



PlateSpin Forge® 11.2

ユーザガイド

2015年10月

保証と著作権

本書および本書に記載されているソフトウェアには、使用許諾契約または守秘契約が適用され、これらの条項の下に提供されます。上記ライセンス契約または守秘契約に明示されている場合を除き、NetIQ社は、本書および本書に記載されているソフトウェアを「現状のまま」提供するものとし、明示的、黙示的を問わず、商品性または特定目的への適合性に対する黙示的な保証を含め、いかなる保証も行いません。州によっては、明示的、黙示的を問わず、特定の取引に関する保証の否認が認められていないため、この記述が適用されない場合もあります。

わかりやすくするため、すべてのモジュール、アダプタ、またはそれに類する要素(「モジュール」)は、そのモジュールが関連または相互作用するNetIQ製品またはソフトウェアの当該バージョンのエンドユーザ使用許諾契約の条項と条件に基づいてライセンスが供与されます。モジュールを接続、複製、または使用することは、これらの条項に従うことに同意したことになります。エンドユーザ使用許諾契約の条項に同意しない場合、モジュールを使用、接続または複製する権利はなく、モジュールのすべての複製を破棄していただく必要があります。詳細についてはNetIQにお問い合わせください。

本書および本書に記載されているソフトウェアは、法律によって認められた場合を除き、NetIQ社が書面をもって事前に許可しない限り、貸出、販売、譲渡することはできません。上記の使用許諾契約または守秘契約に明示されていない限り、NetIQ社の書面による事前の同意がない場合は、本書および本書に記載されているソフトウェアのいかなる部分も、電子的、物理的、またはその他の方式を問わず、いかなる形式や手段においても再現したり、情報取得システムに保存または転送することは禁じられています。本書に記載されている会社名、個人名、データは引用を目的として使用されており、実際の会社、個人、およびデータを示していないことがあります。

本書は技術的な誤りおよび誤植を含むことがあります。本書の情報は定期的に変更されます。定期的な変更は、本書の新版に組み込まれることがあります。NetIQ社は、本書に記載されているソフトウェアに対して、随時改良または変更を行うことがあります。

米国政府の制限付き権利：ソフトウェアおよび文書が、米国政府または米国政府の元請人または下請人(階層を問わず)によって直接または間接的に取得される場合は、48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) および 48 C.F.R. 2.101 および 12.212 (for non-DOD acquisitions) に基づき、ソフトウェアまたは文書の使用、修正、再生、リリース、実行、表示、開示などに関する政府の権利は、このライセンス契約に記載されている商用ライセンスの権利および制限に全面的に従うものとします。

© 2015 NetIQ Corporation. All Rights Reserved.

NetIQの商標については、<https://www.netiq.com/company/legal/> を参照してください。

ライセンスの許諾

PlateSpin Forge 11 以降のバージョン用に購入したライセンスを Platespin Forge 3.3 以前のバージョン用に使用することはできません。

サードパーティのソフトウェア

PlateSpin Forge で使用されているサードパーティのソフトウェアの詳細については、「*PlateSpin におけるサードパーティのライセンス使用法と著作権* (https://www.netiq.com/documentation/platespin_licensing/platespin_licensing_qs/data/platespin_licensing_qs.html)」のページを参照してください。

目次

本書およびライブラリについて	7
NetIQ 社について	9
1 PlateSpin 環境の計画	13
1.1 サポートされる構成	13
1.1.1 サポートされる Windows のワークロード	14
1.1.2 サポートされる Linux のワークロード	16
1.1.3 サポートされる VM コンテナ	18
1.1.4 サポートされるシステムファームウェア	19
1.1.5 サポートされるストレージ	19
1.1.6 PlateSpin Forge Web インタフェースでサポートされるブラウザ	20
1.2 セキュリティとプライバシー	21
1.2.1 送信中のワークロードデータのセキュリティ	21
1.2.2 クライアント/サーバ通信のセキュリティ	21
1.2.3 資格情報のセキュリティ	21
1.2.4 ユーザ権限および認証	21
1.2.5 ネットワークポート設定	22
1.2.6 その他のセキュリティ拡張機能	23
1.3 パフォーマンス	24
1.3.1 製品パフォーマンスの特性	24
1.3.2 データ圧縮	24
1.3.3 帯域幅制限	25
1.3.4 RPO、RTO、および TTO の仕様	25
1.3.5 スケーラビリティ	25
2 PlateSpin Forge アプリケーション環境設定	27
2.1 PlateSpin Forge Web インタフェースの起動	27
2.2 製品ライセンスの有効化	28
2.2.1 オンラインでのライセンスのアクティベーション	28
2.2.2 オフラインでのライセンスのアクティベーション	29
2.3 ユーザ権限および認証の設定	29
2.3.1 PlateSpin Forge の役割ベースのアクセスについて	29
2.3.2 PlateSpin Forge のアクセスおよび権限の管理	31
2.3.3 PlateSpin Forge 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	32
2.4 保護ネットワークにわたるアクセスおよび通信の設定	33
2.4.1 PlateSpin Server ホストおよび Forge VM Web インタフェース用に開くポートの要件	33
2.4.2 ワークロードに関するアクセスおよび通信の要件	34
2.4.3 コンテナに関するアクセスおよび通信の要件	36
2.4.4 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	36
2.4.5 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	37
2.4.6 コンテナとしての VMware DRS クラスターの要件	37
2.5 イベントおよびレポートの自動電子メール通知の設定	38
2.5.1 SMTP 設定	38
2.5.2 電子メールによる自動的なイベント通知のセットアップ	38
2.5.3 電子メールによる自動レプリケーションレポートのセットアップ	40
2.6 PlateSpin Forge の国際バージョンの言語設定	41
2.7 タグによるワークロードのソート	42
2.8 XML 環境設定パラメータを通じた PlateSpin Server の動作の構成	44

2.9	WAN 接続を使用したデータ転送の最適化	44
2.10	VMware vCenter Site Recovery Manager 用サポートの設定	47
2.10.1	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	47
2.10.2	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	47
2.10.3	設定プロセスの促進	49
3	アプライアンスのセットアップとメンテナンス	51
3.1	アプライアンスのネットワーキングの設定	51
3.1.1	アプライアンスホストのネットワーキングの設定	51
3.2	アプライアンスの物理的な移設	52
3.2.1	シナリオ 1 - Forge の移設 (新しい IP アドレスがわかっている場合)	52
3.2.2	シナリオ 2 - Forge の移設 (新しい IP アドレスがわからない場合)	53
3.3	PlateSpin Forge における外部ストレージソリューションの使用	54
3.3.1	Forge での SAN ストレージの使用	55
3.3.2	Forge への SAN LUN の追加	56
3.4	アプライアンスホストにおける Forge 管理 VM へのアクセスおよび使用	56
3.4.1	vSphere Client プログラムのダウンロード	57
3.4.2	vSphere Client の起動および Forge 管理 VM へのアクセス	57
3.4.3	Forge 管理 VM の起動とシャットダウン	57
3.4.4	アプライアンスホストでの Forge VM のスナップショットの管理	58
3.4.5	手動によるアプライアンスホストのデータストアへの VM のインポート	58
3.4.6	PlateSpin Forge 管理 VM にセキュリティ更新を適用する際のガイドライン	59
3.5	工場出荷時のデフォルトへの Forge のリセット	59
4	業務の常時稼働	61
4.1	PlateSpin Forge Web インタフェースへのアクセス	61
4.2	PlateSpin Forge Web インタフェースの要素	62
4.2.1	ナビゲーションバー	63
4.2.2	ビジュアルサマリパネル	63
4.2.3	タスクおよびイベントパネル	64
4.3	ワークロードおよびワークロードコマンド	64
4.3.1	ワークロードの保護と回復のコマンド	65
4.4	PlateSpin Protect および PlateSpin Forge の複数インスタンスの管理	66
4.4.1	PlateSpin Forge 管理コンソールの使用	66
4.4.2	PlateSpin Forge 管理コンソールについて	67
4.4.3	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	68
4.4.4	管理コンソールでのカードの管理	69
4.5	ワークロードとワークロード保護のレポートの作成	69
5	ワークロードの保護と回復	71
5.1	ワークロードの保護と回復の基本ワークフロー	71
5.2	コンテナの追加 (保護ターゲット)	73
5.3	ワークロードの追加	74
5.4	保護詳細の設定およびレプリケーションの準備	75
5.4.1	ワークロード保護の詳細	76
5.5	ワークロード保護の開始	79
5.6	コマンドの中止	80
5.7	フェールオーバー	80
5.7.1	オフラインワークロードの検出	80
5.7.2	フェールオーバーの実行	81
5.7.3	フェールオーバーのテスト機能の使用	81
5.8	フェールバック	82
5.8.1	VM プラットフォームへの自動化されたフェールバック	82

5.8.2	物理マシンへの半自動化されたフェールバック	85
5.8.3	仮想マシンへの半自動化されたフェールバック	86
5.9	ワークロードの再保護	86
6	ワークロード保護の要点	89
6.1	ワークロードライセンスの消費	89
6.2	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	90
6.3	データ転送	90
6.3.1	転送方法	91
6.3.2	データの暗号化	92
6.3.3	Windows ワークロードのボリュームスナップショットディレクトリの場所変更	92
6.3.4	増分レプリケーションのブロック転送でファイルを除外する場合、またはファイルを含める場合	93
6.4	保護ティア	93
6.5	復旧ポイント	95
6.6	初期レプリケーション方法 (フルおよび差分)	95
6.7	サービスおよびデーモンの制御	96
6.8	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)	97
6.9	ボリュームストレージ	97
6.10	ネットワークング	100
6.11	物理マシンへのフェールバック	100
6.11.1	PlateSpin ISO ブートイメージのダウンロード	100
6.11.2	ISO ブートイメージへのデバイスドライバの追加	100
6.11.3	PlateSpin Forge 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	102
6.12	Windows クラスターの保護	103
6.12.1	クラスターワークロードの保護	104
6.12.2	Windows クラスター検出の有効化または無効化	106
6.12.3	リソース名の検索値	106
6.12.4	クォーラムアービトレーションのタイムアウト	107
6.12.5	ローカルボリュームのシリアル番号の設定	107
6.12.6	PlateSpin のフェールオーバー	108
6.12.7	PlateSpin のフェールバック	108
7	物理マシンを操作するための補助ツール	109
7.1	デバイスドライバの管理	109
7.1.1	Windows システム用のデバイスドライバのパッケージ化	109
7.1.2	Linux システム用のデバイスドライバのパッケージ化	110
7.1.3	PlateSpin デバイスドライバデータベースへのドライバのアップロード	110
7.1.4	プラグアンドプレイ (PnP) ID トランスレータ機能の使用	112
8	ProtectAgent ユーティリティ	119
9	トラブルシューティング	123
9.1	ワークロードインベントリのトラブルシューティング (Windows)	123
9.1.1	接続性テストの実行	124
9.1.2	ウイルス対策ソフトウェアの無効化	126
9.1.3	ファイル/共有権限およびアクセスの有効化	126
9.2	ワークロードインベントリのトラブルシューティング (Linux)	127
9.3	レプリケーションの準備コマンドで発生した問題のトラブルシューティング (Windows)	127
9.3.1	グループポリシーおよびユーザ権限	128
9.4	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	128
9.5	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	130
9.6	オンラインヘルプのトラブルシューティング	130

9.7	診断レポートの生成および表示	131
9.8	ワークロードを削除しています	131
9.9	保護後のワークロードのクリーンアップ	132
9.9.1	Windows ワークロードのクリーンアップ	132
9.9.2	Linux ワークロードのクリーンアップ	133
9.10	PlateSpin Forge データベースの縮小	134
9.11	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)	134
A Forge 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		137
A.1	Linux ワークロードの分析	137
A.1.1	リリース文字列の決定	137
A.1.2	アーキテクチャの決定	138
A.2	PlateSpin Forge の事前コンパイルされた「blkwatch」ドライバ (Linux)	138
A.2.1	リスト項目の構文	138
A.2.2	ディストリビューションのリスト	138
A.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	139
B 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		141
C PlateSpin Forge Web インタフェースのブランディングの変更		143
C.1	環境設定パラメータによるインタフェースのブランディングの変更	143
C.2	Windows レジストリでの製品名ブランディングの変更	146
D PlateSpin Protect Server API 経由でのワークロード保護機能の使用		149
D.1	API の概要	149
D.2	PlateSpin Protect Server API のマニュアル	149
D.3	サンプルとその他の参照情報	150
用語集		153

本書およびライブラリについて

このユーザガイドでは、PlateSpin Forge の使用について説明します。概念面の情報、ユーザインタフェースの概要、および多用するタスクの手順を追った操作方法について説明しています。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、進行中のワークロード保護プロジェクトで PlateSpin Forge を使用するデータセンター管理者およびオペレータなどの IT スタッフを対象としています。

ライブラリに収録されている情報

この製品のライブラリは、[PlateSpin Forge マニュアル \(https://www.netiq.com/documentation/platespin-forge/\)](https://www.netiq.com/documentation/platespin-forge/) の Web サイトで HTML および PDF の 2 つの形式で提供されています。オンラインドキュメントは、英語のほか、日本語、簡体中国語、繁体中国語、フランス語、ドイツ語、およびスペイン語の各版があります。

PlateSpin Forge ライブラリには次の情報リソースが含まれています。

リリースノート

このリリースの新機能、機能強化、あらゆる既知の問題に関する情報を提供しています。

導入ガイド

ご使用の環境に合わせてアプライアンスを設定する方法について説明しています。

ユーザガイド

概念面の情報、ユーザインタフェースの概要、および多用するタスクの手順を追った操作方法について説明しています。

再構築ガイド

アプライアンスを再構築および再設定する方法について説明しています。

アップグレードガイド

アプライアンスソフトウェアをアップグレードする方法について説明しています。

その他の資料

次のオンラインリソースもご利用ください。

- [PlateSpin Forge フォーラム \(https://forums.netiq.com/forumdisplay.php?56-Platespin-Forge\)](https://forums.netiq.com/forumdisplay.php?56-Platespin-Forge): Web ベースの製品ユーザコミュニティです。他の製品ユーザと製品の機能に関する意見や助言を交換できます。

- ◆ [PlateSpin Forge 製品](https://www.netiq.com/products/forge/) (https://www.netiq.com/products/forge/): Web ベースの製品カタログです。製品の機能、購入方法、技術仕様、FAQ (よくある質問と答え)、ビデオやホワイトペーパーなどの各種リソースを紹介しています。
- ◆ [NetIQ ユーザコミュニティ](https://www.netiq.com/communities/) (https://www.netiq.com/communities/): さまざまなトピックについて議論する Web ベースのコミュニティです。
- ◆ [NetIQ サポートナレッジベース](https://www.netiq.com/support/kb/) (https://www.netiq.com/support/kb/): 詳しい技術情報の記事集です。
- ◆ [NetIQ サポートフォーラム](https://forums.netiq.com/forum.php) (https://forums.netiq.com/forum.php): Web上で製品ユーザがNetIQ製品の機能について議論したり、他の製品ユーザにアドバイスしたりできる場所です。
- ◆ [MyNetIQ](https://www.netiq.com/f/mynetiq/) (https://www.netiq.com/f/mynetiq/): プレミアムホワイトペーパーへのアクセス、Web キャストへの登録、製品の試用版のダウンロードなど、製品の情報やサービスを提供する Web サイトです。

NetIQ 社について

当社はグローバルなエンタープライズソフトウェア企業であり、お客様の環境において絶えず挑戦となる変化、複雑さ、リスクという3つの要素に焦点を当て、それらをお客様が制御するためにどのようにサポートできるかを常に検討しています。

当社の観点

変化に適応すること、複雑さとリスクを管理することは普遍の課題

実際、直面するあらゆる課題の中で、これらは、物理環境、仮想環境、およびクラウドコンピューティング環境の安全な評価、監視、および管理を行うために必要な制御を脅かす最大の要因かもしれません。

重要なビジネスサービスの改善と高速化を可能にする

当社は、IT 組織に可能な限りの制御能力を付与することが、よりタイムリーでコスト効率の高いサービス提供を実現する唯一の方法だと信じています。組織が継続的な変化を遂げ、組織を管理するために必要なテクノロジーが実質的に複雑さを増していくにつれ、変化と複雑さという圧力はこれからも増え続けていくことでしょう。

当社の理念

単なるソフトウェアではなく、インテリジェントなソリューションを販売する

確かな制御手段を提供するために、まずお客様の IT 組織が日々従事している現実のシナリオを把握することに努めます。そのようにしてのみ、実証済みで測定可能な結果を成功裏に生み出す、現実的でインテリジェントな IT ソリューションを開発することができます。これは単にソフトウェアを販売するよりもはるかにやりがいのあることです。

当社の情熱はお客様の成功を推し進めること

お客様が成功するためにわたしたちには何ができるかということが、わたしたちのビジネスの核心にあります。製品の着想から展開まで、当社は次のことを念頭に置いています。お客様は既存資産とシームレスに連動して動作する IT ソリューションを必要としており、展開後も継続的なサポートとトレーニングを必要とし、変化を遂げるときにも共に働きやすいパートナーを必要としています。究極的に、お客様の成功こそがわたしたちの成功なのです。

当社のソリューション

- ◆ ID およびアクセスのガバナンス
- ◆ アクセス管理
- ◆ セキュリティ管理
- ◆ システムおよびアプリケーション管理

- ◆ ワークロード管理
- ◆ サービス管理

セールスサポートへのお問い合わせ

製品、価格、および機能についてのご質問は、地域のパートナーへお問い合わせください。パートナーに連絡できない場合は、弊社のセールスサポートチームへお問い合わせください。

各国共通:	www.netiq.com/about_netiq/officelocations.asp
米国およびカナダ:	1-888-323-6768
電子メール:	info@netiq.com
Web サイト:	www.netiq.com

テクニカルサポートへのお問い合わせ

特定の製品に関する問題については、弊社のテクニカルサポートチームへお問い合わせください。

各国共通:	www.netiq.com/support/contactinfo.asp
北米および南米:	1-713-418-5555
ヨーロッパ、中東、アフリカ:	+353 (0) 91-782 677
電子メール:	support@netiq.com
Web サイト:	www.netiq.com/support

NetIQ 技術サポートのサービスと手順については、『*技術サポートガイド* (https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and)』を参照してください。

マニュアルサポートへのお問い合わせ

弊社の目標は、お客様のニーズを満たすマニュアルの提供です。この製品のマニュアルは、[PlateSpin Forge マニュアル](https://www.netiq.com/documentation/platespin-forge/) (<https://www.netiq.com/documentation/platespin-forge/>) の Web サイトで HTML および PDF の 2 つの形式で提供されています。

マニュアルを改善するためのご提案がございましたら、本マニュアルの HTML 版で、各ページの下にある **comment on this topic** をクリックしてください。Documentation-Feedback@netiq.com 宛てに電子メールを送信することもできます。貴重なご意見をぜひお寄せください。

オンラインユーザコミュニティへのお問い合わせ

NetIQ のオンラインコミュニティである NetIQ Communities は、他のユーザや NetIQ のエキスパートとやり取りできるコラボレーションネットワークです。より迅速な情報、有益なリソースへの役立つリンク、NetIQ エキスパートとのやり取りを提供する NetIQ Communities は、信頼のおける IT 投資が持つ可能性を完全に実現するために必要な知識を習得するために役立ちます。詳細については、<http://community.netiq.com> を参照してください。

1 PlateSpin 環境の計画

PlateSpin Forge は障害復旧のための統合ハードウェアアプライアンスで、組み込まれた仮想化技術により物理ワークロードと仮想ワークロード (オペレーティングシステム、ミドルウェア、およびデータ) を保護します。運用サーバの停止時または障害発生時には、ワークロードがすぐに PlateSpin Forge 復旧環境で稼働し、運用環境が復旧されるまで通常どおり実行し続けることができます。

PlateSpin Forge 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 (モデルに応じて 10 ~ 50)
- ◆ 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

内部の事前にパッケージ化されたストレージでは、Forge の合計ストレージ容量は最大 20 テラバイトとなります。ただし、iSCSI カードまたはファイバチャネルカードを追加して外部ストレージ構成を使用すると、容量はほとんど無制限となります。

この項の情報を使用して、保護および回復環境を計画します。

- ◆ [13 ページのセクション 1.1 「サポートされる構成」](#)
- ◆ [21 ページのセクション 1.2 「セキュリティとプライバシー」](#)
- ◆ [24 ページのセクション 1.3 「パフォーマンス」](#)

1.1 サポートされる構成

PlateSpin Forge はサーバワークロードをサポートして、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を保護します。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 Forge 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 Forge に対して行う改善の多くは、お客様から直接ご提案いただいたものです。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。

- ◆ 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」
- ◆ 16 ページのセクション 1.1.2 「サポートされる Linux のワークロード」
- ◆ 18 ページのセクション 1.1.3 「サポートされる VM コンテナ」
- ◆ 19 ページのセクション 1.1.4 「サポートされるシステムファームウェア」
- ◆ 19 ページのセクション 1.1.5 「サポートされるストレージ」
- ◆ 20 ページのセクション 1.1.6 「PlateSpin Forge Web インタフェースでサポートされるブラウザ」

1.1.1 サポートされる Windows のワークロード

PlateSpin Forge は、ほとんどの Microsoft Windows バージョンのワークロードをサポートします。サポートされている Windows のバージョンのリストについては、[表 1-1](#) を参照してください。

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、いくつかの制約があります。詳細については、[90 ページのセクション 6.3 「データ転送」](#) を参照してください。

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
サーバクラスのワークロード	
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。
サーバベースのクラスタのワークロード	

オペレーティングシステム	備考
Windows Server 2012 R2 サーバベースの Microsoft フェールオーバークラスタ	サポートされるクラスタリング技術は、「ノードおよびディスクマジョリティのクォーラム」モデルおよび「非マジョリティ: ディスク専用クォーラム」モデルです。 ブロックベース転送のみ。
Windows Server 2008 R2 サーバベースの Microsoft フェールオーバークラスタ	サポートされるクラスタリング技術は、「ノードおよびディスクマジョリティのクォーラム」モデルおよび「非マジョリティ: ディスク専用クォーラム」モデルです。 ブロックベース転送のみ。
Windows Server 2003 R2 サーバベースの Windows クラスタサーバ	サポートされるクラスタリング技術は、「シングルクォーラムデバイスクラスタ」モデルです。 ブロックベース転送のみ。
Hypervisor クラスのワークロード	
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。
ワークステーションクラスのワークロード	
Windows 8.1 Windows 8	<p>警告: ワークロードのフェールオーバーとフェールバックを正常に機能させるには、Windows 8 ソースで高パフォーマンスの電源プランを選択する必要があります。</p> <p>この電源プランを Windows のコントロールパネルで設定するには:</p> <ol style="list-style-type: none"> すべてのコントロールパネル項目 > 電源オプションの順に選択します。 電源プランの選択またはカスタマイズダイアログで追加プランの表示 > 高パフォーマンスの順に選択します。 コントロールパネルを閉じます。
Windows 7	Professional、Enterprise、および Ultimate Edition のみ。

サポートされる Windows ファイルシステム

PlateSpin Forge 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をサポートします。

サポートされる Windows クラスタ

サポートされるクラスタでワークロードを保護する方法の詳細については、[103 ページの「Windows クラスタの保護」](#)を参照してください。クラスタノードにローカルストレージが存在する場合は、[141 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」](#)も参照してください。

サポートされる国際バージョン

PlateSpin Forge は、フランス語、ドイツ語、日本語、繁体中国語、および簡体中国語の各バージョンの Microsoft Windows をサポートします。詳細については、[41 ページの「PlateSpin Forge の国際バージョンの言語設定」](#)を参照してください。

