ユーザガイド

Novell® PlateSpin Forge®

3.1

2011 年 10 月

www.novell.com

保証と著作権

米国 Novell, Inc. およびノベル株式会社は、本書の内容または本書を使用した結果について、いかなる保証、表明または約束も行っていません。また、本書の商品性、および特定の目的への適合性について、いかなる明示的または黙示的な保証も否認し、排除します。また、本書の内容は予告なく変更されることがあります。

米国 Novell, Inc. およびノベル株式会社は、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っていません。また、ノベル製ソフトウェアの商品性、および特定の目的への適合性について、いかなる明示的または黙示的な保証も否認し、排除します。米国 Novell, Inc. およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。

本契約の下で提供される製品または技術情報はすべて、米国の輸出管理規定およびその他の国の輸出関連法規の制限を受けます。お客様は、すべての輸出規制を遵守し、製品の輸出、再輸出、または輸入に必要なすべての許可または等級を取得するものとします。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。ノベル製ソフトウェアの輸出に関する詳細については、Novell International Trade Services の Web ページ (http://www.novell.com/info/exports/) を参照してください。弊社は、お客様が必要な輸出承認を取得しなかったことに対し如何なる責任も負わないものとします。

Copyright © 2009-2011 Novell, Inc. All rights reserved. 本ドキュメントの一部または全体を無断で複写転載することは、その形態を問わず禁じます。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

オンラインマニュアル : 本製品とその他の Novell 製品の最新のオンラインマニュアルにアクセスするには、Novell マニュアルの Web ページ (http://www.novell.com/documentation) を参照してください。

Novell の商標

Novell の商標一覧については、「商標とサービスの一覧 (http://www.novell.com/company/legal/trademarks/tmlist.html)」を参照してください。

サードパーティ資料

サードパーティの商標は、それぞれの所有者に帰属します。

目次

このガイドについて 9

1 製品の概要 11

1.1 PlateSpin Forge について . . . 11
1.2 サポートされる構成 . . . 11
1.2.1 サポートされるワークロード . . . 11
1.3 セキュリティとプライバシー . . . 12
1.3.1 送信中のワークロードデータのセキュリティ . . . 12
1.3.2 クライアント / サーバ通信のセキュリティ . . . 13
1.3.3 資格情報のセキュリティ . . . 13
1.3.4 ユーザ権限および認証 . . . 13
1.4 パフォーマンス . . . 13
1.4.1 製品パフォーマンスの特性 . . . 13
1.4.2 データ圧縮 . . . 14
1.4.3 帯域幅制限 . . . 14
1.4.4 RPO、RTO、および TTO の仕様 . . . 14

2 アプリケーション環境設定 17

2.1 製品ライセンス . . . 17
2.1.1 ライセンスアクティベーションコードの取得 . . . 17
2.1.2 オンラインライセンスのアクティベーション . . . 17
2.1.3 オフラインライセンスのアクティベーション . . . 18
2.2 ユーザ権限および認証の設定 . . . 18
2.2.1 PlateSpin Forge のユーザ権限および認証について . . . 18
2.2.2 PlateSpin Forge のアクセスおよび権限の管理 . . . 20
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 . . . 22
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 . . . 23
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 . . . 23
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 . . . 25
2.4 PlateSpin Forge のデフォルトオプションの設定 . . . 26
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 . . . 26
2.4.2 PlateSpin Forge の国際バージョンの言語設定 . . . 28
2.4.3 XML 環境設定パラメータを通じた製品動作の構成 . . . 29
2.4.4 システム変更を適用するための PlateSpin Forge サーバの再起動 . . . 31

3 アプライアンスのセットアップと
メンテナンス 33

3.1 アプライアンスのネットワーキングの設定 . . . 33
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 . . . 33
3.2 PlateSpin Forge の移動およびその IP アドレスの再割り当て . . . 34
3.2.1 Forge アプライアンスバージョン 2 の移設手順 . . . 34
3.2.2 Forge アプライアンスバージョン 1 の移設手順 . . . 38
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 . . . 39
3.3.1 Forge での SAN ストレージの使用 . . . 39
3.3.2 Forge への SAN LUN の追加 . . . 40
3.4 PlateSpin Forge アプライアンスの保守 . . . 41
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 . . . 41
3.5 PlateSpin Forge のアップグレード . . . 45

3.5.1 アップグレードを開始する前に . . . 45
3.5.2 アップグレードタスクのサマリ . . . 46
3.5.3 Forge アップグレード手順 . . . 46

4 業務の常時稼働 49

4.1 PlateSpin Forge Web Client の起動 . . . 49
4.2 PlateSpin Forge Web Client の要素 . . . 50
4.2.1 ナビゲーションバー . . . 51
4.2.2 ビジュアルサマリパネル . . . 51
4.2.3 タスクおよびイベントパネル . . . 52
4.3 ワークロードおよびワークロードコマンド . . . 52
4.3.1 ワークロードの保護と回復のコマンド . . . 53
4.4 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 . . . 54
4.5 PlateSpin Forge の複数インスタンスの管理 . . . 54
4.5.1 PlateSpin Forge 管理コンソールの使用 . . . 54
4.5.2 PlateSpin Forge 管理コンソールについて . . . 55
4.5.3 PlateSpin Forge のインスタンスの管理コンソールへの追加 . . . 56
4.5.4 管理コンソールでのカードの管理 . . . 56
4.6 ワークロードとワークロード保護のレポートの作成 . . . 56

5 ワークロードの保護 59

5.1 ワークロードの保護と回復の基本ワークフロー . . . 59
5.2 ワークロードを保護対象として追加 . . . 60
5.3 保護詳細の設定およびレプリケーションの準備 . . . 61
5.3.1 ワークロード保護の詳細 . . . 62
5.4 ワークロード保護の開始 . . . 64
5.5 フェールオーバー . . . 65
5.5.1 障害検出 . . . 65
5.5.2 フェールオーバーの実行 . . . 66
5.5.3 回復ワークロードおよびフェールオーバー機能のテスト . . . 66
5.6 フェールバック . . . 67
5.6.1 仮想マシンへの自動化されたフェールバック . . . 67
5.6.2 物理マシンへの半自動化されたフェールバック . . . 70
5.6.3 仮想マシンへの半自動化されたフェールバック . . . 71
5.7 高度なワークロード保護に関するトピック . . . 71
5.7.1 Windows クラスタの保護 . . . 71
5.7.2 Xen-on-SLES 上で並行仮想化された VM への Linux フェールバック . . . 72

6 物理マシンを操作するための補助ツール 77

6.1 PlateSpin アナライザを使用したワークロードの分析 (Windows) . . . 77
6.2 デバイスドライバの管理 . . . 78
6.2.1 Windows システム用のデバイスドライバのパッケージ化 . . . 79
6.2.2 Linux システム用のデバイスドライバのパッケージ化 . . . 79
6.2.3 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 . . . 80

7 ワークロード保護の要点 83

7.1 ワークロードの資格情報向けのガイドライン . . . 83
7.2 転送方法 . . . 84
7.3 保護ティア . . . 84
7.4 復旧ポイント . . . 86
7.5 初期レプリケーション方法 (フルおよび差分) . . . 86

7.6 サービスおよびデーモンの制御 87
7.7 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) 88
7.8 ボリューム 88
7.9 ネットワーキング 90
7.10 フェールバック用に物理マシンを PlateSpin Forge に登録 90
7.10.1 ターゲットの物理マシンの登録 91

