

PlateSpin Forge[®] 4.0

ユーザガイド

2014年3月21日



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。また、モジュールを接続、複製、または使用することで、これらの条項に従うことになります。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頂く必要があります。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。

© 2014 NetIQ Corporation and its affiliates. 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。

本製品が FIPS 準拠を主張する場合、以下に示す Microsoft 暗号化コンポーネントを 1 つ以上使用することで準拠しています。以下のコンポーネントは Microsoft によって認定され、CMVP によって FIPS 認定を取得しています。

893 Windows Vista Enhanced Cryptographic Provider (RSAENH)

894 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

989 Windows XP Enhanced Cryptographic Provider (RSAENH)

990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

997 Microsoft Windows XP Kernel Mode Cryptographic Module (FIPS.SYS)

1000 Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)

1001 Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)

1002 Windows Vista Enhanced Cryptographic Provider (RSAENH)

1003 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1006 Windows Server 2008 Code Integrity (ci.dll)

1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)

1008 Microsoft Windows Server 2008

1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1010 Windows Server 2008 Enhanced Cryptographic Provider

1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)

また本製品は、以下に列挙する 1 つ以上の **Open SSL** 暗号化コンポーネントを使用することにより、**FIPS** に準拠している場合があります。これらのコンポーネントは、**Open Source Software Institute** によって認証され、記述どおり **FIPS** 認定を取得しています。

918 - OpenSSL FIPS Object Module v1.1.2 - 02/29/2008 140-2 L1

1051 - OpenSSL FIPS Object Module v 1.2 - 11/17/2008 140-2 L1

1111 - OpenSSL FIPS Runtime Module v 1.2 - 4/03/2009 140-2 L1

メモ : 本製品で使われている **Windows FIPS** アルゴリズムは、**FIPS** モードビットの設定時にのみテストが実施されたものである可能性があります。本製品のリリース時点ではモジュールの証明書は有効ですが、ユーザの責任において、現在のモジュールの状態を確認してください。

エンドユーザ使用許諾契約に明示されている場合を除いて、ここに記載されているすべての内容に対して一切の保証は行いません。明示または黙示のすべての条件、表明、および特定目的への適合性に対する黙示的な保証または条件を含む一切の保証は、適用される法律が許す範囲で除外され、**NetIQ**、供給者、および使用許諾者はそれらについて一切の保証を行いません。

ライセンスの許諾

PlateSpin Forge 4.0 のライセンスを旧バージョンの PlateSpin Forge 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) (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

NetIQ 社について	9
このガイドについて	11
1 製品の概要	13
1.1 PlateSpin Forge について	13
1.2 サポートされる構成	13
1.2.1 サポートされる Windows のワークロード	14
1.2.2 サポートされる Linux のワークロード	15
1.2.3 サポートされる VM コンテナ	15
1.3 セキュリティとプライバシー	16
1.3.1 送信中のワークロードデータのセキュリティ	16
1.3.2 資格情報のセキュリティ	16
1.3.3 ユーザ権限および認証	16
1.4 パフォーマンス	16
1.4.1 製品パフォーマンスの特性	16
1.4.2 データ圧縮	17
1.4.3 帯域幅制限	17
1.4.4 RPO、RTO、および TTO の仕様	18
2 PlateSpin Forge アプリケーション環境設定	19
2.1 製品ライセンス	19
2.1.1 ライセンスアクティベーションコードの取得	19
2.1.2 オンラインライセンスのアクティベーション	19
2.1.3 オフラインライセンスのアクティベーション	20
2.2 ユーザ権限および認証の設定	20
2.2.1 PlateSpin Forge のユーザ権限および認証について	21
2.2.2 PlateSpin Forge のアクセスおよび権限の管理	22
2.2.3 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	24
2.3 保護ネットワークにわたるアクセスおよび通信の要件	25
2.3.1 ワークロードに関するアクセスおよび通信の要件	25
2.3.2 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	27
2.3.3 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	28
2.4 PlateSpin Forge のデフォルトオプションの設定	28
2.4.1 イベントおよびレポートの自動電子メール通知のセットアップ	28
2.4.2 PlateSpin Forge の国際バージョンの言語設定	31
2.4.3 XML 環境設定パラメータを通じた PlateSpin Server の動作の構成	32
3 アプライアンスのセットアップとメンテナンス	35
3.1 アプライアンスのネットワーキングの設定	35
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	35
3.2 PlateSpin Forge の移動およびその IP アドレスの再割り当て	36
3.2.1 Forge アプライアンスバージョン 2 の移設手順	36
3.2.2 Forge アプライアンスバージョン 1 の移設手順	40
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	41
3.3.1 Forge での SAN ストレージの使用	41
3.3.2 Forge への SAN LUN の追加	42
3.4 PlateSpin Forge アプライアンスの保守	43

3.4.1	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	43
3.5	PlateSpin Forge のアップグレード	47
3.5.1	アップグレードを開始する前に	47
3.5.2	アップグレードタスクのサマリ	48
3.5.3	Forge アップグレード手順	48
3.6	工場出荷時のデフォルトへの Forge のリセット	49
4	業務の常時稼働	53
4.1	PlateSpin Forge Web インタフェースの起動	53
4.2	PlateSpin Protect Web インタフェースの要素	54
4.2.1	ナビゲーションバー	55
4.2.2	ビジュアルサマリパネル	55
4.2.3	タスクおよびイベントパネル	56
4.3	ワークロードおよびワークロードコマンド	56
4.3.1	ワークロードの保護と回復のコマンド	57
4.4	PlateSpin Protect および PlateSpin Forge の複数インスタンスの管理	58
4.4.1	PlateSpin Forge 管理コンソールの使用	58
4.4.2	PlateSpin Forge 管理コンソールについて	58
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	59
4.4.4	管理コンソールでのカードの管理	60
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	61
5	ワークロードの保護	63
5.1	ワークロードの保護と回復の基本ワークフロー	63
5.2	保護のためのワークロードの追加	64
5.3	保護詳細の設定およびレプリケーションの準備	66
5.3.1	ワークロード保護の詳細	66
5.4	ワークロード保護の開始	68
5.5	コマンドの中止	69
5.6	フェールオーバー	70
5.6.1	オフラインワークロードの検出	70
5.6.2	フェールオーバーの実行	71
5.6.3	フェールオーバーのテスト機能の使用	71
5.7	フェールバック	72
5.7.1	VM プラットフォームへの自動化されたフェールバック	72
5.7.2	物理マシンへの半自動化されたフェールバック	75
5.7.3	仮想マシンへの半自動化されたフェールバック	76
5.8	ワークロードの再保護	77
6	ワークロード保護の要点	79
6.1	ワークロードライセンスの消費	79
6.2	ワークロードの資格情報向けのガイドライン	80
6.3	データ転送	80
6.3.1	転送方法	80
6.3.2	データの暗号化	82
6.4	保護ティア	82
6.5	復旧ポイント	83
6.6	初期レプリケーション方法 (フルおよび差分)	83
6.7	サービスおよびデーモンの制御	85
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)	85
6.9	ボリューム	86
6.10	ネットワーク	88

6.11	物理マシンへのフェールバック	88
6.11.1	PlateSpin ISO ブートイメージのダウンロード	88
6.11.2	ISO ブートイメージへのデバイスドライバの追加	88
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	89
6.12	高度なワークロード保護に関するトピック	90
6.12.1	Windows クラスターの保護	90
6.12.2	Xen-on-SLES 上で並行仮想化された VM への Linux フェールバック	91
6.12.3	PlateSpin Forge の Web サービス API 経由でのワークロード保護機能の使用	93
7	物理マシンを操作するための補助ツール	95
7.1	PlateSpin Analyzer を使用したデバイスドライバの分析 (Windows)	95
7.2	デバイスドライバの管理	96
7.2.1	Windows システム用のデバイスドライバのパッケージ化	97
7.2.2	Linux システム用のデバイスドライバのパッケージ化	97
7.2.3	PlateSpin Forge 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	98
7.2.4	プラグアンドプレイ (PnP) ID トランスレータ機能の使用	100
8	トラブルシューティング	107
8.1	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)	107
8.1.1	接続性テストの実行	108
8.1.2	ウイルス対策ソフトウェアの無効化	110
8.1.3	ファイル/共有権限およびアクセスの有効化	110
8.2	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)	111
8.3	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)	111
8.3.1	グループポリシーおよびユーザ権限	112
8.4	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	112
8.5	診断レポートの生成および表示	114
8.6	ワークロードを削除しています	115
8.7	保護後のワークロードのクリーンアップ	115
8.7.1	Windows ワークロードのクリーンアップ	115
8.7.2	Linux ワークロードのクリーンアップ	116
8.8	PlateSpin Forge データベースの縮小	118
	用語集	119

NetIQ 社について

Attachmate の 1 事業である NetIQ は、システムおよびセキュリティ管理におけるグローバルリーダーです。60 を超える国々で 12,000 を超えるお客様を擁する NetIQ ソリューションは、技術投資を最大化し、IT プロセスを改良してコスト削減を測定可能にします。弊社のポートフォリオには、受賞歴のある IT プロセス自動化、システム管理、セキュリティ管理、設定監査および制御、エンタープライズアドミニストレーション、ユニファイドコミュニケーション管理向けの管理製品が含まれます。詳細については、www.netiq.com を参照してください。

セールスサポートへのお問い合わせ

商品、価格、機能についてのご質問は、ローカルパートナーへご連絡ください。ローカルパートナーとの連絡が取れない場合、セールスサポートチームへご連絡ください。

各国共通:	www.netiq.com/about_netiq/officelocations.asp
米国およびカナダ:	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@platespin.com
Web サイト:	www.netiq.com/support

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。改善のためのご提案は、www.netiq.com/documentation に掲載されている本マニュアルの HTML 版で、各ページの下にある [コメントを追加] 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 Qmunity 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 Qmunity 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。

このガイドについて

このガイドでは、PlateSpin Forge の使用について説明します。

対象読者

このガイドは、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。

フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインマニュアルの各ページの上部と下部にある [ユーザコメント] 機能を使用してください。

その他のマニュアル

このガイドは、PlateSpin Forge マニュアルセットの一部です。

このリリースをサポートする出版物の完全なリストについては、[PlateSpin Forge 4 オンラインマニュアルの Web サイト \(http://www.netiq.com/documentation/platespin_forge_4\)](http://www.netiq.com/documentation/platespin_forge_4) を参照してください。

マニュアルの更新

このガイドの最新バージョンは、[PlateSpin Forge 4 オンラインマニュアルの Web サイト \(https://www.netiq.com/documentation/platespin_forge_4/\)](https://www.netiq.com/documentation/platespin_forge_4/) から入手できます。

その他の資料

Web 上にある次の資料もご利用ください。

- [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、PlateSpin 製品の情報やサービスを提供する Web サイトです。

技術サポート

[技術サポートガイド \(https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and\)](https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and) にアクセスすると、NetIQ 技術サポートのポリシーおよび手順についてさらに詳しく学ぶことができます。

次のリソースは、PlateSpin Forge に固有のサポートが必要な場合に使用します。

- ◆ 電話 (カナダおよび米国): 1-800-858-4000
- ◆ 電話 (米国外): 1-801-861-4000
- ◆ 電子メール : support@platespin.com
- ◆ 製品固有の情報 : [PlateSpin Forge サポート \(https://www.netiq.com/support/kb/product.php?id=SG_XPLATESPINFORGE_1_2\)](https://www.netiq.com/support/kb/product.php?id=SG_XPLATESPINFORGE_1_2)

1 製品の概要

このセクションでは、次の情報を紹介します。

- ◆ 13 ページのセクション 1.1 「PlateSpin Forge について」
- ◆ 13 ページのセクション 1.2 「サポートされる構成」
- ◆ 16 ページのセクション 1.3 「セキュリティとプライバシー」
- ◆ 16 ページのセクション 1.4 「パフォーマンス」

1.1 PlateSpin Forge について

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 復旧環境で稼動し、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（モデルに応じて 10 ～ 25）を同時保護
- ◆ 運用環境に影響を与えずにフェールオーバーワークロードをテスト
- ◆ 元のインフラまたは完全に新しいインフラ（物理または仮想）にフェールオーバーワークロードをフェールバック
- ◆ SAN などの既存の外部ストレージソリューションの利用

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 3.5 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。

1.2 サポートされる構成

- ◆ 14 ページのセクション 1.2.1 「サポートされる Windows のワークロード」
- ◆ 15 ページのセクション 1.2.2 「サポートされる Linux のワークロード」
- ◆ 15 ページのセクション 1.2.3 「サポートされる VM コンテナ」

1.2.1 サポートされる Windows のワークロード

PlateSpin Forge では、Windows ベースのほとんどのワークロードがサポートされています。

ファイルレベルのレプリケーションとブロックレベルのレプリケーションの両方がサポートされていますが、いくつかの制約があります。詳細については、[80 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 2008 R2 (64 ビット) Windows Server 2008 (64 ビット)	ドメインコントローラ (DC) および Small Business Server (SBS) エディションを含む
Windows Server 2003 最新 SP (64 ビット) Windows Server 2003 最新 SP (32 ビット) Windows Server 2003 R2 (64 ビット) Windows Server 2003 R2 (32 ビット)	ドメインコントローラ (DC) および Small Business Server (SBS) エディションを含む
Windows Server 2000 SP4 (32 ビット)	
ワークステーションクラスのワークロード	
Windows 7	Professional、Enterprise、および Ultimate Edition のみ
Windows Vista	
Windows XP	

サポートされる **Windows のクラス** サポートされる特別なクラス構成については [90 ページの「Windows クラスの保護」](#)を参照

次に、UEFI システムと BIOS システムが保護されており、かつ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。

1.2.2 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。

レプリケーションはブロックレベルで実行されます。このために PlateSpin ソフトウェアでは、特定の Linux ディストリビューションを保護できるように、blkwatch モジュールがコンパイルされている必要があります。

サポートされる Linux のバージョンによっては、PlateSpin blkwatch モジュールを、使用している特定のカーネル用にコンパイルする必要があります。これらのワークロードは明示的に呼び出されます。

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 サーバクラスのワークロード	
Red Hat Enterprise Linux (RHEL) 4.0、5.0 ~ 5.5、6.0 ~ 6.2	
RHEL 5.6 ~ 5.8、6.3	これらのワークロードのインベントリを実行する前に、PlateSpin blkwatch モジュールをコンパイルする必要があります。 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。
SUSE Linux Enterprise Server (SLES) 9、10、11 (SP1、SP2、SP3)	注：SLES -11 SP 2 のカーネルバージョン 3.0.51-0.7.9-pae 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 3.0.51-0.7.9-pae 以降にアップグレードしてください。
<ul style="list-style-type: none">◆ Novell Open Enterprise Server (OES) 11 SP1◆ OES 2 (SP2、SP3)	
Oracle Enterprise Linux (OEL)	<ul style="list-style-type: none">◆ RHEL を実行するワークロードと同じレベルのサポート。◆ Unbreakable Enterprise Kernel を使用するワークロードはサポートされません。

サポートされる Linux ファイルシステム : EXT2、EXT3、EXT4、REISERFS、および NSS (OES 2 ワークロード)。

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。

1.2.3 サポートされる VM コンテナ

PlateSpin Forge は、VMware ESX 4.1(製品の Hypervisor コンポーネントとしての役割を果たすアプリケーションホスト) とともに出荷されます。

1.3 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。

- ◆ [16 ページのセクション 1.3.1 「送信中のワークロードデータのセキュリティ」](#)
- ◆ [16 ページのセクション 1.3.2 「資格情報のセキュリティ」](#)
- ◆ [16 ページのセクション 1.3.3 「ユーザ権限および認証」](#)

1.3.1 送信中のワークロードデータのセキュリティ

ワークロードデータの転送をより安全にするために、データを暗号化するようにワークロード保護を設定できます。暗号化が有効になると、ネットワーク上で複製されたデータは AES (Advanced Encryption Standard) を使用して暗号化されます。

ワークロードごとに暗号化を有効または無効にすることができます。[66 ページの「ワークロード保護の詳細」](#)を参照してください。

1.3.2 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。

1.3.3 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。[20 ページのセクション 2.2 「ユーザ権限および認証の設定」](#)を参照してください。

1.4 パフォーマンス

- ◆ [16 ページのセクション 1.4.1 「製品パフォーマンスの特性」](#)
- ◆ [17 ページのセクション 1.4.2 「データ圧縮」](#)
- ◆ [17 ページのセクション 1.4.3 「帯域幅制限」](#)
- ◆ [18 ページのセクション 1.4.4 「RPO、RTO、および TTO の仕様」](#)

1.4.1 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
- ◆ ネットワークの帯域幅、構成、および条件の詳細

- ◆ 保護されたワークロードの数
- ◆ 保護されていないボリュームの数
- ◆ 保護されていないボリュームのサイズ
- ◆ ソースワークロードのボリューム上のファイル密度 (容量の単位ごとのファイルの数)
- ◆ ソースの I/O レベル (ワークロードがどの程度取り込んでいるか)
- ◆ 同時使用レプリケーションの数
- ◆ データ暗号化が有効か無効か
- ◆ データ圧縮が有効か無効か