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。

ワークロードのファームウェア (UEFI および BIOS) のサポート

Platespin Forge 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。ワークロードはソースからターゲットに転送されますが (ブロック転送とファイル転送の両方が可能)、ソースとターゲットそれぞれのオペレーティングシステムで、サポート対象のファームウェアを使用する必要があります。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、Forge 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。

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 Forge 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、Forge 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、Forge 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 のワークロードを UEFI ベースの物理マシンにフェールバックしようとする、Forge は、その選択を分析し、それが有効ではない (つまり、Windows 2003 では UEFI のブートモードはサポートされていないため、BIOS から UEFI へのファームウェアの遷移はサポートされていない) ことを通知します。
- 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、Forge 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。

ワークロードの複雑なディスクパーティション化のサポート

MBR パーティション化スキームに加え、PlateSpin Forge は、Windows ワークロードのディスクの GPT パーティション化をサポートします。ディスクあたりのパーティションまたはボリュームの数が 57 以下の場合、完全レプリケーションがサポートされています。

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 を更新 (Windows Update) していることを確認してください。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イ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 Forge では、多くの Linux ディストリビューションがサポートされています。サポートされている Linux オペレーティングシステムのリストについては、[表 1-2](#) を参照してください。

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	備考
Linux サーバクラスワークロード	
Red Hat Enterprise Linux (RHEL) 7 Red Hat Enterprise Linux 6 Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 4	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、137 ページの「Forge 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。
SUSE Linux Enterprise Server (SLES) 11 SUSE Linux Enterprise Server 10 SUSE Linux Enterprise Server 9	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、137 ページの「Forge 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。 注：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。
Novell Open Enterprise Server (OES) 11 Novell Open Enterprise Server 2	PlateSpin Forge は、サポートされる SLES ディストリビューションに基づいている場合、OES 2 または OES 11 バージョンのワークロードをサポートします。ただし、別途注記がある場合を除きます。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、137 ページの「Forge 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。 注：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 Enterprise Linux (OEL)	PlateSpin Forge は、サポートされる RHEL ディストリビューションに基づいている場合、OEL バージョンのワークロードをサポートします。ただし、別途注記がある場合を除きます。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、137 ページの「Forge 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。 注：Unbreakable Enterprise Kernel を使用するワークロードはサポートされません。
CentOS 7 CentOS 6 CentOS 5 CentOS 4	PlateSpin Forge は、サポートされる RHEL ディストリビューションに基づいている場合、CentOS バージョンのワークロードをサポートします。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、137 ページの「Forge 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。

サポートされる Linux ファイルシステム

PlateSpin Forge は、EXT2、EXT3、EXT4、REISERFS、XFS、および NSS (OES 2 および OES 11 ワークロード) の各ファイルシステムを、ブロックベース転送に限りサポートします。

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。

ワークロードのファームウェア (UEFI および BIOS) のサポート

PlateSpin Forge は、UEFI と BIOS の各ファームウェアインタフェースをサポートします。

ワークロードの複雑なディスクパーティション化のサポート

MBR パーティション化スキームに加え、PlateSpin Forge は、Linux ワークロードのディスクの GPT パーティション化をサポートします。ディスクあたりのパーティションまたはボリュームの数が 57 以下の場合、完全レプリケーションがサポートされています。

blkwatch ドライバの要件

PlateSpin Forge では、Linux ワークロードのデータのブロックベース転送のために、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 Forge 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、[137 ページの「Forge 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

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 ESXi Server または VMware DRS クラスタのどちらでも可能です。

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	メモ
VMware ESXi 6.0	<ul style="list-style-type: none">◆ 保護とフェールバックのコンテナとしてサポートされています。◆ DRS 環境設定は、[一部自動] または [完全自動] のいずれかにする必要があります ([手動] には設定しないでください)。◆ 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。
VMware ESXi 5.5 (GA2、アップデート 2)	<ul style="list-style-type: none">◆ 保護とフェールバックのコンテナとしてサポートされています。◆ DRS 環境設定は、[一部自動] または [完全自動] のいずれかにする必要があります ([手動] には設定しないでください)。◆ 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。

コンテナ	メモ
VMware ESXi 5.1 (GA2、アップデート 2)	<ul style="list-style-type: none"> ◆ 保護とフェールバックのコンテナとしてサポートされています。 ◆ DRS 環境設定は、[一部自動] または [完全自動] のいずれかにする必要があります ([手動] には設定しないでください)。 ◆ 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 ESXi 4.1 (GA2、アップデート 3)	<ul style="list-style-type: none"> ◆ 保護とフェールバックのコンテナとしてサポートされています。 ◆ DRS 環境設定は、[一部自動] または [完全自動] のいずれかにする必要があります ([手動] には設定しないでください)。 ◆ 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: ESXi バージョンには、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。

1.1.4 サポートされるシステムファームウェア

PlateSpin Forge は、UEFI と BIOS の各ファームウェアインタフェースをサポートします。

Windows システムでは、PlateSpin Forge は、UEFI に対して、Microsoft と同様のサポートを提供します。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](#)」のワークロードのファームウェア (UEFI および BIOS) のサポートを参照してください。

1.1.5 サポートされるストレージ

保護対象のワークロードとストレージは、MBR (マスタブートレコード) または GPT (GUID パーティションテーブル) のパーティション化スキームでパーティション化されたディスク上に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 Forge 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。

PlateSpin Forge では、ベーシックディスク、Windows ダイナミックディスク、LVM (バージョン 2 のみ)、RAID、SAN などの数種類のストレージがサポートされます。

Linux のワークロードの場合、PlateSpin Forge は次の機能を追加で提供します。

- ◆ 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。
- ◆ (OES 11 ワークロード) ソースワークロードの NLVM (Novell Linux Volume Management) レイアウトは、アプライアンスホスト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 ワークロード) ソースワークロードの EVMS レイアウトは、アプライアンスホスト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 PlateSpin Forge Web インタフェースでサポートされるブラウザ

製品の操作のほとんどは、ブラウザベースの PlateSpin Forge 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。

JavaScript を有効にするには：

◆ **Chrome:**

1. Chrome メニューから **[設定]** を選択し、スクロールして **詳細設定を表示** をクリックします。
2. **Privacy (プライバシー)** で、**コンテンツの設定** をクリックします。
3. **JavaScript (JavaScript)** にスクロールして、**すべてのサイトで JavaScript の実行を許可する** を選択します。
4. **完了** をクリックします。

◆ **Firefox:**

1. [Location (ロケーション)] バーに、「about:config」と入力して <Enter> キーを押します。
2. **理解して実行する** をクリックします。
3. **検索** バーに、「javascript.enabled」と入力して <Enter> キーを押します。
4. 検索結果で、javascript.enabled パラメータの値を参照します。この値が false の場合、javascript.enabled を右クリックしてから **Toggle (切り替え)** を選択して、値を true に設定します。

◆ **Internet Explorer:**

1. [ツール] メニューで、**インターネットオプション** を選択します。
2. **セキュリティ** をクリックして、**レベルのカスタマイズ** をクリックします。
3. **Scripting (スクリプティング) > Active scripting (アクティブスクリプティング)** の順にクリックして、**Enable (有効にする)** を選択します。
4. 警告ダイアログボックスでは **はい** をクリックしてから、**OK** をクリックします。
5. **適用 > OK** の順にクリックします。

サポートされるいずれかの言語で PlateSpin Forge Web インタフェースおよび統合ヘルプを使用する方法については、[41 ページの「PlateSpin Forge の国際バージョンの言語設定」](#)を参照してください。

1.2 セキュリティとプライバシー

PlateSpin Forge 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いくつも用意されています。

- [21 ページのセクション 1.2.1 「送信中のワークロードデータのセキュリティ」](#)
- [21 ページのセクション 1.2.2 「クライアント / サーバ通信のセキュリティ」](#)
- [21 ページのセクション 1.2.3 「資格情報のセキュリティ」](#)
- [21 ページのセクション 1.2.4 「ユーザ権限および認証」](#)
- [22 ページのセクション 1.2.5 「ネットワークポート設定」](#)
- [23 ページのセクション 1.2.6 「その他のセキュリティ拡張機能」](#)

1.2.1 送信中のワークロードデータのセキュリティ

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%)スロウ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、[76 ページの「ワークロード保護の詳細」](#)を参照してください。

1.2.2 クライアント / サーバ通信のセキュリティ

PlateSpin Server では、Forge VM で SSL を有効にするので、Web ブラウザと PlateSpin Server の間の安全なデータ転送はすでに HTTPS (Hypertext Transfer Protocol Secure) に設定されています。

1.2.3 資格情報のセキュリティ

さまざまなシステム(ワークロードやフェールバックのターゲットなど)へのアクセスに使用する資格情報は、PlateSpin Forge データベースに保管されるため、Forge VM に対して設定したセキュリティセーフガードの対象となります。

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。

1.2.4 ユーザ権限および認証

PlateSpin Forge は、ユーザの役割に基づいて包括的かつ安全なユーザの承認と認証のメカニズムを備えており、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。詳細については、[29 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。

1.2.5 ネットワークポート設定

表 1-4 は、PlateSpin Forge 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 Forge 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。PlateSpin Server 環境のネットワークアクセス設定の詳細については、33 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設定」を参照してください。

表 1-4 PlateSpin Forge 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	<p>(安全ではない) Forge VM、およびその VM 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。</p> <p>このポートを Forge VM、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。</p>
443	TCP	HTTPS	<p>(安全) SSL が Forge VM 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。</p> <p>このポートを Forge VM、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。</p>
3725	TCP	データ転送	<p>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間のデータ転送で使用されます。</p> <p>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 を許可する必要があります。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。</p>
135 445	TCP	RPC/DCOM	<p>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。</p> <p>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。</p>
137 138 139	TCP	NetBIOS	<p>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。</p> <p>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。</p>

ポート番号	プロトコル	機能	Details (詳細)
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。
139 445	TCP	SMB	これらのポートを Forge VM およびソースワークロード で開きます。
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。
25	UDP	SMTP	このポートを、Forge VM とメールリレーホストで開き ます。
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、Forge VM 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。
1434	TCP	SQL	Microsoft SQL Server 専用の管理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。

1.2.6 その他のセキュリティ拡張機能

PlateSpin Forge は、[ナレッジベースの記事 7015818 \(https://www.netiq.com/support/kb/doc.php?id=7015818\)](https://www.netiq.com/support/kb/doc.php?id=7015818) で、PlateSpin サーバからの潜在的な POODLE (Padding Oracle On Downgraded Legacy Encryption) 攻撃に対する脆弱性を排除する方法について、情報を提供しています。

1.3 パフォーマンス

- ◆ 24 ページのセクション 1.3.1 「製品パフォーマンスの特性」
- ◆ 24 ページのセクション 1.3.2 「データ圧縮」
- ◆ 25 ページのセクション 1.3.3 「帯域幅制限」
- ◆ 25 ページのセクション 1.3.4 「RPO、RTO、および TTO の仕様」
- ◆ 25 ページのセクション 1.3.5 「スケーラビリティ」

1.3.1 製品パフォーマンスの特性

PlateSpin Forge 製品のパフォーマンス特性は、次を含め、多くの要因に依存します。

- ◆ 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
- ◆ 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。

1.3.2 データ圧縮

必要に応じて、PlateSpin Forge は、ワークロードのデータをネットワーク上で送信する前に圧縮できます。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。93 ページの「保護ティア」を参照してください。

1.3.3 帯域幅制限

PlateSpin Forge は、ワークロード保護の過程で、直接の送信元 - 対 - 送信先の通信により、使わ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処理量を指定できます。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。93 ページの「保護ティア」を参照してください。

1.3.4 RPO、RTO、および TTO の仕様

- ◆ **目標復旧時点 (RPO):** データ紛失の許容量 (時間で測定) 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時間で決定され、PlateSpin Forge 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):** フェールオーバー操作 (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る) に必要な時間を記述します。
ワークロードをその仮想レプリカにフェールオーバーするワークロードにおける 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。80 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):** サービスを復旧させるある程度の自信を持って障害復旧テストを行うのに必要な時間について説明します。
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、81 ページの「フェールオーバーのテスト機能の使用」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。

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、69 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。

1.3.5 スケーラビリティ

スケーラビリティは、次のような PlateSpin Forge 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。

2 PlateSpin Forge アプリケーション環境設定

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

- [27 ページのセクション 2.1 「PlateSpin Forge Web インタフェースの起動」](#)
- [28 ページのセクション 2.2 「製品ライセンスの有効化」](#)
- [29 ページのセクション 2.3 「ユーザ権限および認証の設定」](#)
- [33 ページのセクション 2.4 「保護ネットワークにわたるアクセスおよび通信の設定」](#)
- [38 ページのセクション 2.5 「イベントおよびレポートの自動電子メール通知の設定」](#)
- [41 ページのセクション 2.6 「PlateSpin Forge の国際バージョンの言語設定」](#)
- [42 ページのセクション 2.7 「タグによるワークロードのソート」](#)
- [44 ページのセクション 2.8 「XML 環境設定パラメータを通じた PlateSpin Server の動作の構成」](#)
- [44 ページのセクション 2.9 「WAN 接続を使用したデータ転送の最適化」](#)
- [47 ページのセクション 2.10 「VMware vCenter Site Recovery Manager 用サポートの設定」](#)

2.1 PlateSpin Forge Web インタフェースの起動

サポートされるいずれかの言語で PlateSpin Forge Web インタフェースおよび統合ヘルプを使用する方法については、[41 ページの「PlateSpin Forge の国際バージョンの言語設定」](#)を参照してください。

