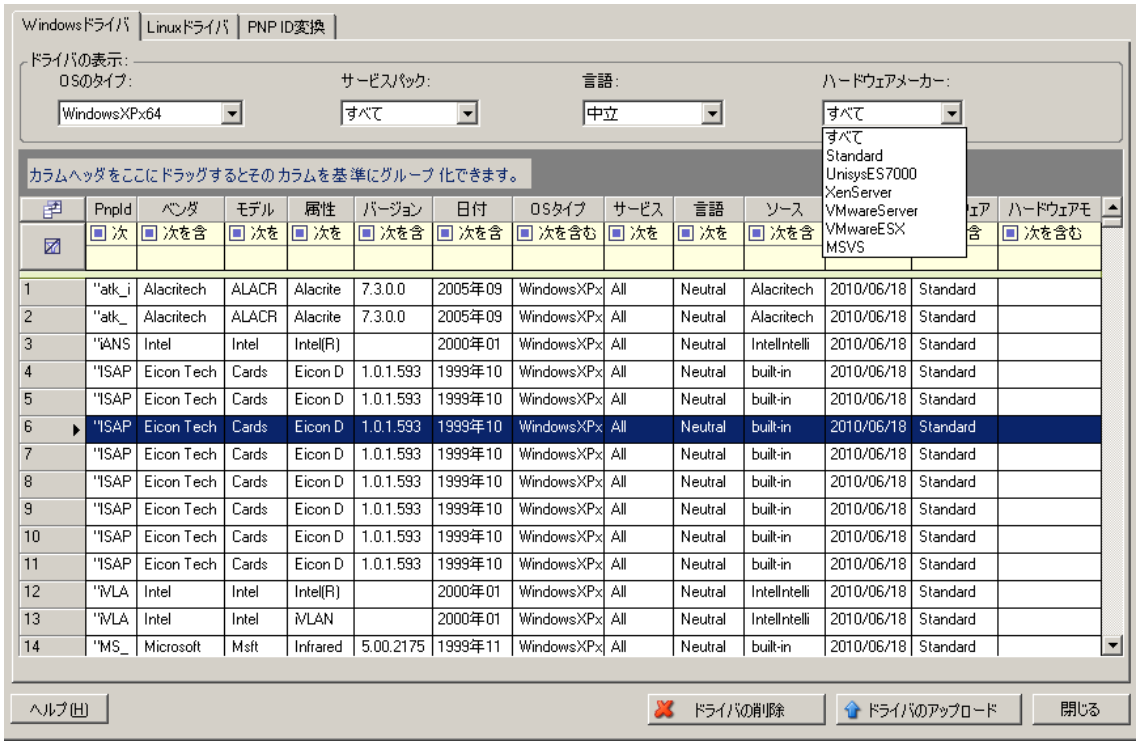
デバイスドライバのアップロード手順 (Windows)

1 必要なデバイスドライバを取得して準備します。「Windows ワークロード用のデバイスドライバのパッケージ化」を参照してください。

2 PlateSpin Server ホストに管理者ユーザとしてログインします。

3 PlateSpin Driver Manager ツールを起動します。C:\Program Files\PlateSpin Protect Server\DriverManager に移動し、DriverManager.exe プログラムを起動します。

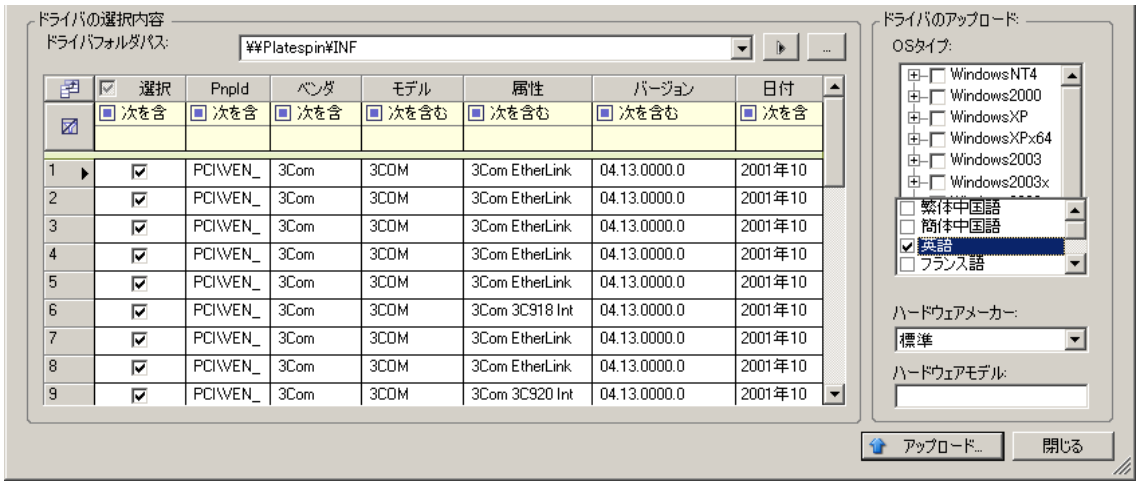
4 **ツール** > **デバイスドライバの管理**の順に選択し、**Windows ドライバ**タブを選択します。



5 ダイアログの下部で、**ドライバのアップロード**をクリックします。

6 [ドライバの選択内容] ダイアログで、必要なドライバファイルが含まれているフォルダをブラウズして、該当する OS タイプ、言語、およびハードウェアメーカーのオプションを選択します。

リストされているターゲット環境に対して特別に設計されたドライバでない限り、**ハードウェアメーカー**オプションとして**標準**を選択します。



7 アップロードをクリックし、プロンプトが表示されたら選択内容を確認します。
システムによって、選択したドライバがドライバデータベースにアップロードされます。

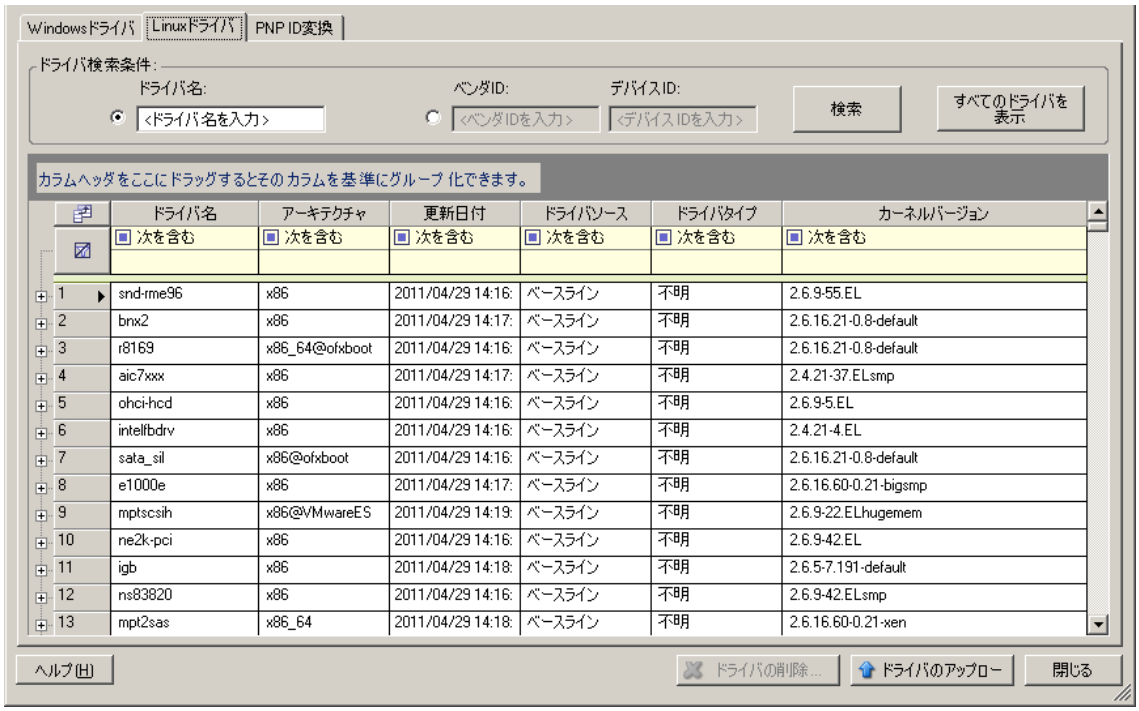
デバイスドライバのアップロード手順 (Linux)

1 必要なデバイスドライバを取得して準備します。「Linux ワークロード用のデバイスドライバのパッケージ化」を参照してください。

2 PlateSpin Server ホストに管理者ユーザとしてログインします。

3 PlateSpin Driver Manager ツールを起動します。C:\Program Files\PlateSpin Protect Server\DriverManager に移動し、DriverManager.exe プログラムを起動します。

4 ツール > デバイスドライバの管理の順に選択し、Linux ドライバタブを選択します。



5 ダイアログの下部で、ドライバのアップロードをクリックします。

6 必要なドライバパッケージ (*.pkg) が含まれているフォルダをブラウズして、**すべてのドライバをアップロード**をクリックします。

システムによって、選択したドライバがドライバデータベースにアップロードされます。

11.2 PlateSpin PnP ID マッピングの管理

「プラグアンドプレイ」(PnP) とは、ネイティブのプラグアンドプレイデバイスに対する接続、設定、および管理をサポートする Windows オペレーティングシステムの機能を指します。Windows では、この機能により、PnP 準拠バスに接続されている PnP 準拠のハードウェアデバイスを容易に検出できます。PnP 準拠デバイスには、製造元によって一連のデバイス ID 文字列が割り当てられます。それらの文字列は、ビルド時にデバイスにプログラミングされます。それらの文字列は、PnP がどのように動作するかの基礎となるものであり、デバイスを適切なドライバに対応させるために使用される Windows の情報ソースの一部となります。

PlateSpin Server がワークロードおよび使用可能なハードウェアを検出すると、検出結果には、それらの PnP ID とそのデータのストレージがワークロードの詳細として含まれます。PlateSpin は、ID を使用して、フェールオーバー / フェールバック操作時にどのドライバを追加する必要があるかを判断します (追加する必要のあるドライバがある場合)。PlateSpin Server は、サポートされている各オペレーティングシステムの、関連付けられているドライバのための、PnP ID のデータベースを維持します。Windows と Linux は、異なる形式の PnP ID を使用するため、Protect Linux RAM ディスク (LRD) によって検出された Windows ワークロードには、Linux 形式の PnP ID が含まれています。

それらの ID は一貫してフォーマットされているので、PlateSpin は、それぞれに標準変換を適用して、対応する Windows PnP ID を決定できます。変換は、PlateSpin 製品内で自動的に行われます。

ユーザ (またはサポート技術者) は PlateSpin デバイスドライバツールの PNP ID 変換オプションを使用して、カスタム PnP ID マッピングを追加、編集、または削除することができます。

カスタム PnP ID マッピングを追加するには :

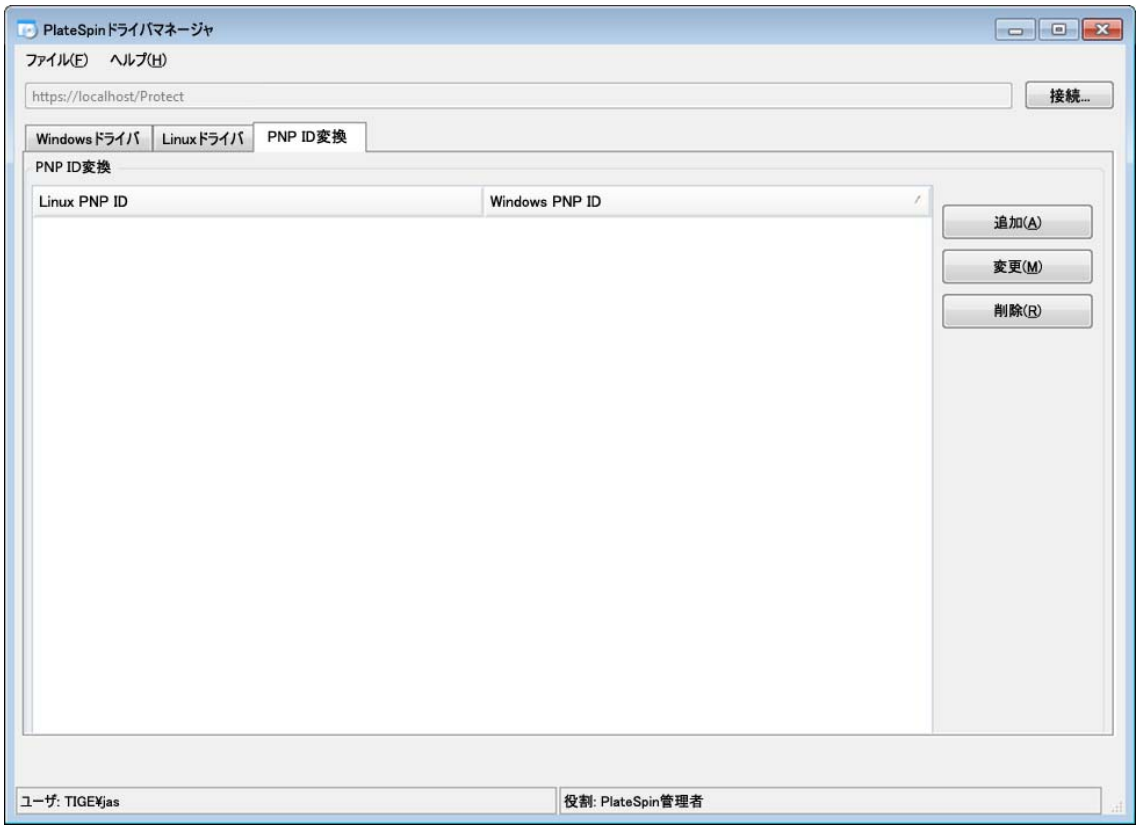
1 PlateSpin Server ホストに管理者ユーザとしてログインします。

2 PlateSpin Driver Manager ツールを起動します。C:\Program Files\PlateSpin Protect Server\DriverManager に移動し、DriverManager.exe プログラムを起動します。

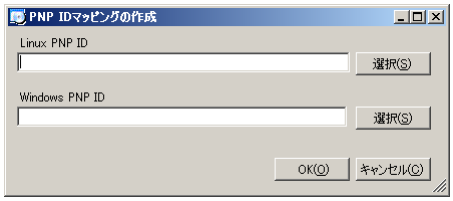
3 PlateSpin Server に接続します。

https://localhost/Protect

4 Driver Manager ツールで、**PNP ID 変換**タブを選択して、**PNP ID 変換**リストを開きます。このリストには、現在知られているカスタムの PnP ID マッピングが含まれます。



5 リストページで、**追加**をクリックして、［PNP ID マッピングの作成］ダイアログを表示します。



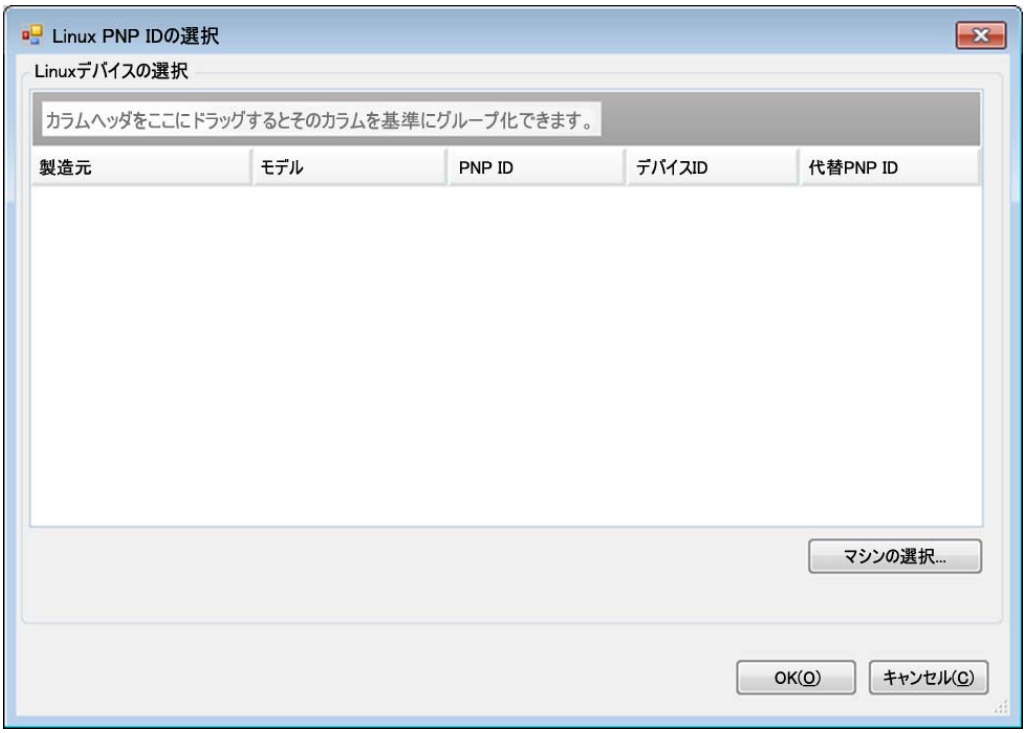
6 **Linux PNP ID** フィールドに、Linux PnP ID を追加します。

6a (条件付き) 使用する Linux PnP ID がわかっている場合は、それを入力します。

または

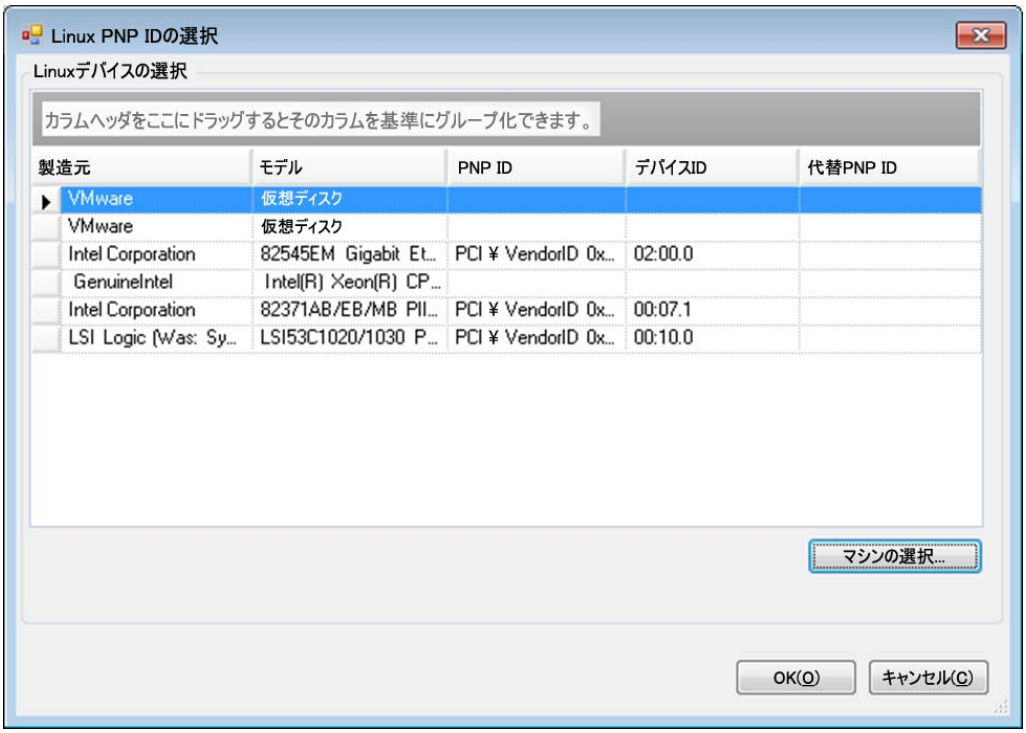
6b (条件付き) 検出済みのワークロードから ID を選択します。

6b1 **Linux PNP ID** フィールドの隣にある**選択**をクリックして、［Linux PnP ID の選択］ダイアログを開きます。



6b2 ダイアログで、**マシンの選択**をクリックして、PlateSpin Linux RAM ディスクによって検出されたマシンのリストを表示します。

6b3 リストでいずれかのデバイスを強調表示し、**選択**をクリックして、[Linux PnP ID の選択] ダイアログのリストに入力します。



6b4 リストでデバイスを選択し、**OK** をクリックして PnP ID に標準変換を適用し、［PnP ID マッピングの作成］ダイアログにそれを表示します。

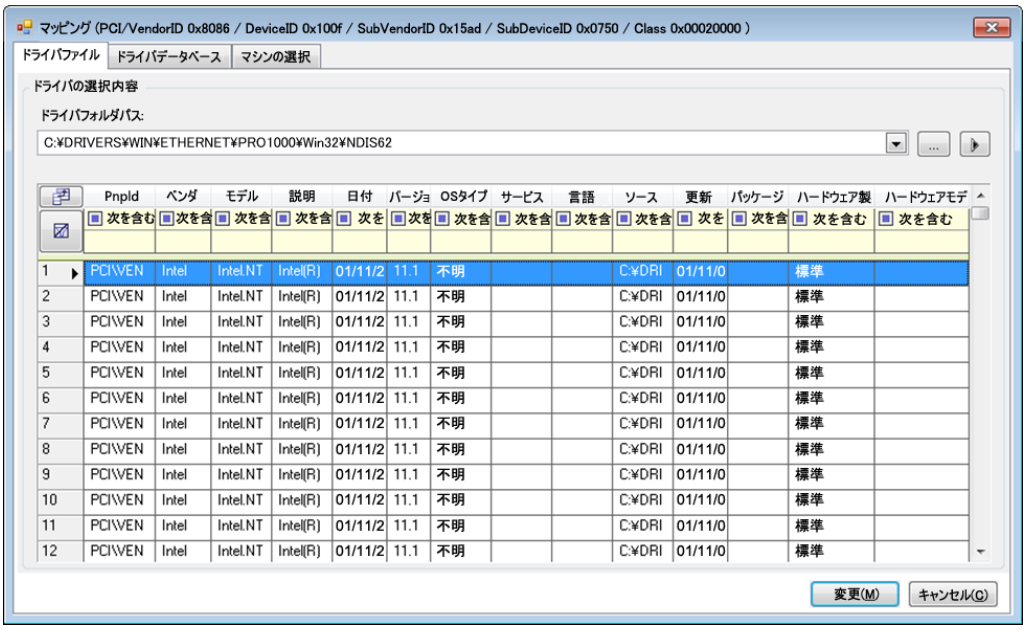
7 **Windows PNP ID** フィールドに、Windows PnP ID を追加します。

7a (条件付き) 使用する Windows PnP ID がわかっている場合は、それを入力します。

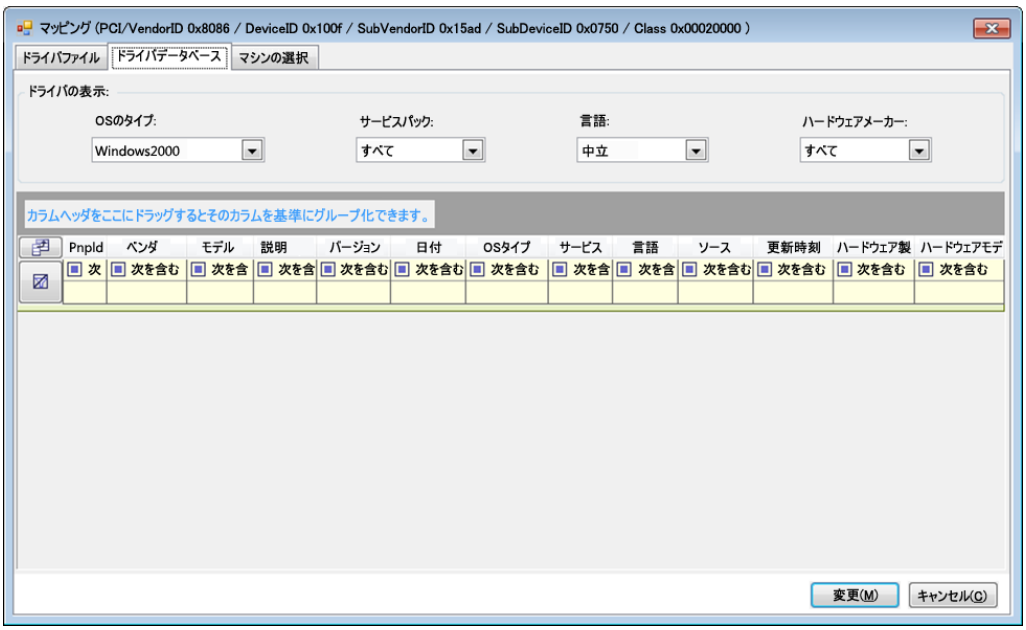
または

7b (条件付き)**Windows PNP ID** フィールドの隣にある**選択**をクリックして、マッピングツールを開きます (このツールには、Windows PnP ID のマッピングに役立つ 3 つの方法があります)。