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

1.4.2 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。82 ページの「保護ティア」を参照してください。

1.4.3 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。82 ページの「保護ティア」を参照してください。

1.4.4 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。[70 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、[71 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、[61 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 PlateSpin Forge アプリケーション環境設定

このセクションでは、次の情報を紹介します。

- ◆ 19 ページのセクション 2.1 「製品ライセンス」
- ◆ 20 ページのセクション 2.2 「ユーザ権限および認証の設定」
- ◆ 25 ページのセクション 2.3 「保護ネットワークにわたるアクセスおよび通信の要件」
- ◆ 28 ページのセクション 2.4 「PlateSpin Forge のデフォルトオプションの設定」

2.1 製品ライセンス

この項では、PlateSpin Forge ソフトウェアの有効化について説明します。

- ◆ 19 ページのセクション 2.1.1 「ライセンスアクティベーションコードの取得」
- ◆ 19 ページのセクション 2.1.2 「オンラインライセンスのアクティベーション」
- ◆ 20 ページのセクション 2.1.3 「オフラインライセンスのアクティベーション」

2.1.1 ライセンスアクティベーションコードの取得

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、Novell Customer Center の Web サイト (<http://www.novell.com/customercenter/>) を通じて要求します。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。

PlateSpin Forge に最初にログインすると、ブラウザが自動的に [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されます。製品ライセンスを有効にするには、[オンラインライセンスのアクティベーション](#)と[オフラインライセンスのアクティベーション](#)の2つのオプションがあります。

2.1.2 オンライン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。

- 1 PlateSpin Forge Web インタフェースで、[設定] > [ライセンス] > [ライセンスの追加] の順にクリックします。[ライセンスのアクティベーション] ページが表示されます。

- 2 [オンラインアクティベーション] を選択して、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。

2.1.3 オフライン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マシンを使用してインターネット経由でライセンスキーを取得します。

注: ライセンスキーを取得するには、Novell アカウントを持っている必要があります。PlateSpin の既存のお客様であり、Novell アカウントを持っていない場合は、最初にアカウントを作成する必要があります。Novell アカウントのユーザ名の入力には、既存の PlateSpin ユーザ名を使用してください (PlateSpin で登録されている有効な電子メールアドレス)。

- 1 [設定] > [ライセンス] の順にクリックし、[ライセンスの追加] をクリックします。[ライセンスアクティベーション] ページが表示されます。
- 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。Novell のユーザ名を使用してログインします。
- 4 該当するフィールドに必要な事項を入力します。
 - ◆ 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 [有効化] をクリックします。

システムによってライセンスキーファイルが生成され、これを保存するようにメッセージが表示されます。

- 6 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運用ホストに転送し、これを使用して運用を有効にします。

2.2 ユーザ権限および認証の設定

- ◆ 21 ページのセクション 2.2.1 「PlateSpin Forge のユーザ権限および認証について」
- ◆ 22 ページのセクション 2.2.2 「PlateSpin Forge のアクセスおよび権限の管理」
- ◆ 24 ページのセクション 2.2.3 「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」

2.2.1 PlateSpin Forge のユーザ権限および認証について

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

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
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設定には、次の 2 つのタスクが含まれます。

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する (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する (24 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)。

2.2.2 PlateSpin Forge のアクセスおよび権限の管理

- ◆ 22 ページの「PlateSpin Forge サーバ管理インタフェースへのアクセス」
- ◆ 23 ページの「PlateSpin Forge ユーザの追加」
- ◆ 23 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」
- ◆ 23 ページの「PlateSpin Forge 管理者パスワードの変更」

PlateSpin Forge サーバ管理インタフェースへのアクセス

Microsoft Windows Server 管理の Web ユーザインタフェースにアクセスするには：

- 1 Web ブラウザを開いて、https://IP_address:8098 にアクセスします。

IP_address の部分を、Forge VM の IP アドレスで置き換えます。

ブラウザがサーバに接続され、デフォルトの [ようこそ] ページが表示されます。

図 2-1 Microsoft Windows Server 管理の Web ユーザインタフェース



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、[23 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。

- 1 Forge VM のサーバ管理 Web ユーザインタフェースにアクセスします。
[22 ページの「PlateSpin Forge サーバ管理インタフェースへのアクセス」](#)を参照してください。
- 2 `[ユーザ]` > `[Local Users (ローカルユーザ)]` の順にクリックします。
`[Local Users on Server (サーバ上のローカルユーザ)]` ページが開きます。
- 3 `[タスク]` の下で、`[新規]` をクリックし、ユーザ名、パスワード、およびその他のオプション情報を入力します。
- 4 `[OK]` をクリックします。
`[Local Users on Server (サーバ上のローカルユーザ)]` ページが再ロードされます。

これで、新しく作成されたユーザにワークロード保護の役割を割り当てることができます。[23 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。[21 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。

- 1 Forge VM のサーバ管理 Web ユーザインタフェースにアクセスします。[22 ページの「PlateSpin Forge サーバ管理インタフェースへのアクセス」](#)を参照してください。
- 2 `[ユーザ]` > `[Local Groups (ローカルグループ)]` の順にクリックします。
`[Local Groups on Server (サーバ上のローカルグループ)]` ページが開きます。
- 3 グループのリストから必要なワークロード保護グループを選択し、`[タスク]` の下の `[プロパティ]` をクリックします。
対応するグループプロパティページが開きます。
- 4 `[メンバー]` をクリックし、リストから必要なユーザを選択して `[追加]` をクリックします。
選択されたユーザが `[メンバー]` リストに追加されます。
- 5 `[OK]` をクリックします。

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。[24 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。

PlateSpin Forge 管理者パスワードの変更

Forge VM の管理者アカウントのパスワードを変更するには：

- 1 Forge VM のサーバ管理 Web ユーザインタフェースにアクセスします。[22 ページの「PlateSpin Forge サーバ管理インタフェースへのアクセス」](#)を参照してください。
- 2 `[Set Administrator Password (管理者パスワードの設定)]` をクリックして新しいパスワードを入力し、それを確認し、`[OK]` をクリックします。

2.2.3 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。23 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。

このグループへのアクセスを許可するユーザを選択:

許可	名前	役割
<input checked="" type="checkbox"/>	N161-2008FR1\Operator1	ワークロード保護オペレータ

OK キャンセル

- 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 checked="" type="checkbox"/>	WIN7-PC	BCM Operators
<input type="checkbox"/>	10.99.161.227	[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]
<input type="checkbox"/>	AE-W2K3-4Y	[未割り当て]
<input type="checkbox"/>	AE-W2K3-5	[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す。

- 7 [作成] をクリックします。
ページが再ロードされ、セキュリティグループのリスト内に新しいグループが表示されます。

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

2.3 保護ネットワークにわたるアクセスおよび通信の要件

- ◆ 25 ページのセクション 2.3.1 「ワークロードに関するアクセスおよび通信の要件」
- ◆ 27 ページのセクション 2.3.2 「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」
- ◆ 28 ページのセクション 2.3.3 「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」

2.3.1 ワークロードに関するアクセスおよび通信の要件

次の表では、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が示されています。

表 2-2 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	Microsoft .NET Framework バージョン 2.0 または 3.5 SP1。	

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 7、 Windows Server 2008、 Windows Vista	<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)。Vista の場合、アカウントを有効にする必要があります (デフォルトでは無効です)。 ◆ [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 137 ~ 139</p> <p>SMB (TCP 139、445 および UDP 137、138)</p> <p>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、サーバー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> <p>netsh firewall set service RemoteAdmin enable</p> <p>netsh の詳細については、Microsoft TechNet の記事 (http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx) を参照してください。</p>	<ul style="list-style-type: none"> ◆ TCP: 3725、135、139、445 ◆ UDP: 137、138、139

ワークロードタイプ	前提条件	必要なポート (デフォルト)
Windows Server 2000、 Windows XP	<ul style="list-style-type: none"> インストールされた Windows Management Instrumentation (WMI) <p>WMI (RPC/DCOM) では、TCP ポート 135 および 445 に加えて、1024 より大きいランダムまたはダイナミックに割り当てられたポートを使用できます。ワークロードの追加中に問題が発生した場合、ワークロードを PlateSpin Forge に追加する間、DMZ にワークロードを一時的に配置するか、またはファイアウォールが設定されたポートを一時的に開くことを検討します。</p> <p>DCOM および RPC に対してポートの範囲を制限する方法など、追加情報については、次の Microsoft 技術情報記事を参照してください。</p> <ul style="list-style-type: none"> ファイアウォールが設定された DCOM の使用 (http://msdn.microsoft.com/en-us/library/ms809327.aspx) ファイアウォールと連携させるための RPC の動的ポート割り当て (http://support.microsoft.com/default.aspx?scid=kb;en-us;154596) NAT ベースのファイアウォールで使用するための DCOM の設定 (http://support.microsoft.com/kb/248809) 	<p>TCP 3725</p> <p>NetBIOS 137 ~ 139</p> <p>SMB (TCP 139、445 および UDP 137、138)</p> <p>RPC (TCP 135)</p>
Linux のすべてのワークロード	Secure Shell (SSH) サーバ	TCP 22、3725

2.3.2 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、[28 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、[\(74 ページ\) 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、Server ホストのローカルアドレスまたは Server 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 (上記の「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。

更新手順については、32 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。

2.3.3 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 PlateSpin Forge のデフォルトオプションの設定

- 28 ページのセクション 2.4.1 「イベントおよびレポートの自動電子メール通知のセットアップ」
- 31 ページのセクション 2.4.2 「PlateSpin Forge の国際バージョンの言語設定」
- 32 ページのセクション 2.4.3 「XML 環境設定パラメータを通じた PlateSpin Server の動作の構成」

2.4.1 イベントおよびレポートの自動電子メール通知のセットアップ

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。

- 28 ページの「SMTP 設定」
- 29 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」
- 31 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 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 2-2 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:	<input type="text" value="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。

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

- 1 使用する PlateSpin Forge の SMTP サーバをセットアップします。28 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]** > **[電子メール]** > **[通知設定]** の順にクリックします。
- 3 **[通知を有効にする]** オプションを選択します。
- 4 **[受信者の編集]** をクリックし、必要な電子メールアドレスをカンマで区切って入力し、**[OK]** をクリックします。

通知設定		保存
<input checked="" type="checkbox"/> 通知を有効にする		
受信者:	アドレス	
削除	dradmin@platespin.com	
削除	john_smith@platespin.com	
削除	sysadmin@platespin.com	
削除	webadmin@platespin.com	
受信者の編集...		

- 5 **[保存]** をクリックします。
一覧された電子メールアドレスを削除するには、削除するアドレスの隣の **[削除]** をクリックします。

以下のイベントが電子メール通知をトリガします。

イベント	備考
ワークロードがオンラインであることが検出されました	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。
ワークロードがオフラインであることが検出されました	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。
完全レプリケーションが正常に完了しました	
完全レプリケーションに失敗しました	
完全レプリケーションが実行されませんでした	[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。
増分レプリケーションが正常に完了しました	
増分レプリケーションに失敗しました	
増分レプリケーションが実行されませんでした	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中に、レプリケーションを手動で一時停止した。 ◆ 手動でトリガしたレプリケーションの実行中に、スケジュールされた増分レプリケーションの実行をシステムが試みた。 ◆ 十分な空きディスク容量がターゲットにないと、システムが判断した。
フェールオーバーのテストが完了しました	[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。
フェールオーバーの準備が完了しました	
フェールオーバーの準備が失敗しました	
フェールオーバーが完了しました	
フェールオーバーに失敗しました	

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。(28 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] > [電子メール] > [レプリケーションレポートの設定] をクリックします。
- 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、[設定] をクリックし、レポートに必要な繰り返しパターンを指定します。
- 5 [受信者] セクションの [受信者の編集] をクリックし、必要な電子メールアドレスをカンマで区切って入力し、[OK] をクリックします。

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			
保護タイプ	許可	コンテナ	電子メール	SMTP	ライセンス
通知設定	レプリケーションレポートの設定				
<input checked="" type="checkbox"/> レプリケーションレポートの有効化 ⚠️ 保存					
レポートの繰り返し	Every day at 12:00 AM (毎日午前12時) 編集				
受信者	アドレス				
	削除	admin@platespin.com			
	削除	john_smith@platespin.com			
	削除	operator@platespin.com			
	受信者の編集...				
アクセスURLの保護	http://localhost:80 ⚠️				

- 6 (オプション) [アクセスURLの保護] 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、61 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。

2.4.2 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。
 - **Internet Explorer:** [ツール] > [インターネットオプション] > [一般] タブ > [言語] の順にクリックします。

- ◆ **Firefox:** [ツール] > [オプション] > [コンテンツ] タブ > [言語] の順にクリックします。
- 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。
53 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。

- 1 Forge VM にアクセスします。
43 ページのセクション 3.4.1 「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) タブで該当するほうをクリックします。
- 3 インストールされていない場合は、必要な言語パックをインストールします。OS のインストールメディアを使用する必要がある場合もあります。
- 4 必要な言語をオペレーティングシステムのインタフェース言語として選択します。メッセージが表示されたら、ログアウトするか、システムを再起動してください。

2.4.3 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 (https://Your_Forge_VM/platespinconfiguration/) にある環境設定 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。

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。この項では、一般的な使用事例に必要な手順に関する情報と共に提供します。

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 Forge VM 上で、指定のディレクトリに移動します。
- 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特定の状況について説明します。

- ◆ 33 ページの「WAN 接続を使用したデータ転送の最適化」

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、32 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 を通し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 2-3 は、デフォルト値と高レイテンシの WAN 環境で推奨される値が示された設定パラメータ値を一覧表示します。

表 2-3 https://Your_Forge_VM/platespinconfiguration/ におけるデフォルトおよび最適化環境設定パラメータ

パラメータ	デフォルト値	最適化された値
fileTransferMinCompressionLimit	0 (無効)	最大 65536 (64KB)
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。		
fileTransferCompressionThreadsCount	2	該当なし
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。圧縮が無効になっている場合は、これは無視されます。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。		
fileTransferSendReceiveBufferSize	0 (8192 バイト)	最大 5242880 (5MB)
ファイル転送接続に関する TCP/IP のウィンドウサイズの設定です。このパラメータは、TCP 受信確認なしで送信されるバイト数を制御します。		
値を 0 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。		
$((\text{リンク速度 (Mbps)}/8) * \text{遅延 (秒)}) * 1000 * 1000$		
たとえば、10 ミリ秒の遅延のある 100Mbps のリンクでは、適切なバッファサイズは次のようになります。		
$(100/8) * 0.01 * 1000 * 1000 = 125000 \text{ bytes}$		

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。

- [35 ページのセクション 3.1「アプライアンスのネットワークの設定」](#)
- [36 ページのセクション 3.2「PlateSpin Forge の移動およびその IP アドレスの再割り当て」](#)
- [41 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」](#)
- [43 ページのセクション 3.4「PlateSpin Forge アプライアンスの保守」](#)
- [47 ページのセクション 3.5「PlateSpin Forge のアップグレード」](#)
- [49 ページのセクション 3.6「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クの設定

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

- [35 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クの設定」](#)

3.1.1 アプライアンスホストのネットワークの設定

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 クライアント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 PlateSpin Forge の移動およびその IP アドレスの再割り当て

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 (『Forge 導入ガイド』を参照)。

手順はアプライアンスバージョン (1 または 2) によって異なります。ユニットのアプライアンスバージョンを判別する方法については、『Forge 導入ガイド』の「ユニットのアプライアンスバージョンの判別」を参照してください。

- [36 ページのセクション 3.2.1 「Forge アプライアンスバージョン 2 の移設手順」](#)
- [40 ページのセクション 3.2.2 「Forge アプライアンスバージョン 1 の移設手順」](#)

3.2.1 Forge アプライアンスバージョン 2 の移設手順

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 クライアントで、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。

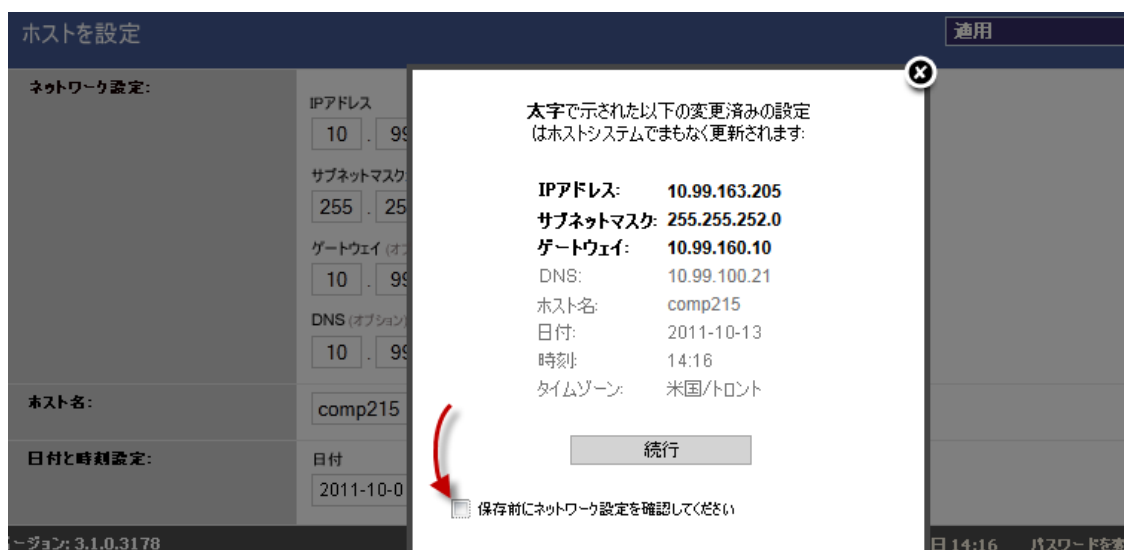
移設プロセスの詳細は、移設場所でのアプライアンスの新しい IP アドレスが知られているか (シナリオ 1)、または知られていないか (シナリオ 2) によって異なります。