PlateSpin Forge Web インタフェースを起動するには：

- 1 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://<hostname | IP_address>/Forge
```

<hostname | IP_address> の部分を、Forge VM 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。

PlateSpin Forge に初めてログインする場合、ブラウザは [ライセンスのアクティベーション] ページにリダイレクトします。

- 2 Forge VM 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。

Forge 管理 VM のデフォルトの資格情報は、ユーザ名 Administrator、パスワード Password1 です。管理者ユーザのパスワードを変更するには、VM の Windows デスクトップにリモートでログインし、Windows 管理ツールを使用して新しいパスワードを設定できます。

PlateSpin の追加ユーザのセットアップについては、[29 ページのセクション 2.3 「ユーザ権限および認証の設定」](#)を参照してください。

2.2 製品ライセンスの有効化

PlateSpin Forge 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。詳細については、[89 ページのセクション 6.1「ワークロードライセンスの消費」](#)を参照してください。

PlateSpin Forge 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 \(http://www.netiq.com/customercenter/\)](http://www.netiq.com/customercenter/) を通じて要求してください。ライセンスのアクティベーションコードは、電子メールで送信されます。

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 \(https://www.netiq.com/selfreg/jsp/createAccount.jsp\)](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。

- [28 ページのセクション 2.2.1「オンラインでのライセンスのアクティベーション」](#)
- [29 ページのセクション 2.2.2「オフラインでのライセンスのアクティベーション」](#)

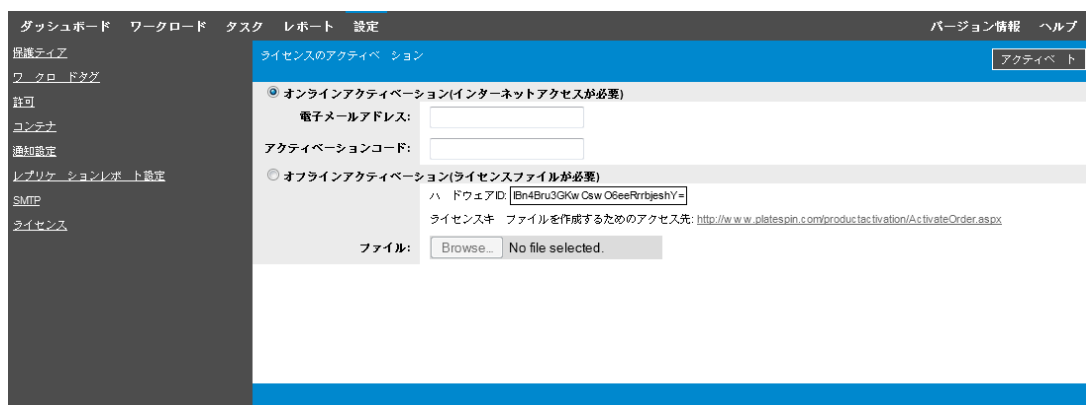
2.2.1 オンラインでのライセンスのアクティベーション

オンラインでアクティベーションするには、PlateSpin Forge 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 プロキシを使用している場合、オンラインアクティベーション中にエラーが発生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 PlateSpin Forge Web インタフェースで、[**Add PlateSpin Forge License (PlateSpin Forge ライセンスの追加)**] > [**Add License (ライセンスを追加する)**] の順にクリックします。



The screenshot shows the 'License Activation' page in the PlateSpin Forge web interface. The page title is 'ライセンスのアクティベーション' (License Activation). There are two radio button options: 'オンラインアクティベーション(インターネットアクセスが必要)' (Online activation (requires internet access)) and 'オフラインアクティベーション(ライセンスファイルが必要)' (Offline activation (requires license file)). The online option is selected. Below the online option, there are input fields for '電子メールアドレス:' (Email address) and 'アクティベーションコード:' (Activation code). Below the offline option, there are input fields for 'ハードウェアID:' (Hardware ID) with the value 'Bn4Bru3GKw Csw 0CeeRrtjeshY=' and 'ライセンスキ' (License key) with a note 'ファイルを作成するためのアクセス先: http://www.platespin.com/productactivation/ActivateOrder.aspx'. There is also a 'ファイル:' (File) field with a 'Browse...' button and the text 'No file selected.'.

- 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。

2.2.2 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 Forge のライセンスキーを取得します。

- 1 PlateSpin Forge Web インタフェースで、[**Add PlateSpin Forge License (PlateSpin Forge ライセンスの追加)**] > [**Add License (ライセンスを追加する)**] の順をクリックします。
- 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 PlateSpin Forge 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。

2.3 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。

- ◆ 29 ページのセクション 2.3.1 「PlateSpin Forge の役割ベースのアクセスについて」
- ◆ 31 ページのセクション 2.3.2 「PlateSpin Forge のアクセスおよび権限の管理」
- ◆ 32 ページのセクション 2.3.3 「PlateSpin Forge 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」

2.3.1 PlateSpin Forge の役割ベースのアクセスについて

PlateSpin Forge 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 Forge 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 Forge に接続しようとする時、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 2-1 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 Forge ソフトウェアでは、どのユーザが PlateSpin Forge 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 Forge への適切な役割ベースのアクセスを設定するには：

- 1 表 2-1 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、32 ページの「PlateSpin Forge 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。

2.3.2 PlateSpin Forge 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。

- ◆ 31 ページの「Forge 管理 VM の管理者ユーザのパスワード変更」
- ◆ 31 ページの「PlateSpin Forge ユーザの追加」
- ◆ 31 ページの「PlateSpin Forge ユーザへのワークロード保護の役割の割り当て」

Forge 管理 VM の管理者ユーザのパスワード変更

Forge 管理 VM のデフォルトの資格情報は、ユーザ名 Administrator、パスワード Password1 です。

管理者ユーザのパスワードを変更するには：

- 1 Forge 管理 VM に対して設定した IP アドレスを使用して、VM とのリモートデスクトップ接続を起動します。
- 2 現在の資格情報を使用して、管理者ユーザとしてログインします。
- 3 Windows 管理ツールを使用して、管理者ユーザの新しいパスワードを設定します。
- 4 ログアウトしてリモートデスクトップ接続を終了します。

PlateSpin Forge ユーザの追加

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

Forge VM 上の既存のユーザに特定の役割権限を付与する方法については、31 ページの「PlateSpin Forge 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。

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。31 ページの「PlateSpin Forge 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。

PlateSpin Forge 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。30 ページの表 2-1 「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。

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。

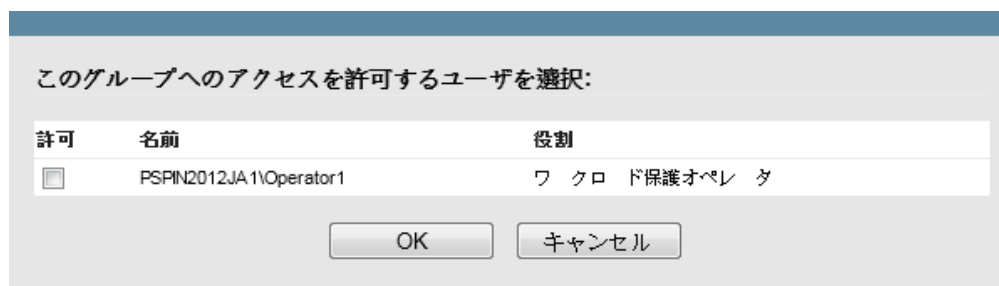
- 2 PlateSpin Server の bin\RestartPlateSpinServer サブディレクトリに移動します。
- 3 RestartPlateSpinServer.exe 実行可能ファイルをダブルクリックします。
確認を求めるコマンドプロンプトウィンドウが開きます。
- 4 「Y」と入力し、<Enter> キーを押します。

ユーザを PlateSpin Forge 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。32 ページの「PlateSpin Forge 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。

2.3.3 PlateSpin Forge 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 Forge 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 Forge ユーザに割り当てます。31 ページの「PlateSpin Forge 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 Forge Web インタフェースを使用し、管理者として PlateSpin Forge 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。
追加したばかりの PlateSpin Forge ユーザは、Forge VM に追加しようとしてもユーザインタフェースで直ちに使用できない場合があります。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。

このグループに含めるワークロードを選択:

含める	ワークロード名	セキュリティグループ
<input type="checkbox"/>	vsles11sp3x64.example.com	[未割り当て]
<input type="checkbox"/>	VVC1	[未割り当て]
<input type="checkbox"/>	AE-W2K3-1	[未割り当て]
<input checked="" type="checkbox"/>	AE-W2K3-3	[未割り当て]
<input checked="" type="checkbox"/>	AE-W2K3-4	[未割り当て]

OK キャンセル

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せん。

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。

2.4 保護ネットワークにわたるアクセスおよび通信の設定

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。

- 33 ページのセクション 2.4.1「PlateSpin Server ホストおよび Forge VM Web インタフェース用に開くポートの要件」
- 34 ページのセクション 2.4.2「ワークロードに関するアクセスおよび通信の要件」
- 36 ページのセクション 2.4.3「コンテナに関するアクセスおよび通信の要件」
- 36 ページのセクション 2.4.4「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」
- 37 ページのセクション 2.4.5「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」
- 37 ページのセクション 2.4.6「コンテナとしての VMware DRS クラスタの要件」

2.4.1 PlateSpin Server ホストおよび Forge VM Web インタフェース用に開くポートの要件

表 2-2 は、PlateSpin Forge Web インタフェースにアクセスできるようにするために Forge VM で開く必要があるポートについて説明しています。

表 2-2 PlateSpin Server ホストおよび Forge VM 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)

2.4.2 ワークロードに関するアクセスおよび通信の要件

表 2-3 は、PlateSpin Forge 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 2-3 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。	<ul style="list-style-type: none"> ◆ Microsoft .NET Framework 3.5 Service Pack 1 ◆ Microsoft .NET Framework 4.0 	

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。	<ul style="list-style-type: none"> ◆ 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。 <ul style="list-style-type: none"> ◆ 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。 <ul style="list-style-type: none"> ◆ 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) 	<p>TCP 3725</p> <p>NetBIOS (TCP 137 - 139)</p> <p>SMB (TCP 139、445 および UDP 137、138)</p> <p>RPC (TCP 135、445)</p>
Windows Server 2003 (SP1 Standard、SP2 Enterprise、および R2 SP2 Enterprise を含む)。	<p>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。</p> <pre>netsh firewall set service RemoteAdmin enable</pre> <p>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。</p>	<p>TCP 3725、135、139、445</p> <p>UDP 137、138、139</p>

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

2.4.3 コンテナに関するアクセスおよび通信の要件

表 2-4 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 2-4 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。	<ul style="list-style-type: none"> ◆ 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)

2.4.4 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路の保護

場合によっては、ソース、ターゲット、または PlateSpin Forge 自体は、NAT (ネットワークアドレストランスレータ) の背後にある内部 (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 Forge 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 Server 環境設定* ツールで、そのホストに割り当てられた追加 IP アドレスを次のとおり、記録します。詳細については、[37 ページの「NAT 全体で機能するアプリケーションの設定」](#) を参照してください。
- ◆ **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、[\(84 ページ\) 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、Forge VM のローカルアドレスまたはサーバの *PlateSpin Server 環境設定ツール* 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 (上述の「PlateSpin Server」を参照)。

NAT 全体で機能するアプリケーションの設定

NAT を有効にした環境全体で PlateSpin Server が機能できるようにするには、スタートアップ時にサーバが読み取る *PlateSpin Server 環境設定ツール* のデータベースに PlateSpin Server の追加 IP アドレスを記録する必要があります。

更手順については、44 ページの「XML 環境設定パラメータを通じた PlateSpin Server の動作の構成」を参照してください。

2.4.5 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 (<https://www.netiq.com/support/kb/doc.php?id=7010676>) を参照してください。

2.4.6 コンテナとしての VMware DRS クラスタの要件

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しないでください。詳細については、73 ページの「コンテナの追加 (保護ターゲット)」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、部分的に自動化されているか完全に自動化されている。
- ◆ 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 ESX サーバで共有されている。
- ◆ 少なくとも 1 つの vSwitch および仮想ポートグループ、または vNetwork Distributed Switch が、VMware Cluster のすべての ESX サーバに共通である。
- ◆ 各保護コントラクトのフェールオーバーワークロード (VM) が、VMware Cluster のすべての ESX サーバ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ている。

2.5 イベントおよびレポートの自動電子メール通知の設定

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 Forge を設定することができます。この機能では、使用する PlateSpin Forge の有効な SMTP サーバを最初に指定する必要があります。

- ◆ [38 ページのセクション 2.5.1 「SMTP 設定」](#)
- ◆ [38 ページのセクション 2.5.2 「電子メールによる自動的なイベント通知のセットアップ」](#)
- ◆ [40 ページのセクション 2.5.3 「電子メールによる自動レプリケーションレポートのセットアップ」](#)

2.5.1 SMTP 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 Forge Web インタフェースを使用します。

図 2-1 SMTP (シンプルメール転送プロトコル) の設定

SMTPの設定		保存
SMTPサーバアドレス:	<input type="text"/>	
ポート:	25	
返信用アドレス:	<input type="text"/>	
ユーザ名:	<input type="text"/>	
パスワード:	<input type="password"/>	
確認:	<input type="password"/>	

SMTP 設定を行うには :

- 1 PlateSpin Forge Web インタフェースで、**[設定]** > **[SMTP]** の順にクリックします。
- 2 電子メールでイベントの通知および進行状況の通知を受信するために、SMTP サーバの **[アドレス]**、**[ポート]** (デフォルトは 25)、および **[返信用アドレス]** を指定します。
- 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。

2.5.2 電子メールによる自動的なイベント通知のセットアップ

自動的なイベント通知をセットアップするには :

- 1 使用する PlateSpin Forge の SMTP サーバをセットアップします。 [38 ページの「SMTP 設定」](#) を参照してください。
- 2 PlateSpin Forge 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 [OB] 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。

通知が設定されている場合、表 2-5 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。これらのイベントは必ず、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。

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 2-5 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。 <ul style="list-style-type: none">◆ スケジュールされた増分レプリケーションの期限内に、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。

イベントの種類	備考
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	
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。

2.5.3 電子メールによる自動レプリケーションレポートのセットアップ

電子メールでレプリケーションレポートを自動的に送信するように PlateSpin Forge をセットアップするには:

- 1 使用する PlateSpin Forge の SMTP サーバをセットアップします。(38 ページ) SMTP 設定を参照してください。
- 2 PlateSpin Forge 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) Forge の [Access URL (アクセス URL)] セクションで、PlateSpin サーバに対するデフォルト以外の URL (例: Forge VM が複数の NIC を持つ場合や 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、69 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。

2.6 PlateSpin Forge の国際バージョンの言語設定

PlateSpin Forge では、簡体中国語、繁体中国語、フランス語、ドイツ語、および日本語に対する NLS (National Language Support) が提供されます。

PlateSpin Forge Web インタフェースおよび統合ヘルプをこれらいずれかの言語で使用するには、該当する言語を Web ブラウザに追加し、優先順位の最上部に移動させる必要があります。

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 Forge 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。27 ページの「PlateSpin Forge Web インタフェースの起動」を参照してください。

注：(簡体中国語および繁体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 Forge Server に接続しようとする、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。

PlateSpin Forge 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 Forge VM 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 Forge VM にアクセスします。
[56 ページの「アプライアンスホストにおける Forge 管理 VM へのアクセスおよび使用」](#)を参照してください。
- 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 [Keyboards and Languages (キーボードと言語)] (Windows Server 2008) タブで該当する方をクリックします。
- 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。

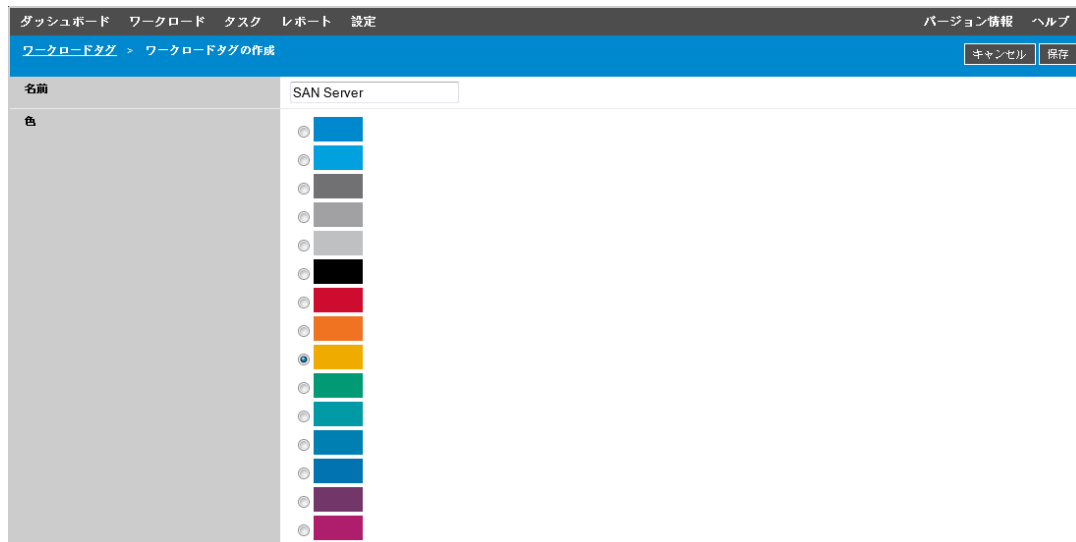
2.7 タグによるワークロードのソート

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、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、自身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。

ワークロードタグを設定するには：

- 1 PlateSpin Forge 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。

使用可能なワークロードタグを編集または削除するには：

- 1 PlateSpin Forge 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。
- 3 不要なタグを削除します。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。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。

ワークロードにタグを 1 つ追加 (「関連付ける」) には：

- 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。



ワークロードから 1 つのタグを削除 (「関連付け解除」) するには：

- 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。



2.8 XML 環境設定パラメータを通じた PlateSpin Server の動作の構成

PlateSpin Server の動作の一部は、Forge VM 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： 通常の場合では、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、https://Your_PlateSpin_Server/platespinconfiguration/ を開きます。
- 2 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。

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。

次の項目では、XML 設定値を使用して製品動作を変更する必要がある可能性のある特定の状況について説明します。

- ◆ [44 ページの「WAN 接続を使用したデータ転送の最適化」](#)
- ◆ [44 ページの「WAN 接続を使用したデータ転送の最適化」](#)
- ◆ [143 ページの「PlateSpin Forge Web インタフェースのブランディングの変更」](#)

2.9 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、Forge VM 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。一般的な手順については、[44 ページの「XML 環境設定パラメータを通じた PlateSpin Server の動作の構成」](#)を参照してください。

これらの設定を使用して WAN を通じてのデータ転送を最適化します。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。

[表 2-6](#) に、ファイル転送速度を制御する環境設定パラメータおよびそ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 2-6 https://Your_PlateSpin_Server/platespinconfiguration/ のデフォルトおよび最適化されたファイル転送環境設定パラメータ

パラメータ	デフォルト値	Maximum Value
AlwaysUseNonVSSFileTransferForWindows2003	False	
FileTransferCompressionThreadsCount	2	該当なし
<p>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。</p>		
FileTransferBufferThresholdPercentage	10	
<p>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。</p>		
FileTransferKeepAliveTimeOutMilliSec	120000	
<p>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。</p>		
FileTransferLongerThan24HoursSupport	True	
FileTransferLowMemoryThresholdInBytes	536870912	
<p>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、ネットワーク動作の増加を引き起こします。</p>		
FileTransferMaxBufferSizeForLowMemoryInBytes	5242880	
<p>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。</p>		
FileTransferMaxBufferSizeInBytes	31457280	
<p>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。</p>		
FileTransferMaxPacketSizeInButes	1048576	
<p>送信する最大パケットサイズを決定します。</p>		
FileTransferMinCompressionLimit	0 (無効)	最大 65536 (64KB)
<p>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。</p>		
FileTransferPort	3725	

パラメータ	デフォルト値	Maximum Value
FileTransferSendReceiveBufferSize	0 (8192 バイト)	最大 5242880 (5MB)
<p>ファイル転送接続の TCP/IP ウィンドウ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。</p> <p>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。</p> $((\text{リンク速度 (Mbps)/8}) * \text{遅延 (秒)}) * 1000 * 1000$ <p>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。</p> $(100/8) * 0.01 * 1000 * 1000 = 125000 \text{ bytes}$		
FileTransferSendReceiveBufferSizeLinux	0 (253952 バイト)	
<p>Linux でのファイル転送接続の TCP/IP ウィンドウ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。</p> <p>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。</p> <p>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。</p>		
FileTransferShutDownTimeOutInMinutes	1090	
FileTransferTCPTimeOutMilliSec	30000	
<p>TCP Send Timeout と TCP Receive Timeout の両方の値を設定します。</p>		
PostFileTransferActionsRequiredTimeInMinutes	60	

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

PlateSpin Forge 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 Forge 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 Forge を設定した場合、シームレスに動作できます。

- PlateSpin Forge ISO および フロッピーが VMware .vmx 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 Forge 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。
- [47 ページのセクション 2.10.1「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」](#)
- [47 ページのセクション 2.10.2「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」](#)
- [49 ページのセクション 2.10.3「設定プロセスの促進」](#)

2.10.1 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。

2.10.2 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 Forge 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 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、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 VMware Server から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% にコピーします。%GUID% の値は、VMware Server とその VMware ツールアーキテクチャのバージョンによって異なります。
次の表は、パッケージを正しいディレクトリにコピーするために必要なサーババージョン、VMware ツールアーキテクチャ、および GUID 識別子を示しています。

VMware Server バージョン	VMware ツールアーキテクチャ	GUID
4.0	x86	D052CBAC-0A98-4880-8BCC-FE0608F0930F
4.0	x64	80B50267-B30C-4001-ABDF-EA288D1FD09C
4.1	x86	F2957064-65D7-4bda-A52B-3F5859624602
4.1	x64	80B1C53C-6B43-4843-9D63-E9911E9A15D5
5.0	x86	AD4FDE1D-DE86-4d05-B147-071F4E1D0326
5.0	x64	F7C9BC91-7733-4790-B7AF-62E074B73882
5.1	x86	34DD2CBE-183E-492f-9B36-7A8326080755
5.1	x64	AD4FDE1D-DE86-4d05-B147-071F4E1D0326
5.5	x86	660C345A-7A91-458b-BC47-6A3914723EF7
5.5	x64	8546D4EF-8CA5-4a51-A3A3-6240171BE278

2.10.3 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。

3 アプライアンスのセットアップとメンテナンス

この項では、定期的に完了しなければならない可能性のあるアプライアンスのセットアップと保守のタスクについて説明します。

- 51 ページのセクション 3.1 「アプライアンスのネットワーキングの設定」
- 52 ページのセクション 3.2 「アプライアンスの物理的な移設」
- 54 ページのセクション 3.3 「PlateSpin Forge における外部ストレージソリューションの使用」
- 56 ページのセクション 3.4 「アプライアンスホストにおける Forge 管理 VM へのアクセスおよび使用」
- 59 ページのセクション 3.5 「工場出荷時のデフォルトへの Forge のリセット」

3.1 アプライアンスのネットワーキングの設定

この項では、アプライアンスホストのネットワーキングの設定のカスタマイズ方法について説明します。

- 51 ページのセクション 3.1.1 「アプライアンスホストのネットワーキングの設定」

3.1.1 アプライアンスホストのネットワーキングの設定

PlateSpin Forge アプライアンスには、外部アクセス用に設定された 6 つの物理ネットワークインタフェースがあります。

- **外部テストネットワーク**：フェールオーバーのテスト機能を使用してフェールオーバーのワークロードをテストする際に、ネットワークトラフィックを隔離します。
- **内部テストネットワーク**：運用ネットワークから完全に隔離した状態でワークロードのフェールオーバーをテストします。
- **レプリケーションネットワーク**：運用ワークロードと管理 VM 内のそのレプリカ間での進行中トラフィック専用ネットワークをシステムに提供します。
- **運用ネットワーク**：フェールオーバーまたはフェールバック実行時の実際のビジネスを継続させるためのネットワークです。
- **管理ネットワーク**：Forge 管理 VM ネットワーク。
- **アプライアンスホストネットワーク**：Hypervisor 管理ネットワーク。このネットワークは、PlateSpin Forge Web インタフェースでは選択できません。

デフォルトでは、PlateSpin Forge には 6 つすべての物理ネットワークインタフェースが付属しています。これらのインタフェースは、ハイパーバイザ内で 1 つの vSwitch にマップされています。ご使用の環境により一層合うようにマッピングをカスタマイズできます。たとえば、1 つが運用のための接続に使用され、他方はレプリケーション専用で使用される、2 つの NIC を持つワークロードを保護できます。追加情報については、[ナレッジベースの記事 7921062 \(https://www.netiq.com/support/kb/doc.php?id=7921062\)](https://www.netiq.com/support/kb/doc.php?id=7921062) を参照してください。

さらに、ネットワークトラフィックの制御をさらに微調整するには、上記のポートグループごとに異なる VLAN ID を割り当てることを考慮してください。これにより、運用ネットワークがワークロード保護および回復操作によって妨害されないようにできます。[ナレッジベースの記事 21057 \(https://www.netiq.com/support/kb/doc.php?id=7921057\)](https://www.netiq.com/support/kb/doc.php?id=7921057) を参照してください。

3.2 アプライアンスの物理的な移設

PlateSpin Forge アプライアンスを移動するには、そのコンポーネントの IP アドレスを変更し、新しい環境を反映する必要があります。これらの IP アドレスは、アプライアンスの初期設定時に指定したものです (『PlateSpin Forge 導入ガイド』を参照)。

移設手順を開始する前に以下を実行します。

- 1 すべてのレプリケーションスケジュールを一時停止し、ワークロードごとに少なくとも 1 つの増分が実行されていることを確認します。
 - 1a PlateSpin Forge Web インタフェースで、すべてのワークロードを選択し、**Pause (一時停止)** をクリックして、**Execute (実行)** をクリックします。
 - 1b すべてのワークロードに対して **[Paused (一時停止中)]** と表示されていることを確認します。

移設プロセスの詳細は、移設場所でのアプライアンスの新しい IP アドレスが知られているか (シナリオ 1)、または知られていないか (シナリオ 2) によって異なります。

- [52 ページのセクション 3.2.1「シナリオ 1 - Forge の移設 \(新しい IP アドレスがわかっている場合\)」](#)
- [53 ページのセクション 3.2.2「シナリオ 2 - Forge の移設 \(新しい IP アドレスがわからない場合\)」](#)

3.2.1 シナリオ 1 - Forge の移設 (新しい IP アドレスがわかっている場合)

新しい IP アドレスがわかっているときに Forge アプライアンスハードウェアを移設するには：

- 1 すべてのレプリケーションを一時停止します。上記の [ステップ 1a](#) と [ステップ 1b](#) を参照してください。
- 2 Forge Appliance Configuration Console (Forge ACC) を起動します。ブラウザを開いて、`http://<Forge_IP_address>:10000` に移動してください。
- 3 forgeuser アカントを使用してログインして、**[ホストの設定]** をクリックします。
- 4 新しいネットワークパラメータを入力し、**[適用]** をクリックします。
- 5 設定プロセスの完了、およびブラウザウィンドウに **[設定に成功しました]** ポップアップウィンドウが表示されるまで待ちます。

注： アプライアンスの接続を物理的に外して新しいサブネットに接続するまで、ポップアップウィンドウにある新しい Forge ACC アドレスのリンクは機能しません。

- 6 アプライアンスをシャットダウンします。
 - 6a 次の手順で Forge Management VM をシャットダウンします。57 ページの「Forge 管理 VM の起動とシャットダウン」を参照してください。
 - 6b アプライアンスホストをシャットダウンします。
 - 6b1 Forge コンソールで、<Alt> + <F2> を押して ESX Server コンソールに切り替えます。
 - 6b2 スーパーユーザでログインします (ユーザ root および関連付けられたパスワードを使用)。
 - 6b3 次のコマンドを入力し、<Enter> を押します。

```
shutdown -h now
```
 - 6c アプライアンスの電源をオフにします。
- 7 アプライアンスの接続を外し、新しいサイトに移動させて、それを新しいサブネットに接続し、電源をオンにします。

これで新しい IP アドレスが有効になります。
- 8 Forge ACC を起動して forgeuser アカウントを使用してログインし、[Forge VM の設定] をクリックして、必要なパラメータを指定し、次に [適用] をクリックします。
- 9 設定が正しいことを確認し、[続行] をクリックし、プロセスが完了するまで待ちます。

注 : Forge VM が DHCP を使用するように設定された場合は、移設後に以下の手順を実行します。

1. Forge VM の新しい IP アドレスを判別します (vSphere Client プログラムを使用して Forge VM にアクセスし、VM の Windows インタフェースで参照してください。57 ページの「vSphere Client の起動および Forge 管理 VM へのアクセス」を参照してください)。
2. 新しい IP アドレスを使用して PlateSpin Forge Web インタフェースを起動し、コンテナを更新します ([設定] > [コンテナ] > 次に  をクリックしてください)。

-
- 10 一時停止されたレプリケーションを再開します。

3.2.2 シナリオ 2 - Forge の移設 (新しい IP アドレスがわからない場合)

新しい IP アドレスが不明な場合に Forge アプライアンスハードウェアを移設するには :

- 1 すべてのレプリケーションを一時停止します。ステップ 1a および 52 ページのステップ 1b を参照してください。
- 2 アプライアンスをシャットダウンします。
 - 2a 次の手順で Forge Management VM をシャットダウンします。57 ページの「Forge 管理 VM の起動とシャットダウン」を参照してください。
 - 2b アプライアンスホストをシャットダウンします。
 - 2b1 Forge コンソールで、<Alt> + <F2> を押して ESX Server コンソールに切り替えます。
 - 2b2 スーパーユーザでログインします (ユーザ root および関連付けられたパスワードを使用)。

2b3 次のコマンドを入力し、<Enter> を押します。