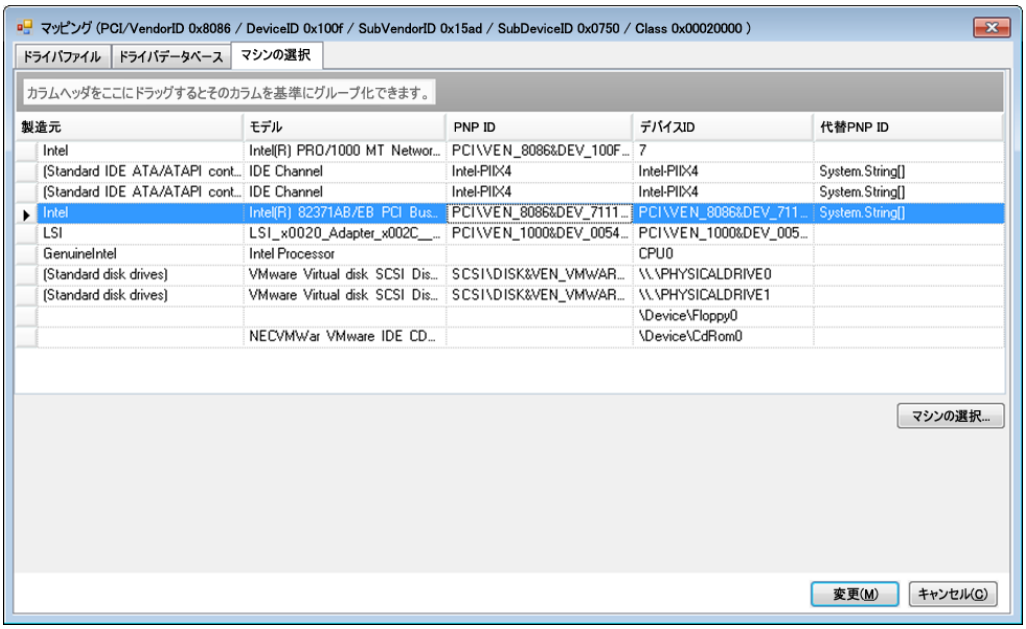
- **ドライバファイル**タブで、Windows ドライバファイル (つまり、*inf 拡張子のファイル) を参照して選択し、目的の PnP ID を選択して、**変更**をクリックします。



- ドライバデータベースタブで、既存のドライバデータベースを参照して選択し、正しい PnP ID を選択して、変更を選択します。



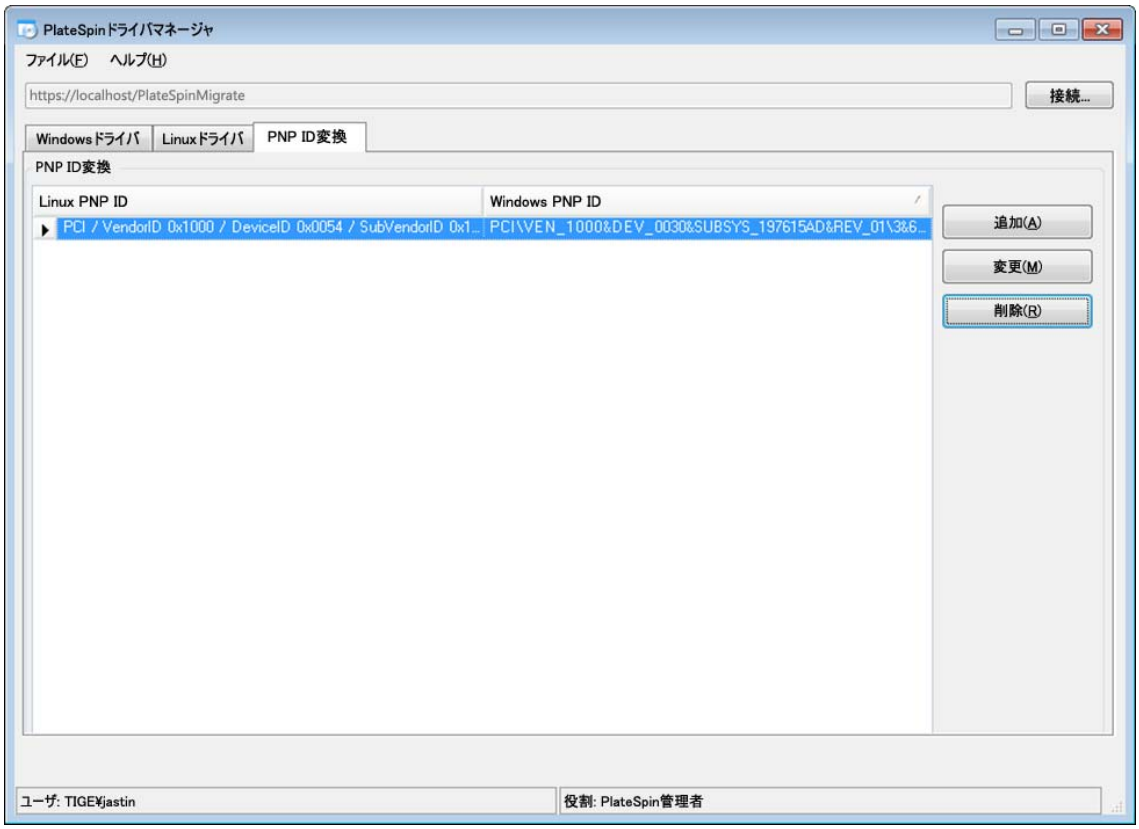
- **Select Machine** タブで、**Select Machine** をクリックし、ライブディスカバリを使用して検出された Windows マシンのリストからマシンを選択し、**OK** をクリックしてそのデバイスを表示し、目的の PnP ID を選択して、［Modify］をクリックします。



重要：関連付けられているドライバパッケージがインストールされていない Windows PnP ID を選択すると、フェールオーバー / フェールバック時にエラーが発生することがあります。

---

8 ［PNP ID マッピングの作成］ダイアログで、正しい Linux PnP ID および正しい Windows PnP が選択されていることを確認し、**OK** をクリックして、PlateSpin Driver Manager の［PNP ID 変換］ページを表示します。



9 (オプション)［PNP ID 変換］リストでマッピングを変更または削除するには、マッピングパターンを選択し、実行する操作に応じて、**削除**または**変更**をクリックします。

削除をクリックすると、(確認ダイアログが表示された後に) マッピングが削除されます。

変更するには、

9a **変更**をクリックして、［PNP ID マッピングの作成］ダイアログを開きます。

9b 114 ページのステップ 7 を繰り返して、Windows PnP ID を変更します。

注 : Linux PnP ID を選択または変更することはできません。

12 保護用の Linux ワークロードの準備

この項のタスクを実行して、PlateSpin Protect での保護のために Linux ワークロードを準備します。

- 119 ページのセクション 12.1「Linux 用のブロックベースドライバの確認」
- 119 ページのセクション 12.2「ブロックレベル転送のためのスナップショットの準備 (Linux)」
- 121 ページのセクション 12.3「すべてのレプリケーションで Freeze と Thaw スクリプト機能を使用する (Linux)」

12.1 Linux 用のブロックベースドライバの確認

blkwatch モジュールがワークロードの Linux ディストリビューションで利用可能であることを確認します。事前設定されたドライバのリストについては、139 ページの 「Protect によってサポートされている Linux ディストリビューション」を参照してください。

非標準のカーネル、カスタマイズされたカーネル、またはより新しいカーネルを持つサポート対象の Linux ワークロードを保護する場合は、ブロックレベルのデータレプリケーションに必要な PlateSpin blkwatch モジュールを再構築します。

ナレッジベースの記事 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873) を参照してください。

12.2 ブロックレベル転送のためのスナップショットの準備 (Linux)

ブロックレベルのデータ転送用にスナップショットを準備することをお勧めします。各ボリュームグループにスナップショットのための十分な空き容量 (すべてのパーティションの合計の少なくとも 10%) があることを確認してください。スナップショットが使用できない場合、Protect はデータ転送用にソースワークロード上で各ブロックを順番にロックおよびロック解除します。

- 119 ページのセクション 12.2.1「Linux ボリュームレプリケーション用の LVM スナップショットの設定」
- 120 ページのセクション 12.2.2「NSS プールレプリケーション用の NSS スナップショットの設定」

12.2.1 Linux ボリュームレプリケーション用の LVM スナップショットの設定

LVM スナップショットが利用可能な場合、blkwatch ドライバは LVM スナップショットを利用します。スナップショットからブロックをコピーすることで、開いているファイルが競合する問題を回避できます。

LVM ストレージについては、ナレッジベースの記事 7005872 (https://www.netiq.com/support/kb/doc.php?id=7005872) を参照してください。

12.2.2 NSS プールレプリケーション用の NSS スナップショットの設定

Open Enterprise Server を実行している Linux ワークロードについては、NSS プール用の LVM スナップショットソリューションは存在しません。NSS プールのレプリケーション時には、データ転送するために Protect が各ブロックを順番にロックおよびロック解除します。開いているファイルの潜在的な競合を回避し、レプリケーションパフォーマンスを改善するためには、レプリケーション用に NSS プールスナップショットを利用できます。

すべての NSS プールスナップショットに使用する未フォーマットの単一ディスクを追加したり、NSS プールごとに個別の未フォーマットのディスクを追加したりすることができます。最善のパフォーマンスは、プールごとに個別のディスクを追加することで得られます。ワークロード保護をセットアップする前にディスクを追加します。使用するディスクを準備すると、PlateSpin はレプリケーション時にプールに対して NSS スナップショットを設定します。

注 : デフォルトでは、PlateSpin は NSS プールスナップショット用に、最大の空き領域 (パーティション化されていない領域) を持つ NLVM 管理対象ディスクを使用します。レプリケーション用の NSS プールスナップショットがルートファイルシステムと同じディスクに配置されていたり、ディスク IO が絶えず発生する別のディスクに配置されていることが判明した場合は、/etc/platespin/platespin.conf ファイルを使用して適切なディスクに NSS スナップショットを指定します。

NSS スナップショットが Open Enterprise Server で機能する方法については、『*Linux 用の NSS ファイルシステム管理ガイド*』の「プールスナップショットの使用および管理のためのガイドライン」(http://www.novell.com/documentation/oes2015/stor_nss_lx/data/br18up4.html) を参照してください。

NSS プールのスナップショットに使用する 1 つ以上のディスクを設定するには :

1. OES ソースワークロードで、すべての NSS プールのスナップショットに対して使用するように未フォーマットの Linux ディスクを追加します。または、NSS プールごとに個別のディスクを作成することもできます。

   ディスクのサイズは、NSS プール上の使用済みデータ量の約 20% である必要があります。レプリケーションの時間間隔の間に発生する可能性のあるデータ量の変更や増大に従ってサイズを調整します。

2. ステップ 1 で作成した各ディスクについては、NLVM によって管理されるようにディスクを初期化します。

   ディスクを初期化するには、NSSMU または NLVM コマンドを使用できます。デバイス形式は、GPT または DOS のいずれかにすることができます。

   - NSSMU を使用するには :
     1. NSSMU を起動し、**デバイス**を選択します。
     2. 新しいディスクを選択し、F3 キーを押して初期化します。
   - NLVM コマンドを使用するには :
     1. のコマンドラインで、次のように入力します。

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

3 各 NSS プールのスナップショットに使用するディスクを指定する必要がある場合があります。OES ソースワークロード上で platespin.conf ファイルを作成し、NSS プールを新しいディスクに関連付けます。

3a テキストエディタで、/etc/platespin/platespin.conf にファイルを作成します。

3b NSS プールごとに、次の構文を使用して Customlocation パラメータの下にデバイスとサイズ情報を追加します。

```
[Customlocation] /dev/pool/<yourPoolName>=<device>:<maxUnpartitionSize-in-MB>
```

たとえば、最大サイズが 12228MB のデバイス sdc にスナップショットを追加するには、NSSPOOL という名前のプールに次のエントリを指定します。

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

4 ファイルを保存します。

5 ソース OES ワークロードに対するワークロード保護の設定を引き続き行います。

12.3 すべてのレプリケーションで Freeze と Thaw スクリプト機能を使用する (Linux)

Linux システムの場合、PlateSpin Protect は、カスタムスクリプトである freeze と thaw の自動実行を行う能力があります。これは、自動的にデーモン制御機能を補足するものです。

freeze スクリプトはレプリケーションの先頭で実行され、thaw はレプリケーションの末尾で実行されます。

ユーザインタフェース経由で使用できる自動化されたデーモン制御機能を補足するために、この機能を使用することを考慮してください (171 ページの 「ソースサービス / デーモンの制御 :」を参照)。たとえば、レプリケーション中に特定のデーモンを停止する代わりに、それらを一時的にフリーズさせるのにこの機能を使用してください。

この機能を実装するには、Linux ワークロード保護をセットアップする前に、次のプロシージャを実行します。

1 次のファイルを作成します。

- platespin.freeze.sh: レプリケーションの最初に実行するシェルスクリプト
- platespin.thaw.sh: レプリケーションの最後に実行するシェルスクリプト
- platespin.conf: タイムアウト値とともに必要な引数を定義するテキストファイル

platespin.conf ファイルの内容に関して使用する必要のある構文は次のとおりです。

```
[ServiceControl]

FreezeArguments=< 引数 >

ThawArguments=< 引数 >

TimeOut=< タイムアウト >
```

< 引数 > の部分を必要なコマンド引数で置き換え (スペース区切り)、< タイムアウト > の部分をタイムアウト値 (秒) で置き換えます。値が指定されない場合、デフォルトのタイムアウトが使用されます (60 秒間)。

2 Linux ソースワークロードの次のディレクトリに、.conf ファイルとともにスクリプトを保存します。

/etc/platespin

13 Windows クラスタ保護の準備

PlateSpin Protect では、Microsoft Windows クラスタのビジネスサービスの保護をサポートしています。サポートされる Microsoft Windows クラスタオペレーティングシステムは次のとおりです。

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

詳細については、14 ページのセクション 1.1.1「サポートされる Windows のワークロード」の「クラスタ」を参照してください。

注 : Windows のクラスタ管理ソフトウェアは、クラスタノード上で実行されているリソースに対して、フェールオーバーとフェールバックの制御を提供します。このマニュアルでは、このアクションのことを「クラスタノードのフェールオーバー」または「クラスタノードのフェールバック」と呼んでいます。

PlateSpin Server は、クラスタを表す保護ワークロードに対して、フェールオーバーとフェールバックの制御を提供します。このマニュアルでは、このアクションのことを「PlateSpin のフェールオーバー」または「PlateSpin のフェールバック」と呼んでいます。

13.1 クラスタワークロード保護の計画

PlateSpin 環境でアクティブノードの検出が有効になっている (デフォルト) 場合、Windows クラスタの保護は、仮想の 1 ノードクラスタ (ソースインフラストラクチャのトラブルシューティング時に使用可能) にストリームされるアクティブノード上の変更による増分レプリケーションで実現できます。アクティブノードの検出を無効にした場合、Windows クラスタの各ノードはスタンドアロンノードとして検出および保護することができます。

Windows クラスタを保護対象に設定する前に、現在の環境が前提条件を満たしていること、およびクラスタワークロードの保護条件を理解していることを確認します。

- 124 ページのセクション 13.1.1「クラスタ保護の前提条件」
- 125 ページのセクション 13.1.2「クラスタ用のブロックベース転送」
- 127 ページのセクション 13.1.3「レプリケーションでのクラスタノードのフェールオーバーの影響」
- 129 ページのセクション 13.1.4「クラスタノードの類似性」
- 129 ページのセクション 13.1.5「保護のセットアップ」

13.1.1 クラスタ保護の前提条件

クラスタ保護のサポート範囲は、表 13-1 に記載されている条件に従う必要があります。PlateSpin 環境でクラスタの保護を設定する際には次の要件を検討してください。

表 13-1 *クラスタ保護の要件*

要件	説明
Windows クラスタとしてのアクティブノードの検出	PlateSpin グローバル環境設定 DiscoverActiveNodeAsWindowsCluster は、Windows クラスタをクラスタとして保護するか、別個のスタンドアロンマシンとして保護するかどうかを判断します。 ◆ **True (デフォルト):** アクティブノードが Windows クラスタとして検出されます。 ◆ **False:** 個々のノードはスタンドアロンマシンとして検出できます。 詳細については、129 ページのセクション 13.2「Windows アクティブノードの検出の設定」を参照してください。
リソース名の検索値	PlateSpin グローバル環境設定 MicrosoftClusterIPAddressNames は、PlateSpin 環境で検出可能なクラスタリソース名を判断します。共有クラスタの IP アドレスリソース名を、クラスタ上の他の IP アドレスリソース名から区別するため、検索値を指定する必要があります。 詳細については、130 ページのセクション 13.4「リソース名の検索値の追加」を参照してください。

要件	説明
Windows クラスタモード	PlateSpin グローバル環境設定 WindowsClusterMode は、増分レプリケーションのブロックベースのデータ転送方法を判断します。 ◆ **デフォルト :** ドライバレス同期。 ◆ **SingleNodeBBT:** ドライバベースのブロックベース転送。 次を参照してください。 ◆ 125 ページの 「クラスタ用のブロックベース転送」 ◆ 130 ページの 「クラスタ用のブロックベース転送方法の設定」
アクティブノードのホスト名または IP アドレス	**ワークロードの追加**操作を実行する場合、クラスタのアクティブノードのホスト名または IP アドレスを指定する必要があります。Microsoft によるセキュリティ変更のため、仮想クラスタ名 (つまり、共有クラスタ IP アドレス) を使用して Windows クラスタを検出することはできなくなりました。
解決可能なホスト名	PlateSpin Server は、クラスタの各ノードのホスト名を IP アドレスで解決できる必要があります。 **注 :** IP アドレスによってホスト名を解決するには、DNS 前方向検索および後方向検索が必要です。
クォーラムリソース	クラスタのクォーラムリソースは、ノード上で、保護されるクラスタのリソースグループ (サービス) と一緒に用いられる必要があります。
クラスタノードの類似性	デフォルトの Windows クラスタモードでは、ノードが類似している場合、アクティブになる任意のノードからドライブレス同期を続行できます。それらが一致しない場合、元々検出されていたアクティブノードでのみレプリケーションが発生する可能性があります。 詳細については、129 ページの 「クラスタノードの類似性」を参照してください。
PowerShell 2.0	Windows PowerShell 2.0 を、クラスタの各ノードにインストールする必要があります。

13.1.2 クラスタ用のブロックベース転送

クラスタ用のブロックベース転送は、スタンドアロンサーバ用とは異なる方法で動作します。最初のレプリケーションでは、完全なコピー (フル) が作成されるか、またはクラスタのアクティブノード上で実行されるドライバレスの同期方法が使用されます。後続の増分レプリケーションでは、ブロックベースのデータ転送でドライブレスの方法またはドラバベースの方法を使用できます。

注 : Protect では、クラスタ用のファイルベース転送がサポートされていません。

PlateSpin グローバル環境設定 WindowsClusterMode は、増分レプリケーションのブロックベースのデータ転送方法を判断します。

- **デフォルト :** ドライバレス同期。
- **SingleNodeBBT:** ドライバベースのブロックベース転送。ファイバチャネル SAN でのみ使用してください。

警告 : 共有 iSCSI ドライブを使用するクラスタで SingleNodeBBT を使用しないでください。クラスタが使用不能になります。

表 13-2 では、2 つの方法について説明および比較しています。

表 13-2 増分レプリケーション用のブロックベースのデータ転送方法の比較

検討事項	デフォルト BBT	シングルノード BBT
データ転送方法	現在のアクティブノード上で MD5 ベースレプリケーションとともにドライブレス同期を使用します。	元々検出されていたアクティブノード上にインストールされた BBT ドライバを使用します。
パフォーマンス	潜在的に低速な増分レプリケーション。	増分レプリケーションのパフォーマンスが大幅に向上します。
ドライバ	◆ インストールする BBT ドライバはありません。 ◆ ソースクラスタノード上で再起動は必要ありません。	◆ Protect Agent ユーティリティを使用して、クラスタの元々検出されていたアクティブノード上に BBT ドライバをインストールします。 ◆ ドライバを適用するためにノードを再起動します。これにより、クラスタ内の別のノードへのフェールオーバーが開始します。再起動後、元々検出されていたノードを再びアクティブノードにします。 ◆ レプリケーションを実行し、シングルノードブロック転送を使用するには、同じノードがアクティブなままである必要があります。 ◆ BBT ドライバをインストールした後で、ドライバベースの増分レプリケーションを開始するには、完全レプリケーションまたはドライバレス増分レプリケーションのいずれかを実行する必要があります。
サポートされる Windows クラスタ	サポートされている Windows Server クラスタと連携動作します。	Windows Server 2008 R2 以降と連携動作します。 他のサポートされる Windows クラスタでは、レプリケーションにドライバレス同期方法が使用されます。
最初の増分レプリケーション	アクティブノード上でドライバレス同期を使用します。	BBT ドライバがインストールされた後で完全レプリケーションが完了した場合、元々検出されていたアクティブノード上でドライバベースのブロックベース転送を使用します。 それ以外の場合、元々検出されていたアクティブノード上でドライバレス同期を使用します。

検討事項	デフォルト BBT	シングルノード BBT
後続の増分レプリケーション	アクティブノード上でドライバレス同期を使用します。	元々検出されていたアクティブノード上でドライバベースのブロックベース転送を使用します。 クラスタがノードを切り替える場合、元々アクティブなノードが再びアクティブになった後で、最初の増分レプリケーションにドライバレス同期方法が使用されます。 詳細については、127 ページの 「レプリケーションでのクラスタノードのフェールオーバーの影響」を参照してください。

13.1.3 レプリケーションでのクラスタノードのフェールオーバーの影響

表 13-3 では、レプリケーションでのクラスタノードフェールオーバーの影響と、Protect 管理者による実行が必要なアクションについて説明します。

表 13-3 *レプリケーションでのクラスタノードのフェールオーバーの影響*

クラスタノードフェールオーバーまたはフェールバック	デフォルト BBT	シングルノード BBT
最初の完全レプリケーション時にクラスタノードフェールオーバーが発生する	レプリケーションが失敗します。最初の完全レプリケーションは、クラスタノードフェールオーバーなしで正常に完了する必要があります。 1. Protect からクラスタを削除します。 2. (オプション) 元々検出されていたアクティブノードを再びアクティブノードにします。 3. アクティブノードを使用してクラスタを再度追加します。 4. 最初の完全レプリケーションを再度実行します。	

クラスタノードフェールオーバーまたはフェールバック	デフォルト BBT	シングルノード BBT
後続の完全レプリケーションまたは後続の増分レプリケーション時にクラスタノードフェールオーバーが発生する	レプリケーションコマンドが中止され、レプリケーションを再実行する必要があることを示すメッセージが表示されます。 新しいアクティブノードのプロファイルが、障害の発生したアクティブノードと同様の場合は、保護コントラクトが有効なままになります。 1. 現在のアクティブノード上でレプリケーションを再実行します。 新しいアクティブノードのプロファイルが、障害が発生したアクティブノードと同様ではない場合は、保護コントラクトは元々アクティブなノード上でのみ有効になります。 1. 元々検出されていたアクティブノードを再びアクティブノードにします。 2. アクティブノード上でレプリケーションを再実行します。	レプリケーションコマンドが中止され、レプリケーションを再実行する必要があることを示すメッセージが表示されます。元々検出されていたアクティブノード上でのみ保護コントラクトが有効です。 1. 元々検出されていたアクティブノードを再びアクティブノードにします。 2. アクティブノード上でレプリケーションを再実行します。 クラスタフェールオーバー / フェールバックイベント後のこの最初の増分レプリケーションでは、自動的にドライバレス同期が使用されます。後続の増分レプリケーションではシングルノード BBT で指定されているように、ブロックベースドライバが使用されます。
レプリケーション間でクラスタノードフェールオーバーが発生する	新しいアクティブノードのプロファイルが、障害が発生したアクティブノードと同様な場合、次回の増分レプリケーションでは保護コントラクトの処理がスケジュールどおりに続行されます。それ以外の場合は、次回の増分レプリケーションコマンドが失敗します。 スケジュール済みの増分レプリケーションが失敗する場合 : 1. 元々検出されていたアクティブノードを再びアクティブノードにします。 2. 増分レプリケーションを実行します。	アクティブノードがレプリケーション間で切り替わる場合は増分レプリケーションが失敗します。 1. 元々検出されていたアクティブノードが再びアクティブノードになっていることを確認します。 2. 増分レプリケーションを実行します。 クラスタフェールオーバー / フェールバックイベント後のこの最初の増分レプリケーションでは、自動的にドライバレス同期が使用されます。後続の増分レプリケーションではシングルノード BBT で指定されているように、ブロックベースドライバが使用されます。