8 トラブルシューティング 93

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). 93
8.1.1 接続性テストの実行 94
8.1.2 ウイルス対策ソフトウェアの無効化 96
8.1.3 ファイル / 共有権限およびアクセスの有効化 96
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). 97
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). . . 97
8.3.1 グループポリシーおよびユーザ権限 98
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 98
8.5 診断レポートの生成および表示 99
8.6 保護後のワークロードのクリーンアップ 100
8.6.1 Windows ワークロードのクリーンアップ 100
8.6.2 Linux ワークロードのクリーンアップ 101
8.6.3 ワークロードを削除しています 102

用語集 103

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。

- 11 ページの第 1 章「製品の概要」
- 49 ページの第 4 章「業務の常時稼働」
- 59 ページの第 5 章「ワークロードの保護」
- 77 ページの第 6 章「物理マシンを操作するための補助ツール」
- 83 ページの第 7 章「ワークロード保護の要点」
- 93 ページの第 8 章「トラブルシューティング」
- 103 ページの 「用語集」

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下部にある［ユーザコメント］機能を使用するか、Novell マニュアルフィードバックサイト (http://www.novell.com/documentation/feedback.html) を通じてご意見をお寄せください。

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 3 オンラインマニュアルの Web サイト (http://www.novell.com/documentation/platespin_forge_3) 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 Protect 10 オンラインマニュアルの Web サイト (http://www.novell.com/documentation/platespin_protect_10) 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。

- Novell ユーザフォーラム (http://forums.novell.com): 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。
- Novell ナレッジベース (http://www.novell.com/support): 詳しい技術情報の記事集です。

技術サポート

- 電話 (北米): +1-877-528-3774 (1 87 PlateSpin)

- 電話 (グローバル): +1-416-203-4799
- 電子メール : support@platespin.com

PlateSpin 技術サポートの Web サイト (http://www.platespin.com/support) もご利用いただけます。

製品の概要 1

- 11 ページのセクション 1.1「PlateSpin Forge について」
- 11 ページのセクション 1.2「サポートされる構成」
- 12 ページのセクション 1.3「セキュリティとプライバシー」
- 13 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。

- 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
- 障害時に迅速にワークロードを回復
- 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

- 11 ページのセクション 1.2.1「サポートされるワークロード」

1.2.1 サポートされるワークロード

PlateSpin Forge では、Windows と Linux の両方のワークロードをサポートします。

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
Windows 7	Windows 7 Home Edition はサポートされていません
Windows Server 2008 R2	ドメインコントローラ (DC) システムおよび Small Business Server (SBS) エディションを含む
Windows Server 2008	ドメインコントローラ (DC) システムおよび Small Business Server (SBS) エディションを含む

オペレーティングシステム	備考
Windows Vista	Business、Enterprise、および Ultimate のエディション、SP1 以降
Windows Server 2003	ドメインコントローラ (DC) システムおよび Small Business Server (SBS) エディションを含む
Windows XP Professional	
Windows Server 2000	
Windows クラスタ	

サポートされる国際バージョン (Windows): フランス語、ドイツ語、日本語、繁体字中国語、および簡体字中国語

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
Open Enterprise Server 2、SP2 および SP3
Oracle Enterprise Linux (OEL) 5.3、5.4
SUSE Linux Enterprise Server (SLES) 9、10、11
Red Hat Enterprise Linux (RHEL) 4、5

サポートされる国際バージョン (Linux): これらの Linux システムのすべての国際バージョンがサポートされます。

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。

- 12 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」
- 13 ページのセクション 1.3.2「クライアント / サーバ通信のセキュリティ」
- 13 ページのセクション 1.3.3「資格情報のセキュリティ」
- 13 ページのセクション 1.3.4「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。

各ワークロード保護に対して暗号化を有効または無効にすることができます。その際に、暗号化はワークロード保護の詳細のパラメータになります。62 ページの 「ワークロード保護の詳細」を参照してください。

1.3.2 クライアント / サーバ通信のセキュリティ

PlateSpin Forge Server と PlateSpin Forge Web Client の間のデータ転送は、HTTP（デフォルト）または HTTPS（ハイパーテキスト転送プロトコルセキュア）のいずれかを使用するように設定できます。

クライアントとサーバ間のデータ転送の安全性を確保するためには、Forge VM で SSL を有効化し、サーバ環境設定を更新して変更を反映させ（31 ページの 「SSL 通信を有効化するパラメータ」を参照）、サーバ URL の指定時に HTTPS を使用してください。

1.3.3 資格情報のセキュリティ

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

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

1.3.4 ユーザ権限および認証

PlateSpin Forge は、ユーザの役割に基づいて包括的かつ安全なユーザの承認と認証のメカニズムを備えており、ユーザが実行できるアプリケーションのアクセスと操作を制御します。18 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

- 13 ページのセクション 1.4.1「製品パフォーマンスの特性」
- 14 ページのセクション 1.4.2「データ圧縮」
- 14 ページのセクション 1.4.3「帯域幅制限」
- 14 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。

データ圧縮は保護ごとまたは保護ティアごとに設定できます。84 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、ワークロードの保護中にソースからターゲットへの直接通信で消費される帯域幅の使用可能量をユーザが制御できるようにします。つまり、ユーザは各保護スケジュールに対するスループットレートを指定できます。これによって、レプリケーショントラフィックによる運用ネットワークの輻輳を回避し、PlateSpin Forge Server の全体的な負荷を軽減することが可能です。

帯域幅制限は、ワークロード保護の通信先の保護ティアのパラメータです。84 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、およびネットワーク速度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 (ワークロードレプリカをオンラインにし、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。65 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。

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。

さまざまな状況でテスト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取得し、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。56 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。

アプリケーション環境設定 2

- 17 ページのセクション 2.1「製品ライセンス」
- 18 ページのセクション 2.2「ユーザ権限および認証の設定」
- 23 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」
- 26 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。

- 17 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」
- 17 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」
- 18 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 プロキシは、オンラインアクティベーション中に失敗する可能性があります。HTTP プロキシ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 クライアントで、*［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］*を選択します。

3 ハードウェア ID を使用して、PlateSpin 製品アクティベーション Web サイト (http://www.platespin.com/productactivation/ActivateOrder.aspx) でライセンスキーファイルを作成します。この処理には、注文時に指定したユーザ名、パスワード、電子メールアドレス、および受け取ったアクティベーションコードも必要です。

4 ファイルのパスを入力するか、該当する場所を参照して、*［有効にする］*をクリックします。

ライセンスキーファイルが保存され、Forge アプライアンス製品がこのファイルに基づいて有効になります。

2.2 ユーザ権限および認証の設定

- 18 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」
- 20 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」
- 22 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 :** 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。
- **ワークロード保護のオペレータ :** 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。

ユーザが PlateSpin Forge に接続しようとすると、ブラウザを介して提供される資格情報が IIS によって検証されます。ユーザがワークロード保護の役割のメンバーに含まれない場合は、接続が拒否されます。ユーザが Forge VM のローカル管理者である場合、このアカウントは暗黙的にワークロード保護管理者とみなされます。

表 2-1 *ワークロード保護の役割および権限の詳細*

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

さらに、PlateSpin Forge ソフトウェアでは、どの OS レベルユーザが 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OSレベルのユーザを追加する。
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。

2.2.2 PlateSpin Forge のアクセスおよび権限の管理

- 20 ページの 「PlateSpin Forge サーバ管理インタフェースへのアクセス」
- 20 ページの 「PlateSpin Forge ユーザの追加」
- 21 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」
- 21 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、21 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。

20 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。21 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。19 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。20 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。22 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。20 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。21 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 Client 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。