```
shutdown -h now
```


2c アプライアンスの電源をオフにします。

- 3 アプライアンスの接続を外し、それを移動させて新しいネットワークに接続し、次に電源をオンにします。
- 4 現在の IP アドレス (以前のサイトの IP アドレス) で Forge と通信できるようにするために、コンピュータ (ノートパソコン推奨) をセットアップし、次にそれをアプライアンスに接続します。
『*PlateSpin Forge 導入ガイド*』を参照してください。
- 5 Forge ACC を起動します。ブラウザを開いて、http://<Forge_IP_address>:10000 に移動してください。
- 6 forgeuser アカウントを使用してログインして、**[ホストの設定]** をクリックします。
- 7 新しいネットワークパラメータを入力し、**[適用]** をクリックします。
- 8 設定プロセスの完了、およびブラウザウィンドウに **[設定に成功しました]** ポップアップウィンドウが表示されるまで待ちます。

注: アプライアンスの接続を物理的に外して新しいサブネットに接続するまで、ポップアップウィンドウにある新しい ForgeACC アドレスのリンクは機能しません。

- 9 アプライアンスからコンピュータの接続を外し、アプライアンスを新しいサブネットに接続します。
これで新しい IP アドレスが有効になります。
- 10 Forge ACC を起動して forgeuser アカウントを使用してログインし、**[Forge VM の設定]** をクリックして、必要なパラメータを指定し、次に **[適用]** をクリックします。
- 11 設定が正しいことを確認し、**[続行]** をクリックし、プロセスが完了するまで待ちます。

注: Forge VM が DHCP を使用するよう設定された場合は、移設後に以下の手順を実行します。

1. Forge VM の新しい IP アドレスを判別します (vSphere Client プログラムを使用して Forge VM にアクセスし、VM の Windows インタフェースで参照してください。[57 ページの「vSphere Client の起動および Forge 管理 VM へのアクセス」](#)を参照してください)。
 2. 新しい IP アドレスを使用して PlateSpin Forge Web インタフェースを起動し、コンテナを更新します (**[設定]** > **[コンテナ]** > 次に  をクリックしてください)。
-

- 12 一時停止されたレプリケーションを再開します。

3.3 PlateSpin Forge における外部ストレージソリューションの使用

以下の項では、PlateSpin Forge 用の外部ストレージのセットアップおよび設定に役立つ情報について説明しています。

- ◆ [55 ページのセクション 3.3.1 「Forge での SAN ストレージの使用」](#)
- ◆ [56 ページのセクション 3.3.2 「Forge への SAN LUN の追加」](#)

3.3.1 Forge での SAN ストレージの使用

PlateSpin Forge では、SAN (ストレージエリアネットワーク) の実装など、既存の外部ストレージソリューションがサポートされています。Fibre Channel (FC) ソリューションおよび iSCSI ソリューションの両方がサポートされています。ファイバチャネルおよび iSCSI HBA をサポートする SAN では、Forge アプライアンスは SAN アレイに接続することができます。SAN アレイ LUN (論理ユニット) を使用してワークロードデータを保存できます。Forge を SAN と共に使用すると、柔軟性、効率性、また信頼性が向上します。

それぞれの SAN 製品には独自の微妙な差異や相違点があり、これらの特性はハードウェア製造業者間で移行されるものではありません。このような特徴は、これらの製品が Forge 管理 VM と接続し、相互作用する方法を考えると特に著しいものとなります。したがって、このガイドでは、考えられるそれぞれの環境や状況に対する特定の設定手順は記載されていません。

前述したような特定の情報が必要な場合は、ハードウェアベンダまたは SAN 製品の販売担当者に連絡することが最適な解決策です。多くのハードウェアベンダが、これらのタスクを詳細に説明したサポートガイドを提供しています。次のサイトから豊富な情報を入手できます。

VMware マニュアルの Web サイト (<http://www.vmware.com/support/pubs/>)。

- ◆ 『*Fibre Channel SAN Configuration Guide*』では、ファイバチャネルストレージエリアネットワーク環境の ESX Server の使用について説明しています。
- ◆ 『*iSCSI SAN Configuration Guide*』では、iSCSI ストレージエリアネットワーク環境の ESX Server の使用について説明しています。
- ◆ 『*VMware I/O Compatibility Guide*』では、現在承認されている HBA、HBA ドライバ、およびドライババージョンが一覧表示されています。
- ◆ 『*VMware Storage/SAN Compatibility Guide*』では、現在承認されているストレージアレイが一覧表示されています。
- ◆ 『*VMware Release Notes*』では、既知の問題および回避策に関する情報が提供されています。
- ◆ VMware ナレッジベースでは、一般的な問題および回避策に関する情報が提供されています。

以下のベンダは、VMware でテスト済みのストレージ製品を提供しています。

- ◆ 3PAR (<http://www.3par.com>)
- ◆ Bull (<http://www.bull.com>) (FC のみ)
- ◆ Dell (<http://www.dell.com>)
- ◆ Dell Compellent (<http://www.dell.com/us/business/p/dell-compellent>)
- ◆ EMC (<http://www.emc.com>)
- ◆ EqualLogic (<http://www.equallogic.com>) (iSCSI のみ)
- ◆ Fujitsu (<http://www.fujitsu.com>) および Fujitsu Siemens (<http://www.fujitsu-siemens.com>)
- ◆ HP (<http://www.hp.com>)
- ◆ Hitachi (<http://www.hitachi.com>) および Hitachi Data Systems (<http://www.hds.com>) (FC のみ)
- ◆ IBM (<http://www.ibm.com>)
- ◆ NEC (<http://www.nec.com>) (FC のみ)
- ◆ Network Appliance (NetApp) (<http://www.netapp.com>)
- ◆ Nihon Unisys (<http://www.unisys.com>) (FC のみ)


- Pillar Data (<http://www.pillardata.com>) (FC のみ)
- Sun Microsystems (<http://www.sun.com>)
- Xiotech (<http://www.xitech.com>) (FC のみ)

iSCSI の詳細については、Storage Networking Industry Association の Web サイト (http://www.snia.org/education/storage_networking_primer/ipstorage/) にアクセスしてください。

3.3.2 Forge への SAN LUN の追加

PlateSpin Forge では、SAN (ストレージエリアネットワーク) の使用をサポートしていますが、Forge で既存の SAN にアクセスできるようにするには、SAN 論理ユニット (LUN) が Forge の ESX に追加されている必要があります。

- 1 SAN システムをセットアップして設定します。
- 2 アプリケーションホストへアクセスします (57 ページの「vSphere Client プログラムのダウンロード」を参照)。
- 3 VMware クライアントインターフェースで、ルート (トップレベル) ノードをクリックし、**[環境設定]** タブをクリックします。
- 4 右上の **[Add Storage (ストレージの追加)]** ハイパーリンクをクリックします。
- 5 Add Storage (ストレージの追加) ウィザードで、データストア情報を指定するように要求されるまで **[Next (次へ)]** をクリックします。
- 6 データストア名を指定し、ウィザードの後続のページで **[Next (次へ)]** をクリックします。ウィザードが終了したら、**[終了]** をクリックします。
- 7 **[Hardware (ハードウェア)]** の下の **[Storage (ストレージ)]** をクリックして、Forge のデータストアを確認します。新しく追加された SAN LUN がウィンドウに表示されているはずです。
- 8 VMware クライアントプログラムを終了します。

PlateSpin Forge Web インターフェースには、次のレプリケーションが実行されて [Application Host (アプリケーションホスト)] が更新されるまで、新しいデータストアが表示されません。**[Settings (設定)]** > **[Containers (コンテナ)]** を選択し、アプライアンスのホスト名の近くにある  をクリックして強制的に更新できます。

3.4 アプライアンスホストにおける Forge 管理 VM へのアクセスおよび使用

Forge Management VM にアクセスして、ここで説明する保守タスクを時々実行するか、PlateSpin サポートの助言があった場合に実行する必要があります。

OS インターフェースと VM の設定を含め、Forge 管理 VM にアクセスするには、vSphere Client ソフトウェアを使用します。

- 57 ページのセクション 3.4.1 「vSphere Client プログラムのダウンロード」
- 57 ページのセクション 3.4.2 「vSphere Client の起動および Forge 管理 VM へのアクセス」
- 57 ページのセクション 3.4.3 「Forge 管理 VM の起動とシャットダウン」
- 58 ページのセクション 3.4.4 「アプライアンスホストでの Forge VM のスナップショットの管理」

- ◆ 58 ページのセクション 3.4.5「手動によるアプライアンスホストのデータストアへの VM のインポート」
- ◆ 59 ページのセクション 3.4.6「PlateSpin Forge 管理 VM にセキュリティ更新を適用する際のガイドライン」

3.4.1 vSphere Client プログラムのダウンロード

アプライアンスホストからクライアントソフトウェアをダウンロードし、PlateSpin Forge の外部にある Windows ワークステーションにそれをインストールします。

vSphere Client をダウンロードするには：

- 1 クライアントソフトウェアをダウンロードします。
 - ◆ Forge アプライアンスバージョン 3 および VMware ESXi 5.5 Update 1 の場合は、[VMware vSphere Client 5.5 Update 1 プログラム](#)をダウンロードします。
- 2 ダウンロードされたインストールプログラムを起動して、ソフトウェアをインストールします。

3.4.2 vSphere Client の起動および Forge 管理 VM へのアクセス

vSphere Client を起動するには：

- 1 [スタート] > [すべてのプログラム] > [VMWare] > [VMware vSphere Client] または [Virtual Infrastructure Client] の順にクリックします。
vSphere Client のログインウィンドウが表示されます。
- 2 証明書の警告は無視し、管理者レベルの資格情報を指定してログインします。
vSphere Client プログラムが開きます。
- 3 左側のインベントリパネルで、[PlateSpin Forge VM (PlateSpin Forge 管理 VM)] の項目を探して選択します。右パネルの一番上で [Console (コンソール)] タブをクリックします。
Client のコンソールエリアに、Forge 管理 VM の Windows インタフェースが表示されます。

物理マシン上で Windows を操作するのと同様にコンソールを使用して管理 VM を操作します。

管理 VM をアンロックするには、コンソール内をクリックし、<Ctrl> + <Alt> + <Insert> を押します。

vSphere Client プログラム外で作業するためにカーソルを解放するには、<Ctrl>+<Alt> を押します。

3.4.3 Forge 管理 VM の起動とシャットダウン

アプライアンスを移動する場合など、Forge 管理 VM をシャットダウンし再起動する必要がある場合があります。

VM をシャットダウンして再起動するには：

- 1 vSphere Client を使用して、Forge 管理 VM ホストにアクセスします。57 ページの「[vSphere Client プログラムのダウンロード](#)」を参照してください。
- 2 Windows の標準的な手順に従って VM をシャットダウンします ([スタート] > [シャットダウン])。

管理 VM を再起動するには：

- 1 左側のインベントリパネルで、[PlateSpin Forge Management VM (PlateSpin Forge 管理 VM)] の項目を右クリックし、[Power on (電源オン)] を選択します。

3.4.4 アプライアンスホストでの Forge VM のスナップショットの管理

Forge ソフトウェアをアップグレードする場合、またはトラブルシューティングのタスクを実施する場合など、場合によっては管理 VM の特定の時点でのスナップショットを取得する必要があります。また、場合によってはストレージ領域を開放するためにスナップショット (復旧ポイント) を削除する必要があります。

Forge 管理 VM のスナップショットを管理するには：

- 1 vSphere Client を使用して、アプライアンスホストにアクセスします。57 ページの「[vSphere Client プログラムのダウンロード](#)」を参照してください。
- 2 左のインベントリパネルで、[PlateSpin Forge Management VM (PlateSpin Forge 管理 VM)] の項目を右クリックして、[Snapshot (スナップショット)] > [Take Snapshot (スナップショットの取得)] の順に選択します。
- 3 スナップショットの名前と説明を入力し、[OK] をクリックします。

管理 VM を以前の状態に戻すには：

- 1 左のインベントリパネルで、[PlateSpin Forge Management VM (PlateSpin Forge 管理 VM)] の項目を右クリックして、[Snapshot (スナップショット)] > [Snapshot Manager (スナップショットマネージャ)] の順に選択します。
- 2 VM の状態のツリー表示の中で、スナップショットを選択し、[Go to (移動)] をクリックします。


復旧ポイントを表すスナップショットを削除するには：

- 1 左のインベントリパネルで、[PlateSpin Forge Management VM (PlateSpin Forge 管理 VM)] の項目を右クリックして、[Snapshot (スナップショット)] > [Snapshot Manager (スナップショットマネージャ)] の順に選択します。
- 2 VM の状態のツリー表示の中で、スナップショットを選択し、[Remove (削除)] をクリックします。

3.4.5 手動によるアプライアンスホストのデータストアへの VM のインポート

VM をアプライアンスのホストのデータストアに手動でインポートするには：

- 1 運用サイトで、運用ワークロードから VM を作成し (たとえば、PlateSpin Migrate を使用)、ESX ホストのデータベースから VM ファイルをポータブルハードドライブまたは USB フラッシュドライブなどのポータブルメディアにコピーします。クライアントソフトウェアのデータストアブラウザを使用し、ファイルを参照して見つけます。

- 2 障害復旧サイトで、Forge に対するネットワークアクセスがあり、vSphere Client プログラムがインストールされているワークステーションにメディアを接続します。57 ページの「vSphere Client プログラムのダウンロード」を参照してください。
- 3 vSphere Client のデータストアブラウザを使用して Forge データストア (**Storage1**) にアクセスし、一時メディアから VM ファイルをアップロードします。アップロードされた VM を使用してそれをアプライアンスホストに登録します (右クリック > **[Add to Inventory (インベントリに追加)]**)。
- 4 PlateSpin Forge インベントリを更新します (PlateSpin Forge Web インタフェースで、**[設定]** > **[Containers (コンテナ)]** の順にクリックし、アプライアンスホストの隣にある  をクリックします)。

ヒント：フェールオーバーワークロードが別個に作成されるようにする場合は、このオプションの使用を考慮してください (95 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)。

3.4.6 PlateSpin Forge 管理 VM にセキュリティ更新を適用する際のガイドライン

セキュリティパッチを Forge 管理 VM に適用するには：

- 1 保守期間中に、VMware vSphere Client プログラムを使用して Forge 管理 VM にアクセスします。57 ページの「vSphere Client プログラムのダウンロード」を参照してください。
- 2 Forge 管理 VM の Windows インタフェースの中から、Microsoft が提供するセキュリティ更新がないか確認します。
- 3 PlateSpin Forge Web インタフェースを使用し、すべてのレプリケーションスケジュールを一時停止して未完了のレプリケーションがあれば完了したことを確認し、PlateSpin Forge を保守モードに切り替えます。
- 4 Forge 管理 VM のスナップショットを取得します。58 ページの「アプライアンスホストでの Forge VM のスナップショットの管理」を参照してください。
- 5 必要なセキュリティパッチをダウンロードしてインストールします。インストールが終了したら、Forge 管理 VM を再起動します。
- 6 PlateSpin Forge Web インタフェースを使用して、**ステップ 3** で一時停止したレプリケーションを再開し、レプリケーションが適切に動作していることを確認します。
- 7 **ステップ 4** で作成した Forge 管理 VM のスナップショットを削除します。58 ページの「アプライアンスホストでの Forge VM のスナップショットの管理」を参照してください。

3.5 工場出荷時のデフォルトへの Forge のリセット

ヒント：ご使用の Forge のモデルによっては、このプロセスには 45 分、またはそれ以上かかる場合があります。

Forge アプライアンスユニットを工場出荷時のデフォルトの状態にリセットするには：

- 1 外部 / リモート / 共有ストレージシステム (iSCSI、ファイバチャネル、NFS) をすべて Forge から接続解除します。
- 2 すべてのネットワークケーブルを Forge から取り外します。

警告：同じ物理スイッチに接続された複数の Forge アプライアンスを工場出荷時の設定にリセットする場合、この手順を省略すると、IP アドレスの競合が発生して障害につながる可能性があります。

3 次の手順でアプライアンスホストを再起動します。

3a 直接、または iDRAC を使用して、Hypervisor (VMware ESXi) にログインします。

3b <F2> を押して ESXi コンソールを開きます。

重要：このページに表示されるアプライアンスの、工場出荷時の設定にリセットする IP アドレスを覚えておく必要があります。Forge ACC にログインし、既知の有効な IP アドレスにコンテナを「移設する」には、このアドレスが必要です。IP を適切にリセットするには、「52 ページの「アプライアンスの物理的な移設」」で説明されるプロシーダを使用します。

3c ESXi コンソールをシャットダウンするには <F12> を押します。

3d 管理者レベルの資格情報を使用してログインします。

3e <F2> を押して ESXi をシャットダウンするか、アプライアンスを再起動します。

3f Forge CD メディアからブートし (または iDRAC を介して ISO に接続し)、SYSLINUX メニューが表示されるのを待機します。

4 [PlateSpin Forge Factory Reset] オプションを選択して、<Enter> を押します。この操作は、デフォルトの設定が自動的に適用される前に実行してください (約 10 秒間)。

5 工場出荷時設定へのリセット処理が完了するまで待ちます。

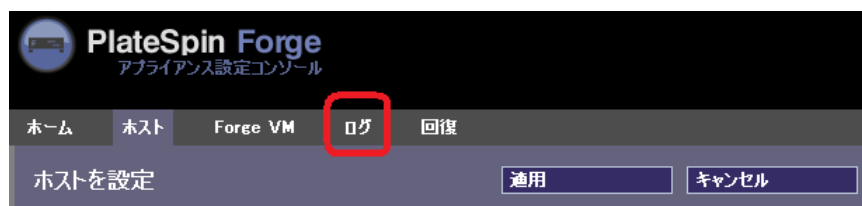
リセット処理が正常に完了すると、次のようなコマンドプロンプトウィンドウが表示されます。

失敗した場合の作業

◆ PlateSpin サポートに問い合わせ、ログファイルを提供する準備をします。リセット処理のトラブルシューティングに必要なログファイルは次のとおりです。

- ◆ /var/log/forge/forge-recovery.log
- ◆ /var/log/forge/INSTALL_LOG.log
- ◆ /var/log/weasel.log
- ◆ /vmfs/volumes/forgeSystem/PLATESPINFORGE_LOGS/forge.log

これらのログファイルの内容は、Forge ACC インタフェースからも参照できます。



◆ PlateSpin サポートから入手できる *Field Rebuild Kit* を使用して Forge を再構築することを検討します。

4 業務の常時稼働

この項では、PlateSpin Forge の基本的な特徴とインタフェースについて説明します。

- ◆ 61 ページのセクション 4.1 「PlateSpin Forge Web インタフェースへのアクセス」
- ◆ 62 ページのセクション 4.2 「PlateSpin Forge Web インタフェースの要素」
- ◆ 64 ページのセクション 4.3 「ワークロードおよびワークロードコマンド」
- ◆ 66 ページのセクション 4.4 「PlateSpin Protect および PlateSpin Forge の複数インスタンスの管理」
- ◆ 69 ページのセクション 4.5 「ワークロードとワークロード保護のレポートの作成」

4.1 PlateSpin Forge Web インタフェースへのアクセス

PlateSpin Forge Web インタフェースを起動するには：

- 1 Web ブラウザを開き、次のページにアクセスします。

`https://<hostname | IP_address>/Forge`

<hostname | IP_address> の部分を、Forge VM 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。

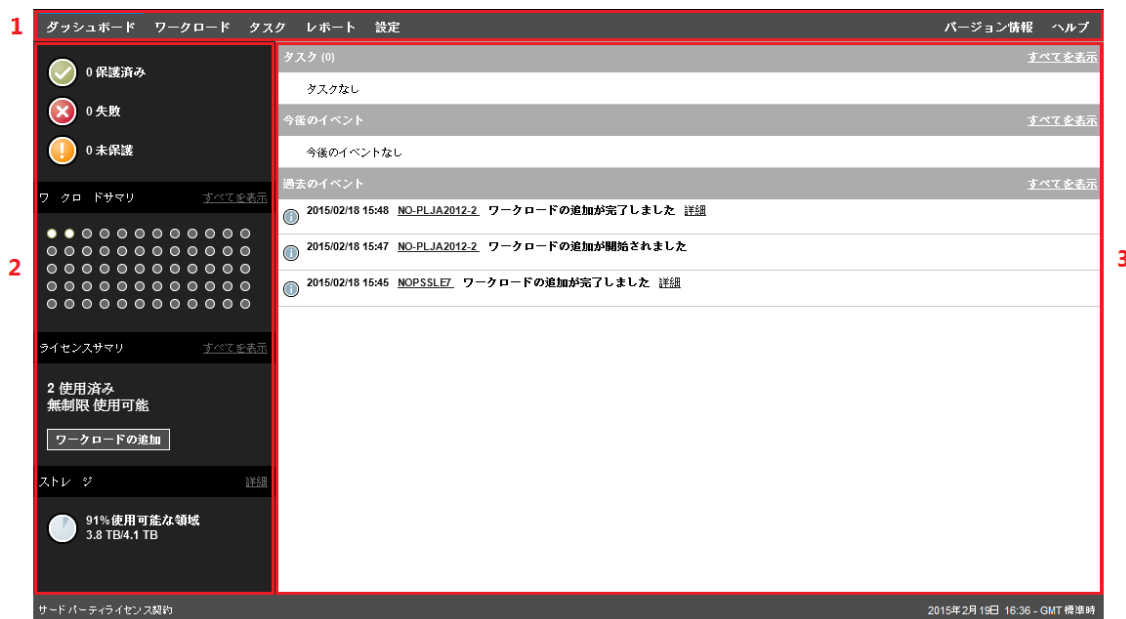
- 2 Forge VM のローカル管理者ユーザの資格情報を使用してログインするか、認証済みユーザとしてログインします。

PlateSpin の追加ユーザのセットアップについては、29 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。

4.2 PlateSpin Forge Web インタフェースの要素

PlateSpin Forge 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 4-1 PlateSpin Forge 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 Forge 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 Forge 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。

- ◆ [63 ページのセクション 4.2.1 「ナビゲーションバー」](#)
- ◆ [63 ページのセクション 4.2.2 「ビジュアルサマリパネル」](#)
- ◆ [64 ページのセクション 4.2.3 「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、[143 ページの「PlateSpin Forge 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。

4.2.1 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。64 ページの「ワークロードおよびワークロードコマンド」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。69 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**：93 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)**：42 ページの「タグによるワークロードのソート」を参照してください。
 - ◆ **許可**：29 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。
 - ◆ **通知設定**：38 ページの「電子メールによる自動的なイベント通知のセットアップ」。
 - ◆ **レプリケーションレポートの設定**：40 ページの「電子メールによる自動レプリケーションレポートのセットアップ」
 - ◆ **SMTP**：詳細については、38 ページの「SMTP 設定」を参照してください。
 - ◆ **ライセンス**：詳細については、28 ページの「製品ライセンスの有効化」を参照してください。

4.2.2 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 4-1 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 4-1 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 Forge 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。

4.2.3 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)。38 ページの「[イベントおよびレポートの自動電子メール通知の設定](#)」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。

4.3 ワークロードおよびワークロードコマンド

[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。

図 4-2 [ワークロード] ページ



注: すべてのタイムスタンプは、Forge VM 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 PlateSpin Forge 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せん。

4.3.1 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 4-3 ワークロードコマンド



表 4-2 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 4-2 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。
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。

4.4 PlateSpin Protect および PlateSpin Forge の複数インスタンスの管理

PlateSpin Forge には、Web ベースのクライアントアプリケーションである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。

- ◆ [66 ページのセクション 4.4.1 「PlateSpin Forge 管理コンソールの使用」](#)
- ◆ [67 ページのセクション 4.4.2 「PlateSpin Forge 管理コンソールについて」](#)
- ◆ [68 ページのセクション 4.4.3 「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」](#)
- ◆ [69 ページのセクション 4.4.4 「管理コンソールでのカードの管理」](#)

4.4.1 PlateSpin Forge 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 Forge 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://<IP_address | hostname>/console`

<IP_address | hostname> の部分は、マネージャとして指定されている Forge VM 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。
コンソールのデフォルトの [ダッシュボード] ページが表示されます。

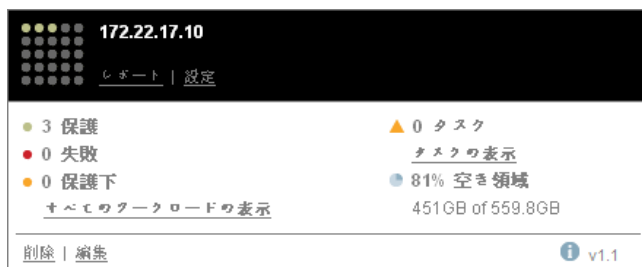
図 4-4 管理コンソールのデフォルトのダッシュボードページ



4.4.2 PlateSpin Forge 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 4-5 PlateSpin Forge 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。

4.4.3 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。

4.4.4 管理コンソールでのカードの管理

管理コンソールでカードの詳細を変更するには：

- 1 編集するカード上で**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。
- 2 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。

管理コンソールからカードを削除するには：

- 1 削除するカードにある**削除**の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。
- 2 **OK** をクリックします。
特定のカードがダッシュボードから削除されます。

4.5 ワークロードとワークロード保護のレポートの作成

PlateSpin Forge 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の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 4-6 レプリケーション履歴レポートのオプション

日付	レプリケーションイベント	合計時間	転送時間	転送サイズ	転送速度
2015/02/18 17:45	ワークロードがビジーであったため増分レプリケーションがスケジュール通りに実行されませんでした	--	--	0 MB	0.00 Mbps
2015/02/18 17:30	ワークロードがビジーであったため増分レプリケーションがスケジュール通りに実行されませんでした	--	--	0 MB	0.00 Mbps
2015/02/18 17:00	ワークロードがビジーであったため増分レプリケーションがスケジュール通りに実行されませんでした	--	--	0 MB	0.00 Mbps
2015/02/18 16:45	ワークロードがビジーであったため増分レプリケーションがスケジュール通りに実行されませんでした	--	--	0 MB	0.00 Mbps

レポートを生成するには：

- 1 PlateSpin Protect 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。

5 ワークロードの保護と回復

PlateSpin Forge 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 Forge 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。

- ◆ 71 ページのセクション 5.1 「ワークロードの保護と回復の基本ワークフロー」
- ◆ 73 ページのセクション 5.2 「コンテナの追加 (保護ターゲット)」
- ◆ 74 ページのセクション 5.3 「ワークロードの追加」
- ◆ 75 ページのセクション 5.4 「保護詳細の設定およびレプリケーションの準備」
- ◆ 79 ページのセクション 5.5 「ワークロード保護の開始」
- ◆ 80 ページのセクション 5.6 「コマンドの中止」
- ◆ 80 ページのセクション 5.7 「フェールオーバー」
- ◆ 82 ページのセクション 5.8 「フェールバック」
- ◆ 86 ページのセクション 5.9 「ワークロードの再保護」

5.1 ワークロードの保護と回復の基本ワークフロー

PlateSpin Forge では、ワークロード保護と回復に対して次のワークフローが定義されています。

- 1 準備 : このステップには、ワークロード、コンテナ、および環境が必要な基準を確実に満たすようにするための準備手順が含まれます。
 - 1a PlateSpin Forge 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。
 - 1b 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。

33 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設定」を参照してください。
 - 1c (Linux のみ)
 - ◆ (条件付き) 標準外のカーネル、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のであれば、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 \(https://www.netiq.com/support/kb/doc.php?id=7005873\)](https://www.netiq.com/support/kb/doc.php?id=7005873) を参照してください。
 - ◆ (推奨) ブロックレベルのデータ転送用に LVM スナップショットを準備します。各ボリュームグループに LVM 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。

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。

- (オプション)各レプリケーションのソースワークロードで実行するfreezeおよびthawスクリプトを準備します。

詳細については、97 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。

- 2 **インベントリ**: このステップでは、PlateSpin Server データベースにワークロードを追加します。

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。73 ページの「コンテナの追加 (保護ターゲット)」および 74 ページの「ワークロードの追加」を参照してください。

- 3 **保護コントラクトの定義**: このステップでは、保護コントラクトの詳細と仕様を定義し、レプリケーションの準備を行います。

詳細については、75 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。

- 4 **保護の開始**: このステップでは、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、79 ページの「ワークロード保護の開始」を参照してください。

- 5 **保護ライフサイクルにおけるオプションのステップ** 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。

- **手動での増分実行**: **増分の実行**をクリックして、ワークロード保護コントラクト以外で、増分レプリケーションを手動で実行することができます。
- **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。詳細については、[フェールオーバーのテスト機能の使用](#)を参照してください。

- 6 **フェールオーバー**: このステップでは、保護されたワークロードを、アプライアンスホスト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、80 ページの「フェールオーバー」を参照してください。

- 7 **フェールバック**: 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、82 ページの「フェールバック」を参照してください。

- 8 **再保護**: 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、86 ページの「ワークロードの再保護」を参照してください。

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せん。64 ページの「ワークロードおよびワークロードコマンド」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。

5.2 コンテナの追加 (保護ターゲット)

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 Forge は、アプライアンスの保護コンテナに常駐します。ターゲット VM インフラストラクチャに常駐するフェールバックのみを定義できます。

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 PlateSpin Forge Web インタフェースで、[設定] > [コンテナ] > [コンテナの追加] の順にクリックします。

名前	オペレーティングシステム	目的	CPU	メモリ	空き容量	最終リフレッシュ
Portsmouth	VMware ESX Server 5.1.0.799733	保護およびフェール バック	4 x Intel(R) Core(TM) i5 CPU 750 @ 2.67GHz	16.0 GB	3.8 TB	0 時間前

- 2 次のパラメータを指定します。

- ◆ **タイプ:** コンテナのタイプを選択します。
 - ◆ **VMware ESX サーバ**
 - ◆ **VMware DRS クラスタ**

VM コンテナ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。

- ◆ **ホスト名または IP:** コンテナのホスト名または IP アドレスを入力します。
- ◆ **vCenter ホスト名または IP:** (DRS クラスタのみ) vCenter サーバのホスト名または IP アドレスを入力します。
- ◆ **クラスタ名:** (DRS クラスタのみ) 必要な DRS クラスタの名前を入力します。

DRS クラスタを追加または更新するときに、次のような場合は基礎のディスクバリエーション操作が失敗します。



- ◆ クラスタには、ESX ホストが含まれていません。
- ◆ クラスタ名は vCenter サーバ全体で一意ではありません (一意のインベントリパスであった場合でも)。
- ◆ クラスタメンバーはアクセスできません (例 : vCenter サーバがメンテナンスモードであるため)。
- ◆ **ユーザ名 / パスワード:** ターゲットホストにアクセスするために管理者レベルの資格情報を指定します。詳細については、[90 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。

- ◆ **目的:** (VM コンテナのみ) VM コンテナに必要な目的を選択します。


- ◆ **フェールバック**

PlateSpin Forge では、フェールバック操作用のコンテナのみを追加できます。

3 [追加] をクリックします。

PlateSpin Forge 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。

コンテナをリフレッシュするには:

- 1 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。

コンテナを削除するには:

- 1 削除したいコンテナの隣にある削除をクリックします。

5.3 ワークロードの追加

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。
[71 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」のステップ 1](#) 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。

PlateSpin Forge 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 (90 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 Forge がワークロードにアクセスできることを確認するには、[[資格情報のテスト](#)] 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 Forge 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、73 ページの「[コンテナの追加 \(保護ターゲット\)](#)」を参照してください。
- 6 75 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。

5.4 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。保護および回復のワークフロー (71 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) の各フェーズにおいて、関連する設定が保護詳細から読み込まれます。

ワークロードの保護詳細を設定するには：

- 1 ワークロードを追加します。74 ページの「[ワークロードの追加](#)」を参照してください。
- 2 コンテナを追加します。73 ページの「[コンテナの追加 \(保護ターゲット\)](#)」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 Forge 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、95 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 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。76 ページの「[ワークロード保護の詳細](#)」を参照してください。
- 6 PlateSpin Forge 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。
- 7 **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。

5.4.1 ワークロード保護の詳細

ワークロード保護の詳細は、[表 5-1](#) 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 5-1 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、 93 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、 90 ページの「データ転送」 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。 92 ページの「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、 92 ページの「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、 90 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。

パラメータの設定	Details (詳細)
CPU	<p>(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。</p> <p>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。</p> <p>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。</p>
CPU の数	<p>(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。</p>
レプリケーションネットワーク	<p>レプリケーションのトラフィックをアプライアンスホストで定義された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、100 ページの「ネットワーキング」を参照してください。</p> <p>この設定では、PlateSpin Forge 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、小さな 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 Forge 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。</p>
Allowed Networks (許可されているネットワーク)	<p>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。</p>
Resource Pool for Target VM (ターゲット VM のリソースプール)	<p>(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。</p>
VM Folder for Target VM (ターゲット VM の VM フォルダ)	<p>(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。</p>
Configuration File Datastore (環境設定ファイルのデータストア)	<p>VM 環境設定ファイルの保存用に、アプライアンスホスト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、95 ページの「復旧ポイント」を参照してください。</p>
保護ボリューム	<p>保護するボリュームを選択し、アプライアンスホスト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。</p>

パラメータの設定	Details (詳細)
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 デモンを選択します。詳細については、 96 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。
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、 100 ページの「ネットワークング」 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。 96 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。 100 ページの「ネットワークング」 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、 100 ページの「ネットワークング」 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。

パラメータの設定	Details (詳細)
サービス / デモンの状態の変更	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、 96 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。 42 ページの「タグによるワークロードのソート」 を参照してください。

5.5 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なら、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 Forge 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。

5.6 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)**) を表すリンクをクリックします。

PlateSpin Forge 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。

5.7 フェールオーバー

フェールオーバーとは、障害が発生したワークロードのビジネス機能が PlateSpin Forge VM コンテナ内のフェールオーバーワークロードによって引き継がれる動作のことをいいます。

- [80 ページのセクション 5.7.1 「オフラインワークロードの検出」](#)
- [81 ページのセクション 5.7.2 「フェールオーバーの実行」](#)
- [81 ページのセクション 5.7.3 「フェールオーバーのテスト機能の使用」](#)

5.7.1 オフラインワークロードの検出

PlateSpin Forge 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 Forge 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。[76 ページの「ワークロード保護の詳細」](#)の中の「[Tier Settings \(ティアの設定\)](#)」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 Forge は指定した受信者に同時に通知メールを送信します。[38 ページの「イベントおよびレポートの自動電子メール通知の設定」](#)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 ([80 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、[81 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 5-1 は、ワークロードの障害を検出した際の PlateSpin Forge 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 5-1 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」)



5.7.2 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。76 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 5-1](#) 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 (95 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**を示すはずですが。

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、81 ページの「フェールオーバーのテスト機能の使用」を参照してください。

5.7.3 フェールオーバーのテスト機能の使用

PlateSpin Forge 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、テスト用に制限され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する [フェールオーバーのテスト] コマンドを使用して行われます。

コマンドを実行すると、PlateSpin Forge 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。76 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 (95 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 Forge 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 を使用してアプライアンスホスト内のフェールオーバーワークロードにアクセスします。
詳細については、[57 ページの「vSphere Client プログラムのダウンロード」](#)を参照してください。
- 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 Forge 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。

5.8 フェールバック

フェールオーバー後の次の論理的な手順としては、フェールバック操作になります。これは、フェールオーバーワークロードを元の物理インフラ、あるいは新しいインフラに移します。

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。

- ◆ [82 ページのセクション 5.8.1「VM プラットフォームへの自動化されたフェールバック」](#)
- ◆ [85 ページのセクション 5.8.2「物理マシンへの半自動化されたフェールバック」](#)
- ◆ [86 ページのセクション 5.8.3「仮想マシンへの半自動化されたフェールバック」](#)

5.8.1 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 Forge 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 (90 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、95 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 Forge 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。84 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 5-2 を参照してください。
PlateSpin Forge がコマンドを実行します。[フェールバック後の設定] のパラメータセットで [フェールバック後に再保護] を選択した場合、再保護のコマンドが PlateSpin Forge Web インタフェースに表示されます。

図 5-2 フェールバックコマンドの詳細

ダッシュボード ワークロード タスク レポート 設定 バージョン情報 ヘルプ

保護の記録 コマンドの詳細

NO-PLJA2012-2

最初のレプリケーションを実行しています

ステータス: 実行しています
期間: 18分 5秒
ステップ: データのコピ (83%)

最後の完全レプリケーション: --
最後の増分レプリケーション: --
最終フェールバックテスト: --
スケジューリング: アクティブ
レプリケーション履歴: --
タスク: --

データ転送のリリース制御 (50%)

コマンドサマリ

ステータス: 実行しています

開始時刻: 2015/02/18 17:28

期間: 18分 5秒

ステップ	ステータス	開始時刻	終了時刻	期間	診断
ソスマシンのリフレッシュ	完了	2015/02/18 17:28	2015/02/18 17:29	45秒	--
ブロックバースコンゴネットのインストール	完了	2015/02/18 17:29	2015/02/18 17:32	3分 1秒	--
① データのコピ	実行しています (83%)	2015/02/18 17:32	--	14分 15秒	--

診断: 生成

レプリケーション転送サマリ

平均転送速度: 252.16 Mbps

期間: 7分 52秒

転送されたデータの合計: 13.5 GB

転送されたファイルの合計: 20,082

ワークロードコマンド

中止 設定 スケジュール一時停止

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 5-2 を参照してください。

表 5-2 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、90 ページの「データ転送」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、アプライアンスホスト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、100 ページの「ネットワーク」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、96 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」を参照してください。
ワークロードの設定	
CPU	<p>(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。</p> <p>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。</p> <p>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。</p>

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、 96 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 PlateSpin Forge 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。

5.8.2 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、[100 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 Forge 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、[109 ページの「デバイスドライバの管理」](#)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 ([90 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。
95 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 Forge 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。

5.8.3 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
```