13.1.4 クラスタノードの類似性

デフォルトの Windows クラスタモードの場合、レプリケーションプロセスでの中断を回避するため、クラスタノードが類似プロファイルを持っている必要があります。クラスタノードのプロファイルは、次のすべての条件を満たす場合、類似していると見なされます。

- ノードのローカルボリューム (システムボリュームおよびシステム予約済みボリューム) のシリアル番号は各クラスタノードで同一である必要があります。

  注 : カスタマイズされた*ボリュームマネージャ*ユーティリティを使用して、ローカルボリュームのシリアル番号をクラスタの各ノードで一致するように変更します。詳細については、143 ページの 「クラスタノードにおけるローカルストレージのシリアル番号の同期」を参照してください。

  クラスタの各ノードのローカルボリュームでシリアル番号が異なる場合、クラスタノードでのフェールオーバーの実行後にレプリケーションを実行できません。たとえば、クラスタノードでのフェールオーバーの実行時には、アクティブノードであるノード 1 に障害が発生し、クラスタソフトウェアによってノード 2 がアクティブノードに設定されます。2 つのノードのローカルドライブでシリアル番号が異なる場合、ワークロードの次回のレプリケーションコマンドが失敗します。
- 各ノードが同じ数のボリュームを持っている必要があります。
- 各ボリュームが各ノードでまったく同じサイズである必要があります。
- 各ノードがまったく同数のネットワーク接続を持っている必要があります。

13.1.5 保護のセットアップ

Windows クラスタの保護を設定するには、通常のワークロード保護ワークフローに従います。クラスタのアクティブノードのホスト名または IP アドレスを指定してください。詳細については、39 ページの 「ワークロードの保護と回復の基本ワークフロー」を参照してください。

13.2 Windows アクティブノードの検出の設定

PlateSpin グローバル環境設定 DiscoverActiveNodeAsWindowsCluster に従って、Windows Server クラスタを、クラスタまたは個別のスタンドアロンマシンとして検出できます。

Windows クラスタをクラスタとして検出する場合は、DiscoverActiveNodeAsWindowsCluster パラメータを True に設定します。これがデフォルトの設定です。クラスタ検出、インベントリ、ワークロード保護では、クラスタ名と管理共有を使用するかわりに、クラスタのアクティブノードのホスト名または IP アドレスを使用します。クラスタの非アクティブノードに対して別個のワークロードは設定しません。クラスタワークロード保護の他の要件については、124 ページの 「クラスタ保護の前提条件」を参照してください。

すべての Windows クラスタを個別のスタンドアロンマシンとして検出する場合は、DiscoverActiveNodeAsWindowsCluster パラメータを False に設定します。この設定により、PlateSpin Server は、Windows フェールオーバークラスタのすべてのノードをスタンドアロンマシンとして検出できるようになります。つまり、クラスタのアクティブノードと非アクティブノードを、クラスタ非対応の通常の Windows ワークロードとしてインベントリします。

クラスタ検出を有効または無効にするには :

1. PlateSpin Server 環境設定ページに移動します。これは次の場所にあります。

   https://<p*latespin-server-ip-address*>/PlateSpinConfiguration
2. DiscoverActiveNodeAsWindowsCluster を検索して、**編集**をクリックします。
3. **Value (値)** フィールドで、クラスタ検出を有効にする場合は **True** を選択し、クラスタ検出を無効にする場合は **False** を選択します。
4. **保存**をクリックします。

13.3 クラスタ用のブロックベース転送方法の設定

Windows クラスタの増分レプリケーションでは、PlateSpin グローバル環境設定 WindowsClusterMode に従って、ブロックベースのデータ転送にドライバレスの方法 (デフォルト) またはドライバベースの方法 (SingleNodeBBT) を使用できます。詳細については、125 ページの「クラスタ用のブロックベース転送」を参照してください。

WindowsClusterMode を設定するには :

1. PlateSpin Server 環境設定ページに移動します。これは次の場所にあります。

   https://<p*latespin-server-ip-address*>/PlateSpinConfiguration
2. WindowsClusterMode を検索して、**編集**をクリックします。
3. **値**フィールドで、増分レプリケーション用にドライバレス同期を使用する場合は**デフォルト**を選択し、増分レプリケーション用にブロックベースのドライバを使用する場合は **SingleNodeBBT** を選択します。
4. ［**保存**］をクリックします。

13.4 リソース名の検索値の追加

Windows フェールオーバークラスタ内のアクティブノードを容易に識別するため、PlateSpin Protect は、共有クラスタ IP アドレスリソースの名前を、クラスタ上にある他の IP アドレスリソースの名前と区別する必要があります。共有クラスタ IP アドレスリソースは、クラスタのアクティブノードに存在します。

PlateSpin Server 環境設定ページのグローバルパラメータ MicrosoftClusterIPAddressNames に、Windows クラスタワークロードの検出で使用する検索値のリストが含まれています。Windows クラスタワークロードを追加する場合、クラスタの現在アクティブになっているノードの IP アドレスを指定する必要があります。PlateSpin Protect は、そのノード上でクラスタの IP アドレスリソースの名前を検索し、リストにある値の指定した文字で「始まる」名前を見つけます。そのため、各検索値には、特定のクラスタ上にある共有クラスタ IP アドレスリソースを区別するのに十分な数の文字が含まれている必要があります。ただし、他の Windows クラスタでの検出に適用できるよう十分に短くすることができます。

たとえば、検索値 Clust IP Address または Clust IP は、10.10.10.201 に対応するリソース名 *Clust IP Address* と、10.10.10.101 に対応するリソース名 *Clust IP Address* に一致します。

共有クラスタ IP アドレスリソースのデフォルト名は、英語の場合は Cluster IP Address で、クラスタノードが別の言語で設定されている場合は同等の語句です。MicrosoftClusterIPAddressNames リストのデフォルトの検索値には、英語のリソース名 Cluster IP Address と、サポートされる言語それぞれのリソース名が含まれています。

共有クラスタ IP アドレスリソースのリソース名はユーザが設定可能であるため、必要に応じてリストに他の検索値を追加する必要があります。リソース名を変更した場合、関連する検索値を MicrosoftClusterIPAddressNames リストに追加する必要があります。たとえば、リソース名 Win2012-CLUS10-IP-ADDRESS を指定した場合、その値をリストに追加する必要があります。複数のクラスタで同じ命名規則を使用している場合、Win2012-CLUS というエントリは、その一連の文字で始まる任意のリソース名に一致します。

MicrosoftClusterIPAddressNames リストに検索値を追加するには :

1. PlateSpin Server 環境設定ページに移動します。これは次の場所にあります。

   https://<p*latespin-server-ip-address*>/PlateSpinConfiguration
2. MicrosoftClusterIPAddressNames を検索して、**編集**をクリックします。
3. **Value (値)** フィールドで、検索値を 1 つ以上リストに追加します。
4. **保存**をクリックします。

13.5 クォーラムアービトレーションのタイムアウト

PlateSpin Server 環境設定ページのグローバルパラメータ FailoverQuorumArbitrationTimeout を使用して、PlateSpin 環境の Windows Server フェールオーバークラスタに対して QuorumArbitrationTimeMax レジストリキーを設定できます。デフォルトのタイムアウトは 60 秒で、Microsoft によるこの設定のデフォルト値と一致しています。Microsoft Developer Network の Web サイトで「*QuorumArbitrationTimeMax* (https://msdn.microsoft.com/en-us/library/aa369123%28v=vs.85%29.aspx?f=255&MSPPError=-2147217396)」を参照してください。フェールオーバーおよびフェールバック時のクォーラムアービトレーション時には、指定したタイムアウト間隔が遵守されます。

すべての Windows フェールオーバークラスタに対してクォーラムアービトレーションのタイムアウトを設定するには :

1. PlateSpin Server 環境設定ページに移動します。これは次の場所にあります。

   https://<p*latespin-server-ip-address*>/PlatespinConfiguration
2. FailoverQuorumArbitrationTimeout を検索して、**編集**をクリックします。
3. **Value (値)** フィールドで、クォーラムアービトレーションに対して許可する最大秒数を指定します。
4. **保存**をクリックします。

13.6 ローカルボリュームのシリアル番号の設定

*ボリュームマネージャ*ユーティリティを使用して、ローカルボリュームのシリアル番号をクラスタの各ノードで一致するように変更できます。詳細については、143 ページの 「クラスタノードにおけるローカルストレージのシリアル番号の同期」を参照してください。

13.7 PlateSpin のフェールオーバー

PlateSpin のフェールオーバー操作が完了して、1 つのノードからなる仮想クラスタがオンラインになると、アクティブノードが 1 つのマルチノードクラスタが表示されます (アクティブノード以外のノードは使用できない状態になっています)。

Windows クラスタで PlateSpin のフェールオーバーを実行するには (または Windows クラスタ上で PlateSpin のフェールオーバーをテストするには)、そのクラスタがドメインコントローラに接続できなければなりません。フェールオーバーのテスト機能を使用するには、該当のクラスタとともにドメインコントローラを保護する必要があります。このテストでは、まずドメインコントローラを起動し、続いて (分離したネットワーク上で)Windows クラスタのワークロードを起動します。

13.8 PlateSpin のフェールバック

PlateSpin のフェールバック操作では、Windows クラスタのワークロードのフルレプリケーションが必要になります。

PlateSpin のフェールバックを物理ターゲットへのフルレプリケーションとして設定した場合は、次の方法のいずれかを使用できます。

- 1 つのノードからなる PlateSpin 仮想クラスタ上のすべてのディスクを、フェールバックターゲット上の単一のローカルディスクにマップする。
- 別のディスク (ディスク 2) を物理フェールバックマシンに追加する。フェールオーバーマシンのシステムボリュームをディスク 1 に復元し、フェールオーバーマシンの追加ディスク (以前の共有ディスク) をディスク 2 に復元するように PlateSpin のフェールバック操作を設定できます。これによって、システムディスクを元のソースと同じサイズのストレージに復元することができます。

PlateSpin のフェールバックが完了したら、追加ノードを新しく復元されたクラスタに再度参加させる前に、共有ストレージを再接続してクラスタ環境を再構築する必要があります。

注 : クラスタが **Ready To Reprotect (再保護の準備完了)** の段階である場合は、まずフェールバックターゲットを再構築して復元し、ターゲットがクラスタとして検出されるようにします。再構築プロセスの一部として、PlateSpin クラスタドライバを手動でアンインストールする必要があります。

PlateSpin でフェールオーバーおよびフェールバックが生じた後にクラスタ環境を再構築する方法の詳細については、次のリソースを参照してください。

- **Windows Server 2012 R2 フェールオーバークラスタ (物理再構築または仮想再構築へのフェールバック):** ナレッジベースの記事 7016770 (http://www.netiq.com/support/kb/doc.php?id=7016770) を参照してください。
- **Windows Server 2008 R2 フェールオーバークラスタ (物理再構築または仮想再構築へのフェールバック):** ナレッジベースの記事 7015576 (http://www.netiq.com/support/kb/doc.php?id=7015576) を参照してください。

---

14 ワークロードの検出とインベントリのトラブルシューティング

この項は、ワークロードの検出とインベントリの実行中に最も頻繁に起こる問題のトラブルシューティングに役立ちます。

14.1 Windows ワークロードの検出のトラブルシューティング

この項の情報を使用して、Windows ワークロードのワークロードインベントリへの追加時および検出時における問題をトラブルシューティングして解決してください。

14.1.1 最も頻繁に起こる問題およびその解決方法

問題またはメッセージ	解決方法
資格情報のドメインが無効か空です	このエラーは資格情報のフォーマットが不正な場合に発生します。 hostname\LocalAdmin という資格情報のフォーマットでローカル管理者アカウントを使用して検出してみてください。. または、domain\DomainAdmin という資格情報フォーマットでドメイン管理者アカウントを使用して検出してみてください。

問題またはメッセージ	解決方法
Windows サーバに接続できません ... アクセスが拒否されました	ワークロードを追加しようとする際に、非管理者アカウントが使用されました。管理者アカウントを使用するか、このユーザを管理者グループに追加して再試行します。 このメッセージは、WMI 接続性に障害が発生したことを示す場合もあります。次の考えられる解決策について、それぞれ試してみてから 135 ページの 「WMI の接続性テスト」を再実行してください。テストが成功したら、ワークロードを再度追加します。 ◆ 136 ページの 「DCOM の接続性のトラブルシューティング」 ◆ 136 ページの 「RPC サービスの接続性のトラブルシューティング」
Windows サーバに接続できません ... ネットワークパスが見つかりませんでした	ネットワークの接続性の障害です。135 ページの 「接続性テストの実行」で、テストを実行します。このテストが失敗した場合は、PlateSpin Protect とワークロードが同じネットワーク上にあるか確認します。ネットワークを再設定して再試行してください。
サーバ詳細の検出 {hostname}" が失敗しました。進捗状況 : 0% ステータス : 開始していません	このエラーには複数の原因があり、それぞれに固有の解決策があります。 ◆ 認証を有効にしたローカルプロキシを使用している環境では、プロキシをバイパスするか適切な権限を追加します。詳細については、ナレッジベースの記事 7920339 (https://www.netiq.com/support/kb/doc.php?id=7920339) を参照してください。 ◆ ローカルポリシーまたはドメインポリシーによって必要な許可が制限される場合、ナレッジベースの記事 7920862 (https://www.netiq.com/support/kb/doc.php?id=7920862) で説明されている手順に従います。
エラーメッセージが表示されワークロードの検出が失敗する ファイル output.xml が見つかりませんでした または ネットワークパスが見つかりません または (Windows クラスタの検出試行時に) インベントリを検出できませんでした。インベントリ結果で何も返されませんでした。	「output.xml ファイルが見つかりませんでした」というエラーにはいくつかの理由があります。 ◆ ソース上のウイルス対策ソフトウェアが検出を妨げている場合があります。ウイルス対策ソフトウェアを無効にし、これが問題の原因かどうか判断します。137 ページの 「ウイルス対策ソフトウェアの無効化」を参照してください。 ◆ Microsoft ネットワーク向けのファイルおよびプリンタ共有が有効になっていない可能性があります。ネットワークインタフェースカードのプロパティのところでこれを有効にします。 ◆ ソース上の Admin$ 共有にアクセスできない可能性があります。Protect がこれらの共有にアクセスできることを確認します。詳細については、137 ページの 「ファイル / 共有権限およびアクセスの有効化」を参照してください。 ◆ サーバまたはワークステーションのサービスが実行されていない可能性があります。実行されていない場合は、それらを有効にし、起動モードを自動に設定します。 ◆ Windows リモートレジストリサービスが無効です。サービスを開始し、起動タイプを自動に設定します。

14.1.2 OFX コントローラのハートビート起動遅延の変更

タイミングの問題によって発生する検出エラーを回避するため、OFX コントローラに 15 秒 (15000ms) のデフォルトのハートビート起動遅延を設定します。この設定はソースワークロード上に HeartbeatStartupDelayInMS レジストリキーを追加することによって可能になります。このレジストリキーはデフォルトでは設定されていません。

より短い期間またはより長い期間のハートビート遅延を有効にするには :

1. ソースワークロードで、Windows レジストリエディタを開きます。
2. ソースワークロード上のオペレーティングシステムアーキテクチャに応じて、レジストリエディタの次の場所に移動します。

   64 ビットのソースワークロードのパス :

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

   32 ビットのソースワークロードのパス :

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

3. REG_SZ という種類の HeartbeatStartupDelayInMS という名前のキーを追加して、その値を希望のミリ秒数に設定します。デフォルトの設定は 15000 である必要があります。

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

4. ソースワークロードを再起動します。

14.1.3 接続性テストの実行

- 135 ページの 「ネットワークの接続性テスト」
- 135 ページの 「WMI の接続性テスト」
- 136 ページの 「DCOM の接続性のトラブルシューティング」
- 136 ページの 「RPC サービスの接続性のトラブルシューティング」

ネットワークの接続性テスト

この基本的なネットワークの接続性テストを実行し、保護しようとしているワークロードと Protect が通信できるか判断します。

1. ご使用の PlateSpin Server ホストに移動します。
2. コマンドプロンプトを開き、ワークロードに対して ping を行います。

   ping *workload_ip*

WMI の接続性テスト

1. ご使用の PlateSpin Server ホストに移動します。
2. **スタート > ファイル名を指定して実行**の順にクリックし、「Wbemtest」と入力して <Enter> キーを押します。
3. **接続**をクリックします。

4 **名前空間**に、検出しようとしているワークロード名に \root\cimv2 を付加して入力します。たとえば、ホスト名が win2k の場合、次のように入力します。

\\win2k\root\cimv2

5 hostname\LocalAdmin または domain\DomainAdmin のいずれかのフォーマットを使用して適切な資格情報を入力します。

6 **［接続］**をクリックし、WMI 接続をテストします。

エラーメッセージが返されたら、Protect とワークロードの間で WMI 接続が確立できていません。

DCOM の接続性のトラブルシューティング

1 保護するワークロードにログインします。

2 **スタート > ファイル名を指定して実行**をクリックします。

3「dcomcnfg」と入力し、<Enter> キーを押します。

4 次の手順で接続性を確認します。

- Windows システム (XP/Vista/2003/2008/7) の場合、[コンポーネント サービス] ウィンドウが表示されます。コンポーネントサービス管理ツールのコンソールツリーに含まれる**コンピュータ**フォルダで、DCOM 接続性のチェックをするコンピュータを右クリックし、**プロパティ**をクリックします。**既定のプロパティ**タブをクリックし、**このコンピュータ上で分散 COM を有効にする**が選択されていることを確認します。
- Windows 2000 Server マシン上で、［DCOM Configuration (DCOM の構成)］ダイアログが表示されます。**既定のプロパティ**タブをクリックし、**このコンピュータ上で分散 COM を有効にする**が選択されていることを確認します。

5 DCOM が有効でない場合は有効にし、サーバを再起動するか、Windows Management Instrumentation サービスを再起動します。その後、再度ワークロードを追加してください。

RPC サービスの接続性のトラブルシューティング

RPC サービスには次の 3 種類の潜在的な妨害物があります。

- Windows サービス
- Windows ファイアウォール
- ネットワークファイアウォール

Windows サービスの場合、ワークロード上で RPC サービスが実行中であることを確認します。サービスパネルにアクセスするには、コマンドプロンプトから services.msc を実行します。Windows ファイアウォールの場合、次の方法を試すことができます。ハードウェアファイアウォールの場合、次の方法を試すことができます。

- Protect およびワークロードをファイアウォールの同じ側に置く
- Protect とワークロードの間の特定のポートを開く (31 ページの「保護ネットワークにわたるアクセスおよび通信の要件」を参照)

14.1.4 ウイルス対策ソフトウェアの無効化

ウイルス対策ソフトウェアは、時々、WMI とリモートレジストリ関連の Protect の機能をブロックします。ワークロードインベントリが正常に行われるようにするためには、まずワークロードでウイルス対策サービスを無効にする必要があります。

さらに、ウイルス対策ソフトウェアは、特定のプロセスや実行ファイルへのアクセスのみを許可し、特定のファイルへのアクセスをロックする場合があります。このロックにより、ファイルベースのデータレプリケーションが妨害されてしまう場合があります。そのような場合は、ワークロード保護を設定する際にウイルス対策ソフトウェアによってインストールされ使用されるサービスなどを選択して無効化できます。これらのサービスはファイル転送中のみ無効化され、転送プロセスが終了すると再開されます。サービスの無効化は、ブロックベレルのデータレプリケーションでは不要です。

14.1.5 ファイル / 共有権限およびアクセスの有効化

ワークロードを正常に保護するには、PlateSpin Protect を正常に展開し、ソフトウェアをワークロード内にインストールする必要があります。これらのコンポーネントをワークロードに展開するにあたり、さらにはワークロードの追加プロセスで、Protect はワークロードの管理共有を使用します。Protect は、共有に対して管理者アクセスが必要です。そのためには、ローカル管理者アカウントまたはドメイン管理者アカウントを使用します。

管理共有が有効であることを確認するには :

1. デスクトップ上の**マイコンピュータ**右クリックし、**管理**を選択します。
2. **システムツール > 共有フォルダ > 共有**の順に展開します。
3. Shared Folders ディレクトリの中には、他の共有とともに Admin$ が表示されるはずです。

共有が有効になっていることを確認したら、PlateSpin Server ホスト内部からそれらにアクセスできることを確認します。

1. ご使用の PlateSpin Server ホストに移動します。
2. **スタート > 名前を指定して実行**の順にクリックし、「\\< サーバホスト >\Admin$」と入力し、**OK** をクリックします。
3. 要求されたら、Protect ワークロードインベントリにワークロードを追加するのに使用するのと同様の資格情報を使用します。

   ディレクトリが開き、その内容を参照して変更できます。
4. IPC$ 共有を除くすべての共有に、このプロセスを繰り返します。

   Windows は、資格情報の検証および認証の目的で IPC$ 共有を使用します。この共有は、ワークロード上のフォルダまたはファイルにマップされていないので、テストは常に失敗しますが、共有が表示されることには変わりありません。

PlateSpin Protect はボリュームの既存の内容を変更しませんが、アクセスと権限が必要な独自のディレクトリを作成します。

14.2 Linux ワークロードの検出のトラブルシューティング

問題またはメッセージ	解決方法
<IP_address> 上で実行中の SSH サーバのみならず、<ip_address>/sdk の VMware 仮想インフラ Web サービスのいずれにも接続できません。	このメッセージにはさまざまな原因があります。 ◆ ワークロードに到達できません。 ◆ ワークロードで SSH が実行されていません。 ◆ ファイアウォールがオンで、必要なポートが開いていません。 ◆ ワークロードの特定のオペレーティングシステムがサポートされません。 ワークロードのネットワークとアクセス要件については、31 ページの「保護ネットワークにわたるアクセスおよび通信の要件」を参照してください。
アクセスが拒否されました	この認証の問題は、ユーザ名が無効であるか、パスワードが無効であるかのいずれかを示します。適切なワークロードアクセス資格情報については、167 ページの 「ワークロードおよびコンテナの資格情報向けのガイドライン」を参照してください。

14.3 ターゲットホスト検出のトラブルシューティング

問題またはメッセージ	解決方法
ESXi 4.1 の場合、dvSwitch ポートグループが同じ名前を共有している場合、直接的にホスト検出を行うと VM ポートグループの欠落が発生します。	ポートグループ名がターゲット VMware ホストで固有であることを確認してください。

B Protect によってサポートされている Linux ディストリビューション

PlateSpin Protect ソフトウェアには、多数の非デバッグ Linux ディストリビューション (32 ビットおよび 64 ビット) 用に、事前コンパイルされたバージョンの blkwatch ドライバが付属しています。

B.1 Linux ワークロードの分析

PlateSpin Protect に Linux ディストリビューション用の blkwatch ドライバが付属しているかどうかを判断する前に、Linux ワークロードのカーネルに関する理解を深め、サポートされているディストリビューションのリストでそのカーネル名を検索する必要があります。

B.1.1 リリース文字列の決定

ワークロードの Linux 端末で、次のコマンドを実行して、Linux ワークロードのカーネルのリリース文字列を決定できます。

uname -r

たとえば、uname -r を実行する場合、次の出力が表示される場合があります。

3.0.76-0.11-default

ディストリビューションのリストを検索すると、この文字列に一致する次の 2 つのエントリがあることがわかります。

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

検索結果は、この製品には 32 ビット (x86) および 64 ビット (x86_64) アーキテクチャのドライバがあることを示しています。

B.1.2 アーキテクチャの決定

ワークロードの Linux 端末で次のコマンドを実行することにより、Linux ワークロードのアーキテクチャを決定できます。

uname -m

たとえば、uname -m を実行すると、次の出力が表示される場合があります。

x86_64

この情報を使用して、ワークロードのアーキテクチャが 64 ビットであるかどうかを判断できます。

B.2 Linux ディストリビューション用に事前コンパイルされた blkwatch ドライバ

PlateSpin Protect には、多数の非デバッグ Linux ディストリビューションに対応した、事前コンパイル済みの blkwatch ドライバが用意されています。ディストリビューションのリストを検索して、Linux ワークロードカーネルのリリース文字列とアーキテクチャが、リスト内のサポートされているディストリビューションに一致するかどうかを判断できます。リリース文字列とアーキテクチャが見つかった場合、PlateSpin Protect には事前コンパイルされたバージョンの blkwatch ドライバが含まれています。