- [36 ページの「シナリオ 1 - Forge の移設 \(新しい IP アドレスがわかっている場合\)」](#)
- [38 ページの「シナリオ 2 - Forge の移設 \(新しい IP アドレスがわからない場合\)」](#)

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)

- 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 (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。
- 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 確認のポップアップウィンドウで、新しい設定が正確であることを確認し、[保存する前にネットワーク設定を検証する]の選択を解除し、[続行]をクリックします。



- 6 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 ACC アドレスのリンクは機能しません。

- 7 アプライアンスをシャットダウンします。
- 7a** 次の手順で Forge Management VM をシャットダウンします。45 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。
- 7b** アプライアンスホストをシャットダウンします。
- 7b1** 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。
- 7b2** 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)。

7b3 次のコマンドを入力し、<Enter>を押します。

```
shutdown -h now
```

7c アプライアンスの電源をオフにします。

8 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。

9 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。

10 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 (VMware クライアント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。44 ページの「[VMware 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]* > *[次へ]*  をクリックしてください)。

11 一時停止されたレプリケーションを再開します。

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)

1 すべてのレプリケーションを一時停止します。36 ページの [ステップ 1](#) 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。45 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。

『[導入ガイド](#)』の「[Forge ACC アプライアンスバージョン 2 の設定手順](#)」を参照してください。

5 Forge Appliance Configuration Console (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 確認のポップアップウィンドウで、新しい設定が正確であることを確認し、[保存する前にネットワーク設定を検証する] の選択を解除し、[続行] をクリックします。



- 9 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 ACC アドレスのリンクは機能しません。

- 10 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。
- 11 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。
- 12 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 (VMware クライアント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。44 ページの「[VMware 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] > [次へ]  をクリックしてください)。

13 一時停止されたレプリケーションを再開します。

3.2.2 Forge アプライアンスバージョン 1 の移設手順

- 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 クライアントで、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。
- 2 次の手順で Forge Management VM をシャットダウンします。45 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。
- 3 アプライアンスホストをシャットダウンします。
 - 3a 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 (Forge コンソールに戻るには、<Alt> + <F1> を押します)。
 - 3b スーパーユーザでログインします (root および関連するパスワード)。
 - 3c 次のコマンドを入力し、<Enter> を押します。

```
shutdown -h now
```
 - 3d アプライアンスの電源をオフにします。
- 4 アプライアンスを新しい場所に移動してハードウェアをセットアップし、必要なケーブルを接続してアプライアンスの電源をオンにします。
- 5 次の手順でアプライアンスのネットワーク設定を更新します。
 - 5a Forge コンソールからスーパーユーザでログインします (root および関連するパスワード)。
 - 5b 必要に応じて、アプライアンスホストの IP アドレス、ネットマスク、およびゲートウェイの IP アドレスの設定を更新します。静的 IP のリースが有効な場合のみ、DHCP を使用できます。複数アプライアンスの環境では、ホスト名の競合を防ぐためにアプライアンスに一意的なホスト名を割り当てます。
 - 5c 必要に応じて、Forge 管理 VM の IP アドレス、ネットマスク、ゲートウェイの IP アドレス、およびドメイン提携の設定を更新します。
 - 5d [OK] を選択し、更新内容を確認して再度 [OK] を選択します。

- 6 一時停止されたレプリケーション用にネットワーク設定を更新します。PlateSpin Forge Web クライアントで、一時停止されたワークロードごとに次の内容を実行します。
 - 6a 一時停止されたワークロードの保護の詳細の中の [Replication Settings (レプリケーションの設定)] セクションにアクセスします。
 - 6b [Replication Network (レプリケーションネットワーク)] の値を更新し、ネットワークの変更を反映させます。
 - 6c 設定を保存します。
- 7 レプリケーションの再開 : PlateSpin Forge Web クライアントですべてのワークロードを選択し、[Resume Schedule (スケジュールの再開)], [Execute (実行)] の順にクリックします。

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。

- ◆ [41 ページのセクション 3.3.1 「Forge での SAN ストレージの使用」](#)
- ◆ [42 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。ファイバチャネル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)
- ◆ Compellent (<http://www.compellent.com>)
- ◆ Dell (<http://www.dell.com>)
- ◆ EMC (<http://www.emc.com>)
- ◆ EqualLogic (<http://www.equallogic.com>) (iSCSI のみ)
- ◆ 富士通 (<http://www.fujitsu.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.xiootech.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/tech_activities/ip_storage/iscsi/ 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 (44 ページの「VMware 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が。
- 8 VMware クライアントプログラムを終了します。

PlateSpin Forge Web Client には、次のレプリケーションが実行されて [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 PlateSpin Forge アプライアンスの保守

この項のトピックでは、PlateSpin Forge アプライアンスの保守に関するタスクについて説明します。

- ◆ [43 ページのセクション 3.4.1「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」](#)

3.4.1 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、VMware クライアントソフトウェアを使用します。

注：VMware クライアントソフトウェアは ESX バージョン 3.5 (Forge アプライアンスバージョン 1) と ESX バージョン 4.1 (Forge アプライアンスバージョン 2 システム) とでは異なります。

- ◆ ESX 3.5 では VMware Virtual Infrastructure Client (VIC) が必要です。
- ◆ ESX 4.1 では VMware vSphere Client が必要です。

便宜を図り容易に参照できるように、これらのプログラムは「*VMware Client*」と称される場合があります。さらに、*Virtual Infrastructure Client (VIC)* と *vSphere Client* という用語は互い同じ意味で用いられる場合があります。

-
- ◆ [44 ページの「VMware Client プログラムのダウンロード」](#)
 - ◆ [44 ページの「VMware Client の起動および Forge 管理 VM へのアクセス」](#)
 - ◆ [45 ページの「Forge 管理 VM の起動とシャットダウン」](#)
 - ◆ [46 ページの「アプライアンスホストでの Forge スナップショットの管理」](#)
 - ◆ [46 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」](#)
 - ◆ [47 ページの「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」](#)

VMware 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。

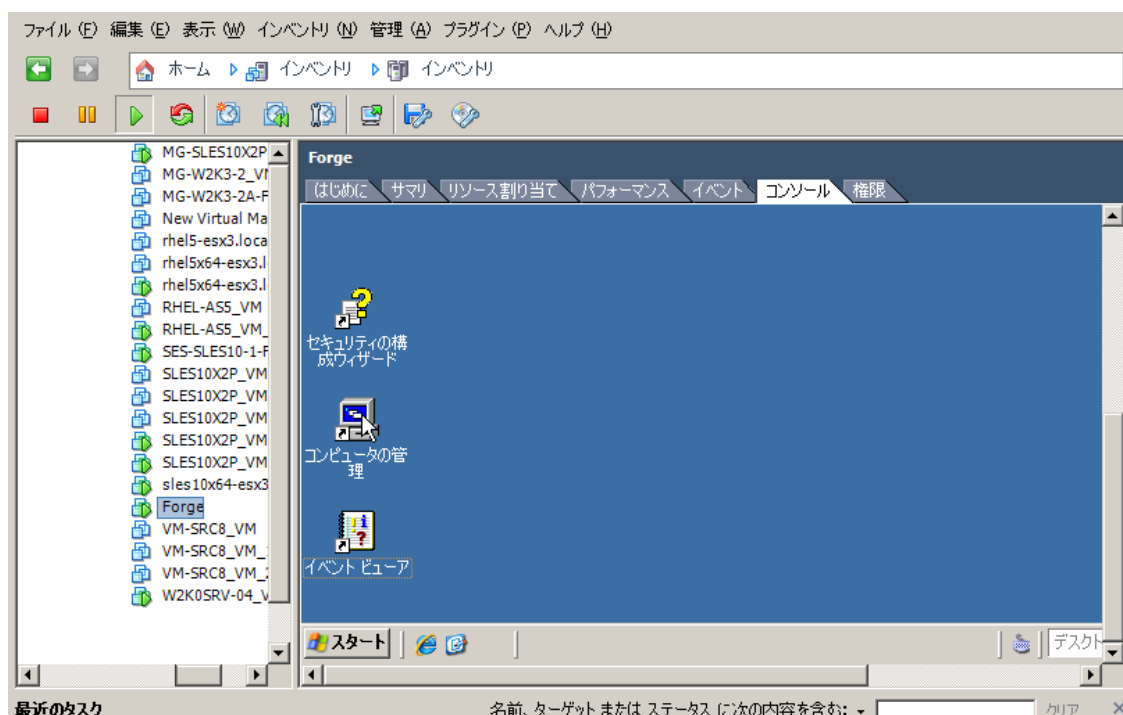
- 1 クライアントソフトウェアをダウンロードします。
 - ◆ (条件付き: VMware ESX 4.1でのForgeアプライアンスバージョン2の場合) [VMware vSphere Client プログラム \(http://vsphereclient.vmware.com/vsphereclient/3/4/5/0/4/3/VMware-viclient-all-4.1.0-345043.exe\)](http://vsphereclient.vmware.com/vsphereclient/3/4/5/0/4/3/VMware-viclient-all-4.1.0-345043.exe) をダウンロードします。
または
 - ◆ (条件付き: VMware ESX 3.5でのForgeアプライアンスバージョン1の場合) Webブラウザを開いて、アプライアンスホストの IP アドレスを使用し、アプライアンスホスト (VMware ESX) のホームページに移動します。セキュリティ証明書関連の警告は無視します。VMWare ESX Server の [ようこそ] ページで *[Virtual Infrastructure Client のダウンロード]* ハイパーリンクをクリックして、インストール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。

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

- 1 [スタート] > [すべてのプログラム] > [VMWare] > [VMware vSphere Client] > [Virtual Infrastructure Client] の順にクリックします。
VMware クライアント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。
VMware クライアント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。

VMware クライアント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。

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。

- 1 VMware Client を使用して、Forge 管理 VM ホストにアクセスします。44 ページの「[VMware 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。

アプライアンスホストでの Forge 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。

- 1 VMware Client を使用して、アプライアンスホストにアクセスします。44 ページの「[VMware 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。

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

この手順を使用して、アプライアンスホストのデータストアに VM を手動でインポートします。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 (83 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)。

- 1 運用サイトで、運用ワークロードから VM (ESX 3.5 以降) 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、VMware クライアント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。44 ページの「[VMware Client プログラムのダウンロード](#)」を参照してください。

- 3 VMware 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 クライアントで、*[Settings (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)。

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

この項では、Forge 管理 VM へのセキュリティパッチの適用に関する一般的なガイドラインについて説明します。

- 1 保守期間中に、VMware クライアントプログラムを使用して Forge 管理 VM にアクセスします。[44 ページの「VMware 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 クライアントを使用し、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。[46 ページの「アプライアンスホストでの Forge 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 クライアントを使用して、[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。[46 ページの「アプライアンスホストでの Forge スナップショットの管理」](#)を参照してください。

3.5 PlateSpin Forge のアップグレード

Forge ソフトウェアは、バージョン 3.3 および 3.4 からアップグレードできます。

この項の残りの部分では、PlateSpin Forge アプライアンスのアップグレードについて説明します。

- ◆ [47 ページのセクション 3.5.1 「アップグレードを開始する前に」](#)
- ◆ [48 ページのセクション 3.5.2 「アップグレードタスクのサマリ」](#)
- ◆ [48 ページのセクション 3.5.3 「Forge アップグレード手順」](#)

3.5.1 アップグレードを開始する前に

アップグレードを開始する前に、次の必要条件が揃っているか確認します。

- ◆ Forge セットアップインストールの実行可能ファイル。

- ◆ 以下に関する IP アドレスおよび適切な資格情報：
 - ◆ Forge アプライアンス (Forge Web クライアントインタフェースおよび Forge 管理 VM に使用)
 - ◆ Forge アプライアンスホスト (VMware ESX サーバ)
- ◆ VMware クライアントプログラム。44 ページの「VMware Client プログラムのダウンロード」を参照してください。

3.5.2 アップグレードタスクのサマリ

Forge アプライアンスをアップグレードするには、次のタスクを順番に実行する必要があります。

1. 現在実行中のレプリケーションがないこと、またはレプリケーションがアップグレード中に実行されるようにスケジュールされていないことを確認します。
2. スナップショットを作成して管理 VM の現在の状態を保存します。
3. Microsoft .NET Framework ソフトウェアとセキュリティパッチを適用して、Forge 管理 VM を更新します。
4. 必要なセットアップ実行可能ファイルを Forge 管理 VM 内でローカルにコピーし実行します。
5. アップグレード後、アプライアンスの操作が適切かを検証します。

3.5.3 Forge アップグレード手順

このフェーズでは、保護されたワークロードのスケジュール設定済みのすべてのレプリケーションを一時停止して、実行中のレプリケーションが完了するのを待機します。

- 1 PlateSpin Forge Web クライアントを使用し、スケジュールされたすべてのレプリケーションを一時停止します。進行中のレプリケーションがあれば、完了するまで待ちます。保護されたワークロードのレプリケーションの状態が [Replication Status (レプリケーションステータス)] 列で [idle (アイドル)] になっていることを確認します。

53 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。

- 2 Forge 管理 VM の電源をオフにします。45 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。
- 3 スナップショットを作成して Forge 管理 VM をバックアップします。46 ページの「アプライアンスホストでの Forge スナップショットの管理」を参照してください。
- 4 Forge 管理 VM の電源をオンにし、VMware クライアントプログラムを使用してアクセスし、次の操作を実行します。
 - 4a Microsoft .NET Framework ソフトウェアをインストールします。Forge 4 には、Microsoft .NET Framework 3.5 SP1 および Microsoft .NET Framework 4.0 が必要です。
 - 4b 利用可能なセキュリティ更新プログラムを適用し、Windows を更新します。
 - 4c Forge 管理 VM を再起動します。
- 5 Forge セットアップインストール実行可能ファイルを Forge 管理 VM 内で実行し、画面の指示に従います。
- 6 PlateSpin Forge Web クライアントを使用し、一時停止されたすべてのレプリケーションを再開します。
- 7 VMware クライアントプログラムを使用して、ステップ 3 で作成したスナップショットを削除します。

重要: フェールバック用に PlateSpin Forge ドライバデータベースにアップロードされたドライバは、保持されません。そのようなドライバは、アップグレード後に再度アップロードする必要があります。

3.6 工場出荷時のデフォルトへの Forge のリセット

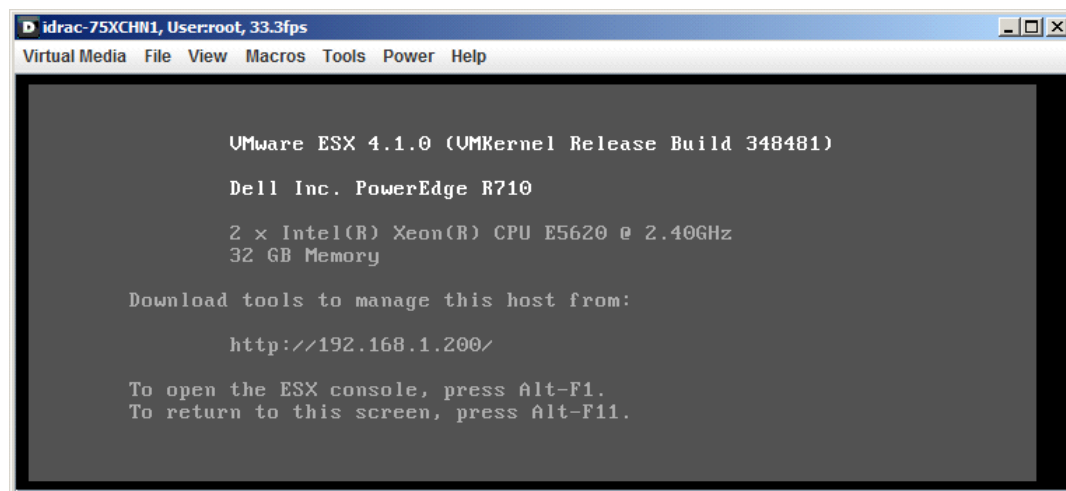
この項では、Forge 4、アプライアンスバージョン 2 ユニットを工場出荷時のデフォルト状態にリセットする方法について説明します。