5.9 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完了すると、[再保護] コマンドが PlateSpin Forge Web インタフェースで使用可能になり、システムは保護コントラクトの初期設定のときに指定したものと同一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、[82 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。

6 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。

- ◆ 89 ページのセクション 6.1 「ワークロードライセンスの消費」
- ◆ 90 ページのセクション 6.2 「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」
- ◆ 90 ページのセクション 6.3 「データ転送」
- ◆ 93 ページのセクション 6.4 「保護ティア」
- ◆ 95 ページのセクション 6.5 「復旧ポイント」
- ◆ 95 ページのセクション 6.6 「初期レプリケーション方法 (フルおよび差分)」
- ◆ 96 ページのセクション 6.7 「サービスおよびデーモンの制御」
- ◆ 97 ページのセクション 6.8 「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)」
- ◆ 97 ページのセクション 6.9 「ボリュームストレージ」
- ◆ 100 ページのセクション 6.10 「ネットワーキング」
- ◆ 100 ページのセクション 6.11 「物理マシンへのフェールバック」
- ◆ 103 ページのセクション 6.12 「Windows クラスターの保護」

6.1 ワークロードライセンスの消費

PlateSpin Forge 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。PlateSpin Forge Web インタフェースの [ダッシュボード] ページの [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、および消費済みライセンスの現在の数が表示されます。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。

製品ライセンスとライセンス有効化に関する詳細は、28 ページの「製品ライセンスの有効化」を参照してください。

6.2 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 Forge 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 Forge によって要求されます。

表 6-1 ワークロードの資格情報

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。 <ul style="list-style-type: none">◆ ドメインメンバーのマシン用: <code>authority\principal</code>◆ ワークグループメンバーのマシン用: <code>hostname</code>
Windows クラスタ	ドメインの管理者資格情報	
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、 <code>sudo</code> 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。
VMware ESX/ESXi 4.1、ESXi 5.0、ESXi 5.1、ESXi 5.5	適切な役割設定を持つ VMware アカウントです。	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。	

6.3 データ転送

次の項目では、ワークロードからレプリカへのデータ転送のメカニズムとオプションについて説明します。

- ◆ [91 ページのセクション 6.3.1 「転送方法」](#)
- ◆ [92 ページのセクション 6.3.2 「データの暗号化」](#)
- ◆ [92 ページのセクション 6.3.3 「Windows ワークロードのボリュームスナップショットディレクトリの場所変更」](#)
- ◆ [93 ページのセクション 6.3.4 「増分レプリケーションのブロック転送でファイルを除外する場合、またはファイルを含める場合」](#)

6.3.1 転送方法

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 Forge 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。

- ◆ 91 ページの「Windows ワークロードでサポートされている転送方法」
- ◆ 92 ページの「Linux ワークロードでサポートされている転送方法」

Windows ワークロードでサポートされている転送方法

Windows ワークロードの場合、PlateSpin Forge 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 Forge 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。

Linux ワークロードでサポートされている転送方法

Linux ワークロードの場合、PlateSpin Forge は、ブロック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のみを提供します。データ転送は、(可能な場合)LVM スナップショットを利用するブロックレベルのデータ転送コンポーネントを使用します (これはデフォルトであり、推奨されるオプションです)。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。

PlateSpin Forge 配布パッケージに含まれる Linux のブロックベースコンポーネントは、サポートされる Linux ディストリビューションの非デバッグの標準カーネル用にコンパイル済みです。標準外のカーネル、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使用しているのであれば、特定のカーネル向けにブロックベースのコンポーネントを再構築できます。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。

コンポーネント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。

6.3.2 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%) スロウ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、76 ページの「ワークロード保護の詳細」を参照してください。

6.3.3 Windows ワークロードのボリュームスナップショットディレクトリの場所変更

PlateSpin Server は、ボリュームスナップショットをデフォルトで次の場所に保存します。

```
\\ProgramData\PlateSpin\Volume Snapshots
```

次のような場合、このパスを変更する必要があります。

- パスの現在のドライブに、Windows ワークロードスナップショットで使用可能な十分な領域がない場合
- 場所を移動してバックアップリストからパスを除外しやすくしたい場合

PlateSpin Server 環境設定ページで PlateSpin Server グローバルパラメータ VssSnapshotMountPath を使用して、スナップショットを保存するサーバ上のカスタムパスを指定できます。このパラメータの値が空の場合、パスはデフォルトのままです。

Windows でボリュームスナップショットディレクトリにカスタムパスを指定するには:

- 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://<platespin-server-ip-address>/PlatespinConfiguration`
- 2 VssSnapshotMountPath を検索して、**編集**をクリックします。

- 3 **Value (値)** フィールドに、Windows ワークロードのボリュームスナップショットを保存する、PlateSpin Server 上のディレクトリの完全なパスを指定します。次に例を示します。

G:\PlateSpin\Volume Snapshots

- 4 **保存**をクリックします。

6.3.4 増分レプリケーションのブロック転送でファイルを除外する場合、またはファイルを含める場合

PlateSpin Forge では、ブロックベースの増分レプリケーションで、一部のファイルがデフォルトで除外されたり、含められます。[Block Based Volume Server Exclude and Include (ブロックベースのボリュームサーバから除外する、またはボリュームサーバに含める)] リストには、デフォルトのファイルに加え、新しいファイルを含められます。新しいリストを追加するには、Platespin Server 環境設定ページで次のグローバルパラメータを使用します。

BlockBasedTransferExcludeFileList

BlockBasedTransferIncludeFileList

ブロックベースの増分レプリケーション時に常に転送するファイルを指定するには :

- 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://<platespin-server-ip-address>/PlatespinConfiguration`
- 2 BlockBasedTransferIncludeFileList を検索して、**編集**をクリックします。
- 3 **Value (値)** フィールドで、ファイル名をリストに追加します。
- 4 **保存**をクリックします。

ブロックベースの増分レプリケーション時に常に除外するファイルを指定するには :

- 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://<platespin-server-ip-address>/PlatespinConfiguration`
- 2 BlockBasedTransferExcludeFileList を検索して、**編集**をクリックします。
- 3 **Value (値)** フィールドで、ファイル名をリストに追加します。
- 4 **保存**をクリックします。

6.4 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 PlateSpin Forge 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、カレンダー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。
ブラックアウト期間	<p>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。</p> <p>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。</p> <p>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。</p>
圧縮レベル	<p>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。24 ページの「データ圧縮」を参照してください。</p> <p>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。</p>
帯域幅制限	<p>これらの設定は、帯域幅制限を制御します。25 ページの「帯域幅制限」を参照してください。</p> <p>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。</p>
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、 95 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。

6.5 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 Forge 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。

アプライアンスから復旧ポイントを削除する方法については、[58 ページの「アプライアンスホストでの Forge VM のスナップショットの管理」](#)を参照してください。

6.6 初期レプリケーション方法 (フルおよび差分)

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。

- ◆ **[Full]：**フルボリューム転送は、運用ワークロードからそのレプリカ (フェールオーバーワークロード) に対して、またはフェールオーバーワークロードからその元となる仮想インフラまたは物理的インフラに対して実施されます。
- ◆ **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アプライアンスホスト内の既存の 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、手動でアプライアンスホストにインポートされる VM。
詳細については、[58 ページの「手動によるアプライアンスホストのデータストアへの VM のインポート」](#)を参照してください。
 - ◆ **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 Forge 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 ([85 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。

PlateSpin Forge 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。

名前	説明	CPU	メモリ	空き領域	最終リフレッシュ	
xlabesxi1	VMware ESXi Server 3.5.0.110271	Intel(R) Pentium(R) 4 CPU 3.20GHz	2.0 GB	457.9 GB	11時間前	削除

仮想マシン:

インベントリネットワーク:

DHCP スタティック

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インベントリ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、ワークロードのアサイン先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。

6.7 サービスおよびデーモンの制御

PlateSpin Forge 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。97 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よ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。

6.8 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 Forge は、カスタムスクリプトである freeze および thaw を自動的に実行でき、これらのスクリプトによって自動デーモン制御機能が補足されます。

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 (96 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
```

6.9 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、PlateSpin Forge 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 Forge 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、19 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 6-1 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 6-1 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

ダッシュボード ワークロード タスク レポート 設定 バージョン情報 ヘルプ

保護の詳細を編集: NOPSSLE7

コンテナの変更 保存して準備 保存 キャンセル

ティアの設定

レプリケーション設定

転送の暗号化 データ転送の暗号化

ソース資格情報

ユーザー:

パスワード:

テスト資格情報

CPU

ソケット:

ソケットごとのコア:

合計コア: 9

レプリケーションネットワーク: VM Network - 10.10.18x

DHCP スタティック MTU:

許可されたネットワーク:

許可	名前	アドレス	DHCPを使用
<input checked="" type="checkbox"/>	eth0	10.10.187.153	False

ターゲットVMのソースプール: cluster60 [編集](#)

ターゲットVMに対するVMフォルダ: dc60 [編集](#)

設定ファイルのデータストア: VOL1-HPSAN-STORAGE (366.5 GB)

保護されたボリューム

含む	名前	使用済み領域	空き容量	データストア	シンディスク
<input checked="" type="checkbox"/>	/ (EXT3 - System)	5.0 GB	8.73 GB	VOL1-HPSAN-STOF	<input type="checkbox"/>
<input type="checkbox"/>	/opt/ovs/ins/mnt/pools/POOL1 (NSSFS)	88.9 MB	11.93 GB	VOL1-HPSAN-STOF	<input type="checkbox"/>

保護された論理ボリューム

含む	名前	使用済み領域	空き容量	ボリュームグループ / OESボリューム
<input checked="" type="checkbox"/>	/rmlst1 (EXT3)	84.5 MB	923.4 MB	VolGroup1
<input checked="" type="checkbox"/>	/rmlst2 (EXT3)	169.5 MB	1.8 GB	VolGroup1

非ボリュームストレージ

含む	パーティション	はスワップ	合計サイズ	データストア	シンディスク
<input checked="" type="checkbox"/>	/dev/ada1	はい	2.01 GB	BBCSLESSAN (3.8)	<input type="checkbox"/>

ボリュームグループ:

含む	名前	合計サイズ	データストア	シンディスク
<input checked="" type="checkbox"/>	VolGroup1	8.0 GB	BBCSLESSAN (3.8)	<input type="checkbox"/>

レプリケーション中に停止するデーモン: [デーモンの追加](#)

フェールオーバー設定

フェールオーバー設定の準備

フェールオーバー設定のテスト

タグ

図 6-2 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 6-2 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)

保護されたボリューム:	含める	名前	合計サイズ	データストア	シンディスク	
	<input checked="" type="checkbox"/>	/ (EXT3 - System)	13.8 GB	BBCSLESSAN	<input type="checkbox"/>	
保護された論理ボリューム:	含める	名前	合計サイズ	ボリュームグループ		
	<input checked="" type="checkbox"/>	/vmtest1 (EXT3)	1007.9 MB	VolGroup1		
	<input checked="" type="checkbox"/>	/vmtest2 (EXT3)	2.0 GB	VolGroup1		
	<input checked="" type="checkbox"/>	/opt/novell/nss/mnt/pools iPOOL1 (NSSFS)	12.0 GB	POOL1		
非ボリュームストレージ:	含める	パーティション	はスワップ	合計サイズ	データストア	シンディスク
	<input checked="" type="checkbox"/>	/dev/sda1	はい	2.0 GB	BBCSLESSAN	<input type="checkbox"/>
ボリュームグループ:	含める	名前	合計サイズ	データストア	シンディスク	
	<input checked="" type="checkbox"/>	VolGroup1	8.0 GB	BBCSLESSAN	<input type="checkbox"/>	
OESボリューム:	含める	名前	合計サイズ	データストア	シンディスク	
	<input checked="" type="checkbox"/>	POOL1	12.0 GB	BBCSLESSAN	<input type="checkbox"/>	
レプリケーション中に停止するデーモン:	-					

図 6-3 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 6-3 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)

保護された論理ボリューム:	含める	名前	使用済み領域	空き容量	ボリュームグループ/EVMSボリューム	
	<input checked="" type="checkbox"/>	/ (REISERFS)	2.2 GB	2.2 GB	システム	
	<input checked="" type="checkbox"/>	/boot (EXT2)	13.0 MB	55.3 MB	/dev/evms/sda1	
	<input checked="" type="checkbox"/>	/opt/novell/nss/mnt/pools/NEVMPool (NSSFS)	23.3 MB	999.6 MB	NEVMPool	
非ボリュームストレージ:	含める	パーティション	はスワップ	合計サイズ	データストア/ボリュームグループ	
	<input checked="" type="checkbox"/>	/dev/system/swap	はい	1.48 GB	システム	
ボリュームグループ:	含める	名前	合計サイズ	データストア	シンディスク	
	<input checked="" type="checkbox"/>	システム	5.9 GB	dev-comp124:storage	<input type="checkbox"/>	
EVMSボリューム:	含める	名前	はスワップ	合計サイズ	データストア	シンディスク
	<input checked="" type="checkbox"/>	/dev/evms/sda1		70.6 MB	dev-comp124:storage	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	NEVMPool		1023.0 MB	dev-comp124:storage	<input type="checkbox"/>
レプリケーション中に停止するデーモン:	デーモンの追加					

6.10 ネットワーキング

PlateSpin Forge 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。

6.11 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 Forge 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 ブート (ISO) イメージを使用して起動することで実行されます。

- ◆ [100 ページのセクション 6.11.1 「PlateSpin ISO ブートイメージのダウンロード」](#)
- ◆ [100 ページのセクション 6.11.2 「ISO ブートイメージへのデバイスドライバの追加」](#)
- ◆ [102 ページのセクション 6.11.3 「PlateSpin Forge 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」](#)

6.11.1 PlateSpin ISO ブートイメージのダウンロード

PlateSpin ISO ブートイメージ (BIOS ファームウェアベースのターゲットの場合は p.iso、UEFI ファームウェアベースのターゲットの場合は bootofx.x2) は、次のパラメータで検索を実行して、NetIQ ダウンロードの [PlateSpin Forge \(http://dl.netiq.com\)](http://dl.netiq.com) エリアからダウンロードできます。

- ◆ **製品またはテクノロジー** : PlateSpin Forge
- ◆ **バージョンの選択** : PlateSpin Forge 11.2
- ◆ **日付範囲** : All Dates

6.11.2 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 \(https://www.netiq.com/support/kb/doc.php?id=7005990\)](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。
-c <path>	<path> は、ConfigureTakeControl.xml ファイルの存在する場所を指定します。

引数	説明
-l [<i><type></i>]	<p><i><type></i> 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。</p> <p>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、<i><kernel_module_directory>/kernel/</i> に存在すると見なされます。</p> <p>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、<i><kernel_module_directory>/kernel/drivers/</i> に存在すると見なされます。</p> <p>ドライバサブセットの例：</p> <pre>-l scsi -l 'net video' -l '/net net'</pre> <p>この引数の特殊な使用法：</p> <p>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</p>

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
```