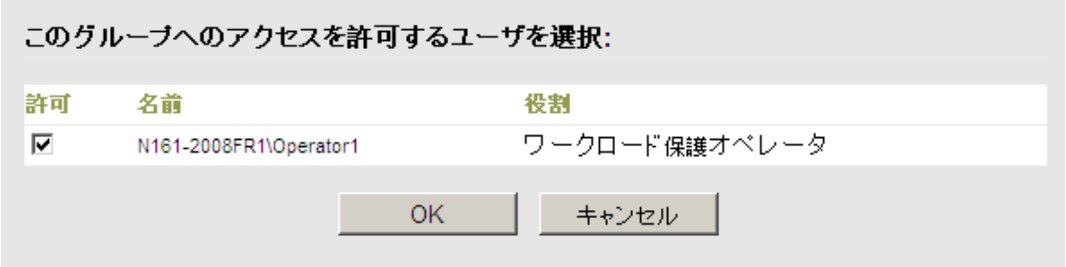
   ［セキュリティグループ］ページが開きます。

3 *［セキュリティグループの作成］*をクリックします。

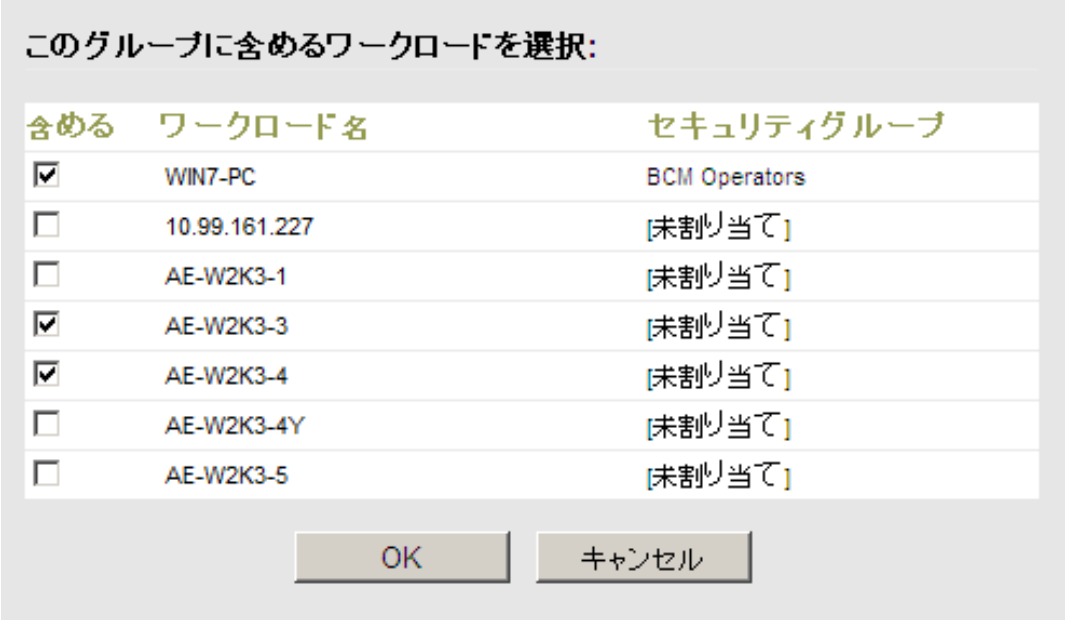
4 *［セキュリティグループ名］*フィールドにセキュリティグループ名を入力します。

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。

   OS レベルのユーザとして追加したばかりの PlateSpin Forge ユーザは、Forge VM に追加しようとしてもユーザインタフェースで直ちに使用できない場合があります。この場合、まず［*ユーザアカウントの更新*］をクリックします。



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



この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

- 23 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」
- 25 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」

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
すべてのワークロード	ping (ICMP エコー要求と応答) 機能。	
Windows のすべてのワークロード	.NEt Framework バージョン 2.0 以降	

ワークロードタイプ	前提条件	必要なポート
Windows 7、 Windows Server 2008、 Windows Vista	◆ 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)。 ◆ 次の受信規則が有効で［許可］に設定された Windows ファイアウォール : ◆ 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) これらのファイアウォール設定は、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) を使用して構成されます。基本的な Windows Firewall ユーティリティ (firewall.cpl) を使用しても同じ結果を実現できます。例外のリストで［*ファイルとプリンタの共有*］項目を選択します。	TCP 3725 NetBIOS 137 ～ 139 SMB (TCP 139、445 および UDP 137、138) TCP 135/445

ワークロードタイプ	前提条件	必要なポート
Windows Server 2000、 Windows XP、 Windows NT 4	◆ インストールされた Windows Management Instrumentation (WMI) Windows NT Server のデフォルトインストールには、WMI は含まれません。Microsoft の Web サイトから WMI Core を入手します。WMI がインストールされていない場合、ワークロードの検出が失敗します。 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。検出プロセス中に問題が発生した場合、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検出プロセスに対してのみ一時的に開くことを検討します。 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。 ◆ 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)	TCP 3725 NetBIOS 137 ～ 139 SMB (TCP 139、445 および UDP 137、138) TCP 135/445
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由の保護

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 Forge Server:** サーバの web.config 設定ファイルで、そのホストに割り当てられた追加 IP アドレスを次の通り、記録します。31 ページの 「PlateSpin Forge Server の追加 IP アドレスのパラメータ（NAT 設定）」を参照してください。
- **ソースのワークロード :** (69 ページ) フェールバック詳細 (ワークロードを VM へ) の回復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る、フェールバックのみに対してサポートされます。
- **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場合は、検出 / 登録パラメータで、パブリック (または外部)IP アドレスを指定してください。

2.4 PlateSpin Forge のデフォルトオプションの設定

- 26 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」
- 28 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」
- 29 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製品動作の構成」
- 31 ページのセクション 2.4.4「システム変更を適用するための PlateSpin Forge サーバの再起動」

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。

- 26 ページの 「SMTP 設定」
- 26 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」
- 28 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）設定を行うには、PlateSpin Forge Web Client 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 設定を行うには :

1. PlateSpin Forge Web クライアントで、*[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*、オプションの*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。SMTP 設定を参照してください。

2 PlateSpin Forge Web Client 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。

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。 保護スケジュールの状態［*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。 保護スケジュールの状態が［*一時停止済み*］ではないワークロードに適用されます。
増分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に失敗しました	
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。
フェールオーバーが完了しました	
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	次の場合に生成されます。 ◆ スケジュールされた増分レプリケーションの期限中に、レプリケーションを手動で一時停止した。 ◆ 手動でトリガしたレプリケーションの実行中に、スケジュールされた増分レプリケーションの実行をシステムが試みた。 ◆ 十分な空きディスク容量がターゲットにないと、システムが判断した。
完全レプリケーションが実行されませんでした	上記の［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。

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。SMTP 設定を参照してください。
2. PlateSpin Forge Web Client で、*［設定］* > *［電子メール］* > *［レプリケーションレポート設定］* の順にクリックします。
3. ［*レプリケーションレポートの有効化*］オプションを選択します。
4. ［*レポートの繰り返し*］の項で、［*設定*］をクリックし、レポートで必要な繰り返しパターンを指定します。
5. ［*受信者*］の項の［*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。
6. （オプション）*［アクセス URL の保護］* セクションで、PlateSpin Forge Server 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については、56 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 Client およびこれらいずれかの言語の統合ヘルプを使用するには、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。49 ページの 「PlateSpin Forge Web Client 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と、Web サーバエラーが発生することあります。適切に動作するようにするには、ブラウザの環境設定を使用して特定の中国語 (たとえば、Chinese [zh-cn] または Chinese [zh-tw]) を追加します。文化的な区別のない Chinese [zh] という言語は使用しないでください。

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。

   41 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)、*［言語］* (Windows Server 2003) または *［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製品動作の構成