ご使用の Forge のモデルによっては、このプロセスには 20 ~ 45 分、またはそれ以上かかる場合があります。

- 1 外部 / リモート / 共有ストレージシステム (iSCSI、FiberChannel、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 DRAC を使用して、Hypervisor (VMware ESX) にログインします。
 - 3b <Alt> + <F1> を押して ESX コンソールを開きます。



重要: アプライアンスの工場出荷時設定へのリセット用 IP アドレスを覚えておく必要があります。ACC にログインし、既知の有効な IP アドレスにコンテナを「移動する」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、「[36 ページのセクション 3.2.1 「Forge アプライアンスバージョン 2 の移設手順」](#)」で説明されるプロシージャを使用します。

- 3c 管理者レベルの資格情報を使用してログインします。
- 3d 「reboot」と入力し、<Enter>を押します。

```
idrac-75XCHN1, User:root, 32.7fps
Virtual Media File View Macros Tools Power Help

VMware ESX 4.1 (Kandinsky)
Kernel 2.6.18-194.ESX on an x86_64

forge login: root
Password:
[root@forge ~]# reboot

Broadcast message from root (tty1) (Fri Sep 23 10:52:46 2011):

The system is going down for reboot NOW!
INIT: Sending processes the TERM signal
-
```

3e 再起動プロセスが完了して、GRUB メニューが表示されるまで待ちます。

```
idrac-75XCHN1, User:root, 23.6fps
Virtual Media File View Macros Tools Power Help

GNU GRUB version 0.97 (640K lower / 3397092K upper memory)

VMware ESX 4.1
Troubleshooting mode
PlateSpin Forge Factory Reset

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, 'a' to modify the kernel arguments
before booting, or 'c' for a command-line.
```

- 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 25 秒間)。
- 5 画面の指示に従い、メッセージが表示されたらリセット用のパスワード (「factoryreset」) を入力し、<Enter>を押します。

```
iDRAC6 KVM
File View Macros Tools Help

Booting 'PlateSpin Forge Factory Reset'

cat /factory_reset/factory_reset_warning.txt
WARNING: You are about to reset the appliance.
Please enter password 'factoryreset' (without the quotes)
to initiate Factory Reset.
Once started, the process cannot be undone.

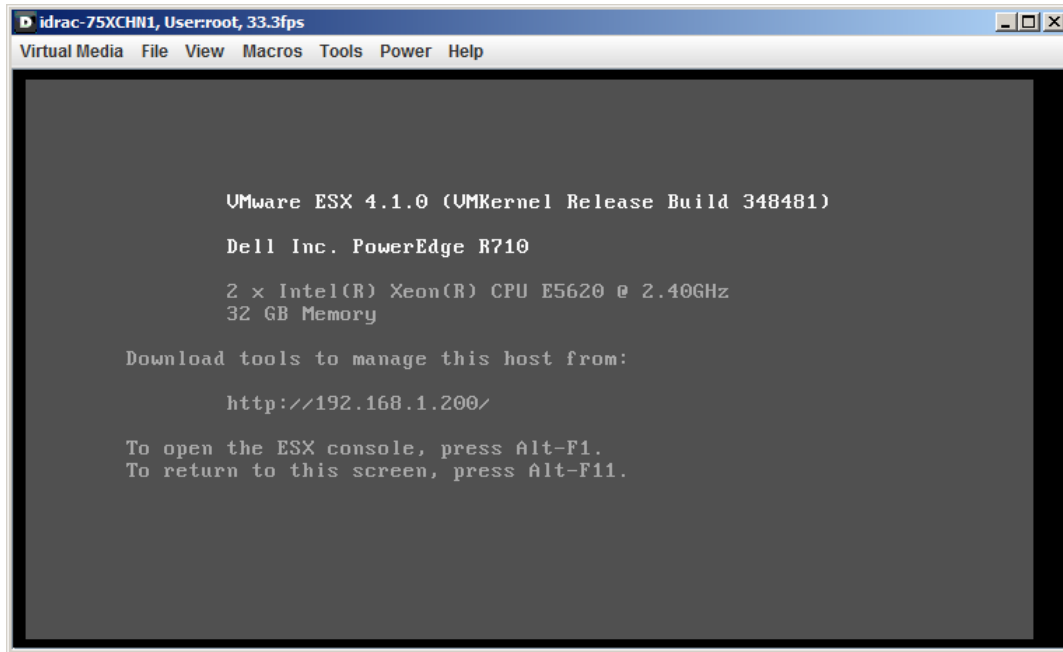
Password: *****_
```

システムのリセット処理が開始されます。

- 6 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。

注: 工場出荷時設定へのリセット処理中に、アプライアンスは2回再起動します。アプライアンスがデフォルトのブート設定を使用して単独で再起動できるようにしてください (VMware ESX 4.1)。2回目のブート時には [PlateSpin Forge Factory Reset] オプションを選択しないでください。

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。



```
idrac-75XCHN1, User:root, 33.3fps
Virtual Media File View Macros Tools Power Help

VMware ESX 4.1.0 (VMKernel Release Build 348481)

Dell Inc. PowerEdge R710

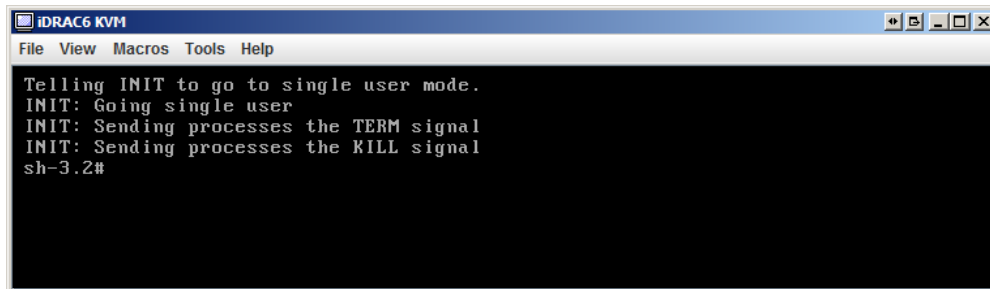
2 x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz
32 GB Memory

Download tools to manage this host from:

http://192.168.1.200/

To open the ESX console, press Alt-F1.
To return to this screen, press Alt-F11.
```

リセット処理が正常に完了しなかった場合、次のような画面が表示されることがあります。



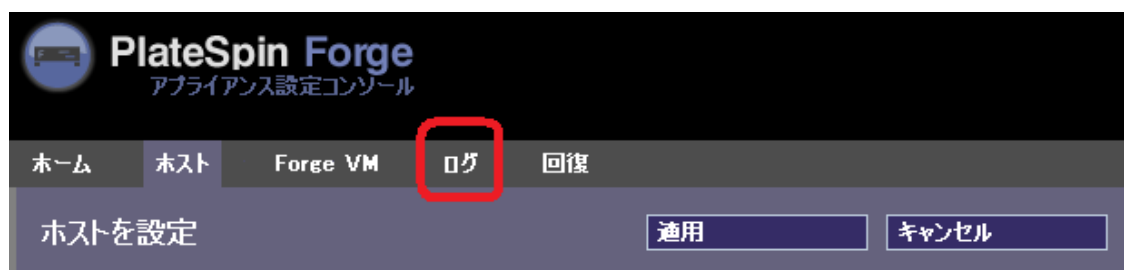
```
iDRAC6 KVM
File View Macros Tools Help

Telling INIT to go to single user mode.
INIT: Going single user
INIT: Sending processes the TERM signal
INIT: Sending processes the KILL signal
sh-3.2#
```

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

これらのログファイルの内容は、Forge Appliance Configuration Console (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。

- ◆ 53 ページのセクション 4.1 「PlateSpin Forge Web インタフェースの起動」
- ◆ 54 ページのセクション 4.2 「PlateSpin Protect Web インタフェースの要素」
- ◆ 56 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」
- ◆ 58 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」
- ◆ 61 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 インタフェースの起動

PlateSpin Forge の操作のほとんどがブラウザベースの PlateSpin Forge Web インタフェースを通じて行われます。

サポートされているブラウザを次に示します。

- ◆ Microsoft Internet Explorer 7 以降
- ◆ Mozilla Firefox (Windows 上) 3.6 以降

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。

- ◆ **Internet Explorer:** [ツール] > [Internet Options (インターネットオプション)] > [セキュリティ] > [インターネット] ゾーン > [カスタムレベル] の順にクリックし、[アクティブスクリプト] 機能に対して [有効にする] オプションを選択します。
- ◆ **Firefox:** [ツール] > [オプション] > [コンテンツ] の順にクリックし、[Java を有効にする] オプションを選択します。