6.11.3 PlateSpin Forge 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、Forge VM のホスト名または IP アドレスを入力します。
- 7 権限を指定して、Forge VM に対して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承認します。
- 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 Forge 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。

6.12 Windows クラスタの保護

PlateSpin Forge 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。サポートされるクラスタリング技術は次のとおりです。

- ◆ **Windows Server 2012 R2:** サーバベースの Microsoft フェールオーバークラスタ(「ノードおよびディスクマジョリティのクォーラム」モデルおよび「マジョリティなし: ディスク専用クォーラム」モデル)
- ◆ **Windows Server 2008 R2:** サーバベースの Microsoft フェールオーバークラスタ(「ノードおよびディスクマジョリティのクォーラム」モデルおよび「マジョリティなし: ディスク専用クォーラム」モデル)
- ◆ **Windows Server 2003 R2:** Server ベースの Windows クラスタサーバ(「シングルクォーラムデバイスクラスタ」モデル)

ご使用の PlateSpin 環境に対して Windows クラスタの検出を有効または無効にできます。詳細については、[106 ページのセクション 6.12.2 「Windows クラスタ検出の有効化または無効化」](#)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。

- ◆ [104 ページのセクション 6.12.1 「クラスタワークロードの保護」](#)
- ◆ [106 ページのセクション 6.12.2 「Windows クラスタ検出の有効化または無効化」](#)
- ◆ [106 ページのセクション 6.12.3 「リソース名の検索値」](#)
- ◆ [107 ページのセクション 6.12.4 「クォーラムアービトレーションのタイムアウト」](#)
- ◆ [107 ページのセクション 6.12.5 「ローカルボリュームのシリアル番号の設定」](#)

- [108 ページのセクション 6.12.6 「PlateSpin のフェールオーバー」](#)
- [108 ページのセクション 6.12.7 「PlateSpin のフェールバック」](#)

6.12.1 クラスタワークロードの保護

クラスタの保護は、アクティブノード上の変更の増分レプリケーションを、ノードが1つの仮想クラスタに流すことで実現します。この仮想クラスタは、ソースインフラのトラブルシューティングで使用できます。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。

- [104 ページの「前提条件」](#)
- [105 ページの「ブロックベース転送」](#)
- [105 ページの「最初の完全レプリケーション中のクラスタノードのフェールオーバー」](#)
- [105 ページの「レプリケーション中のクラスタノードのフェールオーバー」](#)
- [105 ページの「レプリケーション間でのクラスタノードのフェールオーバー」](#)
- [106 ページの「保護のセットアップ」](#)

前提条件

クラスタ保護のサポート範囲は、次の条件に従う必要があります。

- **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。
- **アクティブノードの検出** : PlateSpin グローバル環境設定 DiscoverActiveNodeAsWindowsCluster が True に設定されていることを確認します。これは PlateSpin Server 環境設定ページにあります。これがデフォルトの設定です。詳細については、[106 ページのセクション 6.12.2 「Windows クラスタ検出の有効化または無効化」](#) を参照してください。
- **リソース名の検索値** : PlateSpin Forge で、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、使用する検索値を指定する必要があります。詳細については、[106 ページのセクション 6.12.3 「リソース名の検索値」](#) を参照してください。
- **解決可能なホスト名** : PlateSpin Server は、クラスタに属する各ノードのホスト名を解決する必要があります。

注 : ホスト名は IP アドレスによって解決可能である必要があります。つまり、ホスト名の参照と逆引き参照の両方が必要です。

- **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。
- **PowerShell 2.0** : クラスタの各ノードに Windows PowerShell 2.0 エンジンがインストールされている必要があります。

ブロックベース転送

クラスタワークロードに対してブロックベース転送を使用する場合、ブロックベースのドライバコンポーネントはクラスタノードにインストールされていません。ブロックベース転送は、ドライバを使用しない同期を MD5 ベースのレプリケーションで使用することで発生します。ブロックベースのドライバがインストールされていないので、ソースクラスタノードでの再起動は不要です。

注：ファイルベースの転送は、Microsoft Windows クラスタを保護するためにサポートされていません。

最初の完全レプリケーション中のクラスタノードのフェールオーバー

クラスタワークロードでは、最初の完全レプリケーションが、クラスタノードのフェールオーバーが発生することなく正常に完了する必要があります。最初の完全レプリケーションが完了する前にクラスタノードのフェールオーバーが発生した場合、既存のワークロードを削除し、アクティブノードを使用しているクラスタを追加し直してから、もう一度実行する必要があります。

レプリケーション中のクラスタノードのフェールオーバー

フルまたは増分レプリケーション中のコピー処理が完了する前にクラスタノードフェールオーバーが生じた場合、コマンドは中止され、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。

レプリケーション間でのクラスタノードのフェールオーバー

レプリケーションプロセスが中断されるのを防ぐため、各ノードには類似するプロファイルが必要です。保護されたクラスタで実行する複数回の増分レプリケーションの間でクラスタノードのフェールオーバーが発生した場合および新しいアクティブノードのプロファイルが障害元アクティブノードのプロファイルに類似している場合は、保護契約が次の増分レプリケーションで予定どおり継続されます。それ以外の場合は、次の増分レプリケーションコマンドが失敗します。

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、[141 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。

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 アドレスを指定するようにしてください。詳細については、71 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。

6.12.2 Windows クラスタ検出の有効化または無効化

PlateSpin Forge Server では、各クラスタにあるアクティブノードに基づいて、PlateSpin 環境の Windows Server フェイルオーバークラスタを検出およびインベントリできます。または、アクティブクラスタノードと非アクティブクラスタノードのすべてを、スタンドアロンマシンとして処理できます。

すべての Windows クラスタに対してクラスタ検出を有効にするには、パラメータ `DiscoverActiveNodeAsWindowsCluster` が `True` に設定されていることを確認します。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、およびワークロード保護では、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。そのクラスタ名や管理共有は使用しません。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、104 ページの「前提条件」を参照してください。

すべての Windows クラスタに対してクラスタ検出を無効にするには、パラメータ `DiscoverActiveNodeAsWindowsCluster` を `False` に設定します。この設定により、PlateSpin Server は、Windows フェイ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://<platespin-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。

6.12.3 リソース名の検索値

Windows フェイルオーバークラスタのアクティブノードを特定するため、PlateSpin Forge で、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必要があります。共有クラスタの IP アドレスリソースは、クラスタ上のアクティブノードに存在しません。

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ときには、クラスタで現在アクティブなノードの IP アドレスを指定する必要があります。PlateSpin Forge は、そのノード上にあるクラスタの IP アドレスリソース名を検索し、そのリスト内の各値に含まれる指定の文字で「始まる」リソースを見つけます。つまり、各検索値には、共有クラスタの IP アドレスリソースを区別するのに十分な文字数を含める必要がありますが、同時に他の Windows クラスタに適用できる短いものである必要があります。

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://<platespin-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。

6.12.4 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 \(https://msdn.microsoft.com/en-us/library/aa369123%28v=vs.85%29.aspx?f=255&MSPPError=-2147217396\)](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://<platespin-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。

6.12.5 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、[141 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。

6.12.6 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。

6.12.7 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 \(http://www.netiq.com/support/kb/doc.php?id=7016770\)](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 \(http://www.netiq.com/support/kb/doc.php?id=7015576\)](http://www.netiq.com/support/kb/doc.php?id=7015576) を参照してください。
-

7 物理マシンを操作するための補助ツール

PlateSpin Forge 配布パッケージには、物理マシンをフェールバックターゲットとして操作する場合に使用できるツールが含まれています。

- ◆ [109 ページのセクション 7.1 「デバイスドライバの管理」](#)

7.1 デバイスドライバの管理

PlateSpin Forge には、デバイスドライバのライブラリが付属しており、ターゲットワークロード上に適切なドライバが自動的にインストールされます。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の特定のドライバを指定した場合は、PlateSpin Forge ドライバデータベースにドライバを追加 (アップロード) する必要があります。

次のセクションで、詳細を説明します。

- ◆ [109 ページのセクション 7.1.1 「Windows システム用のデバイスドライバのパッケージ化」](#)
- ◆ [110 ページのセクション 7.1.2 「Linux システム用のデバイスドライバのパッケージ化」](#)
- ◆ [110 ページのセクション 7.1.3 「PlateSpin デバイスドライバデータベースへのドライバのアップロード」](#)
- ◆ [112 ページのセクション 7.1.4 「プラグアンドプレイ \(PnP\) ID トランスレータ機能の使用」](#)

7.1.1 Windows システム用のデバイスドライバのパッケージ化

Windows デバイスドライバを PlateSpin Forge ドライバデータベースにアップロードするためにパッケージ化するには：

- 1 個別のドライバファイル (*.sys、*.inf、*.dll など) をすべてを、ターゲットのインフラストラクチャとデバイスに対して準備します。製造元特有のドライバを .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、ドライバをアップロードする準備が整いました。[110 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のアップロード」](#)を参照してください。

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、デジタル署名されているドライバのみをアップロードします。次のシステムに使用します。

- ◆ すべての 64 ビット Windows システム
 - ◆ Windows Server 2008 および Windows 7 システムの 32 ビットバージョン
-

7.1.2 Linux システム用のデバイスドライバのパッケージ化

Linux デバイスドライバを PlateSpin Forge ドライバデータベースにアップロードするためにパッケージ化するには、PlateSpin ISO ブートイメージに含まれるカスタムユーティリティを使用できません。

- 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
```

たとえば、bnx2x-1.48.107-RHEL4-2.6.9-11.EL-i686.pkg となります。

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。詳細については、[110 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のアップロード」](#)を参照してください。

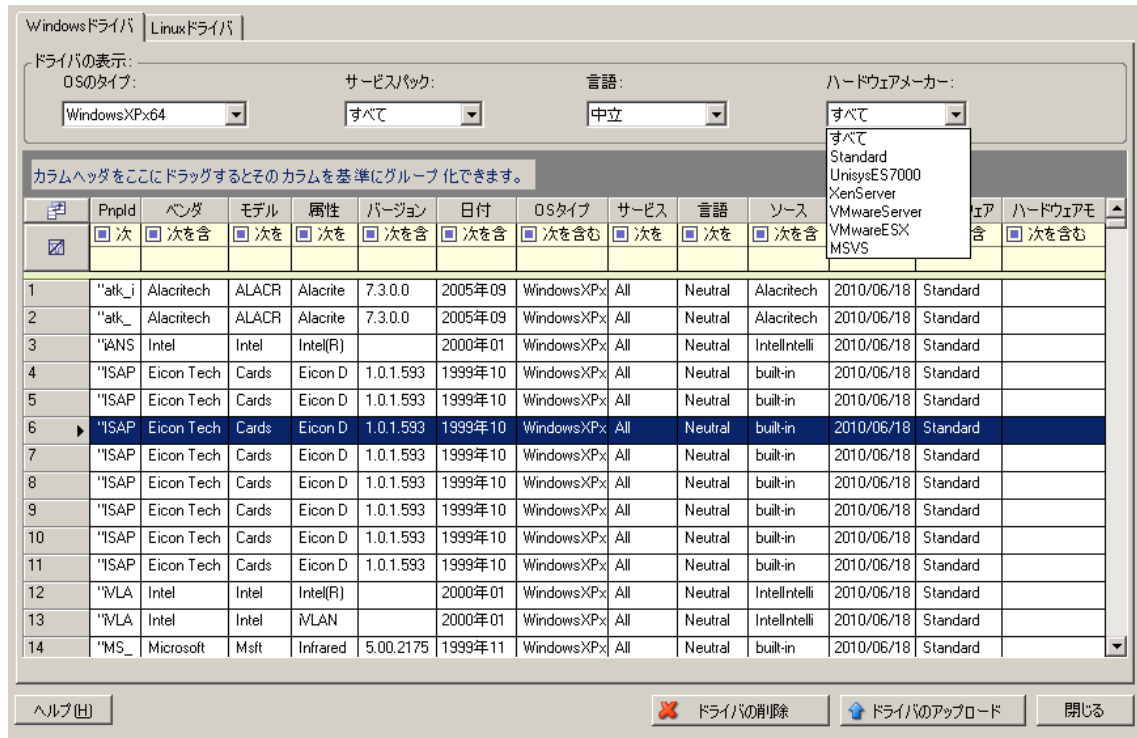
7.1.3 PlateSpin デバイスドライバデータベースへのドライバのアップロード

PlateSpin Driver Manager 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。

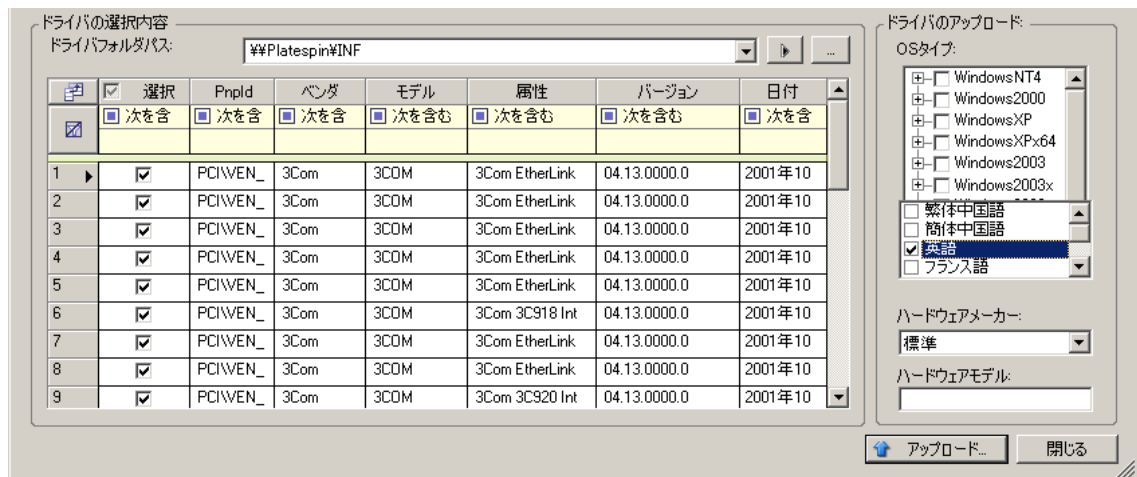
注：アップロード時に、PlateSpin Forge では、選択したオペレーティングシステムタイプまたはそのビット仕様に対してドライバを検証しません。ターゲットのインフラストラクチャに適したドライバのみを必ずアップロードしてください。

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 システム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 Forge VM で、Program Files\PlateSpin Forge Server\DriverManager にある DriverManager.exe プログラムを開始し、**[Windows ドライバ]** タブを選択します。



- 3 [ドライバのアップロード] をクリックし、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。

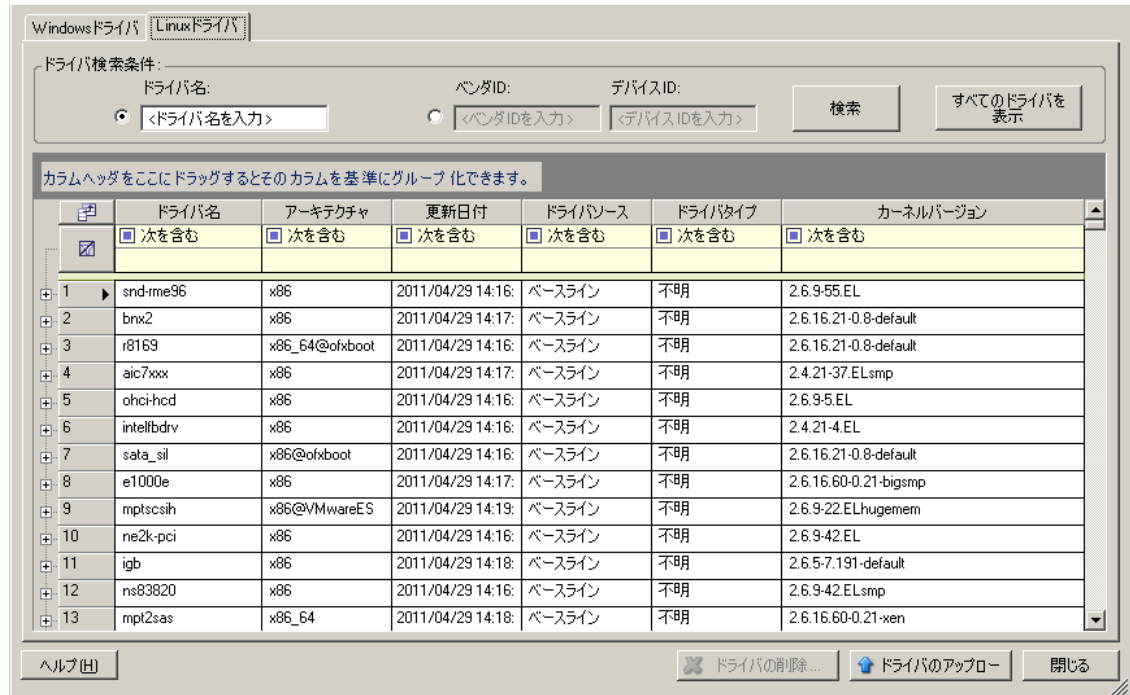


リストされているターゲット環境に対して特別に設計されたドライバでない限り、ハードウェアメーカーオプションとして標準を選択します。

- 4 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 システム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 ツール > デバイスドライバの管理の順にクリックし、Linux ドライバタブを選択します。



- 3 ドライバのアップロードをクリックし、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。

7.1.4 プラグアンドプレイ (PnP) ID トランスレータ機能の使用

「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的基础となるものであり、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。

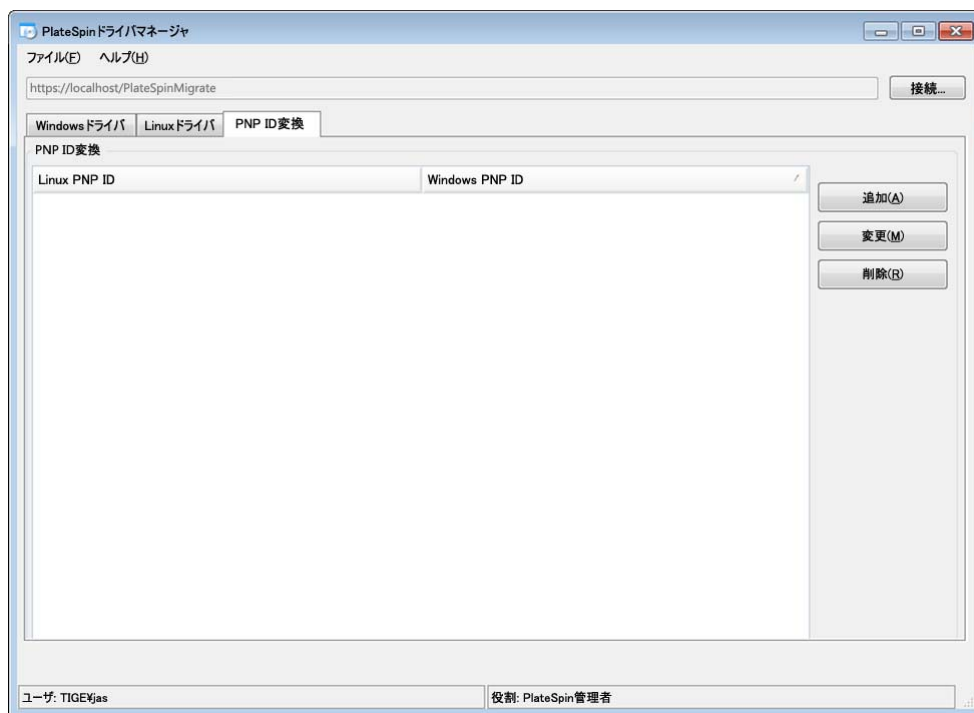
PlateSpin Server がワークロードおよび使用可能なハードウェアを検出すると、検出結果には、それらの PnP ID とそのデータのストレージがワークロードの詳細として含まれます。PlateSpin は、ID を使用して、フェールオーバー/フェールバック操作時にどのドライバを追加する必要があるかを判断します(追加する必要があるドライバがある場合)。PlateSpin Server は、サポートされている各オペレーティングシステムの、関連付けられているドライバのための、PnP ID のデータベース

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、Forge の Linux RAM ディスクによって検出された Windows ワークロードには、Linux 形式の PnP ID が含まれていません。

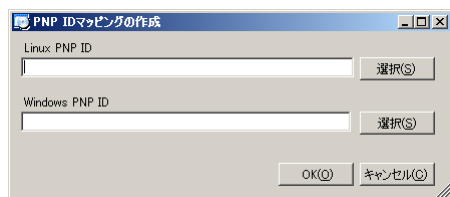
それらの ID は一貫してフォーマットされているので、PlateSpin は、それぞれに標準変換を適用して、対応する Windows PnP ID を決定できます。変換は、PlateSpin 製品内で自動的に行われます。この機能を使用して、管理者またはサポート技術者は、カスタムの PnP マッピングを追加、編集、または削除することができます。

PnP ID 変換機能を使用するには、次の手順に従います。

- 1 PlateSpin Driver Manager ツールを起動し、PlateSpin Server に接続します。
- 2 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、現在既知のカスタム PnP ID マッピングが含まれます。



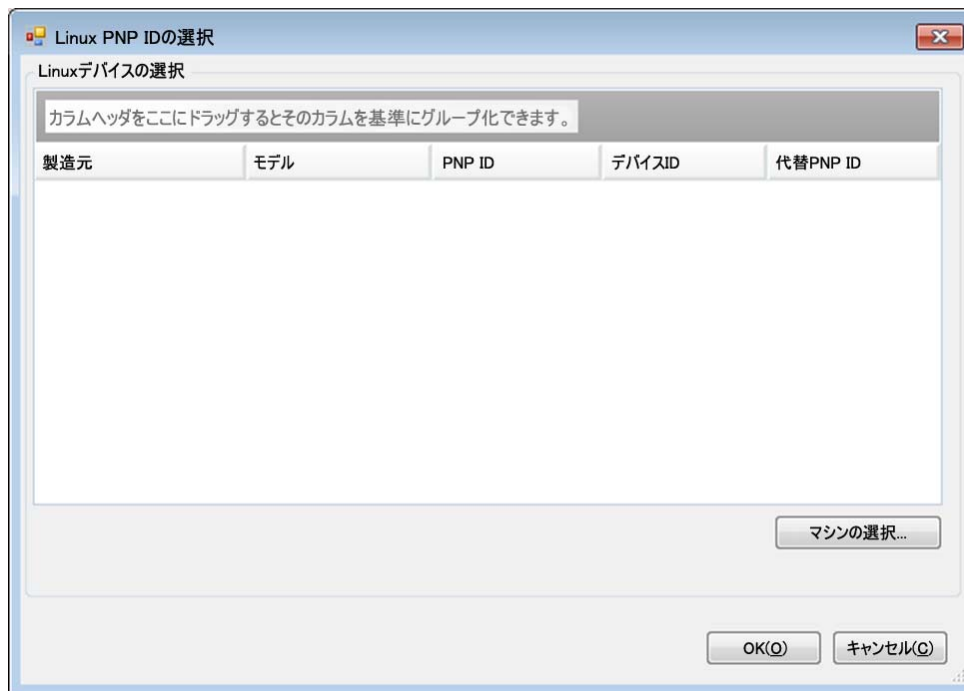
- 3 リストページで、**追加**をクリックして、[PNP ID マッピングの作成] ダイアログを表示します。



- 4 **Linux PnP ID** フィールドに、Linux PnP ID を追加します。
 - 4a (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

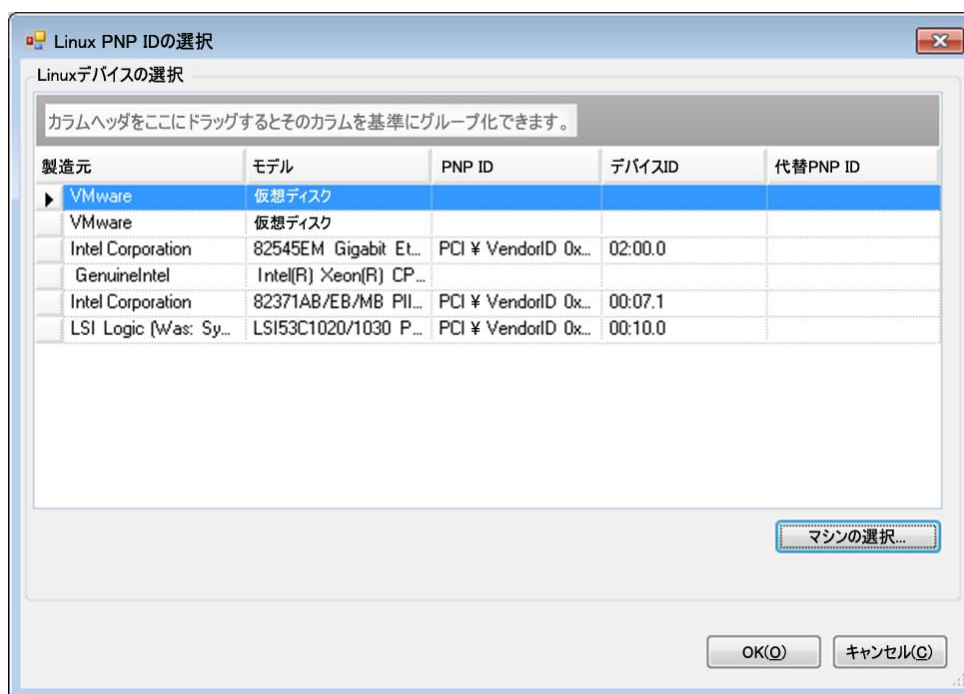
4b (条件付き) 検出済みのワークロードから ID を選択します。

4b1 **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。



4b2 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。

4b3 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。



4b4 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。

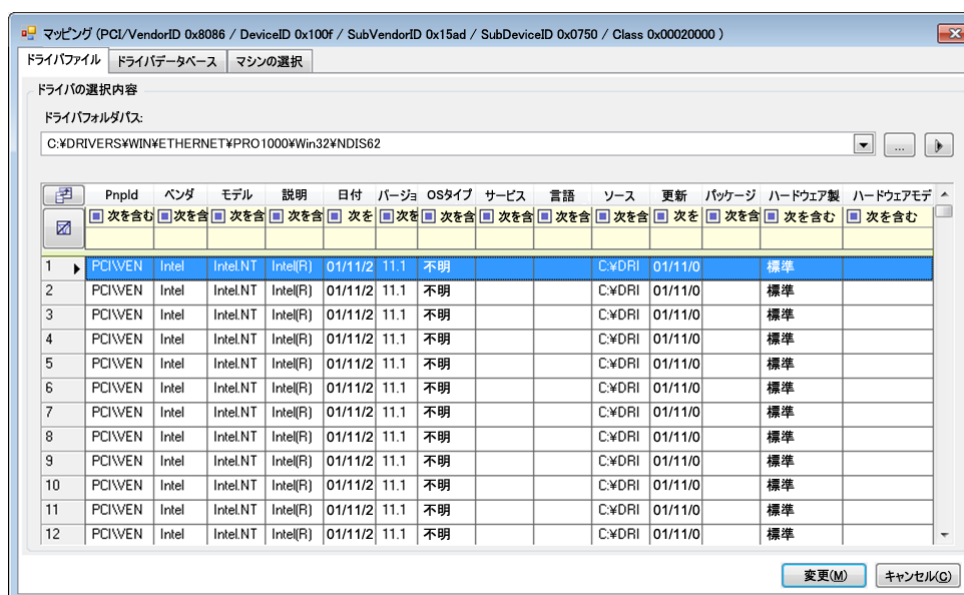
5 **Windows PNP ID** フィールドに、Windows PnP ID を追加します。

5a (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。

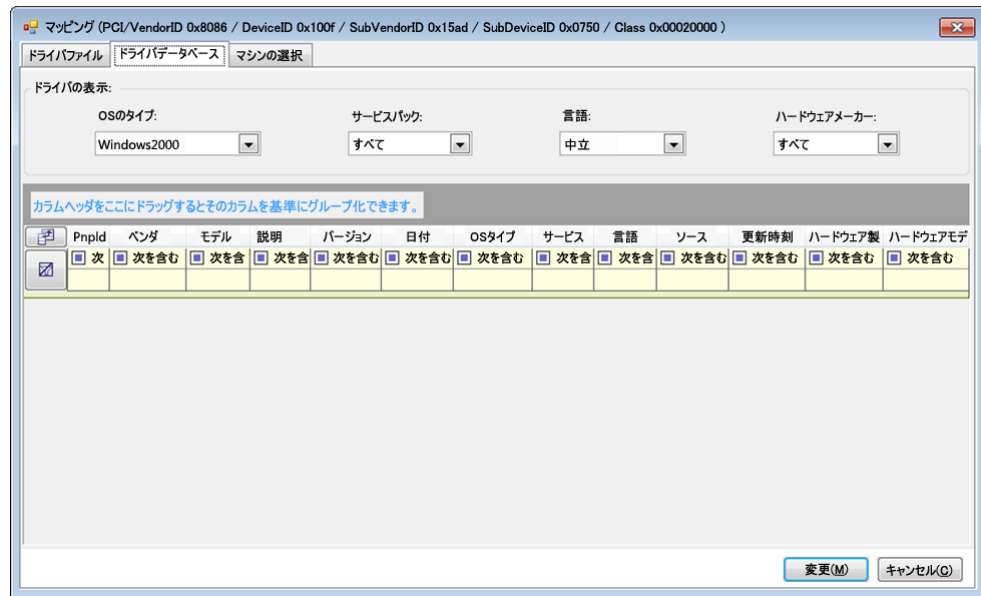
または

5b (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)。

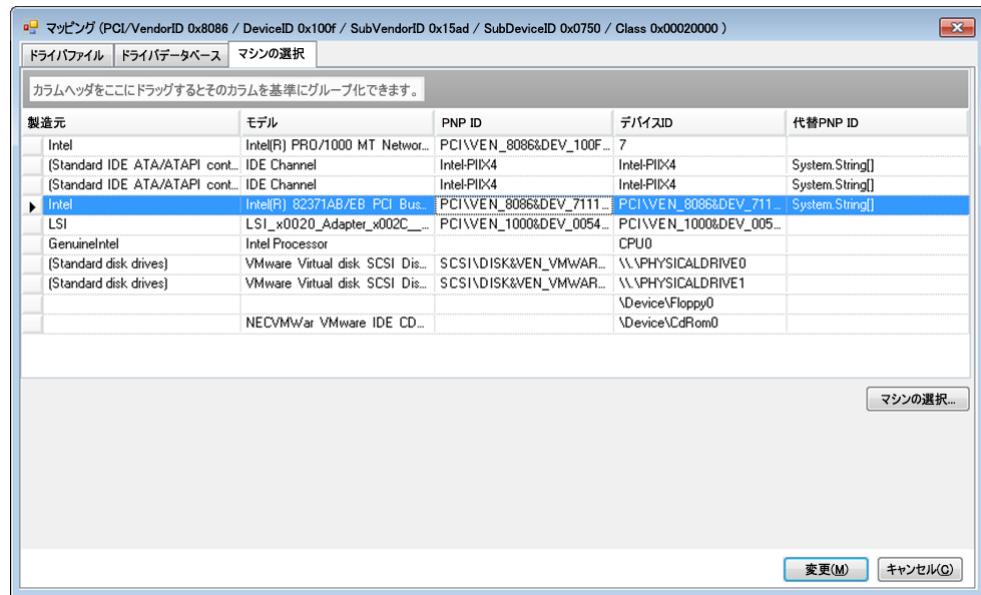
- ◆ **ドライバファイルタブ**で、Windows ドライバファイル (つまり、*.inf 拡張子のファイル) を参照して選択し、目的の PnP ID を選択して、**変更**をクリックします。



- ◆ 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。

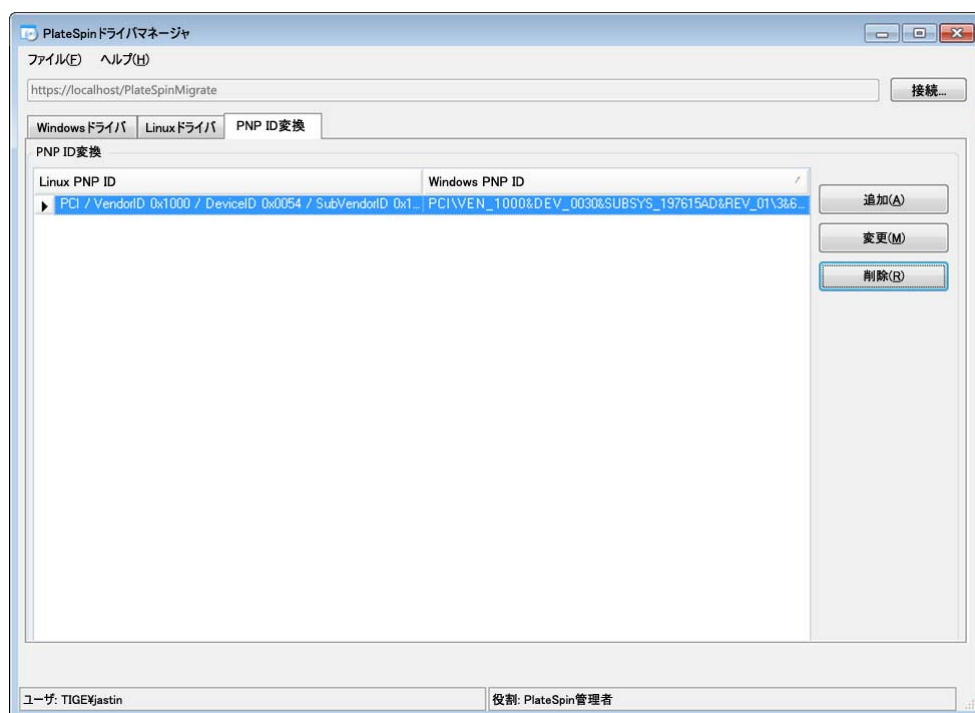


- ◆ **Select Machine** タブで、**Select Machine** をクリックし、ライブディスクバリを使用して検出された Windows マシンのリストからマシンを選択し、**OK** をクリックしてそのデバイスを表示し、目的の PnP ID を選択して、[Modify] をクリックします。



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。

- 6 [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 ID 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。



7 (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、

7a **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。

7b [115 ページのステップ 5](#) 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。

8

ProtectAgent ユーティリティ

ProtectAgent (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する場合は常に再起動する必要がありますが、ProtectAgent を使用すると、アクションを実行するタイミング、つまりサーバを再起動するタイミングを詳細に制御できます。たとえば、ProtectAgent を使用して、ドライバのインストールを、最初のレプリケーションの実行中ではなく、スケジュールされたダウンタイム中に実行できます。

ProtectAgent ユーティリティの構文は次のとおりです。