PlateSpin Forge Server の動作における一部のアスペクトは、Forge VM のホームディレクトリに保存されている *.config ファイル内の環境設定パラメータによって制御されます。

通常の状況では、PlateSpin Support が推奨しない限り、これらの設定を変更しないでください。この項では、一般的な使用事例を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 *.config 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 テキストエディタを使用して *.config ファイルを開きます。

3 *.config ファイルの中で必要なパラメータを探し、引用符 ("") で囲まれている値を変更します。引用符は削除しないでください。このセクションに表示された許容値または PlateSpin Support が推奨する許容値を使用します。

4 *.config ファイルを保存して閉じます。

5 PlateSpin Forge サーバを再起動します。31 ページの 「システム変更を適用するための PlateSpin Forge サーバの再起動」を参照してください。

次のトピックでは、PlateSpin Forge Server の動作に影響する、一般的に使用されるファイルと値に関して説明されています。

- 30 ページの 「WAN 接続を使用した転送を最適化するパラメータ」
- 31 ページの 「SSL 通信を有効化するパラメータ」
- 31 ページの 「レプリケーションの停止ウィンドウを強制するためのパラメータ」
- 31 ページの 「PlateSpin Forge Server の追加 IP アドレスのパラメータ（NAT 設定）」

WAN 接続を使用した転送を最適化するパラメータ

WAN を経由する転送を最適化するには、次の設定を使用します。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が影響されます。

- 環境設定ファイル： productinternal.config
- ロケーション： Program Files\PlateSpin Forge Server\Web

更新手順については、29 ページの 「XML 環境設定パラメータを通じた製品動作の構成」を参照してください。

注：これらの値を変更すると、ローカルのギガビット LAN レプリケーションの速度に悪影響をもたらす可能性があります。

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 *productinternal.config 内のデフォルトおよび最適化された設定パラメータ*

パラメータ	デフォルト値	最適化された値
fileTransferThreadcount ファイルベースのデータ転送用に開かれた TCP 接続の数を制御します。	2	4 ～ 6
fileTransferMinCompressionLimit パケットレベルの圧縮のしきい値をバイトで指定します。	0(無効)	最大 65536 (64 KB)
fileTransferCompressionThreadsCount パケットレベルのデータ圧縮に使用されるスレッド数を制御します。圧縮が無効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。	2	該当なし
fileTransferSendReceiveBufferSize 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。 ((リンク速度 (Mbps)/8)* 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 bytes	0 (8192 バイト)	最大 5242880 (5MB)

SSL 通信を有効化するパラメータ

製品をインストールした*後*でSSL を有効化したサーバと PlateSpin Forge Web Client の間の SSL 通信を有効化するには、次の設定を使用します。製品のインストール時にサーバホスト上で SSL が有効になっていた場合は、この作業は必要ありません。

- **環境設定ファイル：** Platespin.Config
- **ロケーション：** Program Files\PlateSpin Forge Server\Configs
- **値：**次を

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

  次のように変更します。

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

更新手順については、29 ページの 「XML 環境設定パラメータを通じた製品動作の構成」を参照してください。

レプリケーションの停止ウィンドウを強制するためのパラメータ

- **環境設定ファイル：** PlateSpin.Protection.Scheduler.Service.dll.config
- **ロケーション：** Program Files\PlateSpin Forge Server\services\PlateSpinService\Plugins
- **値：** このパラメータは、次の 2 つの値から構成されます。
  - Workload_Scheduling_Blackout_Window_Start: 一時停止の開始時間の時刻を定義します。次の形式を使用してください。

    HH:MM:SS (HH 00-23、MM 00-59、SS 00-59)
  - Workload_Scheduling_Blackout_Window_Length: 一時停止期間の長さを定義します。次の形式を使用してください。

    HH:MM:SS (HH 00-23、MM 00-59、SS 00-59)

更新手順については、29 ページの 「XML 環境設定パラメータを通じた製品動作の構成」を参照してください。

PlateSpin Forge Server の追加 IP アドレスのパラメータ（NAT 設定）

NAT が有効化されている環境全体における通信を目的として PlateSpin Forge Server の追加アドレスを記録するには、次の設定を使用します。

- **環境設定ファイル：** Web.config
- **ロケーション：** Program Files\PlateSpin Forge Server\Web
- **値：** <add key="AlternateServerAddresses" value="" />

  次のように、セミコロンで区切って、追加の IP アドレスを加えてください。

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

2.4.4 システム変更を適用するための PlateSpin Forge サーバの再起動

1. PlateSpin Forge サーバの bin\RestartPlateSpinServer サブディレクトリに移動します。

41 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 RestartPlateSpinServer.exe 実行可能ファイルをダブルクリックします。

確認を求めるコマンドプロンプトウィンドウが開きます。

3 「Y」と入力し、<Enter> キーを押します。

アプライアンスのセットアップとメンテナンス 3

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。

- 33 ページのセクション 3.1「アプライアンスのネットワーキングの設定」
- 34 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」
- 39 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」
- 41 ページのセクション 3.4「PlateSpin Forge アプライアンスの保守」
- 45 ページのセクション 3.5「PlateSpin Forge のアップグレード」

3.1 アプライアンスのネットワーキングの設定

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

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

3.1.1 アプライアンスホストのネットワーキングの設定

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

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

- 34 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」
- 38 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。

- 34 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)」
- 36 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)

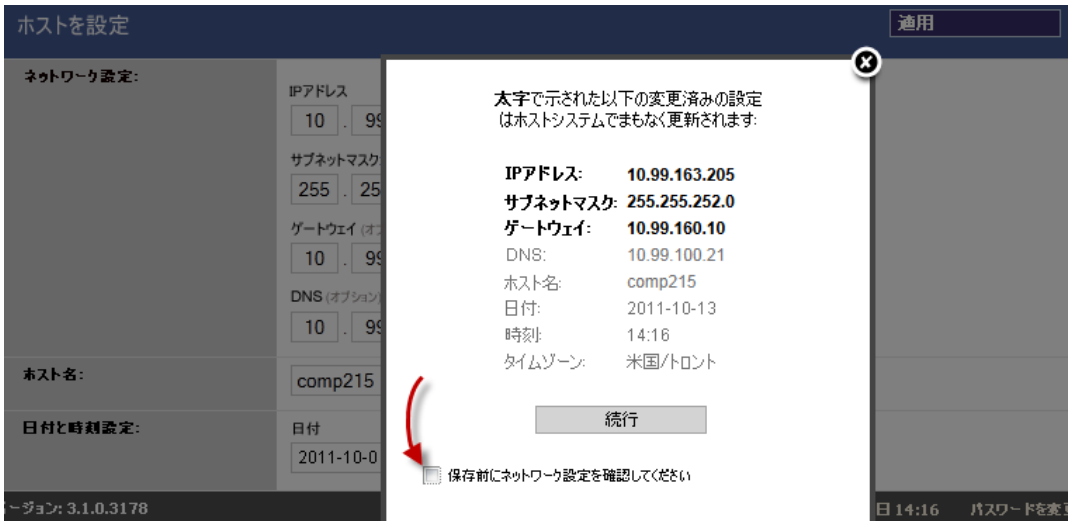
1 すべてのレプリケーションを一時停止します。上記のステップ 1a とステップ 1b を参照してください。