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
```

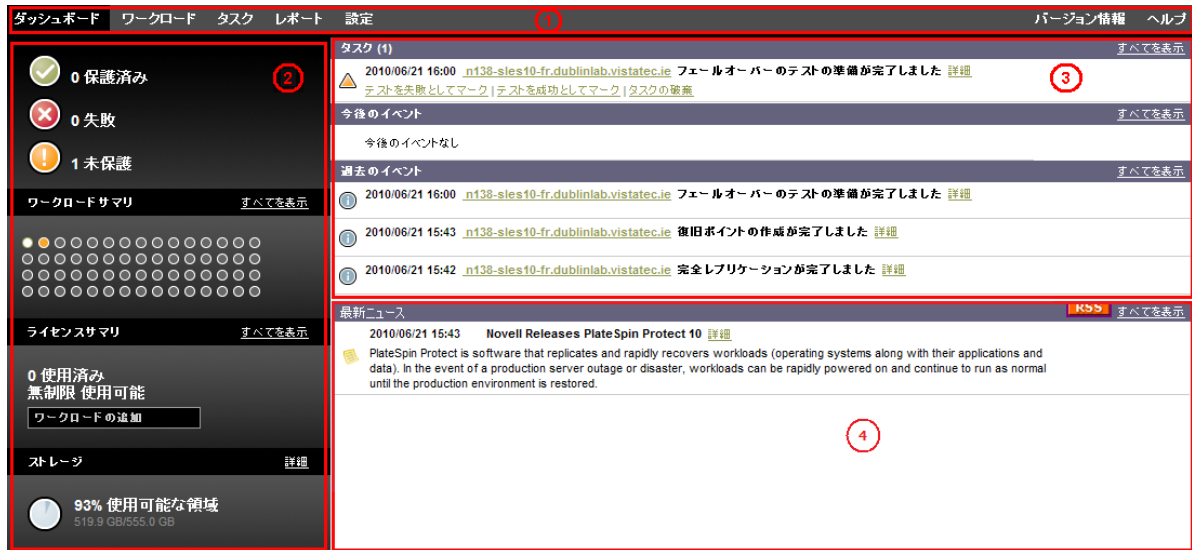
<hostname | IP_address> の部分を、Forge VM のホスト名または IP アドレスで置き換えます。

SSL が有効でない場合は、URL に http を使用します。

4.2 PlateSpin Protect Web インタフェースの要素

PlateSpin Forge Web インタフェースのデフォルトインタフェースは、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を含む [ダッシュボード] ページです。

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。

- ◆ 55 ページのセクション 4.2.1 「ナビゲーションバー」
- ◆ 55 ページのセクション 4.2.2 「ビジュアルサマリパネル」
- ◆ 56 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」

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。56 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。61 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**：82 ページの「保護ティア」を参照してください。
 - ◆ **許可**：20 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。
 - ◆ **Email/SMTP (電子メール/SMTP)**：28 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セットアップ」を参照してください。
 - ◆ **Licenses/License Designations (ライセンス/ライセンスの指定)**：19 ページの「製品ライセンス」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、ライセンス済みのすべてのワークロードと利用可能なストレージの概要レベルのビューが表示されます。

インベントリされたワークロードは、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。

左パネルの中央にある領域は、[ワークロード] ページのグラフィカルサマリを表します。次のドットアイコンを使用して異なる状態のワークロードを表します。

表 4-1 ドットアイコンによるワークロードの表示

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

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表示されています。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。

[ストレージ] には、PlateSpin Forge が利用できるコンテナストレージ領域に関する情報が表示されます。

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)。28 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セットアップ」を参照してください。

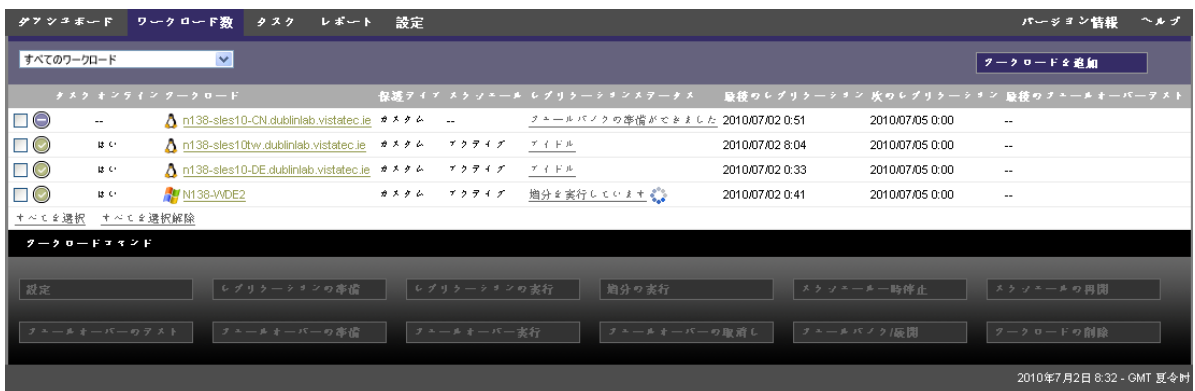
タスクは、ユーザによる操作が必要なイベントに関連付けられている特別なコマンドです。たとえば、[フェールオーバーのテスト] コマンドを完了すると、[テストを成功としてマーク] および [テストを失敗としてマーク] という 2 つのタスクに関連するイベントがシステムによって生成されます。いずれかのタスクをクリックすると、[フェールオーバーのテスト] 操作はキャンセルされ、対応するイベントが履歴に書き込まれます。別の例としては、[完全レプリケーションに失敗しました] イベントが挙げられます。このイベントは、[完全処理の開始] タスクとともに表示されます。現在のタスクの完全なリストは、[タスク] タブ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

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



次の表は、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)。
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 PlateSpin Forge 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 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。

- ◆ 58 ページのセクション 4.4.1 「PlateSpin Forge 管理コンソールの使用」
- ◆ 58 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」
- ◆ 59 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」
- ◆ 60 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

- 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 アドレスまたはホスト名で置き換えます。

- 2 自分のユーザ名および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。

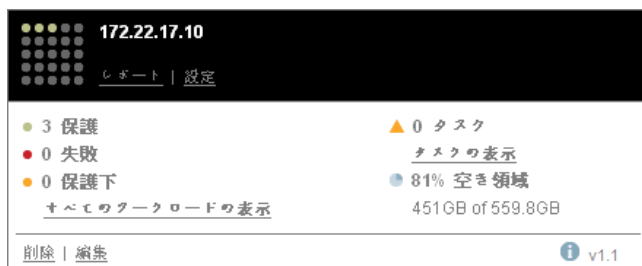
図 4-4 管理コンソールのデフォルトのダッシュボードページ



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 または 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。
[追加 / 編集] ページが表示されます。
- 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) わかりやすい、または識別するための *[表示名]* (最大 15 文字)、*[場所]* (最大 20 文字)、および必要な場合は *[注]* (最大 400 文字) を指定します。
- 6 *[追加/保存]* 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

管理コンソールでは、カードの詳細を変更できます。

- 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レポートを生成できます。

次のレポートタイプがサポートされています。

- **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
2011/4/10 04:01	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
2011/4/17 04:00	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
2011/4/10 04:01	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
2011/4/10 04:00	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

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

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 の VM コンテナ内の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。

- ◆ [63 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」](#)
- ◆ [64 ページのセクション 5.2 「保護のためのワークロードの追加」](#)
- ◆ [66 ページのセクション 5.3 「保護詳細の設定およびレプリケーションの準備」](#)
- ◆ [68 ページのセクション 5.4 「ワークロード保護の開始」](#)
- ◆ [69 ページのセクション 5.5 「コマンドの中止」](#)
- ◆ [70 ページのセクション 5.6 「フェールオーバー」](#)
- ◆ [72 ページのセクション 5.7 「フェールバック」](#)
- ◆ [77 ページのセクション 5.8 「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か確認します。
[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。
[25 ページの「保護ネットワークにわたるアクセスおよび通信の要件」](#)を参照してください。
 - 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、[85 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。詳細については、[64 ページの「保護のため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、[66 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、[68 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、[70 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、[72 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、[77 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。[56 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 保護のための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。

63 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。

名前	説明	CPU	メモリ	空き容量	最終リフレッシュ	
invoy	VMware ESXi Server 4.1.0.260247	4 x Intel(R) Core(TM) i5 CPU 760 @ 2.80GHz	12.0 GB	2.2 TB	7日前	削除
localhost	VMware ESXi Server 4.1.0.260247	4 x Intel(R) Core(TM) i5 CPU 750 @ 2.67GHz	16.0 GB	1.0 TB	17時間前	削除


- 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 (80 ページの「ワークロード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、[Test Credentials (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。

まだコンテナを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。それ以外の場合は、66 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。

5.3 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 (63 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：

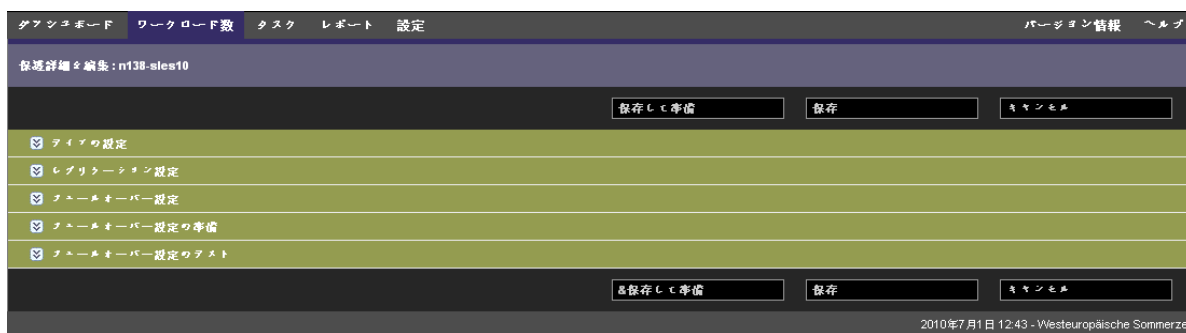
- 1 ワークロードを追加します。64 ページの「保護のためのワークロードの追加」を参照してください。
- 2 [ワークロード] ページで、必要なワークロードを選択し [設定] をクリックします。
または、ワークロードの名前をクリックします。
- 3 [初期レプリケーション方法] を選択します。これは、ワークロードからフェールオーバー VM にボリュームデータを完全に転送するか、既存の VM 上のボリュームと同期するかを示します。詳細については、83 ページの「初期レプリケーション方法 (フルおよび差分)」を参照してください。
- 4 ビジネスの継続性のニーズによって決定される設定の各セットの保護詳細を設定します。66 ページの「ワークロード保護の詳細」を参照してください。
- 5 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。
- 6 [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。

5.3.1 ワークロード保護の詳細

ワークロード保護の詳細は、次の 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。

次の表は、5つのパラメータセットの詳細を示します。

表 5-1 ワークロード保護の詳細

パラメータ セット (設定)	詳細
ティア	現在の保護が使用する保護ティアを示します。82 ページの「保護ティア」を参照してください。
複製	<p>転送方法: (Windows) データ送信メカニズムおよび暗号化によるセキュリティを選択できます。80 ページの「データ転送」を参照してください。</p> <p>暗号の転送: 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。16 ページの「セキュリティとプライバシー」を参照してください。</p> <p>ソース資格情報: ワークロードへのアクセスに必要です。80 ページの「ワークロードの資格情報向けのガイドライン」を参照してください。</p> <p>CPU の数: フェールオーバーワークロードに割り当てられた vCPU の必要数を指定できます (初期のレプリケーションで選択した方法が [完全] の場合にのみ該当)。</p> <p>レプリケーションネットワーク: レプリケーションのトラフィックを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できます。詳細については、88 ページの「ネットワーキング」を参照してください。</p> <p>Configuration File Datastore: VM 環境設定ファイルの保存向けにアプライアンスホストに関連するデータストアを選択できます。83 ページの「復旧ポイント」を参照してください。</p> <p>保護ボリューム: これらのオプションを使用して、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> <p>[シンディスク] オプション: シン仮想ディスク機能を有効にして、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。</p> <p>レプリケーション中のサービス/デーモン状態の停止: レプリケーション時に自動停止する Windows サービスまたは Linux デーモンを選択できます。85 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。</p>
フェールオーバー	<p>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できます。</p> <p>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): これらのオプションを使用して、フェールオーバーワークロードがライブ時にその ID およびドメイン/ワークグループの加入を制限します。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。</p> <p>ネットワーク接続: これらのオプションを使用して、フェールオーバーワークロードの LAN 設定を制御します。88 ページの「ネットワーキング」を参照してください。</p> <p>サービス/デーモンの状態の変更: 特定のアプリケーションサービス (Windows) またはデーモン (Linux) の起動状態を制御できます。85 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。</p>
フェールオーバーの準備	オプションのフェールオーバーの準備操作中にフェールオーバーワークロードの一時ネットワーク設定を制御できます。88 ページの「ネットワーキング」を参照してください。

パラメータ セット (設定) 詳細

テストフェールオーバー VM メモリ: 必要な RAM を一時ワークロードに割り当てることができます。

ホスト名: 一時ワークロードにホスト名を割り当てることができます。

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ることができます。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。

ネットワーク接続: 一時ワークロードの LAN 設定を制御します。88 ページの「[ネットワーキング](#)」を参照してください。

サービス/デーモンの状態の変更: 特定のアプリケーションサービス (Windows) またはデーモン (Linux) の起動状態を制御できます。85 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。

5.4 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。


The screenshot shows the 'Workload Protection' section of the PlateSpin Forge interface. At the top, there are tabs for 'Dashboard', 'Workload', 'Task', 'Report', and 'Settings'. Below the tabs, there is a dropdown menu for 'All Workloads' and a 'Add Workload' button. A table lists workloads with columns for 'Task', 'Online', 'Workload', 'Protection Policy', 'Schedule', 'Replication Status', 'Last Replication', 'Next Replication', and 'Last Failover Test'. Two workloads are listed: 'M138-WFR1' and 'n138-sles10-fr.dublinlab.vistatec.ie'. Below the table, there are buttons for 'Select All' and 'Deselect All'. At the bottom, there is a 'Workload Command' section with several buttons: 'Settings', 'Replication Preparation', 'Replication Execution' (highlighted with a red box), 'Manual Execution', 'Schedule Stop', 'Schedule Restart', 'Failover Test', 'Failover Preparation', 'Failover Execution', 'Failover Cancellation', 'Failover Backup', and 'Workload Deletion'.

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れば、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。

5.5 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であることを示しているリンクをクリックします。

<input type="checkbox"/>		いいえ	CL-2K8R2-VM1	カスタム	アクティブ		アイドル	3/5/2012 12:23 AM	4/11/2012 12:00 AM	--
<input type="checkbox"/>		はい	DL-Sles11x64-Src	every 4 hours (4 時間おき)	アクティブ		フェールオーバーの準備	3/29/2012 8:13 AM	4/9/2012 12:00 PM	3/23/2012 3:32 PM
<input type="checkbox"/>		--	ma-cl-slessp2.site	every 4 hours (4 時間おき)	--		Live (ライブ)	3/15/2012 2:49 PM	--	3/9/2012 2:44 PM
<input type="checkbox"/>		はい	VISTACLIENT	カスタム	アクティブ		増分の実行	3/28/2012 10:21 AM	4/9/2012 12:00 PM	3/23/2012 5:14 PM
<input type="checkbox"/>		--	CL-VISTASP1-SRC	every 4 hours (4 時間おき)	--		Live (ライブ)	2/22/2012 2:55 PM	--	--
<input type="checkbox"/>		はい	CL-XPX64-SRC	カスタム	アクティブ		Live (ライブ)	4/9/2012 10:17 PM	4/9/2012 12:00 PM	3/23/2012 5:15 PM

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。

増分の実行

ワークロード: VISTACLIENT

ステータス: 実行しています

期間: 3d 21h 31m 37s

ステップ: データのコピー (2%)

コントローラの設定 (1%)

最後の完全レプリケーション: 2/17/2012 3:53 PM

最後の増分レプリケーション: 3/28/2012 10:21 AM

最後のフェールオーバーテスト: 3/23/2012 5:14 PM

スケジュール: アクティブ

レプリケーション履歴: View

タスク: --

コマンドサマリ

イベント	詳細	ユーザ	日付
増分レプリケーションが開始しました			4/5/2012 2:00 PM

ステータス: 実行しています

Controller installation has not finished in a timely fashion. (コントローラのインストールはタイムリーに終了しませんでした。)
A controller has already been installed on 10.99.123.164 コントローラは 1099123164 にすでにインストール済みです。)

開始時刻: 4/5/2012 2:00 PM

期間: 3d 21h 31m 37s

ステップ	ステータス	開始時刻	終了時刻	期間	診断
Revert to Snapshot (スナップショットに戻す)	Completed (完了しました)	4/5/2012 2:00 PM	4/5/2012 2:01 PM	1m 7s	--
データのコピー	実行しています (2%)	4/5/2012 2:01 PM	--	3d 21h 30m 30s	-- 診断:

ワークロードコマンド

中止 | 設定 | スケジュールの一時停止

- 3 [中止] をクリックします。

5.6 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。

- ◆ 70 ページのセクション 5.6.1 「オフラインワークロードの検出」
- ◆ 71 ページのセクション 5.6.2 「フェールオーバーの実行」
- ◆ 71 ページのセクション 5.6.3 「フェールオーバーのテスト機能の使用」

5.6.1 オフラインワークロードの検出

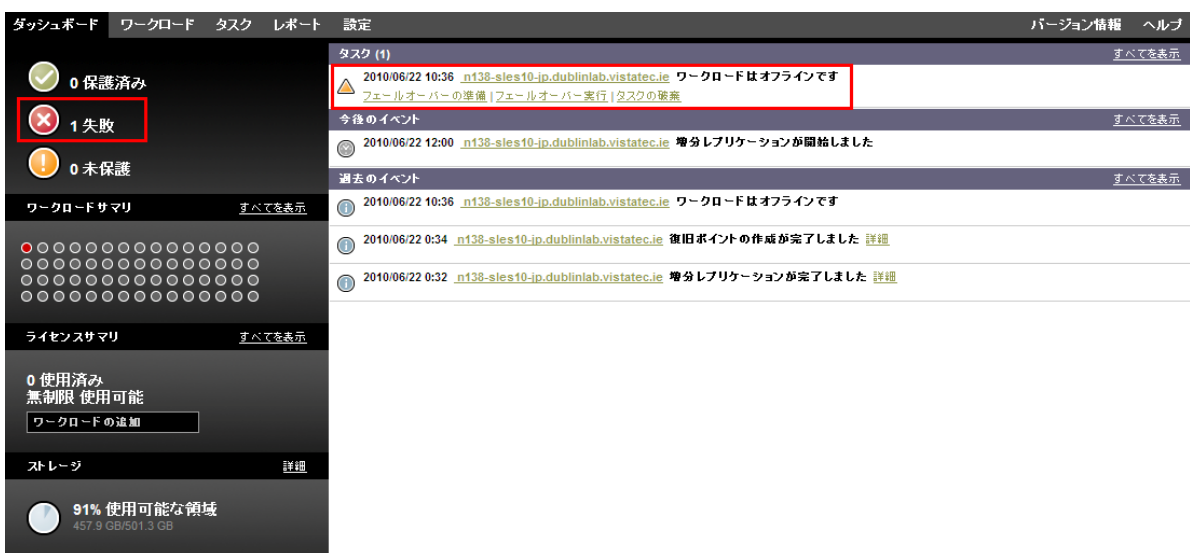
PlateSpin Forge は、保護されたワークロードを絶えず監視しています。事前設定した回数だけワークロードの監視が失敗した場合、PlateSpin Forge によって [ワークロードはオフラインです] イベントが生成されます。ワークロードの障害を判断しログに記録する基準は、ワークロード保護コントラクトのティア設定に含まれています (ティアの 66 ページの「ワークロード保護の詳細」の行を参照)。

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。28 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セットアップ」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 (69 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、71 ページの「フェールオーバーの実行」を参照してください。

次の図は、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」)



5.6.2 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。66 ページの「ワークロード保護の詳細」の中のフェールオーバーの行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 (83 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、71 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。

5.6.3 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フェールオーバー設定のテストがフェールオーバーワークロードに適用されます (66 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」の行を参照)。

- 1 テスト用に適切な時間帯を決定し、レプリケーションが確実に行われなないようにします。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 (83 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、44 ページの「VMware 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。

5.7 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：Xen on SLES および 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。

- ◆ 72 ページのセクション 5.7.1 「VM プラットフォームへの自動化されたフェールバック」
- ◆ 75 ページのセクション 5.7.2 「物理マシンへの半自動化されたフェールバック」
- ◆ 76 ページのセクション 5.7.3 「仮想マシンへの半自動化されたフェールバック」

5.7.1 VM プラットフォームへの自動化されたフェールバック

以下のコンテナは、自動化されたフェールバックターゲットとしてサポートされています。

ターゲット	メモ
vSphere 5.1 での VMware DRS クラスタ	<ul style="list-style-type: none"> ◆ 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。
vSphere 5.0 での VMware DRS クラスタ	<ul style="list-style-type: none"> ◆ 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 5.0 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 5.0 でのみ行うことができます。

ターゲット	メモ
vSphere 4.1 での VMware DRS クラスタ	<ul style="list-style-type: none"> ◆ 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、このクラスタではコンテナとして ESX 4.1 サーバと ESXi 4.1 サーバを組み合わせて使用できます。また、管理は vCenter 4.1 のみ行うことができます。
VMware ESXi 4.1、5.0、5.1	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。
VMware ESX 4.1	

これらの手順を使用して、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します。

- 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 (80 ページの「ワークロード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、83 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。74 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

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。

表 5-2 フェールバック詳細 (VM)

パラメータ セット (設定)	詳細
フェールバック	<p>転送方法: データ送信メカニズムおよび暗号化によるセキュリティを選択できます。80 ページの「データ転送」を参照してください。</p> <p>Failback Network (フェールバックのネットワーク): フェールバックのトラフィックを、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専用ネットワークに送ることができます。88 ページの「ネットワークング」を参照してください。</p> <p>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ンツに関連するデータストアを選択できます。</p> <p>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することができます。</p> <p>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 Windows サービスまたは Linux デーモンを選択できます。85 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。</p> <p>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 アドレスの追加 IP アドレスの入力を受け付けます。27 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。</p>

**パラメータ
セット (設定) 詳細**

ワークロード	<p>CPU の数: ターゲットワークロードに割り当てられる vCPU の必要数を指定できません。</p> <p>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ることができます。</p> <p>Hostname, Domain/Workgroup (ホスト名、ドメイン/ワークグループ): これらのオプションを使用して、ターゲットワークロードの ID およびドメイン/ワークグループの加入を制限します。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。</p> <p>ネットワーク接続: これらのオプションを使用して、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。</p> <p>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) の起動状態を制御できます。85 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。</p>
フェールバック後	<p>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、このオプションを使用します。これは、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。</p> <ul style="list-style-type: none">• 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。

5.7.2 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。[88 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 (オプション: Windows プラットフォーム) PS Analyzer ツールを実行して、欠落しているドライバがないかどうかを判別します。[95 ページの「PlateSpin Analyzer を使用したデバイスドライバの分析 \(Windows\)」](#)を参照してください。
- 3 PS Analyzer によって、ドライバが見つからない、またはドライバに互換性がないことが報告された場合は、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、[96 ページの「デバイスドライバの管理」](#)を参照してください。
- 4 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。
- 5 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 ([80 ページの「ワークロード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。
83 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。

The screenshot shows the 'フェールバックの設定' (Failback Configuration) page. It includes the following fields and options:

- ワークロードの設定 (Workload Configuration):**
 - ホスト名またはIP: MA-Rhel5u3
 - 資格情報 (Credentials):
 - ユーザー名: root
 - パスワード: [masked]
 - 資格情報のテスト: [button]
- フェールバックターゲットの設定 (Failback Target Configuration):**
 - レプリケーション方法 (Replication Method):
 - 完全レプリケーション (Full Replication)
 - 増分レプリケーション (Incremental Replication)
 - ターゲットタイプ (Target Type):
 - 仮想ターゲット (Virtual Target)
 - 物理ターゲット (Physical Target)
 - フェールバックターゲット (Failback Target):

Selection required below (以下の選択が必要) ❌

No physical targets available (使用可能な物理ターゲットはありません)

注: To add a physical target, boot up and register the physical server with PlateSpin Failback ISO Image. (物理ターゲットを追加するには、PlateSpinフェールバックISOイメージを使用して物理サーバを起動し、登録します。) To download, visit the [PlateSpin Resource Center](#) (ダウンロードするには、PlateSpin Resource Centerにアクセスしてください。)
- ワークロードコマンド (Workload Command):**
 - 保存して準備 (Save and Prepare) [button]

- 6 [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。
- 7 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。

5.7.3 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。

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 VM プラットフォームによりサポートされています。

- ◆ SLES 10 SP2 上で実行される Xen
- ◆ Microsoft Hyper-V Server 2008 (R2 ではなく)

また、完全自動化フェールバックサポートが提供されているコンテナに対して、半自動化されたフェールバックを実行することもできます (VMware ESX ターゲットおよび DRS Cluster ターゲット)。

5.8 ワークロードの再保護

再保護の操作は、フェールバック後の次の論理ステップであり、ワークロードの保護ライフサイクルを完了させ、新たに保護ライフサイクルを開始します。フェールバック操作が正常にすると、[再保護] コマンドが 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されている同じ保護の詳細を適用します。

注: [再保護] コマンドは、フェールバックの詳細で [再保護] オプションが選択されている場合にのみ使用可能となります。詳細については、72 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。

- ◆ 79 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」
- ◆ 80 ページのセクション 6.2 「ワークロードの資格情報向けのガイドライン」
- ◆ 80 ページのセクション 6.3 「データ転送」
- ◆ 82 ページのセクション 6.4 「保護ティア」
- ◆ 83 ページのセクション 6.5 「復旧ポイント」
- ◆ 83 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)」
- ◆ 85 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」
- ◆ 85 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)」
- ◆ 86 ページのセクション 6.9 「ボリューム」
- ◆ 88 ページのセクション 6.10 「ネットワークング」
- ◆ 88 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」
- ◆ 90 ページのセクション 6.12 「高度なワークロード保護に関するトピック」

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とおして保護用に特定の数のワークロードを使用する権利が与えられます。保護用のワークロードを追加するたびに、システムではライセンスプールからワークロードライセンスを 1 つ消費します。ワークロードを削除した場合は、最大 5 回まで消費したライセンスを回復できます。

製品ライセンスとライセンス有効化に関する詳細は、19 ページの「製品ライセンス」を参照してください。

6.2 ワークロードの資格情報向けのガイドライン

PlateSpin Forge にはワークロードに対して管理者レベルのアクセス権が必要です。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： <i>authority\principal</i>◆ ワークグループメンバーのマシン用： <i>hostname</i>
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 を参照してください。

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。

- ◆ [80 ページのセクション 6.3.1 「転送方法」](#)
- ◆ [82 ページのセクション 6.3.2 「データの暗号化」](#)

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。

- ◆ [81 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」](#)
- ◆ [81 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、ブロックレベルのデータ転送のための専用のソフトウェアコンポーネントを使用し、Microsoft Volume Snapshot Service (VSS) と、VSS をサポートするアプリケーションおよび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。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。

- ◆ **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。

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。

- **Windows のファイルレベルのレプリケーション** データはファイルごとに複製されます (Windows のみ)。

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 \(https://www.netiq.com/support/kb/doc.php?id=7005872\)](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 \(https://www.netiq.com/support/kb/doc.php?id=7005873\)](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

ワークロードデータをより安全に転送するために、PlateSpin Forge ではデータレプリケーションを暗号化できます。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) または FIPS 対応の暗号化が有効な場合は 3DES 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、データ転送速度を著しくスローダウンさせる可能性があります。

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マイズ可能なコレクションです。

- 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。

次の手順に従って、前もってカスタムの保護ティアを作成することもできます。

- 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。

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	レプリケーションの停止を強制するには、これらの設定を使用します。使用量がピークの時間帯にスケジュール済みレプリケーションを一時停止にするか、VSS 対応アプリケーションと VSS のブロックレベルデータ転送コンポーネント間の競合を防ぐには、この機能の実装を検討してください。 ブラックアウトウィンドウを指定するためには、[編集] をクリックしてから、ブラックアウトの繰り返しパターン (毎日、毎週など) を選択し、ブラックアウト期間の開始と終了時間を指定します。 注: ブラックアウトの開始時間と終了時間は、PlateSpin Server のシステムクロックに基づきます。

圧縮レベル	これらの設定は、転送前にワークロードデータを圧縮するか、またその方法を制御します。 17 ページの「データ圧縮」 を参照してください。 次のいずれかのオプションを選択します。[<i>高速</i>] 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、[<i>最大</i>] 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。[<i>最適</i>] は、中程度で、推奨オプションです。
帯域幅制限	これらの設定は、帯域幅制限を制御します。 17 ページの「帯域幅制限」 を参照してください。 レプリケーションを指定の速度に制限するには、必要な処理量の値を Mbps で指定し、時間パターンを示してください。
維持する復旧ポイント	この保護ティアを使用するワークロード用に維持する復旧ポイントの数を指定します。詳細については、 83 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、[46 ページの「アプライアンスホストでの Forge 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。

- ◆ **フル：**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。
46 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 (75 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。

- 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

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。85 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 (85 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

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、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て保護に必要なボリュームを指定します。

PlateSpin Forge では、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 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。

次の図は、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

ティアの設定					
レプリケーションの設定					
データ転送の暗号化:	いいえ				
ソース資格情報:	root				
CPUの数:	1				
レプリケーションネットワーク:	DHCP - VM Network				
復旧ポイントデータストア:	datastore1 (222.2 GB 空き)				
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	
	<input checked="" type="checkbox"/>	/boot (EXT2-システム)	68.3 MB	SAN-VMware2	
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"/>	/ (REISERFS)	10.0 GB	system	
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	
	<input checked="" type="checkbox"/>	system	19.9 GB	SAN-VMware2	
非ボリュームストレージ:	含める	パーティション	合計サイズ	データストア	はスワップ
	<input checked="" type="checkbox"/>	/dev/system/swap	1008.0 MB	system	はい
レプリケーション中に停止するデーモン:	--				
フェールオーバー設定					
<input checked="" type="checkbox"/> フェールオーバー設定の準備					
<input checked="" type="checkbox"/> フェールオーバー設定のテスト					
<input checked="" type="checkbox"/> 復旧ポイント					
<input checked="" type="checkbox"/> ワークロードの詳細					

次の図は、EVMS 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もつ 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 6-2 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
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	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"/>	NEWPOOL	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**: (複製パラメータセット) 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**: (フェールオーバーパラメータセット) フェールオーバーワークロードが稼動し始めた場合に、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**: (フェールオーバーの準備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。

- ◆ [88 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」](#)
- ◆ [88 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」](#)
- ◆ [89 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

Novell ダウンロード (<http://download.novell.com>) の PlateSpin Forge エリアから、PlateSpin ISO ブートイメージ (PlateSpinFailback.ISO) をダウンロードできます。次のパラメータで検索を実行します。

- ◆ **製品またはテクノロジー**: PlateSpin Forge
- ◆ **バージョンの選択**: PlateSpin Forge 4
- ◆ **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。

- 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](#) 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、root として次のコマンドを実行して、SOURCE ファイルを ISO ファイルにコピーします。