検索が成功しない場合は、ナレッジベースの記事 7005873 の手順に従ってカスタム blkwatch ドライバを作成できます。自己コンパイルドライバは、ディストリビューションのリストに記載された Linux のメジャーおよびマイナーカーネルバージョン、またはそのパッチ適用済みバージョンでのみサポートされます。Linux ワークロードカーネルのリリース文字列のメジャーおよびマイナーカーネルバージョンがリストに記載されたメジャーおよびマイナーカーネルバージョンに一致する場合、自己コンパイルドライバはサポートされます。

- 140 ページのセクション B.2.1「リスト項目の構文」
- 140 ページのセクション B.2.2「ディストリビューションのリスト」
- 141 ページのセクション B.2.3「blkwatch ドライバを使用する他の Linux ディストリビューション」

B.2.1 リスト項目の構文

リストの各項目は、次の構文を使用してフォーマットされます。

<Distro>-<Patch>-<Kernel_Release_String>-<Kernel_Architecture>

したがって、32 ビット (x86) アーキテクチャの 2.6.5-7.139-bigsmp のカーネルリリース文字列を含む SLES 9 SP1 ディストリビューションの場合、次のようなフォーマットで項目が一覧表示されます。

SLES9-SP1-2.6.5-7.139-bigsmp-x86

B.2.2 ディストリビューションのリスト

サポートされているカーネルディストリビューションのリストについては、『*PlateSpin Protect ユーザガイド*』「のディストリビューションのリスト」(https://www.netiq.com/documentation/platespin-protect-11-2-1/protect_user/data/blkwatch-drivers.html#blkwatch-dist-list) を参照してください。

B.2.3 blkwatch ドライバを使用する他の Linux ディストリビューション

ディストリビューションが Red Hat Enterprise Linux または SUSE Linux Enterprise Server のサポートされているリリースバージョンに基づいている場合、PlateSpin Protect では、表 B-1 に示されているその他の Linux ディストリビューションがサポートされます。サポートされている Linux ディストリビューション用に事前コンパイルされた blkwatch ドライバを使用することができます。

表 B-1 *その他の Linux ディストリビューション用の Blkwatch ドライバのサポート*

その他の Linux ディストリビューション	RHEL または SLES 用のサポートされているリリースバージョンに基づく	備考
CentOS	Red Hat Enterprise Linux	
Open Enterprise Server (OES)	SUSE Linux Enterprise Server 11 SP 1 以降	OES 11 SP2 のデフォルトのカーネルバージョン 3.0.13 はサポートされていません。ワークロードのインベントリを実行する前に、バージョン 3.0.27 以降のカーネルにアップグレードしてください。
Oracle Linux (OL) (旧称 : Oracle Enterprise Linux (OEL))	Red Hat Enterprise Linux	Blkwatch のドライバは、標準のカーネルおよび 140 ページのセクション B.2.2「ディストリビューションのリスト」に記載されている Unbreakable Enterprise Kernel (UEK) で利用可能です。その他の Oracle Linux ディストリビューションについては、対応する Red Hat Compatible Kernel (RHCK) に対してのみ事前コンパイル済みのドライバが使用できます。 PlateSpin Protect 11.2 以前のバージョンでは、Oracle Linux Unbreakable Enterprise Kernel を使用したワークロードはサポートされていません。

サポートされているカーネルディストリビューションのリストについては、『*PlateSpin Protect ユーザガイド*』「のディストリビューションのリスト」(https://www.netiq.com/documentation/platespin-protect-11-2-1/protect_user/data/blkwatch-drivers.html#blkwatch-dist-list) を参照してください。

C クラスタノードにおけるローカルストレージのシリアル番号の同期

このセクションでは、保護する Windows クラスタの各ノードでローカルボリュームシリアル番号が一致するように変更するための手順について詳しく説明します。ボリュームマネージャユーティリティ (VolumeManager.exe) を使用して、クラスタノードのローカルストレージでシリアル番号を同期する方法についても説明します。

ユーティリティをダウンロードして実行するには :

1. PlateSpin Protect ダウンロードページから VolumeManager.exe ファイルをダウンロードします。
   - **1a** Micro Focus Downloads (Micro Focus ダウンロード) (https://www.microfocus.com/support-and-services/download/) に移動します。
   - **1b** **Browse by Product (製品別の参照)** リストから PlateSpin Protect を選択するか、**Browse by Product (製品別の参照)** フィールドに製品名を入力して、製品を見つけて選択します。
   - **1c** リリースのリストがある場合は、PlateSpin Protect 11.2.1 を選択します。
   - **1d** [Download overview (ダウンロードの概要)] ページで **proceed to download (ダウンロードの続行)** をクリックして、カスタマアカウント資格情報でログインします。
   - **1e** 米国輸出管理規則を受け入れ、同意するには、**accept (同意する)** をクリックします。
   - **1f** [ダウンロード] ページで、VolumeManager.exe ファイルの横にある**ダウンロード**をクリックして、ファイルを保存します。
2. ダウンロードしたファイルを各クラスタノードのアクセス可能な場所にコピーします。
3. クラスタのアクティブノードで、管理コマンドプロンプトを開き、ダウンロードされたユーティリティの場所に移動して、次のコマンドを実行します。

   VolumeManager.exe -l

   ローカルボリュームとそれらの各シリアル番号のリストが表示されます。次に例を示します。

   ```
   Volume Listing: -------------------- DriveLetter (*:) VolumeId="System
   Reserved" SerialNumber: AABB-CCDD DriveLetter (C:) VolumeId=C:\ SerialNumber:
   1122-3344
   ```

   後から比較するために、これらのシリアル番号をメモするか、表示されたままにします。
4. アクティブノードのすべてのローカルストレージシリアル番号がクラスタ内の他のノードのローカルストレージシリアル番号と一致していることを確認します。
   - **4a** 各クラスタノードで、VolumeManager.exe -l コマンドを実行し、そのボリュームシリアル番号を取得します。
   - **4b** アクティブノード (ステップ 3) のローカルストレージシリアル番号ノード (ステップ 4a) のローカルストレージシリアル番号と比較します。
   - **4c** (条件) アクティブノードとこのノードのシリアル番号が違う場合は、このノードに伝播するシリアル番号をメモして、次のコマンドを実行して設定し、その後シリアル番号を確認します。

     VolumeManager -s <VolumeId> <*serial-number*>

次の 2 つの例は、このコマンドの使用方法を示しています。

- VolumeManager -s "System Reserved" AAAA-AAAA
- VolumeManager -s C:\ 1111-1111

4d クラスタのノードのボリュームシリアル番号がすべて正常に変更されたら、そのノードを再起動する必要があります。

4e クラスタの各ノードに対してステップ 4a からステップ 4d を繰り返します。

5 (条件) クラスタがすでに PlateSpin 環境内で保護されている場合は、アクティブノードでフルレプリケーションを実行して、すべての変更をデータベースへ確実に伝播することをお勧めします。

D Protect Agent ユーティリティ

Protect Agent は、ブロックベース転送ドライバのインストール、アップグレード、クエリ、またはアンインストールを実行するために使用できるコマンドラインユーティリティです。

ドライバをインストール、アンインストール、またはアップグレードしたときは常に再起動が必要ですが、Protect Agent ユーティリティを使用すると、これらの操作を実行するタイミングを柔軟に制御できるため、サーバが再起動されるタイミングも柔軟に制御できます。たとえば、このユーティリティを使用して、最初のレプリケーション時ではなくスケジュールされたダウンタイム時にドライバをインストールできます。

- 145 ページのセクション D.1「Windows 用の Protect Agent ユーティリティの使用」
- 146 ページのセクション D.2「Protect Agent とブロックベース転送ドライバの併用」

D.1 Windows 用の Protect Agent ユーティリティの使用

Windows 用の Protect Agent ユーティリティをソースワークロードにダウンロードするには :

1. ソース Windows コンピュータに管理者ユーザとしてログインします。
2. Web ブラウザで、Web インタフェースを起動してログインします。
3. **ダウンロード**タブをクリックします。
4. Windows ターゲットプラットフォームの Protect Agent アプリケーションのリンクをクリックして、圧縮されている ProtectAgent.cli.exe ファイルを保存します。
5. ファイルのコンテンツを解凍し、実行可能なファイルにアクセスします。
6. (オプション) 次を入力して Protect Agent のヘルプを表示します

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

このユーティリティは、PlateSpin Server ホストで圧縮されたファイルとして入手できます。ファイルのコンテンツを解凍し、実行可能なファイルにアクセスします。

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

Windows 用の Protect Agent ユーティリティを実行するための構文は次のとおりです。

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

表 D-1 では、ProtectAgent.cli.exe コマンドで使用できるコマンド、コマンドオプション、およびスイッチについて説明しています。

表 D-1 *Windows 用の Protect Agent ユーティリティのコマンド、コマンドオプション、およびスイッチ*

使用率	説明
コマンド	
h |? | help	このコマンドの使用方法とオプションを表示します。

使用率	説明
logs|view-logs	アプリケーションログディレクトリを開きます。
status /status [/psserver=%IP%]	このワークロード上の PlateSpin コントローラおよびドライバのインストールステータスを表示します。 PlateSpin Server を指定する場合、サーバからドライバアップグレードが確認されます。
din|driver-install /din [/psserver=%IP%]	PlateSpin ドライバをインストールします。 PlateSpin Server を指定する場合、サーバからドライバアップグレードが確認されます。
dup|driver-upgrade /dup [/psserver=%IP%]	PlateSpin ドライバをアップグレードします。 PlateSpin Server を指定する場合、サーバからドライバアップグレードが確認されます。
dun|driver-uninstall [/dun /psserver=%IP%]	PlateSpin ドライバをアンインストールします。
con | config /con /setting=<*setting_name*>:<*value*> 例 : `ProtectAgent.cli.exe /config /setting=psserver:10.10.10.202`	このワークロード上の設定ファイルで変更する設定名とその値を指定します。 psserver オプションは、OFX コントローラ (ofxcontroller) サービスを停止し、OfxController.exe.config ファイルを変更して新しい IP アドレスを指定した後、サービスを再起動します。PlateSpin Server のパブリック IP アドレスを変更する場合は、サーバに対して設定されているそれぞれのソースワークロードでこのコマンドを実行する必要があります。
スイッチ	
/psserver=%IP%	status、driver-install、または driver-upgrade の各オプションの呼び出し時に、指定されたサーバからブロックベース転送ドライバをダウンロードします。
コマンドオプション	
設定 /setting=<*setting_name*>:<*value*>	変更する環境設定の設定名と値を指定します。 サポートされる設定名は次のとおりです。 psserver altAddress heartbeat

D.2 Protect Agent とブロックベース転送ドライバの併用

Protect Agent ユーティリティには、ブロックベース転送ドライバがバンドルされています。別の方法として、status、driver-install、または driver-upgrade の各オプションの呼び出し時に PlateSpin Server からドライバをダウンロードするために、/psserver= コマンドラインスイッチを指定することができます。この方法は、サーバには新しいドライバパッケージでパッチが適用されていても、Protect Agent コマンドラインユーティリティにはパッチが適用されていない場合に便利です。

注 : 混乱を避けるために、Protect Agent を使用する場合は、ドライバをインストール、アンインストール、またはアップグレードした後、レプリケーションを実行する前に再起動することをお勧めします。

ソースワークロードは、ドライバをインストール、アップグレード、またはアンインストールするたびに再起動する必要があります。再起動により、実行中のドライバは停止し、新しいドライバがシステム再起動時に適用されます。レプリケーションの前にシステムを再起動しなかった場合、ソースはそれらの操作が完了していないかのように動作を続行します。たとえば、ドライバをインストールした後でシステムを再起動しなかった場合、ソースは、レプリケーション中にインストールされたドライバがないかのように動作します。同様に、ドライバをアップグレードした後で再起動しなかった場合、ソースは、システムを再起動するまで実行中のドライバをレプリケーション時に使用し続けます。

インストールされたドライバのバージョンと実行中のドライバのバージョンが異なる場合、status オプションの出力によって、再起動が必要であることが示されます。次に例を示します。