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。

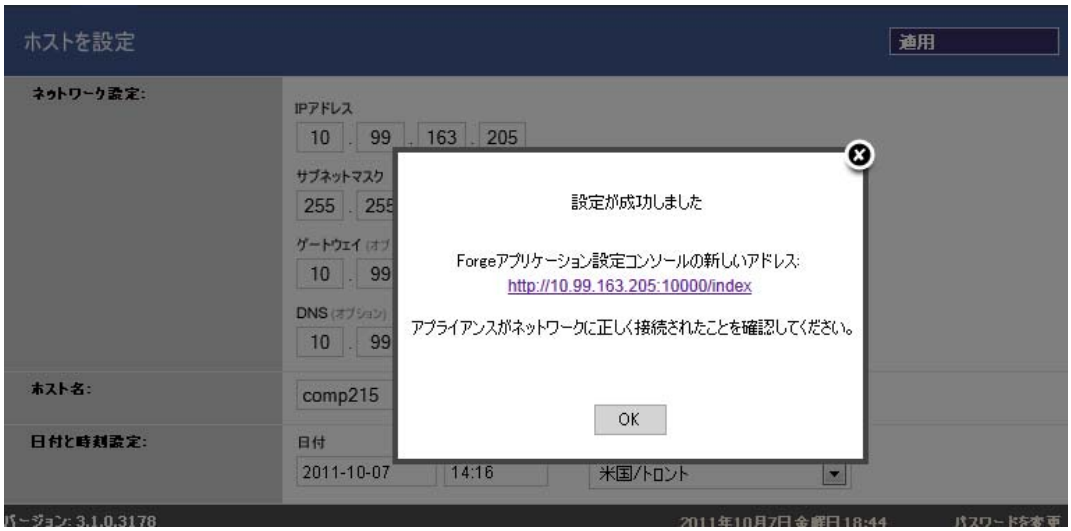
3 forgeuser アカウントを使用してログインして、*[ホストの設定]* をクリックします。

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。43 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 および関連づ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。42 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 Client 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。34 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。43 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 と関連するパスワード)。

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。

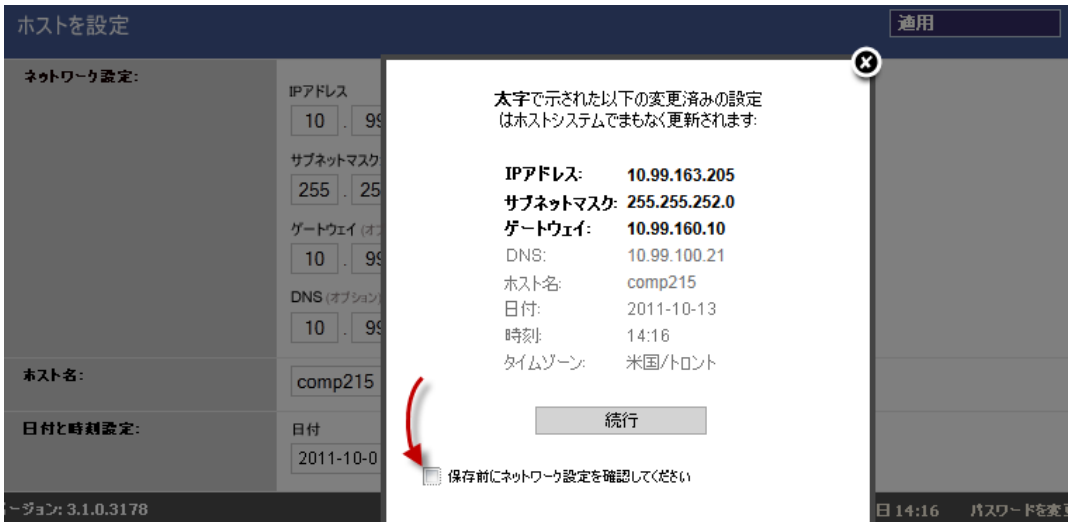
『*導入ガイド*』の「Forge ACC アプライアンスバージョン 2 の設定手順 (http://www.novell.com/documentation/platespin_forge_3/getstart/data/bk2otgs.html#bwkc1x9)」を参照してください。

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。

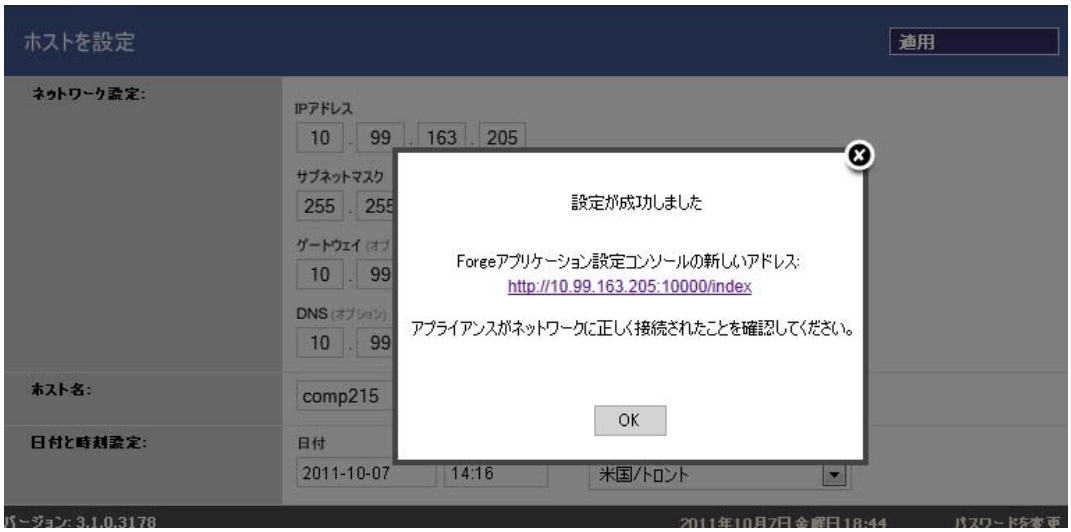
6 forgeuser アカウントを使用してログインして、*[ホストの設定]* をクリックします。

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、次に *[適用]* をクリックします。

12 設定が正しことを確認し、*[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。42 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 Client を起動し、コンテナを更新します (*[設定]* > *[コンテナ]* > *次に*をクリックしてください)。

---

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。43 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の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。

- 39 ページのセクション 3.3.1「Forge での SAN ストレージの使用」
- 40 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）
- Fujitsu (http://www.fujitsu.com) および Fujitsu Siemens (http://www.fujitsu-siemens.com)
- HP (http://www.hp.com)
- Hitachi (http://www.hitachi.com) および Hitachi Data Systems (http://www.hds.com)（FC のみ）
- IBM (http://www.ibm.com)
- NEC (http://www.nec.com)（FC のみ）
- Network Appliance (NetApp) (http://www.netapp.com)
- Nihon Unisys (http://www.unisys.com)（FC のみ）
- Pillar Data (http://www.pillardata.com)（FC のみ）
- Sun Microsystems (http://www.sun.com)
- Xiotech (http://www.xiotech.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 (42 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。

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。

- 41 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。

- 42 ページの 「VMware Client プログラムのダウンロード」
- 42 ページの 「VMware Client の起動および Forge 管理 VM へのアクセス」
- 43 ページの 「Forge 管理 VM の起動とシャットダウン」
- 44 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」
- 44 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」
- 45 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) 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。