```
./rebuildiso.sh <SOURCE> <-m32/-m64> <-i ISO file>
```

注: SOURCE は、次の 1 つ以上のパラメータである必要があります。

-d 追加するドライバ (つまり、*.ko ファイル) があるディレクトリへのパス

-c ConfigureTakeControl.xml ファイルへのパス

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。

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 (最大 512 MB の RAM を持つシステム用)
 - ◆ ps64_512m (512 MB RAM を超えるシステム)
- 5 <Enter> キーを押します。
- 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」と入力します。有効化していない場合は「N」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 高度なワークロード保護に関するトピック

- ◆ 90 ページのセクション 6.12.1「Windows クラスタの保護」
- ◆ 91 ページのセクション 6.12.2「Xen-on-SLES 上で並行仮想化された VM への Linux フェールバック」
- ◆ 93 ページのセクション 6.12.3「PlateSpin Forge の Web サービス API 経由でのワークロード保護機能の使用」

6.12.1 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 2003 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ー」モデル）
- ◆ Windows 2008 Server 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」モデルおよび「マジョリティなし：ディスクのみ」モデル）

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、ソースインフラのトラブルシューティング時に使用できる仮想シングルノードクラスタに流すことで実現します。

現在のリリースにおけるクラスタマイグレーションのサポート範囲は、次の条件に従う必要があります。

- ◆ [ワークロードの追加] 操作を実行する場合、クラスタのクォーラムリソースを現在所有しているアクティブノードを識別する必要があります。これは、クラスタの IP アドレス（仮想 IP アドレス）で識別されます。個別ノードの IP アドレスを指定すると、そのノードが通常のクラスタ非対応の Windows ワークロードとしてインベントリされてしまいます。
- ◆ クラスタのクォーラムリソースは、保護されるクラスタのリソースグループ（サービス）と一緒に用られる必要があります。

保護されたクラスタの増分レプリケーション間でノードのフェールオーバーが発生した場合、PlateSpin Forge は保護イベントを生成します。新しいアクティブノードのプロファイルが障害の発生したアクティブノードと同様の場合は保護コントラクトが継続します。そうでない場合は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、次のような場合に、類似していると見なされます。

- ◆ 同じ数のボリュームがあります。
- ◆ 各ボリュームは、各ノードでまったく同じサイズになります。
- ◆ それらは、まったく同数のネットワーク接続をもちます。

Windows クラスタを保護するには、通常のワークロード保護ワークフローに従います（63 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）。

フェールバック時に、PlateSpin Forge は、共有ボリュームのレイアウトがターゲット上に確実に保持されるようにする検証機能を提供します。ボリュームを正しくマップしていることを確認します。

6.12.2 Xen-on-SLES 上で並行仮想化された VM への Linux フェールバック

Xen-on-SLES 上で並行仮想化された VM へのフェールバックを行うことができます (バージョン 10 のみ)。これは、2 段階プロセスを通じて、間接的に行われます。並行仮想化された VM はまず、完全に仮想化された VM に変換され、後で戻されます。ユーティリティ (xmpsadministrator-) は、PlateSpin ISO ブートイメージに含まれ、VM により使用されます。

ターゲットが新規であるか、既存の並行仮想化された VM であるかに応じて、プロシージャは若干異なります。

- [91 ページの「新たに並行仮想化された VM への Linux フェールバック」](#)
- [93 ページの「既存の並行仮想化された VM への Linux フェールバック」](#)

新たに並行仮想化された VM への Linux フェールバック

- 1 PlateSpin ISO ブートイメージをターゲットの Xen-on-SLES サーバにコピーします。
- 2 仮想マシンマネージャを開始し、次のように、完全に仮想化された VM を作成します。
 - 2a [オペレーティングシステムをインストールする必要がありません] オプションを選択します。
 - 2b ディスクイメージに対して適切なサイズを選択します (ディスクサイズは、フェールオーバー VM と等しいか、それよりも大きい必要があります)。
 - 2c ブート ISO をインストールソースとして選択します。

VM は PlateSpin OS 環境にブートします。物理マシンへのフェールバックの設定で使用されます。
- 3 フェールバックプロシージャを完了してください。 [75 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」](#) を参照してください。

完了時に、VM は完全に仮想化されたマシンとして完全に機能する必要があります。
- 4 VM を再起動し、再び PlateSpin OS 環境にブートされることを確認してください。

```
Welcome to PlateSpin/OS version 9.9.9.9
Available boot options (type the name to boot into):
ps          - PlateSpin Linux for Taking Control (press ENTER to boot into)
ps64       - PlateSpin Linux(x86_64) for Taking Control
ps64_512m  - PlateSpin Linux(x86_64) for Taking Control a Virtual Machine
             which has more than 512M memory
next       - Boot from Next Boot Device Set in BIOS (timeout)
debug      - PlateSpin Linux for Trouble Shooting
switch     - PlateSpin Linux for switching kernel to Xen PU

When no key is pressed for 20 seconds, it will boot from the next boot device.

boot: switch_
```

- 5 boot: プロンプトで、「switch」と入力し、<Enter> キーを押します。

これにより、オペレーティングシステムが並行仮想化されたマシンとしてブート可能になるように再構成されます。完了時に、次のように、出力が表示されます。

```

about to find other volumes in native off-line OS
kjournal starting. Commit interval 5 seconds
EXT3-fs: mounted filesystem with ordered data mode.
found volume /boot in off-line OS
found other 1 volume(s)
mount all the system volumes
kjournal starting. Commit interval 5 seconds
EXT3 FS on hda1, internal journal
EXT3-fs: mounted filesystem with ordered data mode.
volume /boot has been mounted.
all the system volumes are mounted
Switching to Xen kernel for Para-virt machine...
unmount all the system volumes for clean up.
volume /boot has been unmounted
volume / has been unmounted

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

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

#####

[DB]$ _

```

出力の最後のセグメントの `bootloader` 引数を書き留めてください。

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

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

これらは、並行仮想化されたマシンがブートされるカーネルの場所と `initrd` イメージをセットアップするために、`xmps` ユーティリティにより使用されます。

6 仮想マシンの電源を切ります。

```
[DB]$ poweroff
```

7 Xen-on-SLES サーバに `root` としてログインし、PlateSpin ISO ブートイメージをマウントします (コマンドの例は、ISO が `/root` ディレクトリとしてコピーされていることを想定しています)。

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

8 `xmps` ユーティリティを実行して、次のように完全に仮想化された VM の構成に基づいて並行仮想化された VM を作成します。

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

ユーティリティでは次の項目を入力します。

- ◆ 並行仮想化されたマシンの構成が基礎とする完全に仮想化された VM の名前 (SLES10-FV)
- ◆ 作成する仮想マシンの名前 (SLES10-PV)
- ◆ 並行仮想化されたマシンのブートローダ引数 "`--bootloader_args`" (ステップ 5 に表示)

`new_vm_name` として渡された VM と同じ名前をもつ VM の場合、`xmps` ユーティリティが失敗します。

新たに作成された並行仮想化された VM (SLES10-PV) は、Virtual Machine Manager で利用できるようになっているはずで、オンにする準備が完了しています。対応する完全に仮想化されたマシンはリタイヤし、ブートができなくなります。この VM は安全に削除できます (VM 構成のみが削除されます)。

9 PlateSpin ISO ブートイメージをアンマウントします。

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

既存の並行仮想化された VM への Linux フェールバック

- 1 PlateSpin ISO ブートイメージをターゲットの Xen-on-SLES サーバにコピーします。
- 2 XEN SLES サーバに root としてログインし、PlateSpin ISO ブートイメージをマウントします。