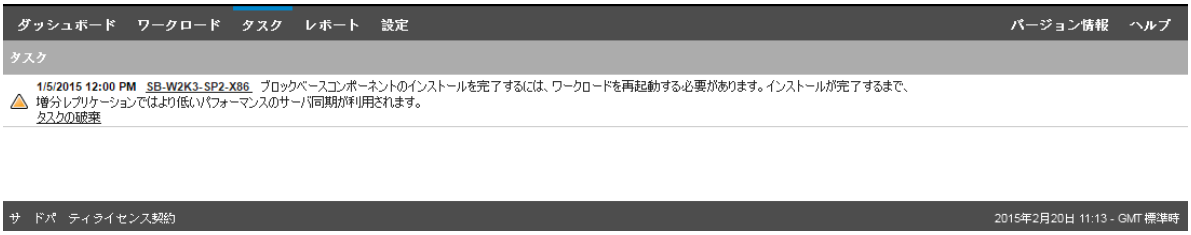
```
C:\ProtectAgent\ProtectAgent.cli.exe status
Step 1 of 2: Querying the PlateSpin controller service
   Done
Step 2 of 2: Querying the installed PlateSpin driver version
   Done

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

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

PlateSpin は、ドライバのインストールまたはアップグレードを完了するために再起動が必要であることをユーザに警告するタスクを作成します。この通知は、［Tasks (タスク)］リスト (図 D-1) に表示されます。

図 D-1　再起動通知タスク



レプリケーション中は、この通知が［コマンドの詳細］ページ (図 D-2) に表示されます。

図 D-2　レプリケーション中の再起動通知

ソースマシンを再起動すると、インストールまたはアップグレードしたドライバが適用されて起動します。ドライバが最近インストールされた場合、ソースのすべての変更が反映されていることを保証するために、再起動後に完全レプリケーションまたはサーバ同期レプリケーションを 1 回実行

する必要があります。このサーバ同期レプリケーション要件は、図 D-3 に示されているように、［ステータス］フィールドで警告として表示されます。後続の増分レプリケーションは警告なしでスケジュールどおりに完了します。

図 D-3　サーバ同期の必要性の通知

IV ワークロードの保護

ターゲットとワークロードを検出した後で、ワークロードの保護コントラクトを設定することにより、保護の準備が整います。

15 ワークロードの保護と回復

PlateSpin Protect は、保護ワークロードのレプリカを作成し、定義したスケジュールに基づいてそのレプリカを定期的に更新します。

レプリカ、すなわち「フェールオーバーワークロード」とは、PlateSpin Protect によって管理される仮想マシンのことで、運用サイトで中断が生じた場合に運用ワークロードのビジネス機能を引き継ぎます。

15.1 ワークロード保護の前提条件

保護のためのコンテナとワークロードの準備詳細については、95 ページのパート III「保護ターゲットとソースの準備」を参照してください。

Active Directory ドメインでは、最初の完全レプリケーションを実行する前に以下のベストプラクティスに従ってください。

- 最初の完全レプリケーションを実行する前に、ソースワークロードで Windows を更新 (Windows Update を実行) していることを確認してください。
- 「*Microsoft KB 822158 記事: 現在サポートされている Windows のバージョンを実行しているエンタープライズコンピュータにおけるウィルススキャンの推奨事項* (https://support.microsoft.com/en-us/kb/822158)」の推奨に従って、ファイルとフォルダの除外をウィルス対策ソフトウェアで設定していることを確認します。
- Windows マシンがドメインコントローラの場合、レプリケーション中はシステムでウィルス対策ソフトウェアを無効にしていることを確認してください。

15.2 保護詳細の設定およびレプリケーションの準備

保護詳細は、ワークロード保護と回復設定、および保護されているワークロードのライフサイクル全体にわたる動作を制御します。保護と回復ワークフローの各段階 (インベントリの追加、最初のレプリケーションおよび継続的なレプリケーション、フェールオーバー、フェールバック、および再保護) で、関連する設定が保護の詳細から確認されます。39 ページの 「ワークロードの保護と回復の基本ワークフロー」を参照してください。ワークロードの保護の完全なライフサイクルに関連する現在アクティブな設定の収集は、ワークロードの「保護コントラクト」と呼ばれています。.

ワークロードの保護詳細を設定するには :

1 コンテナを追加します。98 ページの 「コンテナ (保護ターゲット) の追加」を参照してください。

2 ワークロードを追加します。102 ページの 「ワークロード (保護ソース) の追加」を参照してください。

3 [ワークロード] ページで、必要なワークロードを選択し**設定**をクリックします。

または、ワークロードの名前をクリックします。

注 : PlateSpin Protect インベントリにまだコンテナがない場合は、コンテナの追加を求めるプロンプトが表示されます。下部にある**コンテナの追加**をクリックして、コンテナを追加します。

---

4 **初期レプリケーション方法**を選択します。これは、ワークロードからフェールオーバー VM にボリュームデータを完全に転送するか、既存の VM 上のボリュームと同期するかを示します。詳細については、170 ページの 「初期レプリケーション方法 (フルおよび差分)」を参照してください。

5 保護ターゲットを割り当てます。これは、コンテナか、初期のレプリケーション方法に**増分レプリケーション**を選択した場合は、*準備された*ワークロードにすることができます。詳細については、170 ページの 「初期レプリケーション方法 (フルおよび差分)」を参照してください。

注 : インベントリにコンテナが 1 つしかない場合は、そのコンテナにワークロードが自動的に割り当てられます。

---

6 ビジネスの継続性のニーズによって決定される設定の各セットの保護詳細を設定します。154 ページの 「ワークロード保護の詳細」を参照してください。

7 PlateSpin Protect Web インタフェースによって検証エラーが表示された場合、これを修正します。

8 **保存**をクリックします。

または、**保存して準備**をクリックします。これにより、設定が保存されると同時に**レプリケーションの準備**コマンド (必要に応じてデータ転送ドライバをソースワークロードにインストールし、ワークロードの初期 VM レプリカを作成) が実行されます。

プロセスが終了するのを待ちます。終了したら、**ワークロード環境設定が完了しました**イベントがダッシュボード上に表示されます。

15.2.1 ワークロード保護の詳細

ワークロード保護の詳細は、表 15-1 に示す 5 つのパラメータセットによって表されます。

左側にあるアイコンをクリックすると、各パラメータセットを展開したり、縮小したりできます。

表 15-1　ワークロード保護の詳細

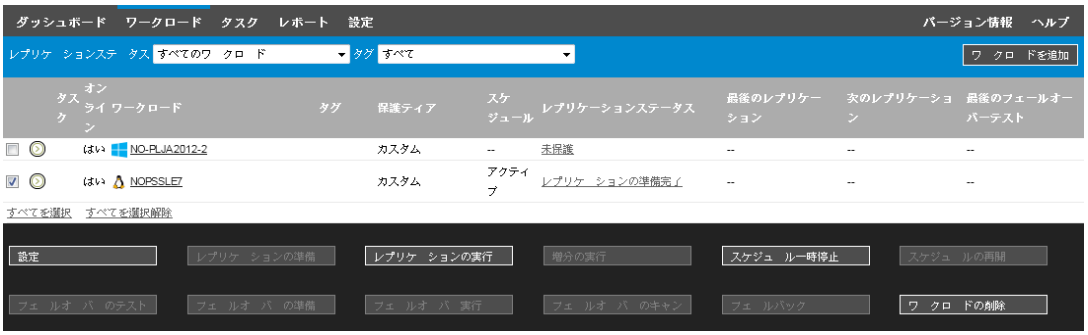
パラメータの設定	Details (詳細)
Tier Settings (ティアの設定)	
保護ティア	現在の保護が使用する保護ティアを指定します。詳細については、168 ページの 「保護ティア」を参照してください。
レプリケーション設定	
転送方法	(Windows) ファイルベースまたはブロックベースのデータ転送メカニズムを選択します。ブロックベースコンポーネントを使用するブロックレベルレプリケーションと使用しないブロックレベルレプリケーションの詳細については、24 ページの 「サポートされるデータ転送方法」を参照してください。 暗号化を有効にするには、**データ転送の暗号化**オプションを選択します。25 ページの 「転送におけるデータの暗号化」を参照してください。
暗号の転送	(Linux) 暗号化を有効にするには、**データ転送の暗号化**オプションを選択します。詳細については、25 ページの 「転送におけるデータの暗号化」を参照してください。
ソース資格情報	ワークロードにアクセスするために必要な資格情報を指定します。詳細については、167 ページの 「ワークロードおよびコンテナの資格情報向けのガイドライン」を参照してください。
CPU	(最小の VM ハードウェアレベル 8 で VMware 5.1、5.5、および 6.0 を使用する VM コンテナ) フェールオーバーワークロードに対し、ソケット数およびソケットあたりのコア数を指定します。合計コア数は自動的に計算されます。このパラメータは、初期レプリケーション設定である**完全**とともにワークロードの初期セットアップに適用されます。 **注 :** ワークロードが使用できるコアの最大数は、外部的な要因によって変わります。たとえば、ゲストオペレーティングシステム、VM のハードウェアバージョン、ESXi ホストの VMware ライセンス、vSphere の ESXi ホストの計算リソースの上限 (「*vSphere 5.1 Configuration Maximums* (http://www.vmware.com/pdf/vsphere5/r51/vsphere-51-configuration-maximums.pdf)」を参照) などです。 ゲスト OS のディストリビューションによっては、コア数およびソケットあたりのコア数の設定が遵守されない場合があります。たとえば、SLES 10 SP4 および OES 2 SP3 を使用するゲスト OS では、インストールされている本来のコア数とソケットの設定が保持されます。一方、SLES、RHEL、および OES の他のディストリビューションでは、この設定が遵守されます。
CPU の数	(VMware 4.1 を使用する VM コンテナ) フェールオーバーワークロードに割り当てる必要がある vCPU (仮想 CPU) の数を指定します。このパラメータは、初期レプリケーション設定である**完全**とともにワークロードの初期セットアップに適用されます。各 vCPU は、VM コンテナ上のゲスト OS には、1 つのコア、1 つのソケットとして表示されます。

パラメータの設定	Details (詳細)
レプリケーションネットワーク	レプリケーションのトラフィックを、VM コンテナで定義されている仮想ネットワークに基づいて分離します。詳細については、174 ページの「ネットワーキング」を参照してください。 この設定では、PlateSpin Protect Linux RAM ディスク (LRD) レプリケーションネットワークが使用する MTU 値も指定できます。この値を設定すると、小さめの MTU 値が設定されているネットワーク (VPN など) 上で超過送信が発生するのを避けることができます。デフォルト値は空の文字列です (テキストボックスには何も表示されません)。LRD でネットワーキングが設定されている場合、ネットワークデバイスで独自にデフォルト値 (通常は 1500) を設定できます。値を入力した場合、PlateSpin Protect は、ネットワークインタフェースを設定する際に MTU を調整します。
Allowed Networks (許可されているネットワーク)	レプリケーショントラフィックに使用する送信元の 1 つまたは複数のネットワークインタフェース (NIC または IP アドレス) を指定します。
Resource Pool for Target VM (ターゲット VM のリソースプール)	(VM コンテナは DRS クラスタの一部です) フェールオーバー VM を作成するリソースプールの場所を指定します。
VM Folder for Target VM (ターゲット VM の VM フォルダ)	(VM コンテナは DRS クラスタの一部です) フェールオーバー VM を作成する VM フォルダの場所を指定します。
Configuration File Datastore (環境設定ファイルのデータストア)	VM 環境設定ファイルの保存用に、VM コンテナに関連付けられているデータストアを選択します。詳細については、169 ページの 「復旧ポイント」を参照してください。
保護ボリューム	保護するボリュームを選択し、VM コンテナの特定のデータストアにそれらのレプリカを割り当てます。
Thin Disk (シンディスク)	シン仮想ディスク機能を有効にする場合に選択します。それにより仮想ディスクがサイズ設定された VM として表示されますが、そのディスク上のデータで実際に必要なディスクスペースのみを消費します。
Protected Logical Volumes (保護する論理ボリューム)	(Linux) Linux ワークロードまたは Open Enterprise Server ワークロード上の NSS プールについて保護対象となる 1 つ以上の LVM 論理ボリュームを指定します。
Non-volume Storage (非ボリュームストレージ)	(Linux) ソースワークロードに関連付けるストレージ領域 (スワップパーティションなど) を指定します。このストレージは、フェールオーバーワークロードで再作成されます。
Volume Groups (ボリュームグループ)	(Linux) レプリケーション設定の［Protected Logical Volumes (保護する論理ボリューム) (保護する論理ボリューム)］セクションにリストされている LVM 論理ボリュームと一緒に保護する LVM ボリュームグループを指定します。
レプリケーション中のサービス / デーモン状態の停止	レプリケーション中に自動停止する Windows サービスまたは Linux デーモンを選択します。詳細については、171 ページの 「サービスおよびデーモンの制御」を参照してください。
フェールオーバーの設定	
VM メモリ	フェールオーバーワークロードに割り当てられるメモリの量を指定します。

パラメータの設定	Details (詳細)
Hostname and Domain/Workgroup affiliation (ホスト名およびドメイン / ワークグループの加入)	フェールオーバーワークロードがライブのときの識別情報およびドメイン / ワークグループの加入を指定します。ドメインの加入には、ドメイン管理者の資格情報が必要です。
Network Connections	フェールオーバーワークロードの LAN 設定を指定します。詳細については、174 ページの 「ネットワーキング」を参照してください。
DNS サーバ	プライマリ DNS サーバおよび代替 DNS (オプション) の IP アドレスを指定します。
サービス / デーモンの状態の変更	特定のアプリケーションサービス (Windows) またはデーモン (Linux) の起動状態を指定します。171 ページの 「サービスおよびデーモンの制御」を参照してください。
Prepare for Failover Settings (フェールオーバーの準備設定)	
Temporary Failover Network (一時フェールオーバーネットワーク)	オプションのフェールオーバーの準備操作中におけるフェールオーバーワークロードの一時的な LAN 設定を指定します。174 ページの 「ネットワーキング」を参照してください。
テストフェールオーバー設定	
VM メモリ	必要な RAM を一時ワークロードに割り当てます。
ホスト名	ホスト名を一時ワークロードに割り当てます。
ドメイン / ワークグループ	一時ワークロードをドメインまたはワークグループに加入させます。ドメインの加入には、ドメイン管理者の資格情報が必要です。
Network Connections	一時ワークロードの LAN 設定を指定します。詳細については、174 ページの 「ネットワーキング」を参照してください。
DNS サーバ	プライマリ DNS サーバおよび代替 DNS (オプション) の IP アドレスを指定します。
サービス / デーモンの状態の変更	特定のアプリケーションサービス (Windows) またはデーモン (Linux) の起動状態を指定します。詳細については、171 ページの 「サービスおよびデーモンの制御」を参照してください。
タグ	
タグ	(オプション) このワークロードにタグを割り当てます。103 ページの「ワークロードのタグ付け」を参照してください。

15.3 ワークロード保護の開始

ワークロード保護は、**レプリケーションの実行**コマンドで開始されます。



次の後に［レプリケーションの実行］コマンドを実行できます。

- ワークロードの追加。
- ワークロードの保護詳細の設定。
- 初めてのレプリケーションの準備。

続行する準備ができたら、次の手順に従います。

1 ［ワークロード］ページで必要なワークロードを選択し、**レプリケーションの実行**をクリックします。

2 **実行**をクリックします。

PlateSpin Protect によって実行が開始され、**データのコピー**手順のプロセスインジケータが表示されます。

注 : ワークロードが保護された後 :

- ブロックレベル保護下のボリュームサイズの変更は、保護を無効にします。適切な手順は以下のとおりです。
  1. 保護からワークロードを削除します。
  2. 必要に応じてボリュームサイズを変更します。
  3. ワークロードを再び追加し、保護の詳細を設定し、そしてレプリケーションを開始することによって、保護を再確立します。
- 保護されたワークロードで重要な変更では、保護を再設定することが必要です。たとえば、保護下のワークロードへのボリュームまたはネットワークの追加などです。

15.4 コマンドの中止

コマンドを実行した後、そのコマンドが実行中でも、特定のコマンドの［コマンドの詳細］ページでコマンドを中止できます。

実行中の任意のコマンドの［コマンドの詳細］ページにアクセスするには :

1 ［ワークロード］ページに移動します。

2 必要なワークロードを探し、そのワークロードで現在実行中のコマンド (Running Incremental (増分の実行中) など) を表すリンクをクリックします。

Web インタフェースに、該当する［コマンドの詳細］ページが表示されます。

3 中止をクリックします。

15.5 フェールオーバー

「フェールオーバー」操作では、PlateSpin Protect VM コンテナ内のフェールオーバーワークロードは、失敗した運用ワークロードのビジネス機能を引き継ぎます。

- 159 ページのセクション 15.5.1「オフラインワークロードの検出」
- 160 ページのセクション 15.5.2「フェールオーバーの実行」
- 160 ページのセクション 15.5.3「フェールオーバー機能のテストの使用」

15.5.1 オフラインワークロードの検出

PlateSpin Protect は、保護されたワークロードを絶えず監視しています。事前設定した回数だけワークロードの監視が失敗した場合、PlateSpin Protect によってワークロードはオフラインですイベントが生成されます。ワークロードの障害を判断しログに記録する基準は、ワークロード保護のティア設定に含まれています。「Tier Settings (ティアの設定)」の中の 154 ページの 「ワークロード保護の詳細」行を参照してください。

SMTP 設定とともに通知が設定された場合、PlateSpin Protect は指定した受信者に同時に通知メールを送信します。68 ページの 「イベントおよびレプリケーションレポートの電子メール通知サービスの設定」を参照してください。

レプリケーションのステータスがアイドルの間にワークロードの障害が検出されたら、フェールオーバーの実行コマンドに進むことができます。増分が実施されている最中にワークロードに障害が発生した場合、ジョブが行き詰まります。このような場合、コマンドを中止して (158 ページの 「コマンドの中止」を参照)、フェールオーバーの実行コマンドに進みます。詳細については、160 ページの 「フェールオーバーの実行」を参照してください。

図 15-1 は、ワークロードの障害を検出した際の Web インタフェースの［ダッシュボード］ページを示します。［タスクおよびイベント］ペインの中の該当するタスクに注目します。

図 15-1 *ワークロードの障害を検出した際のダッシュボードページ (「ワークロードはオフラインです」)*

15.5.2 フェールオーバーの実行

フェールオーバーワークロードのネットワーク ID および LAN 設定を含むフェールオーバーの設定は、設定時にワークロードの保護詳細とともに保存されます。154 ページの 「ワークロード保護の詳細」の「フェールオーバーの設定」を参照してください。

次の方法を使用してフェールオーバーを実行できます。

- ［ワークロード］ページで必要なワークロードを選択して**フェールオーバーの実行**をクリックします。
- ［Tasks and Events (タスクおよびイベント)］ペインの中の**ワークロードはオフラインです**イベントの対応するコマンドのハイパーリンクをクリックします。詳細については、図 15-1 を参照してください。
- **フェールオーバーの準備**コマンドを実行し、前もってフェールオーバー VM をブートします。この時点ではまだフェールオーバーをキャンセルすることができます (ステージドフェールオーバーの場合に便利)。

これらのいずれかの方法を使用してフェールオーバープロセスを開始し、フェールオーバーワークロードに適用する復旧ポイントを選択します (169 ページの 「復旧ポイント」を参照)。**実行**をクリックし、進行状況を監視します。終了すると、ワークロードのレプリケーション状態が**ライブ**を示すはずです。

計画された障害復旧の訓練の一環としてフェールオーバーワークロードをテストする、またはフェールオーバープロセスをテストするには、160 ページの 「フェールオーバー機能のテストの使用」を参照してください。

15.5.3 フェールオーバー機能のテストの使用

PlateSpin Protect には、フェールオーバー機能およびフェールオーバーワークロードの整合性をテストする機能が含まれています。これは、**フェールオーバーのテスト**コマンドを使用して実行されます。このコマンドは、フェールオーバーの機能をテストしてフェールオーバーワークロードの整合性を検証するために、分離したネットワーク環境でフェールオーバーワークロードを起動します。

コマンドを実行すると、PlateSpin Protect によってワークロード保護の詳細に保存された［Test Failover Settings (フェールオーバーのテスト設定)］がフェールオーバーワークロードに適用されます。154 ページの 「ワークロード保護の詳細」の「テストフェールオーバー設定」を参照してください。

フェールオーバーのテスト機能を使用するには :

1. テスト用に適切な時間帯を定義し、レプリケーションが確実に行われないようにします。ワークロードのレプリケーション状態は**アイドル**になります。
2. ［ワークロード］ページで必要なワークロードを選択し、**フェールオーバーのテスト**をクリックして、復旧ポイントを選択し (169 ページの 「復旧ポイント」を参照)、**実行**をクリックします。

   終了すると、PlateSpin Protect によって対応するイベントおよびタスクが一連の適切なコマンドとともに生成されます。

3 フェールオーバーワークロードの整合性とビジネス機能を検証します。VMware vSphere Client を使用して VM コンテナ内のフェールオーバーワークロードにアクセスします。

4 テストを**失敗**または**成功**にマークします。タスク内の対応するコマンドを使用します (**テストを失敗としてマーク**、**テストを成功としてマーク**)。選択したアクションは、ワークロードに関連するイベントの履歴の中に保存され、レポートによって取得されます。**タスクの破棄**は、タスクおよびイベントを破棄します。

テストを失敗としてマークタスクまたは**テストを成功としてマーク**タスクが終了すると、PlateSpin Protect はフェールオーバーワークロードに適用された一時的な設定を破棄し、保護をテスト以前の状態に戻します。

15.6 フェールバック

「フェールバック」操作は、一時的なフェールオーバーワークロードのビジネス機能が必要でなくなった場合に、障害が発生した運用ワークロードのビジネス機能を元の環境に回復します。フェールバックは、フェールオーバー後の次の論理的な手順になります。これは、フェールオーバーワークロードを元のインフラ、あるいは必要な場合は新しいインフラに移行させます。

サポートされるフェールバック方法は、ターゲットインフラのタイプとフェールバックプロセスの自動化の度合いにより異なります。

- **仮想化マシンへの自動化されたフェールバック :** VMware ESX プラットフォームおよび VMware DRS クラスタをサポートしています。
- **物理マシンへの半自動化されたフェールバック :** すべての物理マシンをサポートしています。
- **仮想マシンへの半自動化されたフェールバック :** Microsoft Hyper-V プラットフォームをサポートしています。

次の各項では、詳細について説明します。

- 161 ページのセクション 15.6.1「VM プラットフォームへの自動化されたフェールバック」
- 164 ページのセクション 15.6.2「物理マシンへの半自動化されたフェールバック」
- 165 ページのセクション 15.6.3「仮想マシンへの半自動化されたフェールバック」

15.6.1 VM プラットフォームへの自動化されたフェールバック

PlateSpin Protect は、サポートされている VMware ESXi Server または VMware DRS Cluster 上におけるフェールバックコンテナの自動化されたフェールバックをサポートしています。詳細については、18 ページの 「サポートされる VM コンテナ」を参照してください。

ターゲット VMware コンテナへのフェールオーバーワークロードの自動化されたフェールバックを実行するには :

1 フェールオーバーに続いて、［ワークロード］ページでワークロードを選択し、**フェールバック**をクリックします。

次の選択を行うことを求めるプロンプトが表示されます。

2 次の一連のパラメータを指定します。

- **ワークロードの設定 :** フェールオーバーワークロードのホスト名または IP アドレスを指定し、管理者レベルの資格情報を入力します。必要な資格情報のフォーマットを使用します (167 ページの 「ワークロードおよびコンテナの資格情報向けのガイドライン」を参照)。

- **フェールバックターゲットの設定**：次のパラメータを指定します。
  - **レプリケーション方法**：データレプリケーションの範囲を選択します。**増分**を選択する場合、ターゲットを準備する**必要があります**。詳細については、170 ページの 「初期レプリケーション方法 (フルおよび差分)」を参照してください。
  - **ターゲットタイプ**：**仮想ターゲット**を選択します。フェールバックコンテナがまだない場合は、**コンテナの追加**をクリックし、サポートされるコンテナのインベントリを実行します。

3 **保存して準備**をクリックし、［コマンドの詳細］画面上の進行状況を監視します。

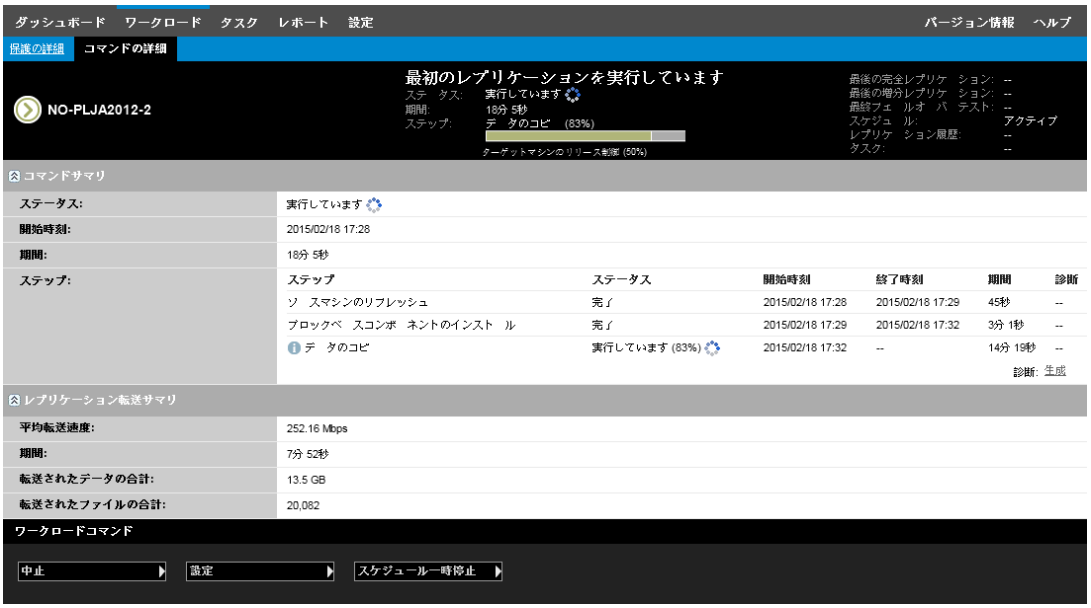
正常に終了すると、PlateSpin Protect によって［フェールバックの準備ができました］画面がロードされ、フェールバック操作の詳細を指定するように要求されます。

4 フェールバックの詳細を設定します。163 ページの 「フェールバック詳細 (ワークロードを VM へ)」を参照してください。

5 **保存してフェールバック**をクリックし、［コマンドの詳細］画面上の進行状況を監視します。図 15-2 を参照してください。

PlateSpin Protect がコマンドを実行します。フェールバック後のパラメータセットの中で**フェールバック後に再保護**を選択した場合は、**再保護**コマンドが Web インタフェースに表示されます。

図 15-2　フェールバックコマンドの詳細



フェールバック詳細 (ワークロードを VM へ)

フェールバック詳細は、仮想マシンへのワークロードのフェールバック操作を実行する際に設定する 3 セットのパラメータによって表されます。パラメータの設定の詳細については、表 15-2 を参照してください。

表 15-2　フェールバック詳細 (ワークロードを VM へ)

パラメータの設定	Details (詳細)
フェールバックの設定	
転送方法	データ転送メカニズムおよび暗号化によるセキュリティを選択します。詳細については、25 ページの 「転送におけるデータの暗号化」を参照してください。
Failback Network (フェールバックのネットワーク)	フェールバックトラフィックに使用するネットワークを指定します。これは、VM コンテナで定義された仮想ネットワークに基づく専用ネットワークです。詳細については、174 ページの 「ネットワーキング」を参照してください。
VM Datastore (VM データストア)	ターゲットワークロード向けにフェールバックコンテナに関連付けられているデータストアを選択します。
ボリュームマッピング	初期レプリケーション方法が「増分」に指定された場合は、同期を行うために、ソースボリュームを選択し、フェールバックターゲット上のボリュームにマップします。
停止するサービス / デーモン	フェールバック時に自動的に停止されるアプリケーションサービス (Windows) またはデーモン (Linux) を指定します。詳細については、171 ページの 「サービスおよびデーモンの制御」を参照してください。
ソースの代替アドレス	該当する場合は、フェールオーバーした VM の追加 IP アドレスを指定します。詳細については、36 ページの 「NAT を通じたパブリックおよびプライベートネットワーク経由の保護の要件」を参照してください。
ワークロードの設定	
CPU	(最小の VM ハードウェアレベル 8 で VMware 5.1、5.5、および 6.0 を使用する VM コンテナ) 仮想ワークロードへのフェールバックに対し、ソケット数およびソケットあたりのコア数を指定します。合計コア数は自動的に計算されます。このパラメータは、初期レプリケーション設定である**完全**とともにワークロードの初期セットアップに適用されます。 **注 :** ワークロードが使用できるコアの最大数は、外部的な要因によって変わります。たとえば、ゲストオペレーティングシステム、VM のハードウェアバージョン、ESXi ホストの VMware ライセンス、vSphere の ESXi ホストの計算リソースの上限 (「*vSphere 5.1 Configuration Maximums* (http://www.vmware.com/pdf/vsphere5/r51/vsphere-51-configuration-maximums.pdf)」を参照) などです。 ゲスト OS のディストリビューションによっては、コア数およびソケットあたりのコア数の設定が遵守されない場合があります。たとえば、SLES 10 SP4 および OES 2 SP3 を使用するゲスト OS では、インストールされている本来のコア数とソケットの設定が保持されます。一方、SLES、RHEL、および OES の他のディストリビューションでは、この設定が遵守されます。

パラメータの設定	Details (詳細)
CPU の数	(VMware 4.1 を使用する VM コンテナ) 仮想ワークロードへのフェールバックに割り当てる必要がある vCPU (仮想 CPU) の数を指定します。このパラメータは、初期レプリケーション設定である**完全**とともにワークロードの初期セットアップに適用されます。各 vCPU は、VM コンテナ上のゲスト OS には、1 つのコア、1 つのソケットとして表示されます。
VM メモリ	必要な RAM をターゲットワークロードに割り当てます。
Hostname, Domain/Workgroup (ホスト名、ドメイン / ワークグループ)	ターゲットワークロードの識別情報およびドメイン / ワークグループの加入を指定します。ドメインの加入には、ドメイン管理者の資格情報が必要です。
Network Connections	基礎となる VM コンテナの仮想ネットワークに基づいてターゲットワークロードのネットワークマッピングを指定します。
Service States to Change (変更するサービス状態)	特定のアプリケーションサービス (Windows) またはデーモン (Linux) の起動状態を指定します。詳細については、171 ページの 「サービスおよびデーモンの制御」を参照してください。
フェールバック後の設定	
ワークロードの再保護	展開後にターゲットワークロード用の保護コントラクトを再作成する場合は、このオプションを選択します。このオプションは、ワークロード用に継続的なイベント履歴を保持し、ワークロードライセンスを自動的に割り当て / 指定します。
フェールバック後に再保護	ターゲットワークロード用の保護コントラクトを再作成する場合は、このオプションを選択します。フェールバックが完了すると、フェールバックしたワークロードの Web インタフェースで**再保護**コマンドが使用できるようになります。
再保護なし	ターゲットワークロード用の保護コントラクトを再作成しない場合は、このオプションを選択します。完了後にフェールバックワークロードを保護するには、そのワークロードを再びインベントリし、保護の詳細を再び設定する必要があります。

15.6.2 物理マシンへの半自動化されたフェールバック

次の手順に従って、フェールオーバー後、ワークロードを物理マシンにフェールバックします。この物理マシンは元のインフラまたは新しいインフラのいずれかにできます。

1. 必要な物理マシンを PlateSpin Server に登録します。詳細については、174 ページの 「物理マシンへのフェールバック」を参照してください。
2. ドライバが見つからない場合またはドライバに互換性がない場合は、必要なドライバを PlateSpin Protect デバイスドライバデータベースにアップロードします。詳細については、107 ページの 「物理フェールバックターゲットのデバイスドライバの準備」を参照してください。
3. フェールオーバーに続いて、［ワークロード］ページでワークロードを選択し、**フェールバック**をクリックします。

4 次の一連のパラメータを指定します。

- **ワークロードの設定 :** フェールオーバーワークロードのホスト名または IP アドレスを指定し、管理者レベルの資格情報を入力します。必要な資格情報のフォーマットを使用します (167 ページの 「ワークロードおよびコンテナの資格情報向けのガイドライン」を参照)。
- **フェールバックターゲットの設定 :** 次のパラメータを指定します。
  - **レプリケーション方法 :** データレプリケーションの範囲を選択します。

    170 ページの 「初期レプリケーション方法 (フルおよび差分)」を参照してください。
  - **ターゲットタイプ : 物理ターゲット**オプションを選択し、ステップ 1 で登録した物理マシンを選択します。

5 **保存して準備**をクリックし、[コマンドの詳細] 画面上の進行状況を監視します。

正常に終了すると、PlateSpin Protect によって [フェールバックの準備ができました] 画面がロードされ、フェールバック操作の詳細を指定するように要求されます。

6 フェールバックの詳細を設定し、**保存してフェールバック**をクリックします。

[コマンドの詳細] ページの進行状況を監視します。

15.6.3 仮想マシンへの半自動化されたフェールバック

このフェールバックタイプは、本来サポートされている VMware コンテナ以外の VM ターゲットについて、物理マシンへの半自動化されたフェールバックと同様のプロセスに従います。VM への半自動化されたフェールバックは、次のターゲットプラットフォームに対してサポートされています。

完全自動化フェールバックがサポートされているコンテナ (VMware ESX ターゲットおよび DRS クラスターゲット) に対して、半自動化されたフェールバックを実行できます。

また、Microsoft Hyper-V Server 2012 ホスト上のターゲット VM プラットフォームの半自動化されたフェールバックも実行できます。

フェールオーバー時に Hyper-V VM を起動するには :

1 テキストエディタで各 Hyper-V ホストの /etc/vmware/config ファイルを変更して、次の行を追加します。