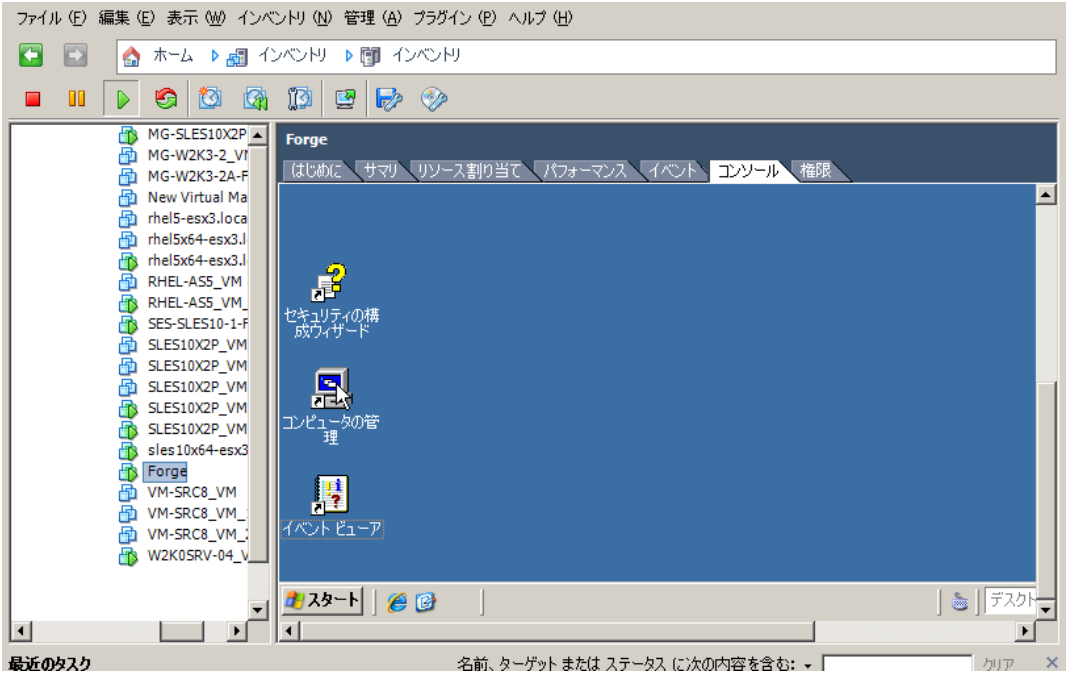
VMware Client の起動および Forge 管理 VM へのアクセス

1 *［スタート］*＞*［すべてのプログラム］*＞*［VMWare］*＞*［VMware vSphere Client］*＞*［Virtual Infrastrucure 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、ルート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 Management 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。42 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。42 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。回復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（86 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。42 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。42 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。44 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。44 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

この項では、PlateSpin Forge アプライアンスのアップグレードついて説明します。

- 45 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」
- 46 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」
- 46 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。42 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. 最新の 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。

49 ページの 「PlateSpin Forge Web Client 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。43 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。44 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 1.x アプライアンスの場合、VM ハードディスク 2 の独立モードを無効にします。

4a 左の［Inventory (インベントリ)］パネルで、［Forge Management VM (Forge 管理 VM)］を右クリックして、*［Edit Settings (設定の編集)］* を選択します。

［Virtual Machine Properties (仮想マシンプロパティ)］ウィンドウが表示されます。

4b *［Hardware (ハードウェア)］* タブで、*［Hard Disk 2 (ハードディスク 2)］* をクリックします。

4c 右側で、*［独立］* チェックボックスを選択解除します。

5 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。

   5a 最新の Microsoft .NET Framework ソフトウェアをインストールします。Forge 3 には、少なくとも Microsoft .NET Framework 3.5 SP1 (http://www.microsoft.com/downloads/details.aspx?FamilyId=AB99342F-5D1A-413D-8319-81DA479AB0D7) が必要です。

   5b 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。

   5c Forge 管理 VM を再起動します。

6 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。

注 : インストールプログラムでは、アップグレードプロセス中にエクスポートしたデータが自動的に再インポートされないことがあります。このような状況では、PlateSpin.ImportExport.exe ユーティリティを使用して、サーバホストの \Documents and Settings\< ユーザプロファイル >\Application Data\PlateSpin ディレクトリからこのデータを回復してください。ナレッジベースの記事 7921084 (http://www.novell.com/support/viewContent.do?externalId=7921084) を参照してください。

---

7 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。

8 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。

業務の常時稼働

4

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。

- 49 ページのセクション 4.1「PlateSpin Forge Web Client の起動」
- 50 ページのセクション 4.2「PlateSpin Forge Web Client の要素」
- 52 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」
- 54 ページのセクション 4.4「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」
- 54 ページのセクション 4.5「PlateSpin Forge の複数インスタンスの管理」
- 56 ページのセクション 4.6「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 Client 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 Client を介して行われます。

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。
- **Fiefox:** *［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。

サポートされている言語で PlateSpin Forge Web Client および統合ヘルプを使用する方法については、28 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」を参照してください。

PlateSpin Forge Web Client 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。

   http://<*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 が有効な場合は、URL に https を使用します。

4.2 PlateSpin Forge Web Client の要素

PlateSpin Forge Web Client 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 Client 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。

- **ナビゲーションバー：** PlateSpin Forge Web Client のほとんどのページ上に表示されます。
- **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。
- **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。
- **最新ニュースパネル：**製品や関連更新プログラムに関する情報が、RSS を通じて提供されます。PlateSpin Forge ニュースフィードを購読するには、*[RSS]*をクリックします。

次の各項目では、詳細が表示されます。

- 51 ページのセクション 4.2.1「ナビゲーションバー」
- 51 ページのセクション 4.2.2「ビジュアルサマリパネル」
- 52 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。52 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。56 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 :** 84 ページの 「保護ティア」を参照してください。
  - **許可 :** 18 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):** 26 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):** 17 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アプライアンスで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)。26 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 Client を実行しているホストのタイムゾーンとは異なる可能性があります。クライアントウィンドウの右下にサーバの日時が表示されます。

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 VM を作成します。
レプリケーションの実行	ソースワークロードのレプリケーションを指定されたパラメータに従って開始します。
増分の実行	ワークロード保護スケジュール以外で、ソースからターゲットに変更されたデータを個別に転送します。
スケジュールの一時停止	保護を中断し、保護ワークロードからのデータ転送を一時停止します。
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、回復ワークロードをコンテナ内の隔離された環境でオンラインにします。
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回復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回復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 / 展開	フェールオーバー操作に引き続き、回復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 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

アプリケーション内から protection.webservices API を使用することで、ワークロード保護機能をプログラムで利用できます。Web サービスをサポートするあらゆるプログラミング言語またはスクリプト言語を使用できます。

http://<*hostname* | *IP_address*>/protection.webservices

<*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。

ワークロード保護の一般的な操作を記述するには、Python で記述された参考のサンプルをガイドとして使用してください。Microsoft Silverlight アプリケーションとそのソースコードも、参照目的で提供されています。

4.5 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 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。

- 54 ページのセクション 4.5.1「PlateSpin Forge 管理コンソールの使用」
- 55 ページのセクション 4.5.2「PlateSpin Forge 管理コンソールについて」
- 56 ページのセクション 4.5.3「PlateSpin Forge のインスタンスの管理コンソールへの追加」
- 56 ページのセクション 4.5.4「管理コンソールでのカードの管理」

4.5.1 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。

   http://<*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。

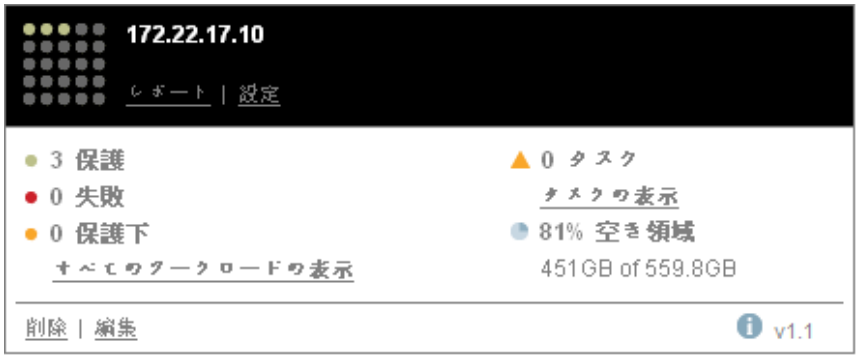
   コンソールのデフォルトの［ダッシュボード］ページが表示されます。

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

4.5.2 PlateSpin Forge 管理コンソールについて

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 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。