```
ProtectAgent.cli.exe [Option] [/psserver=%IP%]
```

表 8-1 では、ProtectAgent.cli.exe コマンドで使用できるオプションとスイッチについて説明します。

表 8-1 ProtectAgent コマンドのオプションとスイッチ

使用法	説明
オプション	
h ? help	このコマンドの使用方法和オプションを表示します。
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	PlateSpin のコントローラとドライバのインストールステータスを表示します。
din driver-install	PlateSpin ドライバをインストールします。
dup driver-upgrade	PlateSpin ドライバをアップグレードします。
dun driver-uninstall	PlateSpin ドライバをアンインストールします。
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。

ProtectAgent 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、ProtectAgent 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、ProtectAgent 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。

システムは、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 8-1) に表示されます。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 8-2) に表示されます。

図 8-1 再起動通知タスク

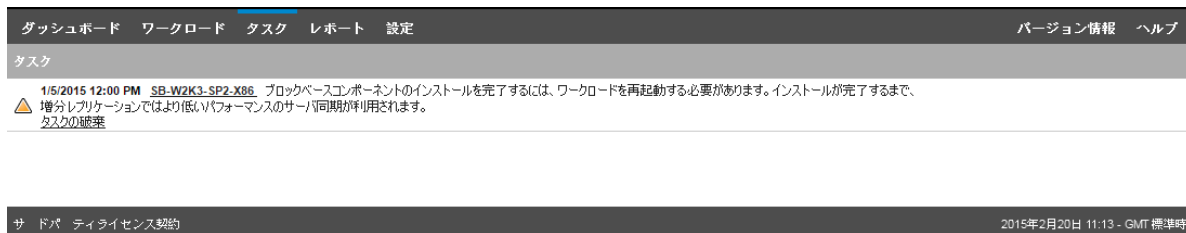


図 8-2 レプリケーション中の再起動通知

The screenshot shows the NO-PROUS1 management interface. At the top, there are navigation tabs: ダッシュボード, ワークロード, タスク, レポート, 設定. On the right, there are links for バージョン情報 and ヘルプ. Below the navigation, there are tabs for 保護の管理 and コマンドの詳細. The main content area is titled "最初のレプリケーションを実行しています" (Running the first replication). It shows the status as "実行しています" (Running) with a refresh icon. The duration is 17分 24秒 and the progress is 84% for the "データのコピー" (Data copy) step. A progress bar for "ターゲットマシンのリソース制限 (50%)" is also visible. On the right, there is a list of replication details: 最後の完全レプリケーション: --, 最後の増分レプリケーション: --, 最終フェールオーバーテスト: --, スケジュール: アクティブ, レプリケーション履歴: --, タスク: --. Below this, there is a "コマンドサマリ" (Command Summary) section with a warning icon and text: "ブロックベースコンポーネントのインストールを完了するには、ワークロードを再起動する必要があります。インストールが完了するまで、増分レプリケーションではより低いパフォーマンスのサーバ同期が利用されます。" (To complete the installation of the block-based component, you need to restart the workload. Until the installation is complete, incremental replication will use server synchronization with lower performance). The status is "実行しています" (Running). The start time is 2015/02/19 16:31 and the duration is 17分 24秒. A table follows with columns: ステップ (Step), ステータス (Status), 開始時刻 (Start Time), 終了時刻 (End Time), 期間 (Duration), and 診断 (Diagnosis). The table shows two steps: "ソースマシンのリフレッシュ" (Refresh source machine) which is completed, and "データのコピー" (Data copy) which is running at 84%. Below the table is a "レプリケーション転送サマリ" (Replication Transfer Summary) section showing: 平均転送速度: 148.66 Mbps, 期間: 7分 16秒, 転送されたデータの合計: 6.8 GB, and 転送されたファイルの合計: 5,507. At the bottom, there is a "ワークロードコマンド" (Workload Command) section with buttons for 中止 (Stop), 設定 (Settings), and スケジュール一時停止 (Pause Schedule). The footer contains "サードパーティライセンス契約" (Third-party license agreement) and "2015年2月19日 16:48 - GMT 標準時" (February 19, 2015 16:48 - GMT Standard Time).

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は、[Status (ステータス)] フィールドで警告として表示されます (図 8-3)。それ以降の増分レプリケーションは、警告なしで完了します。

図 8-3 サーバ同期の必要性の通知

NO-PROUS1

増分を実行しています

ステータス: 実行しています

期間: 7分 47秒

ステップ: データのコピ (69%)

最後の完全レプリケーション: 2015/02/20 0:21

最後の増分レプリケーション: 2015/02/20 9:11

最終フェルオバテスト: --

スケジュール: アクティブ

レプリケーション履歴: 表示

タスク: --

☒ コマンドサマリ

イベント:	イベント	詳細	ユーザ	日付		
イベント:	増分レプリケーションが開始しました		PSPIN2012JA1\Administrator	2015/02/20 9:41		
ステータス:	実行しています ⚠️ ブロックベースのコンポーネントで最近インストールプロセスが完了しました。このレプリケーションでは、サーバ同期の実行が必要です。					
開始時刻:	2015/02/20 9:41					
期間:	7分 47秒					
ステップ:	ステップ	ステータス	開始時刻	終了時刻	期間	診断
	ソ マシンのリフレッシュ	完了	2015/02/20 9:41	2015/02/20 9:42	46秒	--
	スナップショットに戻す	完了	2015/02/20 9:42	2015/02/20 9:43	35秒	--
	データのコピ	実行しています (69%)	2015/02/20 9:43	--	6分 26秒	--
						診断: 生成

☒ レプリケーション転送サマリ

平均転送速度:	108.90 Mbps
期間:	35秒
転送されたデータの合計:	256.4 MB
転送されたファイルの合計:	503

ワークロードコマンド

中止 ▶

設定 ▶

スケジュール一時停止 ▶

Third-Party License Agreements
2015年2月20日 9:49 - GMT 標準時

9 トラブルシューティング

このセクションでは、次の情報を紹介します。

- ◆ 123 ページのセクション 9.1「ワークロードインベントリのトラブルシューティング (Windows)」
- ◆ 127 ページのセクション 9.2「ワークロードインベントリのトラブルシューティング (Linux)」
- ◆ 127 ページのセクション 9.3「レプリケーションの準備コマンドで発生した問題のトラブルシューティング (Windows)」
- ◆ 128 ページのセクション 9.4「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」
- ◆ 130 ページのセクション 9.5「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」
- ◆ 130 ページのセクション 9.6「オンラインヘルプのトラブルシューティング」
- ◆ 131 ページのセクション 9.7「診断レポートの生成および表示」
- ◆ 131 ページのセクション 9.8「ワークロードを削除しています」
- ◆ 132 ページのセクション 9.9「保護後のワークロードのクリーンアップ」
- ◆ 134 ページのセクション 9.10「PlateSpin Forge データベースの縮小」
- ◆ 134 ページのセクション 9.11「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)」

9.1 ワークロードインベントリのトラブルシューティング (Windows)

ワークロードインベントリ中の次の共通の問題に従って、トラブルシューティングが必要な場合があります。

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	<p>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。</p> <p>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。</p> <p>または、domain\DomainAdmin という資格情報の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。</p>
Windows サーバに接続できません ... アクセスが拒否されました	<p>ワークロードを追加しようとする際に、非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。</p> <p>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くださいから 125 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。</p> <ul style="list-style-type: none">◆ 125 ページの「DCOM の接続性のトラブルシューティング」◆ 126 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」

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 ... 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。124 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 Forge とワークロードが同じネットワーク上にあることを確認します。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。 <ul style="list-style-type: none"> ◆ 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	「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。
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。	<ul style="list-style-type: none"> ◆ 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。126 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。PlateSpin Forge 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、126 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。

次のセクションでは、Windows ワークロードのトラブルシューティングについて詳しく説明します。

- ◆ [124 ページのセクション 9.1.1 「接続性テストの実行」](#)
- ◆ [126 ページのセクション 9.1.2 「ウイルス対策ソフトウェアの無効化」](#)
- ◆ [126 ページのセクション 9.1.3 「ファイル / 共有権限およびアクセスの有効化」](#)

9.1.1 接続性テストの実行

- ◆ [125 ページの「ネットワークの接続性テスト」](#)
- ◆ [125 ページの「WMI の接続性テスト」](#)
- ◆ [125 ページの「DCOM の接続性のトラブルシューティング」](#)
- ◆ [126 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コネクティビティのテストを実行して、保護する対象のワークロードと PlateSpin Forge が通信できるかどうかを判断します。

- 1 Forge VM に移動します。

57 ページの「vSphere Client プログラムのダウンロード」を参照してください。

- 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 Forge VM に移動します。

参照先 57 ページの「vSphere Client プログラムのダウンロード」57 ページの「vSphere Client プログラムのダウンロード」。

- 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、PlateSpin Forge 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。

- ◆ PlateSpin Forge 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
- ◆ PlateSpin Forge とワークロードの間の特定のポートを開く ([33 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設定」](#)を参照)。

9.1.2 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 PlateSpin Forge 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。これにより、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、ファイル転送の間のみ無効化され、転送プロセスが終了すると再開されます。これは、ブロックレベルのデータレプリケーション中だけとは限りません。

9.1.3 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 Forge 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、PlateSpin Forge はワークロードの管理共有を使用します。PlateSpin Forge 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が。

共有が有効化されていることを確認したら、Forge VM 内部からそれらにアクセスできることを確認します。

- 1 Forge VM に移動します。
[57 ページの「vSphere Client プログラムのダウンロード」](#)を参照してください。
- 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 入力が求められた場合は、PlateSpin Forge ワークロードインベントリにワークロードを追加するために使用する資格情報を入力します。
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 Forge 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。

9.2 ワークロードインベントリのトラブルシューティング (Linux)

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。	<p>このメッセージにはさまざまな原因があります。</p> <ul style="list-style-type: none"> ◆ 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。 <p>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、33 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設定」を参照してください。</p>
アクセスが拒否されました	<p>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、90 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。</p>

9.3 レプリケーションの準備コマンドで発生した問題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。	<p>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。128 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。</p>

問題またはメッセージ	解決方法
.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。123 ページの「ワークロードインベントリのトラブルシューティング (Windows)」も参照してください。

9.3.1 グループポリシーおよびユーザ権限

PlateSpin Forge とソースワークロードのオペレーティングシステムとの対話形式により、ワークロードの追加に使用される管理者アカウントには、ソースマシンに対する特定のユーザ権限が必要です。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。

9.4 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。
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ため、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。

問題またはメッセージ	解決方法
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、スイッチが自動的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 は、Forge VM の IP アドレスで置き換え)。 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。 44 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 Forge VM 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対して選択されている仮想ネットワークが Forge VM にルートできることを確認します。
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。 <ul style="list-style-type: none"> ◆ 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、Forge VM 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、 128 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。

問題またはメッセージ	解決方法
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。	<p>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。</p> <p>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。</p>

9.5 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) (<https://www.netiq.com/support/kb/doc.php?id=7005495>) を参照してください。

9.6 オンラインヘルプのトラブルシューティング

拡張ブラウザセキュリティ設定を使用した一部のシステム (Windows Server 2008 上の Internet Explorer 8 など) では、目次内の展開アイコンおよび縮小アイコン (+ および -) が機能しない場合があります。この問題を修正するには、ブラウザ内で JavaScript を有効にします。

JavaScript を有効にするには：

- ◆ **Chrome:**

1. Chrome メニューから [設定] を選択し、スクロールして **詳細設定を表示** をクリックします。
2. **Privacy (プライバシー)** で、**コンテンツの設定** をクリックします。
3. **JavaScript (JavaScript)** にスクロールして、**すべてのサイトで JavaScript の実行を許可する** を選択します。
4. **完了** をクリックします。

- ◆ **Firefox:**

1. [Location (ロケーション)] バーに、「about:config」と入力して <Enter> キーを押します。

2. **理解して実行する**をクリックします。
3. **検索**バーに、「javascript.enabled」と入力して <Enter> キーを押します。
4. 検索結果で、javascript.enabled パラメータの値を参照します。この値が false の場合、javascript.enabled を右クリックしてから **Toggle (切り替え)** を選択して、値を true に設定します。

◆ **Internet Explorer:**

1. [ツール] メニューで、**インターネットオプション**を選択します。
2. **セキュリティ**をクリックして、**レベルのカスタマイズ**をクリックします。
3. **Scripting (スクリプティング)>Active scripting (アクティブスクリプティング)**の順にクリックして、**Enable (有効にする)**を選択します。
4. 警告ダイアログボックスでは**はい**をクリックしてから、**OK**をクリックします。
5. **適用 >OK**の順にクリックします。

9.7 診断レポートの生成および表示

PlateSpin Forge 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。

9.8 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 PlateSpin Forge インベントリから削除し、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。
(条件付き) 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、PlateSpin Forge 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を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。

- 2 [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。

9.9 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。

詳細情報については、次のセクションを参照してください。

- ◆ 132 ページのセクション 9.9.1 「Windows ワークロードのクリーンアップ」
- ◆ 133 ページのセクション 9.9.2 「Linux ワークロードのクリーンアップ」

9.9.1 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)	<ol style="list-style-type: none">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。<ul style="list-style-type: none">◆ SteelEye Data Replication for Windows v6 Update2◆ SteelEye DataKeeper For Windows v72. 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	保護されているボリュームごとのルートレベルで、PlateSpinCatalog*.dat という名前のすべてのファイルを削除します。
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。 <ul style="list-style-type: none">◆ 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	<ol style="list-style-type: none">1. コマンドプロンプトを開き、現在のディレクトリを次のディレクトリに変更します。<ul style="list-style-type: none">◆ \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 /uninstall3. platespin* ディレクトリを削除します。

9.9.2 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	<ul style="list-style-type: none">◆ 次のプロセスを終了します。<ul style="list-style-type: none">◆ <code>pkill -9 ofxcontrollerd</code>◆ <code>pkill -9 ofxjobexec</code>◆ 次のように、OFX コントローラ RPM パッケージを削除します。 <code>rpm -e ofxcontrollerd</code>◆ ワークロードのファイルシステムで、<code>/usr/lib/ofx</code> ディレクトリを内容ごと削除します。
ブロックレベルのデータ転送ソフトウェア	<ol style="list-style-type: none">1. ドライバがアクティブであるかどうかを確認します。 <code>lsmod grep blkwatch</code> 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が。 <code>blkwatch_7616 70924 0</code>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。 <code>rmmmod blkwatch_7616</code>3. 次のブートシーケンスからドライバを削除します。 <code>blkconfig -u</code>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。 <code>/lib/modules/[Kernel_Version]/Platespin</code>5. 次のファイルを削除します。 <code>/etc/blkwatch.conf</code>

コンポーネント	削除手順
LVM スナップショット	<p>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、<i>volume_name-PS-snapshot</i> 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。</p> <p>LVM スナップショットを削除するには：</p> <ol style="list-style-type: none"> 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。 <ul style="list-style-type: none"> PlateSpin Forge 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。 <pre># lvdisplay -a</pre> 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。 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。 <pre>lvremove snapshot_name</pre>
ビットマップファイル	<p>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 <i>.blocks_bitmap</i> ファイルを削除します。</p>
ツール	<p>ソースワークロード上で、<i>/sbin</i> から次のファイルを削除します。</p> <ul style="list-style-type: none"> <i>bmaputil</i> <i>blkconfig</i>

9.10 PlateSpin Forge データベースの縮小

PlateSpin Forge 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、Forge 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 \(https://www.netiq.com/support/kb/doc.php?id=7006458\)](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。

9.11 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 で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 の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。
- アンチウイ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次のベストプラクティスを実行することを推奨します。

- ◆ 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 を更新 (Windows Update) していることを確認してください。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イ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。
- ◆ 『*Microsoft Knowledge Article: Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows (KB: 822158)* (<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アンチウイ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。

A Forge 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 Forge 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。このセクションでは、次の情報を紹介します。

- ◆ [137 ページのセクション A.1 「Linux ワークロードの分析」](#)
- ◆ [138 ページのセクション A.2 「PlateSpin Forge の事前コンパイルされた「blkwatch」ドライバ \(Linux\)」](#)

A.1 Linux ワークロードの分析

PlateSpin Forge 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。このセクションでは、次の情報を紹介します。

- ◆ [137 ページのセクション A.1.1 「リリース文字列の決定」](#)
- ◆ [138 ページのセクション A.1.2 「アーキテクチャの決定」](#)

A.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。

A.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。

A.2 PlateSpin Forge の事前コンパイルされた「blkwatch」ドライバ (Linux)

以下は、PlateSpin Forge に blkwatch ドライバが用意されている非デバッグ Linux ディストリビューションのリストです。「[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 Forge 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 (<https://www.netiq.com/support/kb/doc.php?id=7005873>) 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。

- ◆ [138 ページのセクション A.2.1 「リスト項目の構文」](#)
- ◆ [138 ページのセクション A.2.2 「ディストリビューションのリスト」](#)
- ◆ [139 ページのセクション A.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」](#)

A.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-bigsmpt 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-bigsmpt-x86
```