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

2 vSphere Web クライアントで CPU のフェールオーバー VM 設定を変更します。

2a **Virtual Hardware (仮想ハードウェア)** タブで、**CPU (CPU)** を選択します。

2b **Hardware virtualization (ハードウェア仮想化)** で、**Expose hardware assisted virtualization to guest OS (ゲスト OS に対してハードウェアによる仮想化を公開する)** を選択します。

3 vSphere Web クライアントで、CPU ID のフェールオーバー VM 設定を変更します。

3a **VM Options (VM オプション)** タブで **Advanced (詳細設定)** を展開し、**Edit configuration parameters (環境設定パラメータの編集)** を選択します。

3b 次の設定を検証します。

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

15.7 ワークロードの再保護

再保護の操作は、**フェールバック**後の次の論理ステップであり、ワークロードの保護ライフサイクルを完了させ、新たに保護ライフサイクルを開始します。フェールバック操作が正常にすると、**再保護**コマンドが Web インタフェースで使用可能となり、システムは保護コントラクトの初期設定のときに指定されている同じ保護の詳細を適用します。

注 : **再保護**コマンドは、フェールバックの詳細で**再保護**オプションが選択されている場合にのみ使用可能となります。詳細については、161 ページの 「フェールバック」を参照してください。

保護ライフサイクルをカバーするその他のワークフローは、通常のワークロード保護操作と同じであり、必要な回数だけ繰り返すことができます。

16 ワークロード保護の要点

この項では、ワークロード保護コントラクトのさまざまな機能分野について説明します。

16.1 ワークロードおよびコンテナの資格情報向けのガイドライン

PlateSpin Protect には、ワークロードへの管理者レベルのアクセスと、コンテナに対する適切な役割設定が必要です。ワークロード保護および回復のワークフローを通じて、特定の形式で資格情報を指定するように PlateSpin Protect によって要求されます。

表 16-1 *ワークロードおよびコンテナの資格情報*

検出対象	資格情報	備考
Windows のすべてのワークロード	ローカルまたはドメインの管理者資格情報	ユーザ名には次のフォーマットを使用します。 ◆ ドメインメンバーのマシン用 : *authority\principal* ◆ ワークグループメンバーのマシン用 : *hostname*
Windows クラスタ	ドメインの管理者資格情報	ドメインメンバーのマシン用 : *authority\principal*
Linux のすべてのワークロード	ルートレベルのユーザ名とパスワード	ルート以外のアカウントは、sudo を使用できるよう適切に設定する必要があります。ナレッジベースの記事 7920711 (https://www.netiq.com/support/kb/doc.php?id=7920711) を参照してください。

検出対象	資格情報	備考
VMware ESX または ESXi ホスト	適切な役割設定を持つ VMware アカウントです。 Protect のマルチテナンシに対して役割を設定するには、59 ページの 「マルチテナンシに対する VMware の役割の定義」を参照してください。	ESX が Windows ドメイン認証用に設定されている場合は、Windows ドメイン資格情報を使用することもできます。
VMware vCenter Server	適切な役割設定を持つ VMware アカウントです。 Protect のマルチテナンシに対して役割を設定するには、59 ページの 「マルチテナンシに対する VMware の役割の定義」を参照してください。	

16.2 保護ティア

保護ティアは、次のとおり定義するワークロード保護パラメータのカスタムコレクションです。

- レプリケーションの頻度と繰り返しパターン
- データ転送の暗号化を行うかどうか
- データ圧縮を行うかどうか、およびどのように行うか
- データ転送中に指定された処理量に使用可能な帯域幅を制限するかどうか
- ワークロードをオフライン (失敗) したとシステムが見なす基準

保護ティアはすべてのワークロード保護コントラクトの統合部です。ワークロード保護コントラクトの統合段階中に、いくつかの組み込まれた保護ティアの 1 つを選択し、その属性を特定の保護コントラクトの要件に合わせてカスタマイズできます。

カスタム保護ティアを事前作成するには :

1 Web インタフェースで［設定］>［保護ティア］>［保護ティアの作成］の順にクリックします。

2 新しい保護ティアのパラメータを指定します。

パラメータ	アクション
名前	ティアに使用する名前を入力します。
増分反復	増分レプリケーションの頻度および増分反復パターンを指定します。**反復の開始**フィールドに直接入力するか、カレンダアイコンをクリックして日付を選択できます。**なし**を選択すると、反復パターンに増分レプリケーションが使用されません。
完全な反復	完全レプリケーションの頻度および完全な反復パターンを指定します。

パラメータ	アクション
ブラックアウト期間	レプリケーションの停止を強制するには、これらの設定を使用します。使用量がピークの時間帯にスケジュール済みレプリケーションを一時停止にするか、VSS 対応アプリケーションと VSS のブロックレベルデータ転送コンポーネント間の競合を防ぐには、この機能の実装を検討してください。 ブラックアウトウィンドウを指定するためには、**編集**をクリックしてから、ブラックアウトの繰り返しパターン (毎日、毎週など) を選択し、ブラックアウト期間の開始と終了時間を指定します。 **注 :** ブラックアウトの開始時間と終了時間は、PlateSpin Server のシステムクロックに基づきます。
圧縮レベル	これらの設定は、転送前にワークロードデータを圧縮するか、またその方法を制御します。30 ページの 「データ圧縮」を参照してください。 次のいずれかのオプションを選択します。**高速**はソースの最小 CPU リソースを消費しますが、圧縮比率は下がり、**最大**はソースの最大 CPU リソースを消費しますが、圧縮比率は高くなります。**最適**は、中程度で、推奨オプションです。
帯域幅制限	これらの設定は、帯域幅制限を制御します。30 ページの 「帯域幅制限」を参照してください。 レプリケーションを指定の速度に制限するには、必要な処理量の値を Mbps で指定し、時間パターンを示してください。
維持する復旧ポイント	この保護ティアを使用するワークロード用に維持する復旧ポイントの数を指定します。詳細については、169 ページの 「復旧ポイント」を参照してください。
ワークロードの障害	障害が発生したと判断するまでに試行されるワークロード検出回数を指定します。
ワークロードの検出	ワークロード検出を試行する間隔を秒数で指定します。

16.3 復旧ポイント

復旧ポイントとは、ワークロードの特定の時点でのスナップショットです。これを使用すると、複製されたワークロードを特定の状態に復旧できます。

保護された各ワークロードには少なくとも 1 つの復旧ポイントがあり、最大で 32 の復旧ポイントを使用できます。

警告 : 時間とともに蓄積する復旧ポイントによって、PlateSpin Protect のストレージ領域不足になってしまう可能性があります。

16.4 初期レプリケーション方法 (フルおよび差分)

「最初のレプリケーション」とは、保護操作でフェールオーバーワークロード (仮想レプリカ) に運用ワークロードの初期ベースコピーを作成すること、または運用ワークロードのフェールバック操作の準備のために、フェールオーバーワークロードからその元の仮想インフラまたは物理インフラに運用ワークロードの初期ベースコピーを作成することです。

ワークロード保護およびフェールバックの操作では、初期レプリケーションパラメータによってソースからターゲットに転送されるデータの範囲が決定されます。

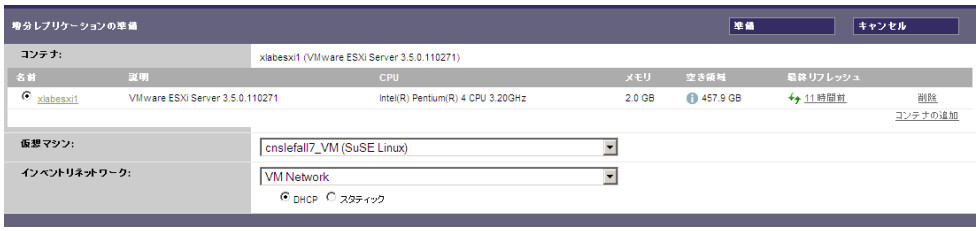
- **フル :** フルワークロード転送はそのデータすべてに基づいて行われます。
- **増分 :** ソースからターゲットに対して差分のみが転送されます。この時、ソースとターゲットは同様のオペレーティングシステムとボリュームプロファイルを使用している必要があります。
  - **保護時 :** 運用ワークロードは VM コンテナ内の既存の VM と比較されます。既存の VM は次のうちの 1 つになります。
    - 以前に保護されたワークロードの回復VM (**ワークロードの削除**コマンドの**VMの削除**オプションの選択は解除されています)。
    - ポータブルメディアによって運用サイトからリモートの回復サイトに物理的に移動されたワークロード VM など、手動で VM コンテナにインポートされる VM。
  - **仮想マシンへのフェールバック時 :** フェールオーバーワークロードは、フェールバックコンテナ内の既存の VM と比較されます。
  - **物理マシンへのフェールバック時 :** ターゲットの物理マシンが PlateSpin Protect に登録されている場合、フェールオーバーワークロードはその物理マシン上のワークロードと比較されます (164 ページの 「物理マシンへの半自動化されたフェールバック」 を参照)。

ワークロード保護および VM ホストへのフェールバック時、初期レプリケーション方法として**増分**を選択すると、選択された操作のソースと同期するのに、ターゲット VM を参照し、見つけ、準備する必要があります。

初期レプリケーション方法を設定するには :

1. **環境設定 (保護の詳細)** や**フェールバック**などの必要なワークロードコマンドを続行します。
2. **初期レプリケーション方法**オプションには、**増分レプリケーション**を選択します。
3. **ワークロードの準備**をクリックします。

   Web インタフェースによって［増分レプリケーションの準備］ページが表示されます。



4. 必要なコンテナ、仮想マシン、および VM との通信に使用するネットワークを選択します。指定されたターゲットコンテナが VMware DRS クラスタである場合、ワークロードのターゲットリソースプールを指定することもできます。

5 **準備**をクリックします。

プロセスが完了し、ユーザインタフェースが元のコマンドに戻るまで待機し、準備済みのワークロードを選択します。

注 : (ブロックレベルデータのレプリケーションのみ) 初めての増分レプリケーションは、その後のレプリケーションよりも大幅に長い時間がかかります。これは、ソースのボリュームとターゲットのボリュームがブロックごとに比較されるからです。その後のレプリケーションは、実行中のワークロードのモニタリング中にブロックベースのコンポーネントにより検出された変更に依存します。

16.5 サービスおよびデーモンの制御

PlateSpin Protect では、サービスおよびデーモンを制御できます。

- **ソースサービス / デーモンの制御 :** データ転送の間、ソースワークロード上で実行中の Windows サービスまたは Linux デーモンを自動的に停止できます。これにより、これらを停止しなかった場合と比較して、ワークロードをより一貫した状態でレプリケーションできるようになります。

  たとえば、Windows のワークロードの場合、ウイルス対策ソフトウェアのサービスや、サードパーティ製の VSS 対応バックアップソフトウェアを停止することを考慮してください。

  レプリケーション中に Linux のソースをさらに制御するには、Linux ワークロードのカスタムスクリプトをレプリケーションごとに実行する機能を検討してください。121 ページの 「すべてのレプリケーションで Freeze と Thaw スクリプト機能を使用する (Linux)」を参照してください。
- **ターゲットの起動状態 / 実行レベルの制御 :** フェールオーバー VM 上のサービス / デーモンの起動状態 (Windows) または実行レベル (Linux) を選択できます。フェールオーバーまたはフェールオーバーのテストの操作を実行する場合、フェールオーバーワークロードが動作を開始した際に実行または停止させるサービスあるいはデーモンを指定できます。

  無効な起動状態を割り当てた方が良い一般的なサービスは、ベンダ特有のサービスで、基礎となる物理インフラストラクチャにそれぞれ結び付いており、仮想マシンでは必要ではありません。

16.6 ボリュームストレージ

ワークロードを保護対象に追加すると、がソースワークロードのストレージメディアをインベントリし、保護に必要なボリュームを指定するために使用する PlateSpin Protect Web インタフェースの中のオプションを自動的にセットアップします。詳細については、21 ページのセクション 1.1.5 「サポートされるストレージ」を参照してください。

図 16-1 は、複数のボリューム、および 1 つのボリュームグループに含まれる 2 つの論理ボリュームを使用する Linux ワークロード用のレプリケーション設定のパラメータセットを示します。

図16-1 保護されたLinuxのワークロードのボリューム、論理ボリューム、およびボリュームグループ

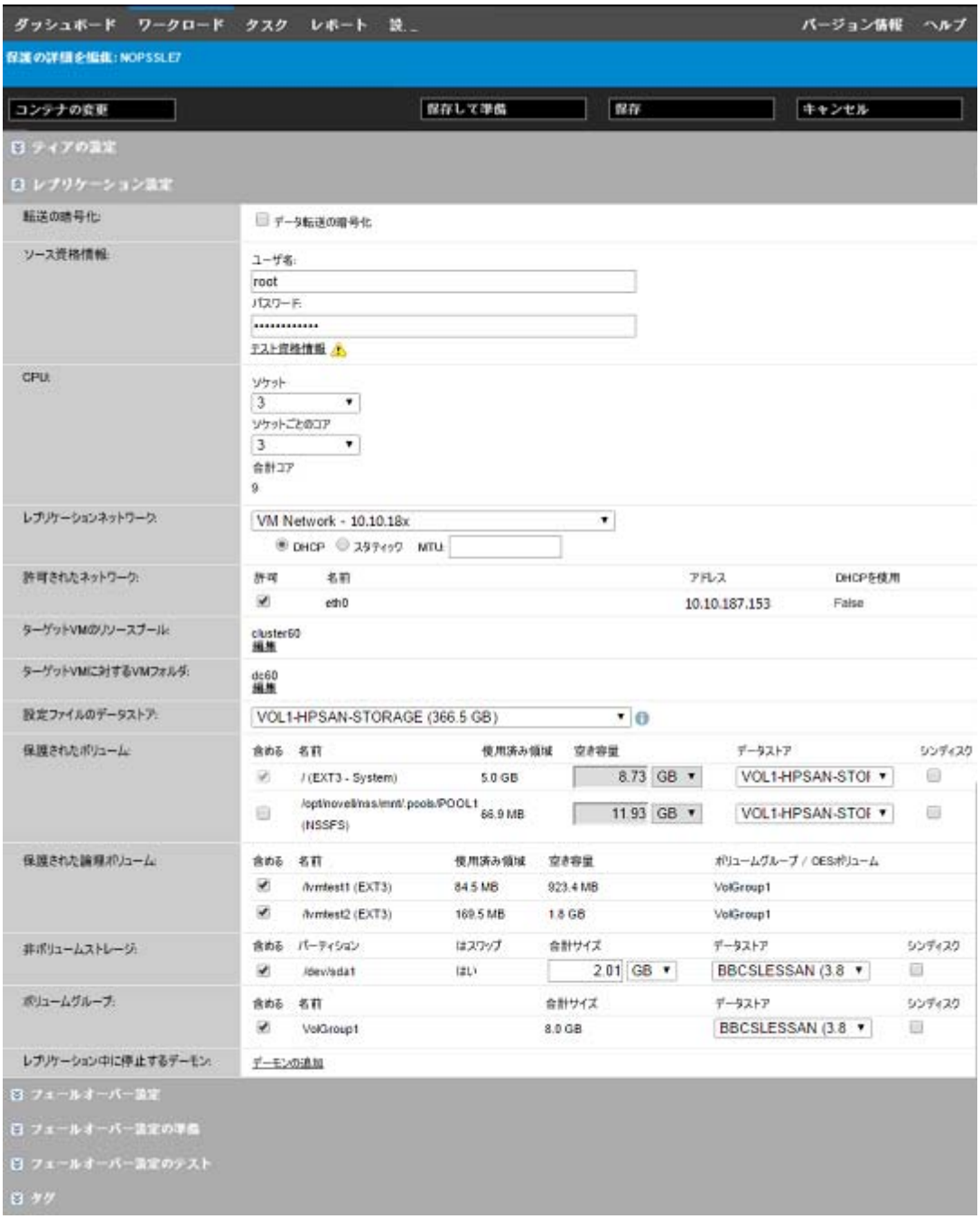


図 16-2 は、LVM2 ボリュームと NSS プールレイアウトが保存され、フェールオーバーワークロードのために作成し直されることを示すオプションを持つ OES 11 ワークロードのボリューム保護オプションを示します。

図 16-2　レプリケーション設定、ボリューム関連オプション (OES 11 ワークロード)

図 16-3 は、EVMS と NSS プールレイアウトが保存され、フェールオーバーワークロードのために作成し直されることを示すオプションを持つ、OES 2 ワークロードのボリューム保護オプションを示します。

図 16-3　レプリケーション設定、ボリューム関連オプション (OES 2 ワークロード)

16.7 ネットワーキング

PlateSpin Protect では、フェールオーバーワークロードのネットワーク ID および LAN 設定を制御して、レプリケーションのトラフィックがメインの LAN または WAN のトラフィックを妨げないようにできます。

ワークロード保護および回復ワークフローの各段階で使用する異なるネットワーキング設定をワークロード保護の詳細に指定できます。

- **レプリケーション：** (レプリケーション設定パラメータセット) 一般的なレプリケーショントラフィックを運用トラフィックから分離するためのものです。
- **フェールオーバー：** (フェールオーバーの設定パラメータセット) フェールオーバーワークロードが稼働し始めた場合に、運用ネットワークの一部に含めるためのものです。
- **フェールオーバーの準備：** (Prepare for Failover Settings (フェールオーバーの準備設定) ネットワークパラメータ) オプションのフェールオーバーの準備段階でのネットワーク設定です。
- **フェールオーバーのテスト：** (テストフェールオーバー設定パラメータセット) フェールオーバーのテスト段階でフェールオーバーワークロードに適用するネットワーク設定です。

16.8 物理マシンへのフェールバック

フェールバックの操作に必要なターゲットインフラストラクチャが物理マシンの場合は、それを PlateSpin Protect に登録する必要があります。

物理マシンの登録は、ターゲットの物理マシンを PlateSpin OFX ISO ブートイメージを使用して起動することで実行されます。

- 174 ページのセクション 16.8.1「PlateSpin OFX ISO ブートイメージのダウンロード」
- 175 ページのセクション 16.8.2「ISO ブートイメージへのデバイスドライバの追加」
- 176 ページのセクション 16.8.3「PlateSpin Protect への、フェールバックターゲットとしての物理マシンの登録」

16.8.1 PlateSpin OFX ISO ブートイメージのダウンロード

PlateSpin Protect ソフトウェアダウンロードページから、BIOS ファームウェアベースのターゲットおよび UEFI ファームウェアベースのターゲット用の PlateSpin OFX ISO ブートイメージ (bootofx.x2p.iso) をダウンロードできます。

1. Micro Focus Downloads (Micro Focus ダウンロード) (https://www.microfocus.com/support-and-services/download/) に移動します。
2. **Browse by Product (製品別の参照)** リストから PlateSpin Protect を選択するか、**Browse by Product (製品別の参照)** フィールドに製品名を入力して、製品を見つけて選択します。
3. ［Download overview (ダウンロードの概要)］ページで **proceed to download (ダウンロードの続行)** をクリックして、カスタマアカウント資格情報でログインします。
4. 米国輸出管理規則を受け入れ、同意するには、**accept (同意する)** をクリックします。
5. ［ダウンロード］ページで、**bootofx.x2p.iso** ファイルの横にあるダウンロードをクリックして、ファイルを保存します。

16.8.2 ISO ブートイメージへのデバイスドライバの追加

カスタムユーティリティを使用して、CD へ書き込む前に追加の Linux デバイスドライバをパッケージ化して PlateSpin ブートイメージに含めることができます。

このユーティリティを使用するには、次の手順に従います。

1 ターゲットハードウェアの製造元に適した *.ko ドライバファイルを取得またはコンパイルします。

重要：ドライバが、ISO ファイルに含まれているカーネルで有効であり (x86 システムの場合は 3.0.93-0.8-pae、x64 システムの場合は 3.0.93-0.8-default)、ターゲットアーキテクチャに適したものであることを確認してください。ナレッジベースの記事 7005990 (https://www.netiq.com/support/kb/doc.php?id=7005990) も参照してください。

---

2 任意の Linux マシンにイメージをマウントします (root 資格情報が必要)。次のコマンド構文を使用します。

mount –o loop <ISO へのパス > < マウントポイント >

3 マウントされた ISO ファイルの /tools サブディレクトリにある rebuildiso.sh スクリプトを一時的な作業ディレクトリにコピーします。終了したら、ISO ファイルをアンマウントします (umount < *マウントポイント* > コマンドを実行)。

4 必要なドライバファイル用に別の作業ディレクトリを作成し、それらのファイルをそのディレクトリに保存します。

5 rebuildiso.sh スクリプトを保存したディレクトリで、次の構文を使用して、rebuildiso.sh スクリプトをルートとして実行します。

./rebuildiso.sh <*ARGS*> [-v] -m32|-m64 -i <*ISO_file*>

次の表は、このコマンドで使用可能なコマンドラインオプションを示しています。

オプション	説明
-i <*ISO_file*>	<*ISO_file*> は、変更、一覧表示などの操作の対象である ISO です。
-v	-l 引数と一緒に使用すると、このオプションにより modinfo が使用され、冗長なドライバ情報が取得されます。
-o	-c 引数または -d 引数と一緒に使用すると、ISO ファイルの古いコピーは上書きされません。
-m32	32 ビットの initrd の追加を指定します。
-m64	64 ビットの initrd の追加を指定します。

次の表は、このコマンドで使用可能な引数を示しています。少なくとも、これらの引数のうちの 1 つをコマンドで使用する必要があります。

引数	説明
-d <*path*>	<*path*> は、ドライバ (つまり、*.ko ファイル) を含む、追加対象のディレクトリを指定します。 コマンドが終了すると、ISO ファイルが追加のドライバで更新されます。

引数	説明
-c <*path*>	<*path*> は、ConfigureTakeControl.xml ファイルの存在する場所を指定します。
-l [<*type*>]	<*type*> は、一覧表示対象のドライバのサブセットを指定します。デフォルト値は、「すべて」のタイプです。 一覧表示されたドライバタイプの中でフォワードスラッシュ (/) で始まるものは、<*kernel_module_directory*>/kernel/ に存在すると見なされます。 一覧表示されたドライバタイプの中でフォワードスラッシュ (/) で始まらないものは、<*kernel_module_directory*/kernel/drivers/ に存在すると見なされます。 **ドライバサブセットの例 :** -l scsi -l 'net|video' -l '/net|net' **この引数の特殊な使用法 :** 各サブセットの使用可能なサブディレクトリを一覧表示する場合は、次のように引数を使用します。-l INDEX

構文の例

- 32 ビットのドライバのインデックスを一覧表示するには :

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

- /misc フォルダにあるドライバを一覧表示するには :

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

- /oem-drivers フォルダから 32 ビットのドライバを追加するには :

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

- /oem-drivers フォルダから 64 ビットのドライバを追加し、カスタマイズされた ConfigureTakeControl.xml ファイルも一緒に追加するには :

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

16.8.3 PlateSpin Protect への、フェールバックターゲットとしての物理マシンの登録

1. PlateSpin ISO ブートイメージを CD に書き込むか、ターゲットをブートできるメディアに保存します。
2. ターゲットに接続されているネットワークスイッチポートが［自動全二重］に設定されていることを確認します。
3. ブート CD を使用して、ターゲットの物理マシンをブートし、コマンドプロンプトウィンドウが開くのを待ちます。
4. (Linux のみ)64 ビットのシステムの場合、最初のブートプロンプトで次を入力します。

   ps64

5 <Enter> を押します。

6 プロンプトが表示されたら、PlateSpin Server ホストのホスト名または IP アドレスを入力します。

7 オーソリティを指定して、PlateSpin Server ホストの管理者レベルの資格情報を入力します。ユーザアカウントには次のフォーマットを使用します。

domain\username または *hostname\username*

利用可能なネットワークカードが検出され、MAC アドレスで表示されます。

8 使用される NIC で DHCP を利用できる場合は、<Enter> キーを押して続行します。DHCP が利用できない場合は、必要な NIC をスタティック IP アドレスを使用して設定します。

9 物理マシンのホスト名を入力するか、Enter キーを押してデフォルト値を受け入れます。

10 HTTPS を使用するかどうかを問うプロンプトが表示されたら、SSL を有効化している場合は「Y」(はい) と入力します。有効化していない場合は「N」(いいえ) と入力します。

しばらくすると、物理マシンが PlateSpin Protect Web インタフェースのフェールバックの設定で利用可能になります。

16.9 Windows クラスタの保護

PlateSpin Protect では、Microsoft Windows Server クラスタのビジネスサービスの保護がサポートされています。Windows Server クラスタのノードを保護するための要件およびオプションについては、123 ページの第 13 章「Windows クラスタ保護の準備」を参照してください。

- 177 ページのセクション 16.9.1「PlateSpin のフェールオーバー」
- 178 ページのセクション 16.9.2「PlateSpin のフェールバック」

16.9.1 PlateSpin のフェールオーバー

PlateSpin のフェールオーバー操作が完了して、1 つのノードからなる仮想クラスタがオンラインになると、アクティブノードが 1 つのマルチノードクラスタが表示されます (アクティブノード以外のノードは使用できない状態になっています)。

Windows クラスタで PlateSpin のフェールオーバーを実行するには (または Windows クラスタ上で PlateSpin のフェールオーバーをテストするには)、そのクラスタがドメインコントローラに接続できなければなりません。フェールオーバーのテスト機能を使用するには、該当のクラスタとともにドメインコントローラを保護する必要があります。このテストでは、まずドメインコントローラを起動し、続いて (分離したネットワーク上で)Windows クラスタのワークロードを起動します。

16.9.2 PlateSpin のフェールバック

PlateSpin のフェールバック操作では、Windows クラスタのワークロードのフルレプリケーションが必要になります。

PlateSpin のフェールバックを物理ターゲットへのフルレプリケーションとして設定した場合は、次の方法のいずれかを使用できます。

- 1 つのノードからなる PlateSpin 仮想クラスタ上のすべてのディスクを、フェールバックターゲット上の単一のローカルディスクにマップする。
- 別のディスク (ディスク 2) を物理フェールバックマシンに追加する。フェールオーバーマシンのシステムボリュームをディスク 1 に復元し、フェールオーバーマシンの追加ディスク (以前の共有ディスク) をディスク 2 に復元するように PlateSpin のフェールバック操作を設定できます。これによって、システムディスクを元のソースと同じサイズのストレージに復元することができます。

PlateSpin のフェールバックが完了したら、追加ノードを新しく復元されたクラスタに再度参加させる前に、共有ストレージを再接続してクラスタ環境を再構築する必要があります。

注 : クラスタが **Ready To Reprotect (再保護の準備完了)** の段階である場合は、まずフェールバックターゲットを再構築して復元し、ターゲットがクラスタとして検出されるようにします。再構築プロセスの一部として、PlateSpin クラスタドライバを手動でアンインストールする必要があります。

PlateSpin でフェールオーバーおよびフェールバックが生じた後にクラスタ環境を再構築する方法の詳細については、次のリソースを参照してください。

- **Windows Server 2012 R2 フェールオーバークラスタ (物理再構築または仮想再構築へのフェールバック):** ナレッジベースの記事 7016770 (http://www.netiq.com/support/kb/doc.php?id=7016770) を参照してください。
- **Windows Server 2008 R2 フェールオーバークラスタ (物理再構築または仮想再構築へのフェールバック):** ナレッジベースの記事 7015576 (http://www.netiq.com/support/kb/doc.php?id=7015576) を参照してください。

---

17 レポートの生成

PlateSpin Web インタフェースを使用して、検出されたワークロードとワークロード保護コントラクトに関するレポートを生成できます。ライセンスレポートの生成については、54 ページのセクション 4.6「テクニカルサポート用のライセンスレポートの生成」を参照してください。

17.1 Protect レポートについて

PlateSpin Protect では、長期間にわたってワークロード保護コントラクトを分析的に洞察するために次のレポートを生成できます。

- **ワークロードの保護：** 選択可能な時間帯にわたって、すべてのワークロードのレプリケーションイベントを報告します。
- **レプリケーション履歴：** 選択可能な時間帯にわたって、選択可能なワークロードごとのレプリケーションタイプ、サイズ、時間、および転送スピードを報告します。
- **レプリケーションウィンドウ：** **平均**、**最新**、**合計**、および**ピーク**の観点から要約できる完全レプリケーションおよび増分レプリケーションの実施状況を報告します。
- **現在の保護ステータス：****ターゲット RPO**、**実際の RPO**、**実際の TTO**、**実際の RTO**、**最後のフェールオーバーテスト**、**最後のレプリケーション**、および**年齢をテスト**の統計を報告します。
- **イベント：** 選択可能な時間帯にわたって、すべてのワークロードのシステムイベントを報告します。
- **イベントスケジュール：** 今後のワークロード保護イベントのみを報告します。

図 17-1 *レプリケーション履歴レポートのオプション*

17.2 ワークロードとワークロード保護のレポートの作成

レポートを生成するには :

1. Web インタフェースで**レポート**をクリックします。

   レポートタイプのリストが表示されます。
2. 必要なレポートタイプの名前をクリックします。
3. レポートを生成するワークロードを 1 つ以上選択します。
4. レポートを表示する期間を設定します。
5. レポート用の適切なパラメータを指定します。
6. 次のいずれかの操作を実行します。
   - ご使用の Web ブラウザでレポートを表示するには、**印刷可能ビュー**をクリックします。
   - ご使用のコンピュータに XML ファイルを保存するには、**XML にエクスポート**をクリックします。

17.3 診断レポートの生成

PlateSpin Protect Web インタフェースで、コマンドを実行した後で、コマンドの詳細に関する詳しい診断レポートを生成できます。

1. **コマンドの詳細**をクリックし、パネルの右下にある **Generate (生成)** リンクをクリックします。

   しばらくすると、ページがリフレッシュされ **Generate (生成)** リンクの上に**ダウンロード**リンクが表示されます。
2. **ダウンロード** をクリックします。

   .zip ファイルには、現在のコマンドに関する包括的な診断情報が含まれます。
3. このファイルを保存した後、その診断情報を抽出して表示します。
4. 技術サポートに連絡する必要がある場合は、この .zip ファイルを準備しておいてください。

18 ワークロードの保護と回復のトラブルシューティング

この項は、ワークロードの保護と回復の実行中に最も頻繁に起こる問題のトラブルシューティングに役立ちます。

ソースワークロードおよびターゲットホストの検出とインベントリの問題については、133 ページの第 14 章「ワークロードの検出とインベントリのトラブルシューティング」を参照してください。

18.1 接続のスループットの最適化

スループットが遅い場合は、接続をテストすることで、何らかの接続または帯域幅の問題がないかどうかを確認して解決することができます。詳細については、201 ページの付録 F「iPerf ネットワークテストツールを使用した PlateSpin 製品のネットワークスループットの最適化」を参照してください。

18.2 トラフィック転送ワークロードのトラブルシューティング

一部のシナリオで、ネットワークトラフィックを転送するワークロードのレプリカ (たとえば、ワークロードの目的が NAT、VPN、またはファイアウォールのネットワークブリッジとして機能することである場合) は、ネットワークパフォーマンスの大幅な低減を示します。これは、LRO (Large Receive Offload) を持つ VMXNET 2 と VMXNET3 アダプタの問題に関連しています。

この問題を回避するには、仮想ネットワークアダプタの LRO を無効にする必要があります。詳細については、ナレッジベースの記事 7005495 (https://www.netiq.com/support/kb/doc.php?id=7005495) を参照してください。

18.3 設定サービスのトラブルシューティング

フェールオーバーのテストまたはフェールオーバーの後に、何らかの設定サービスの問題によりターゲット VM でエラーが発生します。次のような一般的なエラーメッセージが表示されます。

Configuration service in the target machine does not seem to have started. (ターゲットマシン内の設定サービスが開始されていない可能性があります)

このセクションのトラブルシューティングのヒントに、一般的な設定サービスの問題の説明と、問題を解決する代替方法がいくつか示されています。

- 182 ページのセクション 18.3.1「問題の原因の理解」
- 183 ページのセクション 18.3.2「問題解決のために取り得る処置。」
- 186 ページのセクション 18.3.3「追加のトラブルシューティングのヒント」

18.3.1 問題の原因の理解

設定サービスのエラーは、PlateSpin Server がターゲット VM の設定サービスと通信できないことを示しています。問題の考えられる根本的な原因を特定するために、システムを分析します。

- 182 ページの 「ターゲット VM が起動できない」
- 182 ページの 「ネットワークが正しく設定されていない」
- 182 ページの 「フロッピーデバイスとの間でステータスメッセージを読み書きできない」

ターゲット VM が起動できない

設定サービスが正常に起動するには、オペレーティングシステムをターゲット VM にロードする必要があります。起動の失敗は、ドライバの競合、ブートローダエラー、またはディスク破損の可能性があることを示しています。

ターゲット VM でオペレーティングシステムが起動できない場合は、Micro Focus ご注文と配送を利用してサービスチケットを開くことをお勧めします。

ネットワークが正しく設定されていない

ターゲットワークロード上の設定サービスが PlateSpin Server と通信するには、ネットワークを正しく設定する必要があります。

ターゲットワークロードが PlateSpin Server と通信できるように、ネットワークが設定されていることを確認してください。詳細については、31 ページのセクション 1.5「保護ネットワークにわたるアクセスおよび通信の要件」を参照してください。

フロッピーデバイスとの間でステータスメッセージを読み書きできない

VMware VM が PlateSpin Server に関するステータスメッセージを読み書きするために、設定サービスがフロッピーデバイスと通信できる必要があります。

ターゲット VM で、マシンがフロッピーデバイスと通信できることを確認します。

1 VM で、ログファイル (C:\windows\platespin\configuration\data\log.txt) を開きます。

2 以下のメッセージは、フロッピーにアクセスできないことを示している可能性があります。