```
# mkdir /mnt/ps # mount -o loop /root/linuxfailback.iso /mnt/ps
```
- 3 xmps ユーティリティを実行して、次のとおり、並行仮想化された VM (対象のフェールバックターゲット) の構成に基づいて、完全に仮想化された VM を作成します。

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

ユーティリティでは次の項目を入力します。
 - ◆ 既存の並行仮想化されたマシンの名前 (SLES10-PV)。対象のフェールバックターゲットです。
 - ◆ 一時的に完全に仮想化されたマシンの名前 (SLES10-FV)。2 段階フェールバック操作に対して作成されます。
 - ◆ ブート ISO の完全パス (ISO ファイルが /root: /root/linuxfailback.iso の下にあることを想定)new_vm_name として渡された VM と同じ名前をもつ VM の場合、xmps ユーティリティが失敗します。
新しく作成された完全に仮想化されたマシン (SLES10-FV) は、Virtual Machine Manager で使用できるようになります。
- 4 新しく作成された完全に仮想化されたマシン (SLES10-FV) をオンにします。
VM は PlateSpin OS 環境にブートします。物理マシンへのフェールバックの設定で使用されません。
- 5 フェールバックプロシージャを完了してください。75 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」を参照してください。
- 6 VM を再起動し、switch コマンドを実行して、91 ページの「新たに並行仮想化された VM への Linux フェールバック」(ステップ 4 からステップ 9 までのみ) の記述に従ってワークロードを再構成します。

6.12.3 PlateSpin Forge の Web サービス API 経由でのワークロード保護機能の使用

PlateSpin Protect では、REST ベースの API テクノロジー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

Forge 管理者は、コマンドラインから Jscript サンプル (<https://localhost/protectionservices/Documentation/Samples/protect.js>) を利用して、この製品に API を介してアクセスできます。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、<https://localhost/protectionservices/Documentation/AddWorkloadsAndContainersFromCsvFile.htm> の API ドキュメントを参照してください。

- ◆ 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

PlateSpin Forge REST API ホームページ (<https://localhost/protectionservices/> または <https://<server page>/protectionservices/>) には、開発者と管理者にとって有用なコンテンツへのリンクがあります。

このテクノロジプレビューは、その後のリリースのより多くの機能で完全に開発されます。

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。

- 95 ページのセクション 7.1 「PlateSpin Analyzer を使用したデバイスドライバの分析 (Windows)」
- 96 ページのセクション 7.2 「デバイスドライバの管理」

7.1 PlateSpin Analyzer を使用したデバイスドライバの分析 (Windows)

物理マシンに対してワークロードのフェールバックを実行する前に、PlateSpin Analyzer を使用して潜在的なドライバの問題を特定し、前もって修正します。

注：PlateSpin Analyzer では、Windows のワークロードのみを現在サポートしています。

- 1 Forge VM で、次のディレクトリにある Analyzer.Client.exe プログラムを開始します。

Program Files\PlateSpin Forge Server\PlateSpin Analyzer

- 2 ネットワークの選択が [デフォルト] であることを確認し、[すべてのマシン] ドロップダウンリストから必要なマシンを選択します。
- 3 (オプション) 分析時間を短縮するためには、マシンの範囲を特定の言語に制限します。
- 4 [分析] をクリックします。

インベントリされたワークロードのうちの選択数に応じて、分析には数秒から数分かかります。

分析されたサーバは、右側ペインにリストされます。右側のペインで、テスト結果を表示するサーバを選択します。テスト結果は、次のうちの任意の組み合わせが考えられます。

表 7-1 PlateSpin アナライザのテスト結果に含まれるステータスメッセージ

結果	説明
合格	マシンが PlateSpin アナライザのテストに合格しました。
警告	マシンに関して 1 つ以上のテストで警告が返され、マイグレーションに問題がある可能性を示しています。詳細を表示するには、ホスト名をクリックします。
失敗	このマシンに関して、1 つ以上のテストが失敗しました。詳細を表示し、さらに情報を取得するには、ホスト名をクリックします。

[概要] タブには、分析されたマシン数およびチェックされなかったマシン数に加え、テストに合格したマシン数、不合格だったマシン数、または警告ステータスが付加されたマシン数のリストが表示されます。

[テスト結果] タブには、次の情報が表示されます。

表 7-2 PlateSpin アナライザのテスト結果タブ

セクション	詳細
システムテスト	マシンがハードウェアおよびオペレーティングシステムの最小限の要件を満たすかを検証します。
ハードウェアサポート	ハードウェアに互換性があるワークロードかを確認します。
ターゲットハードウェアのサポート	ターゲット物理マシンとして使用するのにハードウェアに互換性があるかをチェックします。
ソフトウェアテスト	トランザクション上の整合性を保証するために、ライブ転送の間シャットダウンする必要のあるアプリケーションとデータベースをチェックします。
互換性のないアプリケーションテスト	マイグレーションプロセスを妨げることが分かっているアプリケーションがシステム上にインストールされていないかを確認します。これらのアプリケーションアイコンは、互換性のないアプリケーションデータベースに保存されています。このデータベース内でエンティティの追加、削除、または編集を行うには、[ツール] メニューから、[互換性のないアプリケーション] を選択します。

[プロパティ] タブには、選択したマシンの詳細が表示されます。

7.2 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。必要なドライバが利用可能かどうか判断するには、PlateSpin アナライザユーティリティを使用します。95 ページの「[PlateSpin Analyzer を使用したデバイスドライバの分析 \(Windows\)](#)」を参照してください。

PlateSpin Analyzer が不明な、または互換性のないドライバに遭遇した場合、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。

- ◆ 97 ページのセクション 7.2.1 「Windows システム用のデバイスドライバのパッケージ化」
- ◆ 97 ページのセクション 7.2.2 「Linux システム用のデバイスドライバのパッケージ化」
- ◆ 98 ページのセクション 7.2.3 「PlateSpin Forge 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」
- ◆ 100 ページのセクション 7.2.4 「プラグアンドプレイ (PnP) ID トランスレータ機能の使用」

7.2.1 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) 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。98 ページの「[PlateSpin Forge 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
 - 32 ビット版の Windows Vista システムと Windows Server 2008 システム、および Windows 7 システム
-

7.2.2 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す。

- 1 Linux ワークステーション上で、デバイスドライバファイル用のディレクトリを作成します。ディレクトリ内のすべてのドライバは、同じカーネルおよびアーキテクチャ用でなければなりません。
- 2 ブートイメージをダウンロードして、それをマウントします。
たとえば、ISO が /root ディレクトリの下でコピーされていると想定して、次のコマンドを発行します。

```
# mkdir /mnt/ps # mount -o loop /root/linuxfailback.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。98 ページの「[PlateSpin Forge 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。

7.2.3 PlateSpin Forge 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

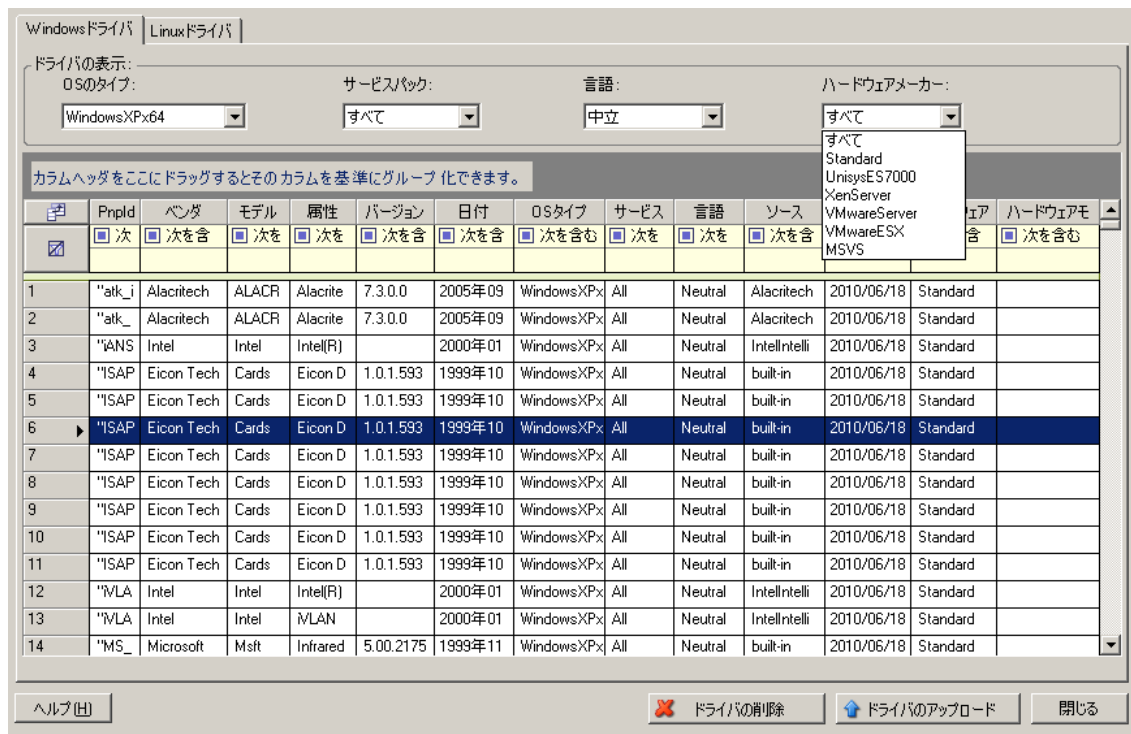
PlateSpin Driver Manager を使用して、デバイスドライバをドライバデータベースにアップロードします。

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アップロードするようにしてください。

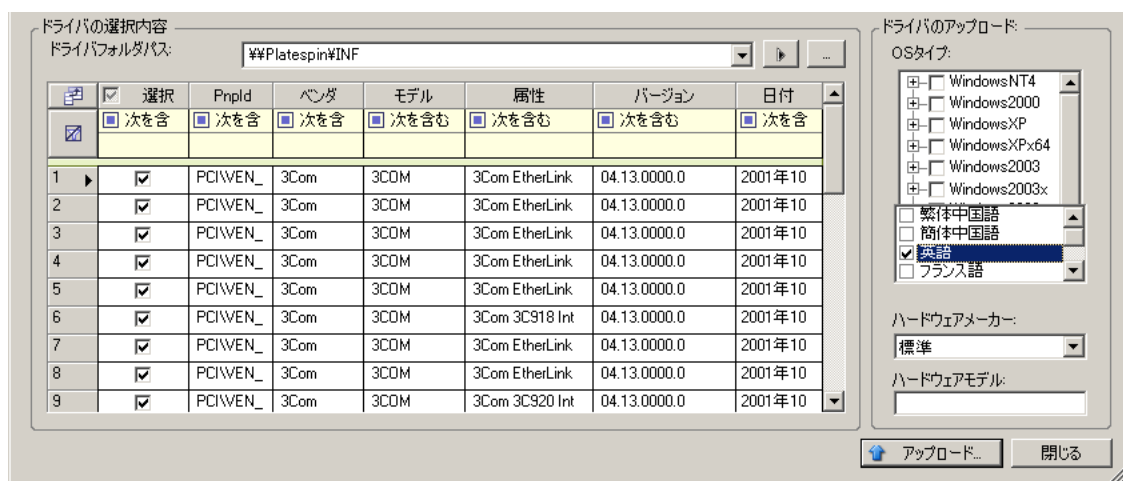
- ◆ 98 ページの「デバイスドライバのアップロード手順 (Windows)」
- ◆ 99 ページの「デバイスドライバのアップロード手順 (Linux)」

デバイスドライバのアップロード手順 (Windows)

- 1 必要なデバイスドライバを取得して準備します。Windows 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。

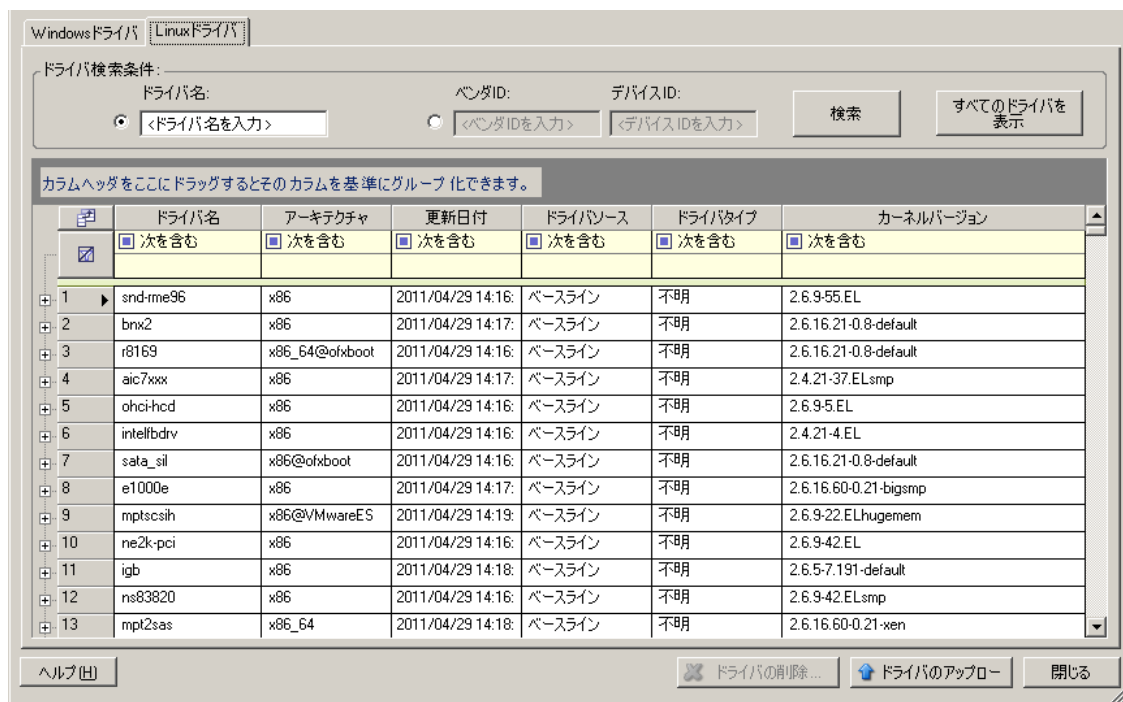


リストされているターゲット環境に対して特別に設計されたドライバでないかぎり、[ハードウェアメーカー] オプションとして [標準] を選択します。

- 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。

7.2.4 プラグアンドプレイ (PnP) ID トランスレータ機能の使用

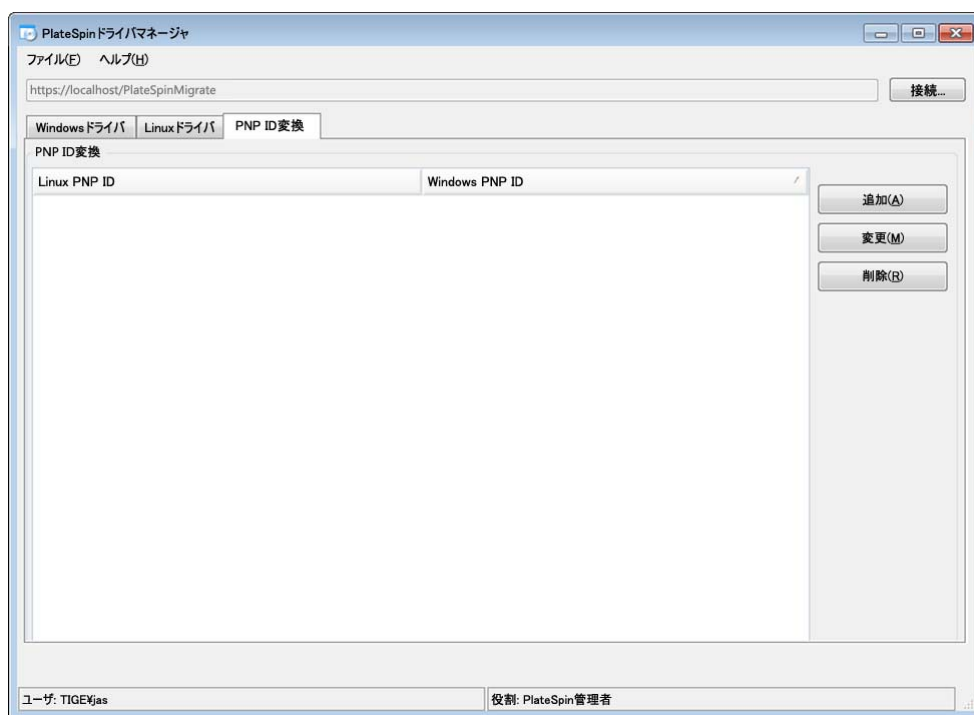
「プラグアンドプレイ」(PnP) とは、ネイティブのプラグアンドプレイデバイスに対する接続、設定、および管理をサポートする Windows オペレーティングシステムの機能を指します。Windows では、この機能により、PnP 準拠バスに接続されている PnP 準拠のハードウェアデバイスを容易に検出できます。PnP 準拠デバイスには、製造元によって一連のデバイス ID 文字列が割り当てられます。それらの文字列は、ビルド時にデバイスにプログラミングされます。それらの文字列は、PnP がどのように動作するか的基础となるものであり、デバイスを適切なドライバに対応させるために使用される Windows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

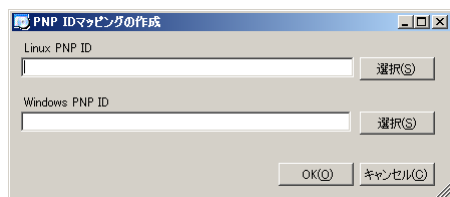
それらの ID は一貫してフォーマットされているので、PlateSpin は、それぞれに標準変換を適用して、対応する Windows PnP ID を決定できます。変換は、PlateSpin 製品内で自動的に行われます。この機能を使用して、管理者またはサポート技術者は、カスタムの PnP マッピングを追加、編集、または削除することができます。

PnP ID 変換機能を使用するには、次の手順に従います。

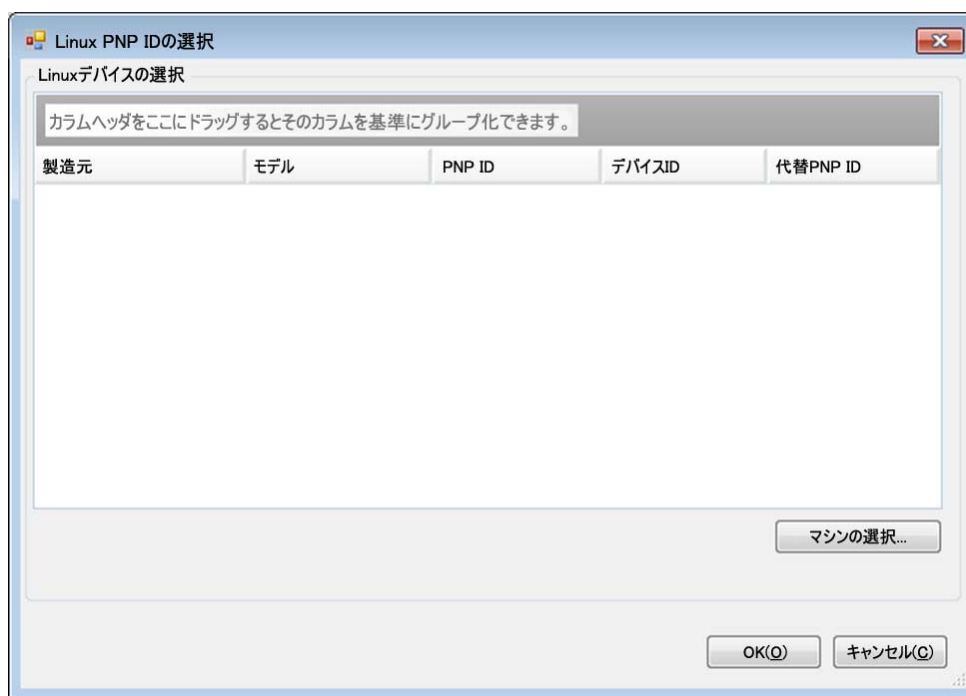
- 1 PlateSpin Driver Manager ツールを起動し、PlateSpin Server に接続します。
- 2 Driver Manager ツールで、[PNP ID 変換] タブを選択して、[PNP ID 変換] リストを開きます。このリストには、現在既知のカスタム PnP ID マッピングが含まれます。