A.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 Forge ユーザガイド](#)』の「[ディストリビューションのリスト](#)」を参照してください。

A.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

CentOS: PlateSpin Forge は、サポートされる Red Hat Enterprise Linux ディストリビューションに基づいている場合、CentOS バージョンのワークロードをサポートします。『[PlateSpin Forge ユーザガイド](#)』の「[ディストリビューションのリスト](#)」で RHEL のエントリを参照してください。

Open Enterprise Server: PlateSpin Forge は、サポートされる SUSE Linux Enterprise Server ディストリビューションに基づいている場合、カーネルバージョン 3.0.27 以上において、OES 2 または OES 11 バージョンのワークロードをサポートします。『[PlateSpin Forge ユーザガイド](#)』の「[ディストリビューションのリスト](#)」で SLES のエントリを参照してください。

Oracle Enterprise Linux: PlateSpin Forge は、サポートされる Red Hat Enterprise Linux ディストリビューションに基づいている場合、Oracle Enterprise Linux バージョンのワークロードをサポートします。ただし、Unbreakable Enterprise Kernel を使用するワークロードを除きます。『[PlateSpin Forge ユーザガイド](#)』の「[ディストリビューションのリスト](#)」で RHEL のエントリを参照してください。

B 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 [NetIQ ダウンロードサイト](#)で、PlateSpin Forge 製品を検索し、[**Submit Query (送信)**] をクリックします。
- 2 [Products (製品)] タブで [PlateSpin Forge 11.2] を選択し、製品固有のダウンロードページに移動して、[**proceed to download (ダウンロードに進む)**] をクリックします。
- 3 ダウンロードページで、**ダウンロードボタン** (VolumeManager.exe 行) をクリックするか、それに相当するダウンロードマネージャリンクを選択します。
- 4 ユーティリティをダウンロードして、それを各クラスタノード上のアクセス可能な場所にコピーします。
- 5 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。

- 6 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。
 - 6a 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。
 - 6b アクティブノード ([ステップ 5](#)) のローカルストレージシリアル番号ノード ([ステップ 6a](#)) のローカルストレージシリアル番号と比較します。
 - 6c (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 <Volumeld> <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

- 6d 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。
 - 6e クラスタの各ノードに対してステップ 6a からステップ 6d を繰り返します。
- 7 (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。

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

PlateSpin Forge 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。

- [143 ページのセクション C.1「環境設定パラメータによるインタフェースのブランディングの変更」](#)
- [146 ページのセクション C.2「Windows レジストリでの製品名ブランディングの変更」](#)

C.1 環境設定パラメータによるインタフェースのブランディングの変更

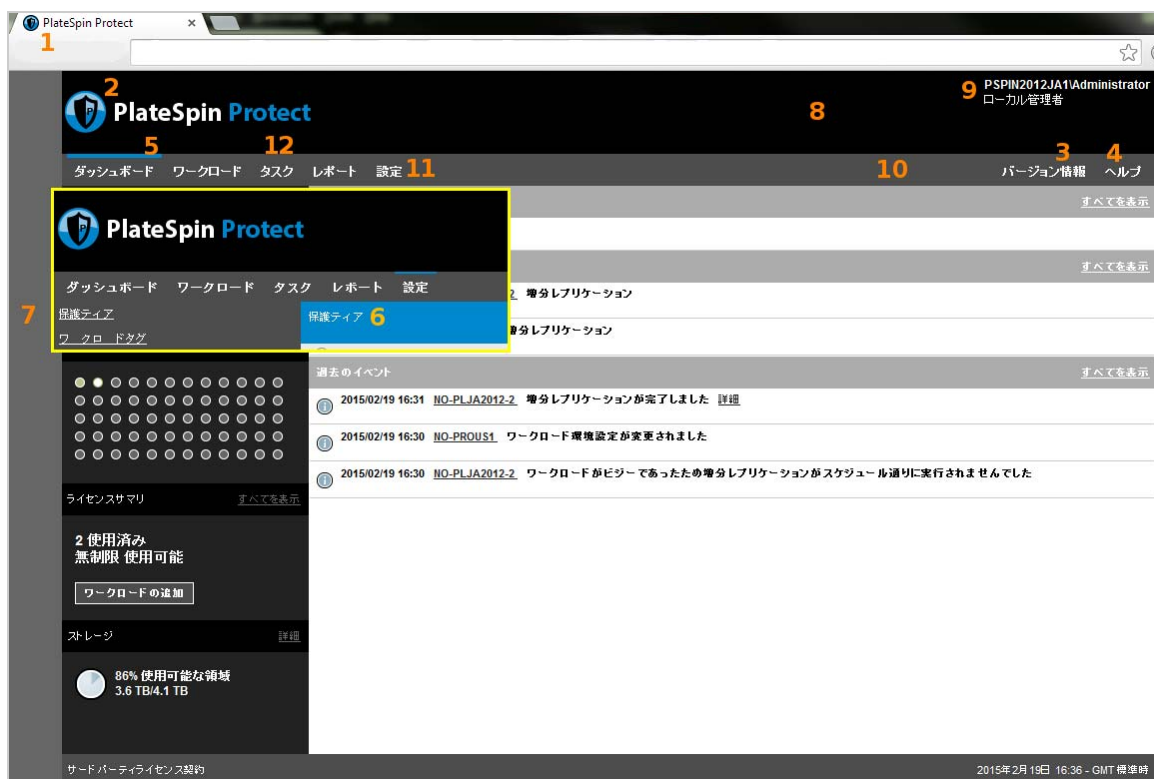
[PlateSpin Server 動作の他の側面](#)と同様に、Web インタフェースの外観は、Forge VM の環境設定 Web ページ (https://Your_PlateSpin_Server/platespinconfiguration/) で設定されている環境設定パラメータを使用して制御します。これらのパラメータを使用すると、Web インタフェースを、ユーザ組織固有の「ルックアンドフィール」にすることができます。この項では、カスタムブランディングを設定する場合に使用できる情報について説明します。

次の手順を使用して、任意の環境設定パラメータを変更し、適用してください。

- 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。
詳細については、[図 C-1](#) を参照して、それぞれの変更可能要素について、設定名、説明、およびデフォルト値を確認してください。
- 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。

Web インタフェースには、各ページを通じて共通の「ルックアンドフィール」要素があります。図 C-1 の PlateSpin Forge 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。

図 C-1 PlateSpin Forge Web インタフェースとラベル付きの設定可能要素 (挿入画像あり)



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)。

ID	設定名と説明	デフォルト値
1	<p>WebUIFaviconUrl</p> <p>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。</p> <ul style="list-style-type: none"> 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。 <p>例 : <code>https://myserver.example.com/dir1/dir2/icons/mycompany_favicon.ico</code></p> <ul style="list-style-type: none"> 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。 <p>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 <code>mycompany\images\icons</code> というパスを作成した場合、次のように指定します。</p> <p><code>~/mycompany/images/icons/mycompany_favicon.ico</code></p> <p>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、<code>C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\mycompany\images\icons\mycompany_favicon.ico</code> になります。</p>	<p>~/doc/en/favicon.ico ¹</p>
2	<p>WebUILogoUrl</p> <p>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。</p> <ul style="list-style-type: none"> 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。 <p>例 : <code>https://myserver.example.com/dir1/dir2/logos/mycompany_logo.png</code></p> <ul style="list-style-type: none"> 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。 <p>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 <code>mycompany\images\logos</code> というパスを作成した場合、次のように指定します。</p> <p><code>~/mycompany/images/logos/mycompany_logo.png</code></p> <p>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、<code>C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\mycompany\images\logos\mycompany_logo.png</code> になります。</p>	<p>~/Resources/protectLogo.png ²</p>
3	<p>WebUIShowAboutTab</p> <p>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。</p>	<p>True</p>
4	<p>WebUIShowHelpTab</p> <p>Help (ヘルプ) タブの表示 (True) / 非表示 (False) をトグルします。</p>	<p>True</p>

ID	設定名と説明	デフォルト値
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。

C.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\ForgeServer\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\SOFTWAREWow6432Node\PlateSpin\Forge

- 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。

D 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 Forge 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は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レビューとして提供されています。

- ◆ [149 ページのセクション D.1 「API の概要」](#)
- ◆ [149 ページのセクション D.2 「PlateSpin Protect Server API のマニュアル」](#)
- ◆ [150 ページのセクション D.3 「サンプルとその他の参照情報」](#)

D.1 API の概要

PlateSpin Forge では、REST ベースの API テクノジ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

D.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、Forge VM で次の場所にアクセスしてください。

`https://<hostname | IP_address>/protectionservices`

<hostname | IP_address> の部分を、Forge VM のホスト名または IP アドレスで置き換えます。SSL が有効でない場合は、URI に http を使用します。

PlateSpin Protect Server API

Version 11.2.0.81

Documentation

Getting started

- [Getting started with API](#)
- [Security and authentication](#)
- [Developer Guidelines](#)
- [Troubleshooting](#)
- [FAQ](#)

How to

- [Steps to protect workload](#)
- [Working with workload](#)
- [Working with container](#)
- [Working with security groups](#)
- [Working with protection tiers](#)
- [Adding multiple workloads and containers](#)
- [Limitations of the API](#)
- [Samples](#)
- [Glossary](#)

REST Resources (auto-generated)

- [Containers](#)
- [Workloads](#)
- [Configuration](#)
- [Operations](#)
- [Protection Tiers](#)
- [Security Groups](#)

Resource representations

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

D.3 サンプルとその他の参照情報

Forge 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。Forge VM で、次の場所にあるサンプルを参照してください。

<https://localhost/protection/services/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。

用語集

管理コンピュータ. アップグレードを実行するためにアプライアンスホストの外部で使用する Windows マシン。Forge ハードウェアアプライアンスの構築および設定手順では、Forge アプライアンスホストとして使用する Dell ハードウェアとの直接接続が必要になるため、このプロセスにはラップトップを使用することをお勧めします。

アプライアンス管理ソフトウェア. インストールや設定 (ホスト / VM の IP アドレス、ホスト名、ユーザパスワードの設定など) を行うために、端末コンソール (getty) またはブラウザベースの独自インタフェース (Forge Appliance Configuration Console (*Forge ACC*)) を使用してアプライアンスに直接接続するソフトウェア。

アプライアンスバージョン. Forge ESX ホストおよび Forge アプライアンス VM のネットワーク設定の管理に使用する **アプライアンス管理ソフトウェア** のバージョン。アプライアンス (バージョン) 1 では getty インタフェースが、アプライアンス (バージョン) 2 では Django Web フレームワークと ACC インタフェースが使用されます。アプライアンスバージョンの更新のきっかけとなるのは、主に基盤となる VMware ESX バージョンへの変更です。

Forge ユニットのアプライアンスバージョンは、以下のいずれか 1 つの方法で判別できます。

- Forge Web インタフェース : ACC の [ヘルプ] > [バージョン情報] ページでアプライアンスバージョン番号を参照してください。これは Forge を再設定する場合にのみ実行できます。
- ローカル設定のインタフェースタイプ : モニタをアプライアンスに接続して、電源を入れます。Forge コンソールのブルースクリーンが表示されている場合は、アプライアンスバージョンは 1 です。ESX 設定画面が表示されている場合は、アプライアンスバージョンは 2 です。
- リモート設定インタフェース : Web ブラウザと Forge ユニットの IP アドレス (`http://<forge_esx_server>:1000`) を使用し、Forge Appliance Configuration Console (ACC) の起動を試してみます。接続できる場合、アプライアンスバージョンは 2 です。

実際の目標復旧時点 (実際の RPO). 「**実際の復旧時点**」を参照してください。

実際の目標復旧時間 (実際の RTO). 「**実際の復旧時間**」を参照してください。

実際のテスト時間目標 (実際の TTO). 「**実際のテスト時間**」を参照してください。

アプライアンスホスト. **コンテナ** を参照してください。

バックアップ. 既存のデータベースデータ (既存のワークロードやコントラクトを含む) をエクスポートするプロセス。このプロセスでは、Forge アプライアンスホストのローカルデータストアに常駐する VM もバックアップされます。

コンテナ. フェールオーバーワークロードを含む VM ホスト (保護ワークロードのブート可能な仮想レプリカ) のことです。

コントラクトデータ. 保護コントラクトのエクスポートデータ。アップグレードユーティリティでは、このデータが zip ファイルに保存されます。

「**保護コントラクト**」も参照してください。

イベント. ワークロード保護ライフサイクルを通して重要な手順に関する情報を含む PlateSpin Server メッセージのことです。

failback (フェールバック). PlateSpin Forge 内の一時的なフェールオーバーワークロードが必要でなくなった場合に、障害が発生したワークロードのビジネス機能を元々の環境に復元する操作のことです。

フェールオーバー. 障害が発生したワークロードのビジネス機能が PlateSpin Forge の VM コンテナ内のフェールオーバーワークロードによって引き継がれます。

フェールオーバーワークロード. 保護ワークロードのブート可能な仮想レプリカです。

Forge アプライアンス. Microsoft Windows OS が動作し、Forge ソフトウェアがインストールされた仮想マシンが含まれる Forge アプライアンスホスト。

Forge インストール/アップグレード実行可能ファイル. Forge アプライアンスソフトウェアをアップグレードする実行可能ファイル。この実行可能ファイル(「アップグレードユーティリティ」とも呼ばれる)は、*Forge Upgrade Kit*に含まれています。

Forge ソフトウェア. 仮想化技術を使用して特定の仮想ワークロード (ESX VM のオペレーティングシステム、ミドルウェア、およびデータ) を保護するために開発された PlateSpin ソフトウェア。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。

完全. 1. (名詞) 保護されたワークロードとその「空白」レプリカ (フェールオーバー VM) 間で、またはフェールオーバーワークロードとその元となる仮想インフラまたは物理的インフラ間で、スケジュールまたは手動により個別に転送することです。

2. (形容詞) 保護されたワークロードの初期レプリカがそのすべてのデータに基づいて作成される、「[レプリケーション \(1\)](#)」の範囲を表します。

増分. 1. (名詞) 保護されたワークロードとそのレプリカ (フェールオーバーワークロード) 間で、スケジュールまたは手動により個別に差分を転送することです。

2. (形容詞) ワークロードの初期レプリカが (ワークロードとそれと対をなす準備されたレプリカに基づいて) 差分的に作成される、「[レプリケーション \(1\)](#)」の範囲を表します。

管理 VM. PlateSpin Forge ソフトウェアを含む管理仮想マシンのことです。

出力ディレクトリ. (出力フォルダとも呼ばれる)。管理コンピュータの重要なバックアップデータが保存されるネットワークロケーション。たとえば、D:\forge_backup\out です。

フェールオーバーの準備. 完全な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する PlateSpin Forge の操作のことです。

保護ティア. カスタマイズ可能なワークロード保護パラメータのコレクションで、レプリケーションの頻度と、ワークロードに障害が発生したとシステムが判断する基準を定義します。

保護契約. ワークロードの保護 (インベントリの追加、初期および進行中のレプリケーション、フェールオーバー、フェールバック、および保護) のライフサイクル完了に関する現在有効になっている設定の集まりです。

再構築. Forge Dell ハードウェア、Forge ESX ホスト、および Windows Server オペレーティングシステム上で動作する Forge アプライアンスを設定するプロセス。

復旧ポイント. 複製されたワークロードを以前の状態に復旧できる、特定の時点のスナップショットです。

レプリケーション

1. **初期のレプリケーション**、ワークロードの最初の基本コピーの作成。「完全レプリケーション」(「[完全 \(2\)](#)」を参照)、または「増分レプリケーション」(「[増分 \(2\)](#)」を参照)として実行できます。
2. 保護ワークロードからコンテナ内のそのレプリカに変更されたデータを転送する操作です。

レプリケーションスケジュール、レプリケーションの頻度と範囲を制御するために設定されるスケジュールです。

再保護、フェールオーバーとフェールバックの操作に続いてワークロードの保護契約を再確立する、PlateSpin Forge のコマンドです。

復元、既存のデータベースデータ (ワークロードやコントラクトを含む) を、[バックアップ](#)前の状態にしてインポートするプロセス。このプロセスでは、以前に Forge アプライアンスホストに常駐していたすべてのローカル VM も復元されます。

実際の復旧時点 (RPA)、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。

目標復旧時点 (RPO)、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間の設定可能な間隔によって定義される、許容できるデータ紛失のことです。つまり、大規模な IT 停止の発生時に許容できるデータ紛失量のことです。RPO は、PlateSpin Forge 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。

実際の復旧時間 (RTA)、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タイムを示す尺度のことです。

目標復旧時間 (RTO)、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許容ダウンタイムを示す尺度のことです。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。

ソース、PlateSpin Forge の操作の開始点であるワークロードまたはそのインフラストラクチャのことです。たとえば、ワークロードの初期保護では、ソースとは運用ワークロードのことを指します。フェールバック操作では、コンテナ内のフェールオーバーワークロードのことを指します。

[ターゲット](#) も参照してください。

ターゲット、PlateSpin Forge コマンドの結果であるワークロードまたはそのインフラストラクチャのことです。たとえば、ワークロードの初期保護では、ターゲットとはコンテナ内のフェールオーバーワークロードのことを指します。フェールバック操作では、運用ワークロードの元のインフラストラクチャか、PlateSpin Forge によってインベントリされた、サポートされる任意のコンテナのいずれかです。

[ソース](#) も参照してください。

フェールオーバーのテスト、フェールオーバー機能をテストし、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隔離された環境でフェールオーバーワークロードを起動する PlateSpin Forge の操作のことです。

実際のテスト時間 (TTA)、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。

目標テスト時間 (TTO). 障害復旧計画をテストできる容易さの尺度のことです。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て、ベンチマークデータを生成できます。

作業ディレクトリ . Forge Upgrade Kit のコピー先であるネットワークロケーション。たとえば、D:\forge_backup\11.0_kit です。

ワークロード . データストアに含まれる保護の基本オブジェクトのことです。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のことです。