```
Failed (5) to write to file \\?\Volume{<guid-number>}\log.zip CopyFile \\?\Volume{<guid-
number>}\windows\platespin\configuration\data\result.txt to \\?\Volume{<guid-
number>}\result.txt failed The output floppy was not accessible after the timeout period
```

18.3.2 問題解決のために取り得る処置。

設定サービスエラーを解決するには、このセクションの解決策のいずれかを試みてください。

- 183 ページの 「ターゲット VM の再起動の最適化をスキップする」
- 183 ページの 「フロッピーデバイスに対する読み書きトラフィックを削減する」
- 185 ページの 「遅延を増やすように起動タイプを変更する」
- 185 ページの 「起動時に競合するサービスが自動的に実行されないように設定する」

ターゲット VM の再起動の最適化をスキップする

デフォルトでは Protect は、フェールオーバープロセスを迅速化するためにターゲット VM で発生する再起動の回数を最小限に抑えようとします。追加の再起動を許可すると、ターゲット VM が PlateSpin Server と通信できる可能性が高まります。

再起動の最適化をスキップするには :

1 PlateSpin Server にログインして、次の PlateSpin Server 設定ページを開きます。

https://*Your_PlateSpin_Server*/platespinconfiguration/

2 パラメータ **ConfigurationServiceValues** を検索します。

3 **ConfigurationServiceValues** パラメータを編集して、**SkipRebootOptimization** オプションを true に設定します。

4 **保存**をクリックします。

5 増分または完全レプリケーションを実行します。

レプリケーションにより、変更された設定もターゲット VM にプロパゲートされます。

6 影響を受けるワークロードに対して［フェールオーバーのテスト］または［フェールオーバー］を再度実行します。

フロッピーデバイスに対する読み書きトラフィックを削減する

診断ログに次のエラーが表示された場合、PlateSpin Server が VMware の入出力フロッピーデバイスに対して読み書きを試みる回数を削減することができます。

Information:1:Attempting floppy download

続いて

Verbose:1:Failed to copy file from remote URL

- または -

Exception: The remote server returned an error: (500) Internal Server Error

このエラーは、VMware がリソースをロックしていることが原因で発生します。これは、PlateSpin Server がステータスをチェックするたびにフロッピーのデタッチとリアタッチを行っていることを示しています。ロックすると、ターゲット VM がフロッピーデバイスとの間で読み書きできなくなる可能性があります。*VMware vCenter Server 4.x,5.x および 6.0 データストアブラウザを使用した場合の電源投入された仮想マシンのダウンロードまたはコピーの失敗 (1019286)* (https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1019286) を参照してください。

フロッピーデバイスのロックの問題が発生した場合は、PlateSpin Server 上の設定サービスのポーリング設定に関する値を増やしてください。

vmwareConfigServicePollStartDelay

このパラメータは、PlateSpin Server が、ターゲットワークロードステータスのポーリングを開始する前に待機する時間の長さを決定します。デフォルト値は 120 秒です (2 分)。

vmwareConfigServicePollIntervalInMilliseconds

このパラメータは、PlateSpin Server がターゲットワークロードとの通信および VMware フロッピーデバイスとの読み書きを試みる頻度を決定します。ポーリング間隔のデフォルト値は 30000ms です (30 秒)。

vmwareConfigServicePollStartTimeout

このパラメータは、PlateSpin Server が、ターゲット VM を起動した後、Web インタフェースにエラーを表示する前に待機する時間の長さを決定します。デフォルト値は 420 秒です (7 分)。

vmwareConfigServicePollUpdateTimeout

このパラメータは、PlateSpin Server が、各ポーリング間隔が経過した後、Web インタフェースにエラーを表示する前に待機する時間の長さを決定します。デフォルト値は 300 秒です (5 分)。

これらのパラメータの値を大きくすると、PlateSpin Server がターゲット VM 上の VMware フロッピーデバイスに対して読み書きを試みる頻度が減ります。

VMware フロッピーデバイスに対する読み書きのトラフィックを削減するには :

1. PlateSpin Server にログインして、次の PlateSpin Server 設定ページを開きます。

   https://*Your_PlateSpin_Server*/platespinconfiguration/

2. 設定サービスのポーリングパラメータを検索して、必要に応じてそれらの値を変更し、**保存**をクリックします。

   次に例を示します。

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

   または

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

3. 増分または完全レプリケーションを実行します。

レプリケーションにより、変更された設定もターゲット VM にプロパゲートされます。

4 影響を受けるワークロードに対して［フェールオーバーのテスト］または［フェールオーバー］を再度実行します。

遅延を増やすように起動タイプを変更する

リソースがアクセス可能になる前に、設定サービスが起動する場合があります。遅延が増大するように設定サービスの起動タイプを変更することができます。

起動タイプを変更するには :

1 PlateSpin Server にログインして、次の PlateSpin Server 設定ページを開きます。

https://*Your_PlateSpin_Server*/platespinconfiguration/

2 パラメータ **windowsConfigServiceStartType** を検索します。

3 **windowsConfigServiceStartType** 値を **AutoDelay** に変更します。

windowsConfigServiceStartType のオプションを以下に示します。

- **GroupDelay** はデフォルト値であり、レジストリの **ServiceGroupOrder** の最後に設定サービスを追加します。
- **AutoDelay** は、サービスが開始される前に待機する時間を最大化します (ブートの 2 分後)。また、ステップ 4 で **ServicesPipeTimeoutForWindowsConfigService** パラメータ値を変更します。
- **NoDelay** は最も効果的なオプションであり、Windows が実行されるとただちにサービスを起動します。ただしこれは、リソースへの接続時に問題が発生する可能性があるため、お勧めしません。

4 (AutoDelay) **ServicesPipeTimeoutForWindowsConfigService** パラメータ設定を 180 秒に変更します。これにより、ステップ 3 で **windowsConfigServiceStartType** に対して AutoDelay を設定したときに、サービスがブート後に起動するのにかかる時間が 120 秒を占めるようになります。

5 **保存**をクリックします。

6 増分または完全レプリケーションを実行します。

レプリケーションにより、変更された設定もターゲット VM にプロパゲートされます。

7 影響を受けるワークロードに対して［フェールオーバーのテスト］または［フェールオーバー］を再度実行します。

起動時に競合するサービスが自動的に実行されないように設定する

フェールオーバーアクション時に、Windows サービスはフロッピードライブのマウントに干渉します。

再起動時に起動するように設定される Windows サービスを決定します。ワイヤレス設定やウィルス対策ソフトウェアなど、設定サービスによるフロッピーへの書き込みに干渉するサービスがいくつかあることが分かっています。これらのサービスが［フェールオーバーのテスト］または［フェールオーバー］で自動的に実行されないように設定してから、［フェールオーバーのテスト］または［フェールオーバー］を再度実行する必要があります。

環境設定ページで［フェールオーバーのテスト］または［フェールオーバー］に対して不必要なすべてのサービスを無効にしてから、［フェールオーバーのテスト］または［フェールオーバー］を再度実行することもできます。

18.3.3 追加のトラブルシューティングのヒント

設定サービスが PlateSpin Server に接続できない場合、診断ではその全体像の一部しか明らかになりません。ターゲット VM からログを取得することも必要です。

- **Windows ワークロード :** 設定サービスのログは、C:\windows\platespin\configuration\data フォルダにあります。
  - log.txt ファイルにはログに記録されたすべての情報が含まれていますが、設定内容を把握する際には Config.ini ファイルが役に立ちます。
  - result.txt ファイルには、実行された設定サービスのステータスが記載されています。
  - ターゲット VM が入力フロッピーデバイスから読み取りできない場合、マージされた Config.ini ファイルが用意されません。このファイルには、テストフェールオーバーネットワーク環境に関するカスタムネットワーク環境設定情報が含まれている場合があります。
  - Config.ini ファイルにネットワーク関連情報 ([NIC0] など) がない場合、ターゲット VM ネットワークアダプタの名前に特殊文字が含まれる場合があります。

    既知の問題として、Config.ini ファイルがフロッピーデバイスからのものとマージされるまで正確でない場合がある、ということが挙げられます。
  - ターゲット VM は、出力フロッピーまたは入力フロッピーに接続できない場合、再起動を試みます (1 回のみ)。この場合は、config.ini.floppyreboot ファイルを参照します。
- **Linux ワークロード :** 設定サービスのログは、/tmp フォルダにあります。
  - 主要なログのファイル名は file*.platespin.fileLogger です。

    /tmp にある設定フォルダを調べることをお勧めします。file*.platespin.fileLogger ファイルを含む設定フォルダに Tar コマンドを実行して、Micro Focus ご注文と配送に送信します。
  - チェック対象となるその他の config ファイルとして以下が挙げられます。

    /tmp/Ofx.RunCommand.Output*

    /tmp/*DiskHelper*

    /tmp/*VmTools*
  - 環境設定ファイルは、/usr/lib/psconfigservice/data/config.conf です。
  - 最終結果ログファイルは、/usr/lib/psconfigservice/data/result.txt です。

18.4 ワークロード準備レプリケーションのトラブルシューティング (Windows)

問題またはメッセージ	解決方法
ソース上のコントローラを設定中にコントローラの接続を確認すると認証エラーが発生します。	ワークロードを追加するのに使用されるアカウントがこのポリシーによって許可される必要があります。187 ページの 「グループポリシーおよびユーザ権限」を参照してください。
.NET Framework がインストールされているかどうか判別できません (例外 : このワークステーションとプライマリドメインの間の信頼性のある関係が設定されていません)。	ソースのリモートレジストリサービスが有効であり、開始されているかどうかを確認してください。133 ページの 「Windows ワークロードの検出のトラブルシューティング」も参照してください。

18.4.1 グループポリシーおよびユーザ権限

PlateSpin Protect がソースワークロードのオペレーティングシステムとやり取りを行う手段のため、ワークロードを追加するのに使用される管理者アカウントがソースマシンに対して特定のユーザ権限を持つことが必要です。ほとんどのインスタンスでは、これらの設定はグループポリシーのデフォルトです。ただし、環境がロックダウンされている場合、次のユーザ権限の割り当てが削除される可能性があります。

- 走査チェックのバイパス
- プロセスレベルトークンの置き換え
- オペレーティングシステムの一部として機能

これらのグループポリシーの設定が行われていることを確認するために、ソースマシンのコマンドラインから gpresult /v を実行するか、その代わりに RSOP.msc を実行することができます。ポリシーが設定されていないか、無効化されている場合、マシンのローカルセキュリティポリシー経由またはマシンに適用される任意のドメイングループポリシー経由のいずれかで有効化できます。

gpupdate /force を使用すると、直ちにポリシーをリフレッシュできます。

18.4.2 2 つ以上のボリュームの同じボリュームシリアル番号がある

問題 : Windows サーバの保護を設定しようとする際に、次のエラーが表示されます。

［ソース］2 つ以上のボリュームの同じシリアル番号があります。ボリュームが固有となるようにシリアル番号を変更しマシンを再検出してください。

解決策 : この問題は、2 つ以上のボリュームのボリュームシリアル番号が同じ場合に発生することがあります。PlateSpin Protect では、シリアル番号を固有にする必要があります。

この問題を解決するには、データボリュームのシリアル番号を適宜変更して、マシンを再検出してください。Windows のネイティブツールを使用してシリアル番号を変更する方法については、「ナレッジベースの記事 7921101」を参照してください。

18.5 ワークロードレプリケーションのトラブルシューティング

問題またはメッセージ	解決方法
仮想マシンのスナップショット取得のスケジュールまたは**開始前に仮想マシンをスナップショットに戻すようにスケジュールする**のいずれかのレプリケーション中に回復可能なエラーが発生しました。	この問題は、サーバに負荷がかかっているため、プロセスの処理に予想よりも時間がかかっている場合に発生します。 レプリケーションが終了するまで待ちます。

問題またはメッセージ	解決方法
暗号化を有効にすると、ファイルベースの増分レプリケーションが完了しない	ファイルベースのデータ転送の対象に設定されている Windows ワークロードの暗号化を有効にすると、増分レプリケーションの転送終了時に Windows レシーバがハングすることがあります。このハングは、暗号化プロセスによって、転送で読み込まれた最後のバイトが間違ってゼロ以外の値に設定された場合に発生します。これは転送するファイルがほかにもあり、ストリームからの読み込みを続行することを意味します。 レプリケーションデータの転送で暗号化を有効にする場合、Windows ワークロードに対してはブロックベースのデータ転送を使用できます。
ワークロード問題でユーザの介入が必要	いくつかのタイプの問題によってこのメッセージが出される可能性があります。ほとんどの場合は、メッセージに問題の特性および問題領域 (接続、資格情報など) に関するもっと詳しい情報が含まれているはずです。トラブルシューティングの後、しばらく待ちます。 メッセージが引き続き表示される場合は、PlateSpin Support に連絡してください。
ディスク領域が不足しているので、すべてのワークロードが回復可能なエラーになっています。	空き領域を確認します。より多くの領域が必要な場合は、ワークロードを削除します。
VM コンテナに多くのデータストアがあると、WAN を通じた保護に時間がかかる	特定の状況下では、ターゲットのブートに必要となる適切な ISO イメージを見つけるのに予想以上の時間がかかります。PlateSpin Server が WAN を通じて VM コンテナに接続されており、VM コンテナに多くのデータストアがある場合に、この状況が発生することがあります。
ネットワーク速度が 1MB 未満で遅い。	ソースマシンのネットワークインタフェースカードがデュプレックス設定でオンになっており、接続先のスイッチの設定と整合していることを確認します。つまり、スイッチが自動に設定されている場合、ソースを 100MB には設定できません。
ネットワーク速度が 1MB 超で遅い。	ソースワークロードから次のコマンドを実行して遅延時間を測定します。 ping *ip* –t (*ip* をご使用の PlateSpin Server ホストの IP アドレスと置き換えます)。 50 回反復して実行するようにし、平均値が遅延時間を示します。 72 ページの 「WAN 接続を使用したデータ転送の最適化」も参照してください。
ファイル転送を開始できません - ポート 3725 がすでに使用中です または 3725 接続できません	ポートが開いてリッスンしていることを確認します。 ワークロード上で netstat -ano を実行します。 ファイアウォールを確認します。 レプリケーションを再試行します。
コントローラの接続が確立されていません レプリケーションが**仮想マシンの制御の取得**手順で失敗する。	このエラーは、レプリケーションのネットワーク情報が無効な場合に発生します。DHCP サーバが利用できないか、レプリケーションの仮想ネットワークが PlateSpin Server ホストにルートできません。 レプリケーション IP をスタティック IP に変更するか、DHCP サーバを有効にします。 レプリケーションに選択された仮想ネットワークが PlateSpin Server ホストに対してルート可能であることを確認します。

問題またはメッセージ	解決方法
レプリケーションジョブが開始しない (0% でスタック)	このエラーには複数の原因があり、それぞれに固有の解決策があります。 ◆ 認証を有効にしたローカルプロキシを使用している環境では、プロキシをバイパスするか適切な権限を追加してこの問題を解決します。ナレッジベースの記事 7920339 (https://www.netiq.com/support/kb/doc.php?id=7920339) を参照してください。 ◆ ローカルポリシーまたはドメインポリシーによって必要な許可が制限される場合、ナレッジベースの記事 7920862 (https://www.netiq.com/support/kb/doc.php?id=7920862) で説明されている手順に従います。 これは、PlateSpin Server ホストがドメインに加入しており、ドメインポリシーが制限付きで適用されている場合に見られる一般的な問題です。詳細については、187 ページの 「グループポリシーおよびユーザ権限」を参照してください。
Windows Update を実行した後は、C:\Windows\SoftwareDistribution フォルダにあるファイルの一部が、ファイルベースの増分レプリケーションでターゲットに転送されなくなります。	これは、Microsoft Windows で一般的な動作です。最適化の目的から、一部のファイルを VSS スナップショットから除外するために、HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot レジストリキーでこれらのファイルが削除対象としてマークされます。詳しくは、Microsoft Developer Network の記事 *「Excluding Files from Shadow Copies」* (http://msdn.microsoft.com/en-us/library/aa819132.aspx) を参照してください。 一般的に、これらのファイルは、Windows Update のインストールで使用されてから削除されるので、Windows Update の実行後は不要になります。これらのファイルを復元するには、フェールオーバー後のターゲットマシン上で Windows Update を実行し、SoftwareDistribution フォルダを元の場所に戻します。

18.6 ワークロードのフェールオーバーまたはフェールバックのトラブルシューティング

問題またはメッセージ	解決方法
フェールバック後に Active Directory ドメインサービスが利用できない (Windows)	chkdsk エラーが発生する場合、フェールオーバー後に Active Directory ドメインサービスが起動しない可能性があります。次の 2 つの chkdsk エラーは回避可能です。 ◆ 最初の完全レプリケーションの実行時にソースマシンに Microsoft 推奨のすべてのパッチまたはアップデートが適用されていない場合の Microsoft Update 関連のログファイル。 ◆ ウィルス対策ソフトウェアから除外する必要があるシステムファイルとシステムフォルダ。 これらの問題を回避するには、最初の完全レプリケーションを実行する前に、153 ページのセクション 15.1「ワークロード保護の前提条件」に記載されているベストプラクティスに従ってください。

問題またはメッセージ	解決方法
フェールバック時に間違った NIC がマッピングされ、フェールバックがハングする	次のいずれかの回避策を使用して、フェールバックが正常に完了するようにします。 ◆ ターゲットが正常に設定されるように、IP 設定を予期されるマッピングに切り替えます。 ◆「takecontrol」ハードウェアを LRD で再起動して、フェールバックターゲットとしてそれを使用するために手順を繰り返します。次回は Protect が正しい Ethernet インタフェースにマッピングされる可能性が高いです。 ◆ Web インタフェースで、ファールバックが完了間際にハングするように思われる場合は、フェールバックターゲットがフェールバックが完了したことを PlateSpin Server と通信できない可能性があります。目的のネットワーク上に正しい NIC が配置されるように、フェールバックターゲットの背部にあるネットワークケーブルを切り替えます。これにより、フェールバックターゲットが PlateSpin Server と通信できるようになり、フェールバックが完了します。
Linux ワークロードの X2P フェールバックにより、X Server グラフィカルユーザインタフェースで障害が発生する	VMware Tools のインストール時に、フェールオーバーした VM が再設定されることによって、この問題が発生します。これを修正するには、次のコマンドを使用して、ファイル名に BeforeVMwareToolsInstall という文字列を持つファイルを検索します。 find / -iname '*BeforeVMwareToolsInstall' 当該ファイルをすべて確認した後で、これらのファイルを元の場所に戻し、ワークロードを再起動して、ワークロードの X Server インタフェースを修正してください。

18.7 PlateSpin Protect データベースの縮小

PlateSpin Protect データベース (OFX、PortabilitySuite、および Protection) が事前定義された容量に達すると、それらのデータベースのクリーンアップが定期的に行われます。それらのデータベースのサイズまたはコンテンツをさらに制限する必要がある場合、Protect では、それらのデータベースのさらなるクリーンアップと縮小を行うためのユーティリティ (PlateSpin.DBCleanup.exe) が提供されています。ナレッジベースの記事 7006458 (https://www.netiq.com/support/kb/doc.php?id=7006458) に、ツールの場所、およびオフラインのデータベース操作で使用する場合に利用可能なオプションの説明が記載されています。

18.8 保護後のワークロードのクリーンアップ

次の手順を使用して、必要に応じて (たとえば、保護の失敗や問題が発生した後など) すべての PlateSpin ソフトウェアコンポーネントからソースワークロードをクリーンアップします。

- 191 ページのセクション 18.8.1「Windows ワークロードのクリーンアップ」
- 191 ページのセクション 18.8.2「Linux ワークロードのクリーンアップ」

18.8.1 Windows ワークロードのクリーンアップ

コンポーネント	削除手順
PlateSpin ブロックベース転送コンポーネント	ナレッジベースの記事 7005616 (https://www.netiq.com/support/kb/doc.php?id=7005616) を参照してください。
サードパーティのブロックベースの転送コンポーネント (提供中止)	1. Windows の［プログラムの追加と削除］アプレット (appwiz.cpl) を使用し、コンポーネントを削除します。ソースに応じて、次のいずれかのバージョンが存在します。 ◆ SteelEye Data Replication for Windows v6 Update2 ◆ SteelEye DataKeeper For Windows v7 2. マシンを再起動します。
ファイルベースの転送コンポーネント	保護されている各ボリュームのルートレベルで、PlateSpinCatalog*.dat という名前のファイルをすべて削除します。
ワークロードインベントリソフトウェア	ワークロードの Windows ディレクトリで次を実行します。 ◆ machinediscovery* という名前のすべてのファイルを削除します。 ◆ platespin という名前のサブディレクトリを削除します。
コントローラソフトウェア	1. ソースワークロード上でコマンドプロンプトを開き、現在のディレクトリを以下に変更します。 ◆ \Program Files\platespin* (32 ビットシステムの場合) ◆ \Program Files (x86)\platespin* (64 ビットシステムの場合) 2. 次のコマンドを実行します。 ofxcontroller.exe /uninstall 3. platespin* ディレクトリを削除します。.

18.8.2 Linux ワークロードのクリーンアップ

コンポーネント	削除手順
コントローラソフトウェア	◆ 次のプロセスを終了します。 ◆ pkill -9 ofxcontrollerd ◆ pkill -9 ofxjobexec ◆ 次のように、OFX コントローラ RPM パッケージを削除します。 rpm -e ofxcontrollerd ◆ ワークロードのファイルシステムで、/usr/lib/ofx ディレクトリを内容ごと削除します。

コンポーネント	削除手順
ブロックレベルのデータ転送ソフトウェア	1. ドライバがアクティブであるかどうかを確認します。 lsmod | grep blkwatch ドライバが引き続きメモリにロードされている場合、結果には以下と類似する行が含まれるはずです。 blkwatch_7616 70924 0 2. (条件付き) ドライバがロードされている場合、メモリからそれを削除してください。 rmmod blkwatch_7616 3. 次のブートシーケンスからドライバを削除します。 blkconfig -u 4. 次のディレクトリを内容と共に削除することにより、ドライバファイルを削除します。 /lib/modules/*[Kernel_Version]*/Platespin 5. 次のファイルを削除します。 /etc/blkwatch.conf
LVM スナップショット	進行中のレプリケーションで使用される LVP スナップショットは、*volume_name*-PS-snapshot 規則に従って名前が付けられます。たとえば、LogVol01 ボリュームには、LogVol01-PS-snapshot という名前が付けられます。 LVM スナップショットを削除するには : 1. 次のいずれかの方法を使用して、必要なワークロードでスナップショットのリストを生成します。 ◆ Web インタフェースを使用して、失敗したジョブのジョブレポートを生成します。レポートには LVM スナップショットに関する情報と名前が含まれているはずです。 - または - ◆ 必要な Linux ワークロードで、次のコマンドを実行しすべてのボリュームおよびスナップショットのリストを表示します。 # lvdisplay -a 2. 削除するスナップショットの名前とロケーションを書き留めます。 3. 次のコマンドを使用してスナップショットを削除します。 lvremove *snapshot_name*

コンポーネント	削除手順
NSS スナップショット	継続的なレプリケーションのために、PlateSpin によって作成され使用される NSS スナップショット。スナップショット名の最後には、接頭辞 PSSNP が付きます。 これらの NSS スナップショットを削除するには : 1. 次のいずれかの方法を使用して、必要なワークロードでスナップショットのリストを生成します。 ◆ Web インタフェースを使用して、失敗したジョブのジョブレポートを生成します。レポートには NSS スナップショットに関する情報と名前が含まれているはずです。 **- OR -** ◆ 必要な Open Enterprise Server ワークロード上で、次のコマンドを入力してすべての NSS スナップショットのリストを表示します。 # NLVM list snaps **- OR -** ◆ 必要な Open Enterprise Server ワークロード上で、NSSMU を起動し、**スナップショット**を選択してスナップショットのリストを表示します。 2. 削除するスナップショットの名前とロケーションを書き留めます。 3. Open Enterprise Server ワークロード上で、次のいずれかの方法を使用して、適切なスナップショットを削除します。 ◆ 次のコマンドを入力します。 NLVM delete snap <*snapshot_name*> **- OR -** ◆ NSSMU を起動し、**スナップショット**を選択します。削除するスナップショットごとに、そのスナップショットをハイライトして、［削除］を押します。
ビットマップファイル	保護されているボリュームごとに、ボリュームのルートで該当する .blocks_bitmap ファイルを削除します。
ツール	ソースワークロード上で、/sbin から次のファイルを削除します。 ◆ bmaputil ◆ blkconfig

V PlateSpin ツール

PlateSpin Protect では、保護環境を強化するための追加のツールが用意されています。

E PlateSpin Protect Server API 経由でのワークロード保護機能の使用

アプリケーション内から PlateSpin Protect Server API (protectionservices) を使用することで、PlateSpin Protect のワークロード保護機能をプログラムで利用できます。HTTP クライアントおよび JSON シリアル化フレームワークをサポートしている任意のプログラミング言語またスクリプト言語を使用できます。

注 : Protect Server API は実験段階です。この項の情報はテクノロジプレビューとして提供されています。

E.1 API の概要

PlateSpin Protect では、REST ベースの API テクノロジプレビューが公開されており、開発者は、この製品と連携させる独自のアプリケーションを構築する際にこの API を使用できます。この API には、次の操作に関する情報が含まれます。

- コンテナの検出
- ワークロードの検出
- 保護の設定
- レプリケーション、フェールオーバー操作、およびフェールバックの実行
- ワークロードおよびコンテナの状態の問い合わせ
- 実行している操作の状態の問い合わせ
- セキュリティグループとその保護対象の問い合わせ

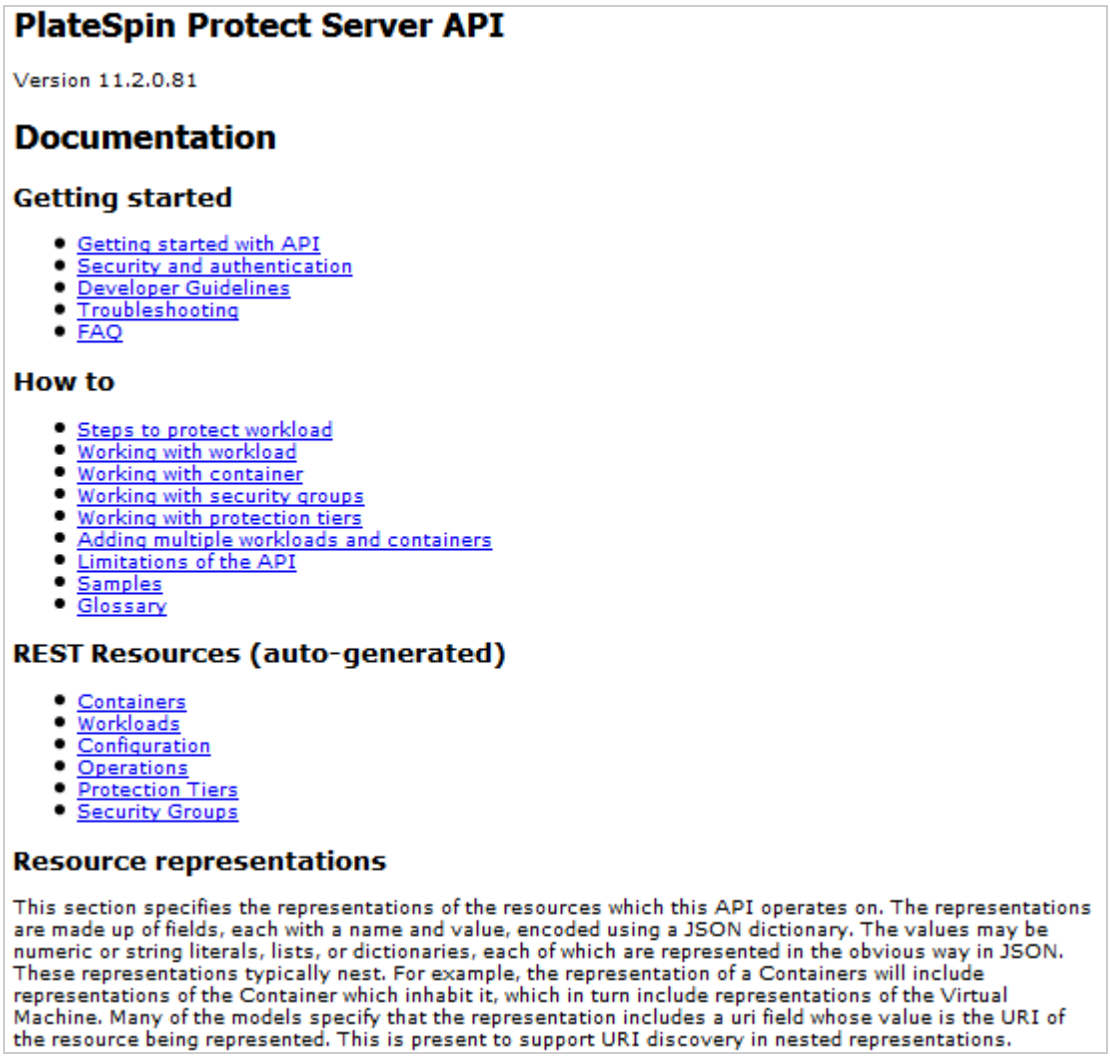
E.2 PlateSpin Protect Server API のマニュアル

protectionservices に関する PlateSpin Protect Server API ホームページでは、開発者と管理者にとって有用なマニュアルとサンプルが提供されています。詳細については、PlateSpin Server ホストで次の場所にアクセスしてください。

https://*Your_PlateSpin_Server*/protectionservices

Your_PlateSpin_Server を PlateSpin Server ホストのホスト名または IP アドレスに置き換えます。SSL が有効でない場合は、URI に http を使用します。

図 E-1 Protect Server API のホームページ



E.3 サンプルとその他の参照情報

Protect 管理者は、コマンドラインから JScript サンプルを利用して、この製品に API を介してアクセスできます。PlateSpin Server ホストで、次の場所にあるサンプルを参照してください。

https://localhost/protectionservices/Documentation/Samples/protect.js

このサンプルは、製品連携のスクリプトをコーディングする助けになります。コマンドラインユーティリティを使用して、次の操作を実行できます。

- 単一ワークロードの追加
- 単一コンテナの追加
- レプリケーション、フェールオーバー、およびフェールバック操作の実行
- 複数のワークロードおよびコンテナの同時追加

注 : この操作の詳細については、次の場所にある API ドキュメントを参照してください。

https://localhost/protectionservices/Documentation/AddWorkloadsAndContainersFromCsvFile.htm

- すべてのワークロードの同時削除
- すべてのコンテナの同時削除

ワークロード保護の一般的な操作を記述するには、Python で記述された参考のサンプルをガイドとして使用してください。Microsoft Silverlight アプリケーションとそのソースコードも、参照目的で提供されています。

F iPerf ネットワークテストツールを使用した PlateSpin 製品のネットワークスループットの最適化

レプリケーションを実行する前に、接続テストを行なって、接続または帯域幅に関する問題があるかどうかを確認し、問題がある場合は解決してください。この項では、オープンソースの iPerf ネットワークテストツールを使用して、接続のスループットを最適化する方法について説明します。

F.1 はじめに

PlateSpin 管理者が、PlateSpin 製品を使用する際に、より良いネットワークスループットを得るために、PlateSpin LRD (Linux RAM ディスク) 管理環境には、iPerf ネットワークテストツールが用意されています。iPerf マニュアルには次のように明記されています : 「iPerf の主要な目的は、特定のパスを介した TCP 接続の微調整を支援することです。TCP に関する最も基本的な微調整の上の問題点は、TCP ウィンドウサイズです。このサイズにより、ネットワークの任意の 1 つのポイントにおけるデータ量が制御されます。」

この README の目的は、PlateSpin 製品の使用に関連して、ネットワークの微調整とテストの基本的な方法について説明することです。最初に、理論上の最適な TCP ウィンドウサイズを計算します。次に、iPerf ツールを使用して、計算されたこのサイズの検証と微調整を行い、発生したスループットを測定します。この方法を使用すると、特定のネットワークで実際に達成できるスループットを決定する際にも役立ちます。

iPerf ツールと PlateSpin 製品では両方とも、実際に *TCP 送受信バッファサイズ*を使用しており、*TCP ウィンドウサイズ*の最終的な内部選択に影響を与えています。将来、これらの用語は区別しないで使われるようになります。

注 : ネットワークスループットに影響を与える要因は多数あります。インターネット上には、理解するのに役立つ豊富な情報があります。このようなリソースの 1 つとして*ネットワークスループットカルキュレータ* (http://wintelguy.com/wanperf.pl) が挙げられます。これは、当該のカスタマーネットワークの特性を考慮して、予想される最大 TCP スループットを計算する際に役立ちます。スループットに関する予想値を適切に設定するために、このオンラインカルキュレータを使用することを強くお勧めします。

F.2 計算

TCP ウィンドウサイズの微調整は、ネットワークリンク速度やネットワークレイテンシを含む、多数の要因に基づいて行われます。PlateSpin 製品に関連する目的の場合、微調整の際の TCP ウィンドウサイズの最初の選択は、次のような標準の計算式 (インターネットやその他の場所で広く使用されています) に基づいて行われます。

ウィンドウサイズ (バイト)=((リンク速度 (Mbps)/8)* 遅延 (秒))*1000*1024

たとえば、150 ミリ秒の遅延のある 54Mbps のリンクでは、適切な初期ウィンドウサイズは次のようになります。

(54/8)*0.15*1000*1024 = 1,036,800 バイト

10 ミリ秒の遅延のある 1000Mbps のリンクでは、適切な初期ウィンドウサイズは次のようになります。

(1000/8)*.01*1000*1024 = 1,280,000 バイト

ネットワークのレイテンシ値を取得するには、コマンドプロンプト (Windows) または端末 (Linux) から ping を使用します。ping 往復時間 (RTT) はおそらく実際のレイテンシと異なっていますが、得られた値はこの方法で使用する分には十分な精度です。

以下に、Windows ping コマンドのサンプル出力を示します。これにより、レイテンシが平均で 164 ms であることがわかります。

ping 10.10.10.232 -n 5