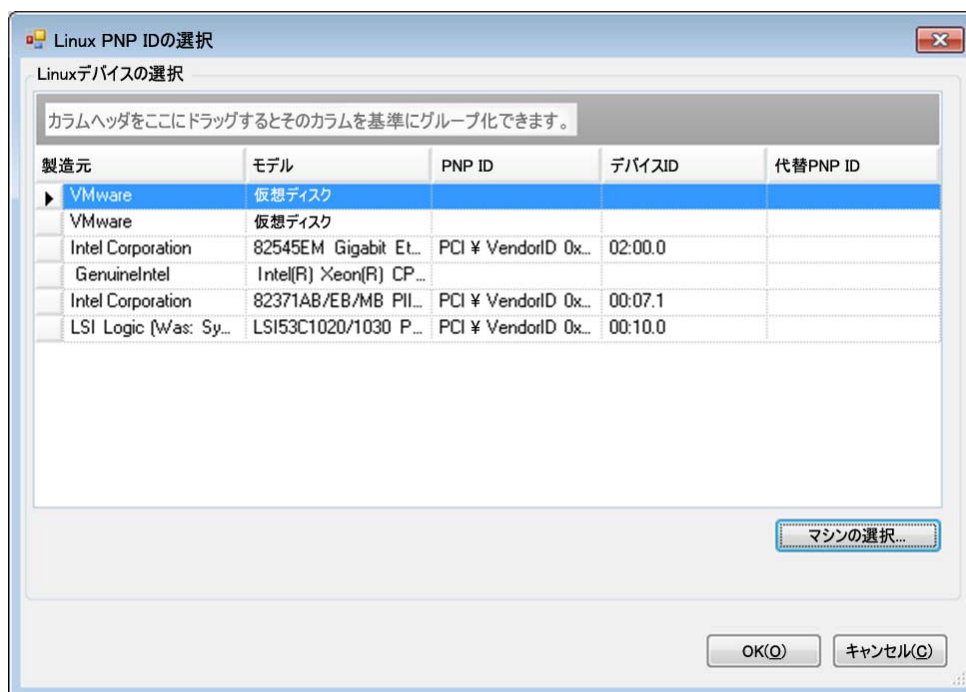
- 3 リストページで、*[追加]* をクリックして、*[PNP ID マッピングの作成]* ダイアログボックスを表示します。



- 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]* ダイアログボックスを開きます。



- 4b2** ダイアログボックスで、[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] ダイアログボックス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] ダイアログボックスにそれを表示します。

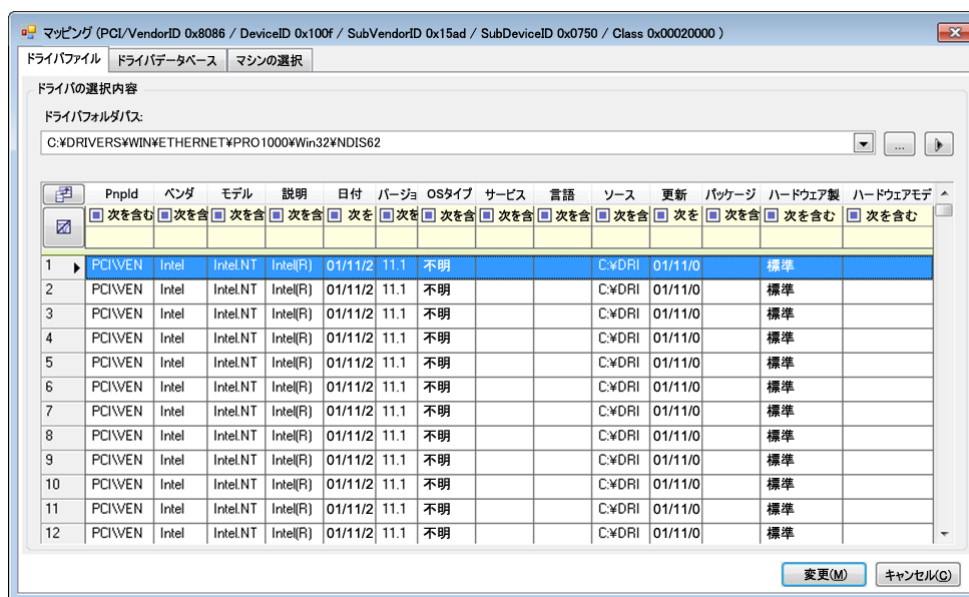
5 [Windows PNP ID] フィールドに、Windows PnP ID を追加します。

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)。

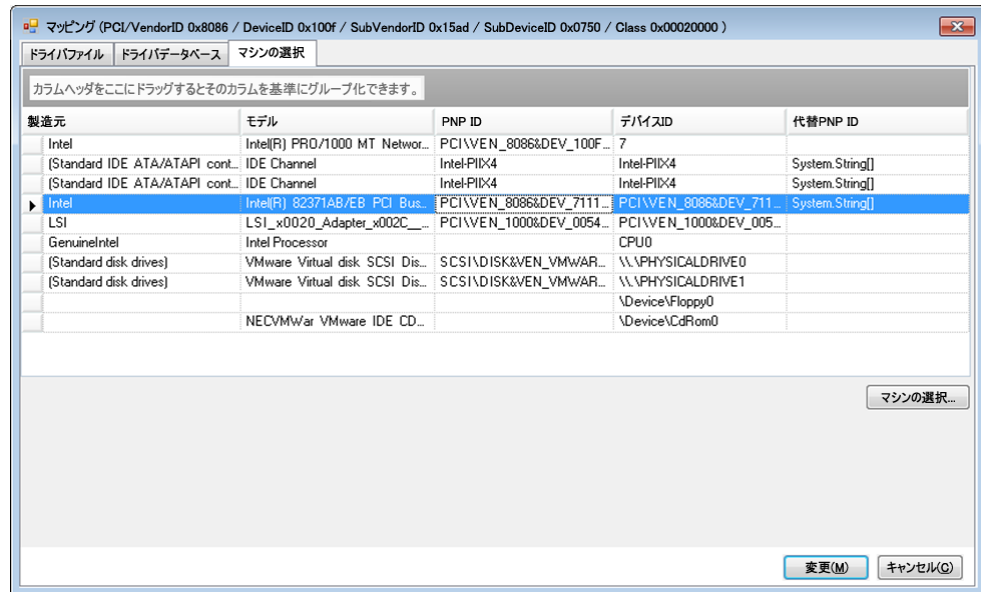
- ◆ [ドライバファイル] タブで、Windows ドライバファイル(つまり、*inf 拡張子のファイル)を参照して選択し、目的の PnP ID を選択して、[変更] をクリックします。



- ◆ [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。

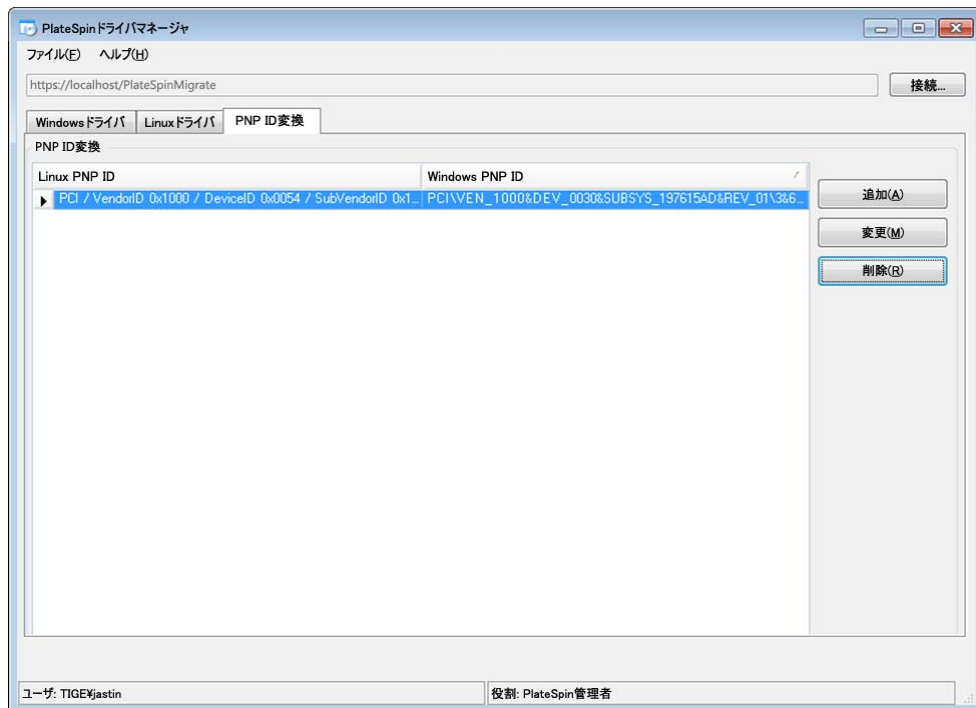


- ◆ [マシンの選択] タブで、[マシンの選択] をクリックし、ライブディスクバリを使用して検出された Windows マシンのリストからマシンを選択し、[OK] をクリックしてそのデバイスを表示し、目的の PnP ID を選択して、[変更] をクリックします。



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] ダイアログボックスで、正しい Linux PnP ID および正しい Windows PnP が選択されていることを確認し、[OK] をクリックして、PlateSpin Driver Manager の [PNP ID 変換] ページを表示します。



- 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、(確認ダイアログボックスが表示された後に) 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] ダイアログボックスを開きます。

7b [103 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 トラブルシューティング

- ◆ 107 ページのセクション 8.1 「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)」
- ◆ 111 ページのセクション 8.2 「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)」
- ◆ 111 ページのセクション 8.3 「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)」
- ◆ 112 ページのセクション 8.4 「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」
- ◆ 114 ページのセクション 8.5 「診断レポートの生成および表示」
- ◆ 115 ページのセクション 8.6 「ワークロードを削除しています」
- ◆ 115 ページのセクション 8.7 「保護後のワークロードのクリーンアップ」
- ◆ 118 ページのセクション 8.8 「PlateSpin Forge データベースの縮小」

8.1 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。109 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">◆ 109 ページの「DCOM の接続性のトラブルシューティング」◆ 110 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。108 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実行してください。
“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せん。 <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権限が制限される場合、ナレッジベースの記事 7920862 (https://www.netiq.com/support/kb/doc.php?id=7920862) で説明してある手順に従います。
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。110 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、110 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、起動モードを自動的に設定します。 ◆ 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、起動タイプを自動的に設定します。

この項では、次の情報についても説明します。

- ◆ 108 ページのセクション 8.1.1 「[接続性テストの実行](#)」
- ◆ 110 ページのセクション 8.1.2 「[ウイルス対策ソフトウェアの無効化](#)」
- ◆ 110 ページのセクション 8.1.3 「[ファイル / 共有権限およびアクセスの有効化](#)」

8.1.1 接続性テストの実行

- ◆ 109 ページの「[ネットワークの接続性テスト](#)」
- ◆ 109 ページの「[WMI の接続性テスト](#)」
- ◆ 109 ページの「[DCOM の接続性のトラブルシューティング](#)」
- ◆ 110 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。

44 ページの「VMware 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 44 ページの「VMware Client プログラムのダウンロード」44 ページの「VMware 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 サーバマシン上で、[DCOM Configuration (DCOM 設定)] 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 (25 ページの「保護ネットワークにわたるアクセスおよび通信の要件」を参照)。

8.1.2 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、WMI とリモートレジストリに関連する PlateSpin Forge の機能の一部を時々ブロックすることがあります。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、ワークロードでウイルス対策サービスを最初に無効化しなければならないことがあります。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。

8.1.3 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。
44 ページの「VMware 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。

8.2 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、25 ページの「保護ネットワークにわたるアクセスおよび通信の要件」を参照してください。</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、80 ページの「ワークロードの資格情報向けのガイドライン」を参照してください。</p>

8.3 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。112 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。107 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。

8.3.1 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` (Windows 2003/XP の場合) または `seccedit /refreshpolicy machine_policy /enforce` (Windows 2000 の場合) を使用して直ちにポリシーをリフレッシュします。

8.4 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
<i>[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。</i>	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の場合)	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。	<p>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。</p> <pre>ping ip-t (ip は、Forge VM の IP アドレスで置き換え)。</pre> <p>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。</p> <p>33 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。</p>
<p>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</p> <p>または</p> <p>3725 接続できません</p>	<p>ポートが開いてリッスンしていることを確認します。</p> <p>ワークロード上で netstat -ano を実行します。</p> <p>ファイアウォールを確認します。</p> <p>レプリケーションを再試行します。</p>
<p>コントローラの接続が確立されていません</p> <p>レプリケーションが <i>[仮想マシンの制御の取得]</i> 手順で失敗する。</p>	<p>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。</p> <p>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。</p> <p>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。</p>

レプリケーションジョブが開始しない (0% でスタック) このエラーには複数の原因があり、それぞれに固有の解決策があります。

- ◆ 認証を有効にしたローカルプロキシを使用している環境では、プロキシをバイパスするか適切な権限を追加してこの問題を解決します。詳細については、[ナレッジベースの記事 20339 \(https://www.netiq.com/support/kb/doc.php?id=7920339\)](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権限が制限される場合、[ナレッジベースの記事 7920862 \(https://www.netiq.com/support/kb/doc.php?id=7920862\)](https://www.netiq.com/support/kb/doc.php?id=7920862) で説明してある手順に従います。

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。[112 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。

8.5 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、[\[診断を生成\]](#) リンクをクリックします。

The screenshot shows the 'コマンド詳細' (Command Details) page for a replication job. The job is 'DI-SLES11.platespin.com' and is currently in the 'データのコピー' (Data Copy) step, which is 83% complete. The overall status is '実行しています' (Running). A red box highlights the '診断を生成' (Generate Report) link in the bottom right corner of the job details section.

しばらくすると、ページがリフレッシュされ [\[生成された診断\]](#) リンクの上に [\[表示\]](#) リンクが表示されます。

- 2 [\[表示\]](#) をクリックします。

現在のコマンドに関する包括的な診断情報を含む新しいページが表示されます。

- 3 診断ページを保存し、技術サポートに連絡をする際に準備してください。

8.6 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。

8.7 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。

8.7.1 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 ブロックベースの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。

コンポーネント 削除手順

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。

8.7.2 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">◆ pkill -9 ofxcontrollerd◆ pkill -9 ofxjobexec◆ 次のように、OFX コントローラ RPM パッケージを削除します。 rpm -e ofxcontrollerd◆ ワークロードのファイルシステムで、/usr/lib/ofx ディレクトリを内容ごと削除します。
--------------	--

コンポーネント 削除手順

ブロックレベル
のデータ転送ソ
フトウェア

1. ドライバがアクティブであるかどうかを確認します。

```
lsmod | grep blkwatch
```

ドライバが引き続きメモリにロードされている場合、結果には以下と類似する行が含まれるはずですが。

```
blkwatch_7616 70924 0
```

2. (条件付き) ドライバがロードされている場合、メモリからそれを削除してください。

```
rmmod blkwatch_7616
```

3. 次のブートシーケンスからドライバを削除します。

```
blkconfig -u
```

4. 次のディレクトリを内容と共に削除することにより、ドライバファイルを削除します。

```
/lib/modules/[Kernel_Version]/Platespin
```

5. 次のファイルを削除します。

```
/etc/blkwatch.conf
```

LVM スナップ
ショット

進行中のレプリケーションで使用される LVP スナップショットは、*volume_name*-PS-snapshot 規則にしたがって名前が付けられます。たとえば、LogVol01 ボリュームには、LogVol01-PS-snapshot という名前が付けられます。

LVM スナップショットを削除するには：

1. 次のいずれかの方法を使用して、必要なワークロードでスナップショットのリストを生成します。

- ◆ 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が。

- または -

- ◆ 必要な Linux ワークロードで、次のコマンドを実行しすべてのボリュームおよびスナップショットのリストを表示します。

```
# lvdisplay -a
```

2. 削除するスナップショットの名前とロケーションを書き留めます。

3. 次のコマンドを使用してスナップショットを削除します。

```
lvremove snapshot_name
```

ビットマップ
ファイル

保護されているボリュームごとに、ボリュームのルートで該当する *.blocks_bitmap* ファイルを削除します。

ツール

ソースワークロード上で、*/sbin* から次のファイルを削除します。

- ◆ *bmaputil*
 - ◆ *blkconfig*
-

8.8 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。

用語集

アプライアンスホスト . [コンテナ](#) を参照してください。

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。

イベント . ワークロード保護ライフサイクルをとお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。

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。

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。

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。

保護コントラクト . 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。

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。

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。

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。

複製 . 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 (すべてのワークロードデータが「ブランク」のフェールオーバー VM に転送される)、または増分レプリケーションとして実行できます ([増分 \(2\)](#) を参照) 。

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。

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。

テストフェールオーバー . 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。

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。

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。