4.5.3 PlateSpin Forge のインスタンスの管理コンソールへの追加

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

PlateSpin 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、*[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. Forge VM の URL を指定します。HTTP プロトコルと HTTPS プロトコルの両方がサポートされています。
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 Forge 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。

4.5.4 管理コンソールでのカードの管理

管理コンソールでは、PlateSpin Forge 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 PlateSpin Forge 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。

   特定のアプライアンスカードがダッシュボードから削除されます。

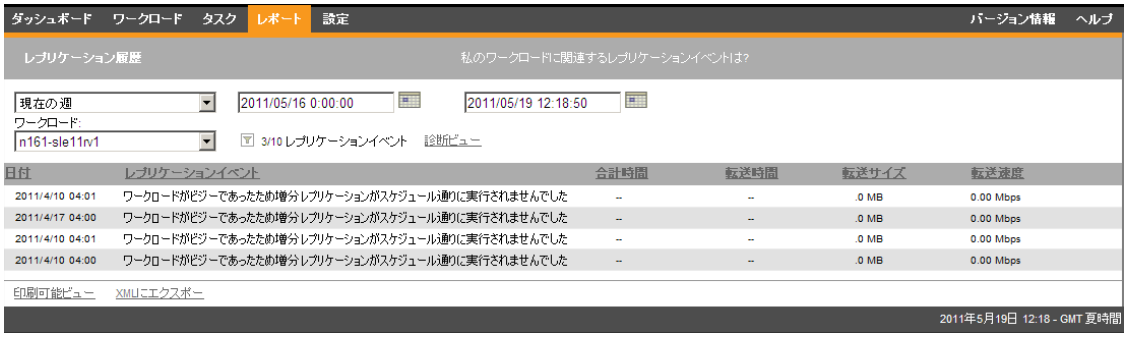
4.6 ワークロードとワークロード保護のレポートの作成

PlateSpin Forge では、長期間にわたってワークロード保護スケジュール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*



レポートを生成するには：

1. PlateSpin Forge Web Client で *［Reports (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。

ワークロードの保護 5

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。

- 59 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」
- 60 ページのセクション 5.2「ワークロードを保護対象として追加」
- 61 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」
- 64 ページのセクション 5.4「ワークロード保護の開始」
- 65 ページのセクション 5.5「フェールオーバー」
- 67 ページのセクション 5.6「フェールバック」
- 71 ページのセクション 5.7「高度なワークロード保護に関するトピック」

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 準備ステップ :

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。

11 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。

23 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 (http://www.novell.com/support/viewContent.do?externalId=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 (http://www.novell.com/support/viewContent.do?externalId=7005872) を参照してください。

- (オプション) レプリケーションごとにソースワークロード上で実行させる任意のカスタムスクリプトを決定し、用意します。

  88 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 ワークロードを追加します。

  60 ページの 「ワークロードを保護対象として追加」を参照してください。

3 保護の詳細を設定し、レプリケーションを準備します。

  61 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 ワークロード保護スケジュールを開始します。

  64 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 (オプション) 増分を手動で実行します。

6 (オプション) フェールオーバー機能をテストします。

  回復ワークロードおよびフェールオーバー機能のテストを参照してください。

7 フェールオーバーを実行します。

  65 ページの 「フェールオーバー」を参照してください。

8 フェールバックを実行します。

  67 ページの 「フェールバック」を参照してください。

9 (オプション) フェールバック後にワークロードを再保護します。

手順 1、8、および 9 を除いて、これらの手順は［ワークロード］ページのワークロードコマンドとして表されています。52 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。

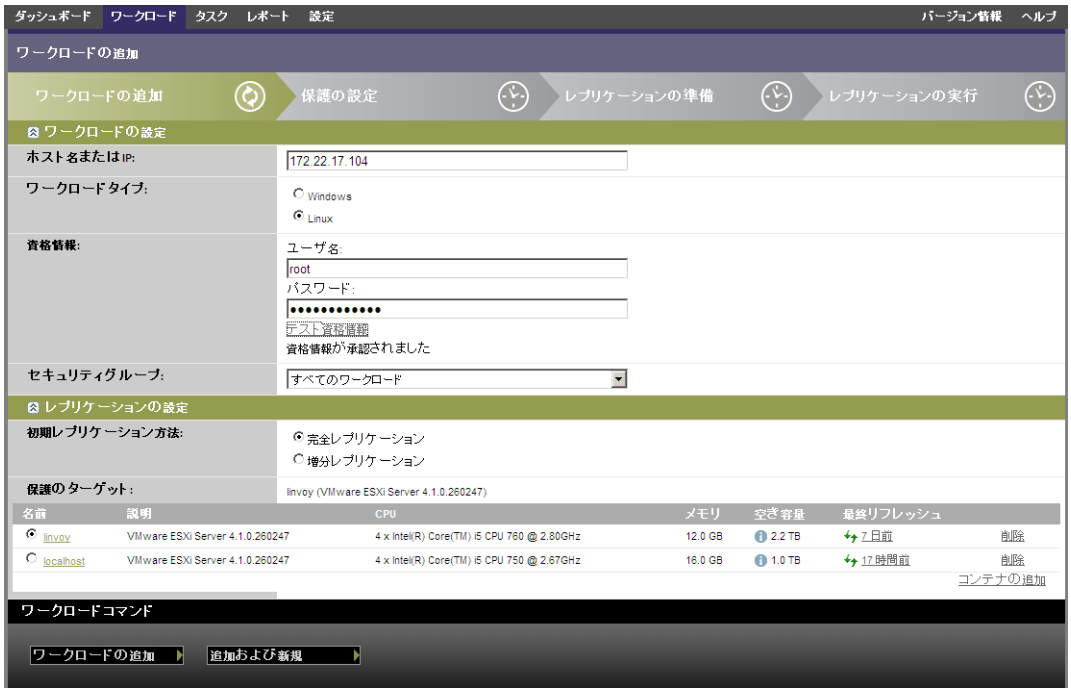
5.2 ワークロードを保護対象として追加

1 準備のために必要な手順を実行します。

  59 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 Client に［ワークロードの追加］ページが表示されます。



3 必要なワークロードの詳細を指定します。

- **ワークロードの設定 :** ワークロードのホスト名または IP アドレス、オペレーティングシステム、管理者レベルの資格情報、およびワークロードが割り当てられるセキュリティグループを指定します。22 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。

  必要な資格情報のフォーマットを使用します (83 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。

- **レプリケーション設定 :** 必要なレプリケーション設定を選択します。86 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 *[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。終了したら、*[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上に表示されます。

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 (59 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。60 ページの 「ワークロードを保護対象として追加」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。

PlateSpin Forge Web Client にワークロードの［保護の詳細］ページが表示されます。

3 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。62 ページの 「ワークロード保護の詳細」を参照してください。