```
Pinging 10.10.10.232 with 32 bytes of data:
Reply from 10.10.10.232: bytes=32 time=154ms TTL=61
Reply from 10.10.10.232: bytes=32 time=157ms TTL=61
Reply from 10.10.10.232: bytes=32 time=204ms TTL=61
Reply from 10.10.10.232: bytes=32 time=153ms TTL=61
Reply from 10.10.10.232: bytes=32 time=153ms TTL=61

Ping statistics for 10.10.10.232:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 153ms, Maximum = 204ms, Average = 164ms
```

以下に、Linux ping コマンドのサンプル出力を示します。これにより、レイテンシが平均で 319 ms であることがわかります。

ping 10.10.10.232 -c 5

```
PING 10.10.10.232 (10.10.10.232) 56(84) bytes of data.
64 bytes from 10.10.10.232: icmp_seq=1 ttl=62 time=0.328 ms
64 bytes from 10.10.10.232: icmp_seq=2 ttl=62 time=0.280 ms
64 bytes from 10.10.10.232: icmp_seq=3 ttl=62 time=0.322 ms
64 bytes from 10.10.10.232: icmp_seq=4 ttl=62 time=0.349 ms
64 bytes from 10.10.10.232: icmp_seq=5 ttl=62 time=0.316 ms

--- 10.10.10.232 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.280/0.319/0.349/0.022 ms
```

実際には、レイテンシ値をより高精度で測定するために、-n または -c オプションを使用して、より多くの ping パケットを指定する必要があります。

F.3 設定

iPerf ツールは、サーバモードまたはクライアントモードで実行されます。

iperf サーバモードの基本的な使用構文は次の通りです。

```
iperf -s -w <win_size>
```

iperf クライアントモードの基本的な使用構文は次の通りです。

```
iperf -c <server_ip> -w <win_size>
```

私達の目的は、ソースとターゲットワークロードの間のネットワークを測定して微調整することです。多くの場合、これらは実際に使用されているソースとターゲットになります。ソースまたはターゲットに対して別のワークロードを使用してテストを完了したい場合は、その代替のワークロードが、元のものと同じネットワーク特性 (NIC やネットワーク接続など) を持っていることが必要です。

注 : PlateSpin サーバからソースまたはターゲットへのスループットはテストしないようにしてください。なぜなら、このトラフィックは最小限のものであり、マイグレーションやレプリケーション時に発生するトラフィックを表していないからです。

ターゲット /iperf サーバとしてライブワークロード (Windows または Linux) を使用できますが、以下の手順は、マイグレーション / レプリケーション時の環境に最も近い環境が実現されるので、強くお勧めします。

ターゲット上で iperf を設定して実行するには :

1. LRD を使用してターゲット起動します。
2. LRD コンソールで、ヘルパーターミナル (Alt-F2 を介してアクセス可能) を使用して、以下の操作を実行します。
   - **2a** オプション 5 を使用してネットワーキングを設定します。
   - **2b** オプション 6 を使用して CD メディアをマウントします。
3. LRD コンソールで、デバッグターミナル (Alt-F7 を介してアクセス可能) に切り替えて、次のコマンドで iPerf ツールの場所に移動します。

   ```
   cd /mnt/cdrom/LRDTools/iperf_2.0.X/linux
   ```

4. サーバモードで iPerf ツールを実行します。以下を入力してください。

   ```
   ./iperf -s -w <win_size>
   ```

ソース上で iperf を設定して実行するには :

1. ソフトウェアまたは物理メディアを使用して LRD ISO をマウントします。
2. コマンドプロンプト (Windows) または端末 (Linux) を開いて、iPerf ツールの場所に移動します :

   ```
   cd <media>/LRDTools/iperf_2.0.X/
   ```

3. ソースオペレーティングシステムによって決定された通りに、windows または linux サブディレクトリに移動します。

```
cd windows

-OR-

cd linux
```

4 クライアントモードで iPerf ツールを実行します。以下を入力してください。

```
iperf -c <target_ip> -w <win_size>
```

注 : 計算のために iperf3 をダウンロードして使用することができます。これは、iperf2 で有効なスループット数を生成できない特定のシナリオにおいて役に立ちます。iperf3 のコマンド構文と出力は若干異なりますが、必要に応じて、新しい出力を調整するとかなり分かりやすくなります。

F.4 手法

計算セクションで計算された初期の win_size から始めて、計算値だけでなく若干大きい値と小さい値を使用して iPerf ツールの数回の反復から得られた出力を記録します。win_size を元の値の約 10% の増分で増減させることをお勧めします。

たとえば、上記の 1,280,000 バイトの例では、約 100,000 バイトの増分で win_size を増減させることができます。

注 : iperf の -w オプションを使用すると、K (キロバイト) または M (メガバイト) などの単位指定が可能です。

同じ例を使用して、手順 4 の win_size として、1.28M、1.38M、1.18M などの -w 値を使用することができます。もちろん、iPerf ツールの各反復に対してのみ実行ステップが繰り返されると仮定されています。

iperf クライアントの反復から得られたサンプル出力は次のようになります。

```
iperf.exe -c 10.10.10.232 -w 1.1M

------------------------------------------------------------
Client connecting to 10.10.10.232, TCP port 5001
TCP window size: 1.10 MByte
------------------------------------------------------------
[296] local 10.10.10.224 port 64667 connected with 10.10.10.232 port 5001
[ ID] Interval       Transfer     Bandwidth
[296]  0.0-10.2 sec  11.3 MBytes  9.29 Mbits/sec
```

参照されるターゲットサーバから得られたサンプル出力は次のようになります。

```
./iperf -s -w .6M

------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 1.20 MByte (WARNING: requested 614 Kbyte)
------------------------------------------------------------
[  4] local 10.10.10.232 port 5001 connected with 10.10.10.224 port 64667
[  4] 0.0-10.2 sec  11.3 MBytes  9.29 Mbits/sec
```

注 :

- クライアントは、1 回の反復の後サーバから切断されますが、サーバは、Ctrl-C を使用して停止するまでリスンし続けます。
- Linux サーバに対して指定されたウィンドウサイズは、目標値の 1/2 です。なぜなら、Linux では当然のことながら要求された TCP バッファサイズを 2 倍にするからです。

数回の反復を使用して、TCP ウィンドウサイズの最適値を決定します。Linux 上で iperf に対して -w オプションを指定した場合には、目標値の 1/2 しか使用されないことを忘れないでくだい。

スループットの増大は、最適な TCP ウィンドウサイズに近づいていることを示しています。最後に、最適な値に近づくにつれて、実際の実行条件をより厳密にシミュレートするように反復の期間を長く使用してください。反復の期間を長くするには、iperf で -t <*time_in_seconds*> オプションを使用します。このオプションは、クライアント側でのみ指定する必要があります。

次に例を示します。

```
iperf.exe -c 10.10.10.232 -w 1.25M -t 60
```

最適値が決定されたら、以下の場所にある適切な PlateSpin サーバに対する FileTransferSendReceiveBufferSize パラメータでこの値を設定します。

https://<*my_ps_server*>/PlatespinConfiguration/

このグローバル値は、PlateSpin サーバ上のすべてのワークロードに適用されます。このため、ワークロードおよびそれらの個々のネットワークのグループ分けは、使用可能な PlateSpin サーバ全体について理にかなった方法で注意して行う必要があります。

F.5 期待事項

TCP 送受信バッファサイズを使用して間接的に TCP ウィンドウサイズを変更することは、特定のシナリオでネットワークスループットを増大させるのに非常に有効な方法となる可能性があります。場合によっては、元のスループットの 2 ～ 3 倍以上が達成されることもあります。ただし、使用パターン、ハードウェア、ソフトウェア、またはその他のインフラストラクチャの変更のために、ネットワーク特性が経時的に変化する可能性があります (多くの場合そうなります)。

計画されたライブマイグレーションまたはレプリケーションタスク時に使用しようとしている時刻でのネットワーク使用パターン下における最適値を計算するために、この方法を使用することを強くお勧めします。また、ネットワーク状態の変化に適応するためにこの設定を定期的に再計算することをお勧めします。