4 検証エラーがあれば修正します。

5 ［*Save*］をクリックします。

代わりに、［*Save & Prepare (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*

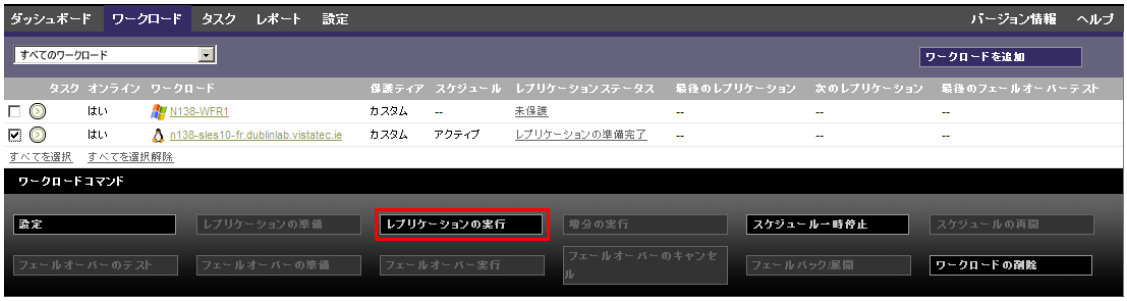
パラメータセット (設定)	詳細
ティア	現在の保護が使用する保護ティアを示します。84 ページの 「保護ティア」を参照してください。

パラメータセット (設定)	詳細
複製	**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。12 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。 **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。84 ページの 「転送方法」を参照してください。 **ソース資格情報 :** ワークロードへのアクセスに必要です。83 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。 **CPU の数 :** 回復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。 **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。90 ページの 「ネットワーキング」を参照してください。 **復旧ポイントデータストア :** 復旧ポイント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。86 ページの 「復旧ポイント」を参照してください。 **保護ボリューム :** 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。次の保護を選択することもできます。 ◆ Linux ワークロード : 論理ボリュームとボリュームグループ ◆ OES 2 ワークロード : EVMS ボリューム 88 ページの 「ボリューム」を参照してください。 **[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、そのディスクで必要なディスクスペースのみを消費します。 **レプリケーション中のサービス / デーモン状態の停止 :** レプリケーション時に自動停止する Windows サービスまたは Linux デーモンを選択できます。87 ページの 「サービスおよびデーモンの制御」を参照してください。
フェールオーバー	**VM メモリ :** フェールオーバー VM に割り当てられるメモリの量を指定できます。 **Hostname and Domain/Workgroup affiliation (ホスト名およびドメイン / ワークグループの加入):** 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。 **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。90 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。87 ページの 「サービスおよびデーモンの制御」を参照してください。
フェールオーバーの準備	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。90 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。90 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。87 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。



次の後に［レプリケーションの実行］コマンドを実行できます。

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

続行する準備ができたら、次の手順に従います。

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

2 *［実行］*をクリックします。

   PlateSpin 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：保護の通信先が設定された後：

- 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. コントラクトを削除します。2。必要に応じてボリュームサイズを変更します。3. 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 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* VM コンテナ内の回復ワークロードによって引き継がれる動作がフェールオーバーと呼ばれます。

- 65 ページのセクション 5.5.1「障害検出」
- 66 ページのセクション 5.5.2「フェールオーバーの実行」
- 66 ページのセクション 5.5.3「回復ワークロードおよびフェールオーバー機能のテスト」

5.5.1 障害検出

事前設定した回数だけワークロードの検出が失敗した場合、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 62 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。26 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 *[フェールオーバーの実行]* コマンドに進みます。66 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 Client 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*

5.5.2 フェールオーバーの実行

回復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。62 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］ペイン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。オプションの *［フェールオーバーの準備］* コマンドを使用し、保存したフェールオーバーの設定を回復ワークロードに適用し、完全フェールオーバーより先にそのワークロードを起動することができます。*［フェールオーバーの準備］* 操作を別途実行し、運用ワークロードに障害が実際に発生したかを確認します。これにより、完全な *［フェールオーバー］* コマンドを実行する際の時間が短縮されます。
- ［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］* イベントの適切なコマンドのハイパーリンクをクリックします。図 5-1 を参照してください。
- VMware vSphere Client を使用して手動で回復ワークロードを起動します。この方法を使用する場合は、vSphere Client のスナップショットマネージャを使用してスナップショット（回復ポイント）を選択します。

  44 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。

  注 : 手動でフェールオーバーを実行すると、システムによってワークロードのレプリケーション時に保存されたフェールオーバー設定が適用されます。

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、回復ワークロードに適用する復旧ポイントを選択します (86 ページの 「復旧ポイント」を参照)。*［実行］* をクリックし、進行状況を監視します。終了すると、ワークロードのレプリケーション状態が *［ライブ］* を示すはずです。

計画された障害復旧の訓練の一環として回復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、66 ページの 「回復ワークロードおよびフェールオーバー機能のテスト」を参照してください。

5.5.3 回復ワークロードおよびフェールオーバー機能のテスト

PlateSpin Forge には、フェールオーバー機能および回復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回復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回復ワークロードに適用されます (テストフェールオーバーの 62 ページの 「ワークロード保護の詳細」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 (86 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 回復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回復ワークロードにアクセスします。

42 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]* タスクが完了すると、PlateSpin Forge は、回復ワークロードに適用された一時的な設定を破棄し、テスト以前の状態に保護を戻します。

5.6 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。

フェールバック方法は、ターゲットインフラの修理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。

- 67 ページのセクション 5.6.1「仮想マシンへの自動化されたフェールバック」
- 70 ページのセクション 5.6.2「物理マシンへの半自動化されたフェールバック」
- 71 ページのセクション 5.6.3「仮想マシンへの半自動化されたフェールバック」

5.6.1 仮想マシンへの自動化されたフェールバック

などのコンテナは、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。

プラットフォーム	メモ
vSphere 4.1 での VMware DRS クラスタ	◆ 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） ◆ クラスタでは、ESX 4.1、ESXi 4.1、または両方を使用できます
VMware ESX 3.5、4.0、4.1、4.1 Update 1	
VMware ESXi 3.5、4.0、4.1、4.1 Update 1	すべての 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。

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 / 展開]* をクリックします。

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 :** 回復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 (83 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。86 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、ホストレベルの資格情報を使用してサポートされる VM ホストをインベントリします。

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。69 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 Client 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	**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。84 ページの 「転送方法」を参照してください。 **Failback Network (フェールバックのネットワーク):** フェールバックのトラフィックを、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。90 ページの 「ネットワーキング」を参照してください。 **VM Datastore (VM データストア):** ターゲットワークロード向けにフェールバックコンテナに関連するデータストアを選択できます。 **Volumes to Copy (コピーするボリューム):** ターゲット上で再作成し、特定のデータストアに割り当てるボリュームを選択できます。 **停止するサービス / デーモン :** フェールバック時に自動的に停止される Windows サービスまたは Linux デーモンを選択できます。87 ページの 「サービスおよびデーモンの制御」を参照してください。 **ソースの代替アドレス :** 該当する場合は、ソースワークロードの追加 IP アドレスの入力を受け付けます。25 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。

パラメータセット (設定)	詳細
ワークロード	***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す。 **VM メモリ :** 必要な RAM をターゲットワークロードに割り当てることができます。 **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。 **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。 **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。87 ページの 「サービスおよびデーモンの制御」を参照してください。
フェールバック後	**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。 ◆ ***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。 ◆ ***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。

5.6.2 物理マシンへの半自動化されたフェールバック

次の手順に従って、フェールオーバー後、ワークロードを物理マシンにフェールバックします。この物理マシンは元のインフラまたは新しいインフラのいずれかにできます。

1. 必要な物理マシンを PlateSpin Forge Server に登録します。90 ページの 「フェールバック用に物理マシンを PlateSpin Forge に登録」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。77 ページの 「PlateSpin アナライザを使用したワークロードの分析 (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。78 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 / 展開］*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 :** 回復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 (83 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。

       86 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。

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。

5.6.3 仮想マシンへの半自動化されたフェールバック

このフェールバックタイプは、本来サポートされている VMware コンテナ以外の VM ターゲットについて、物理マシンへの半自動化されたフェールバックと同様のプロセスに従います。VM への半自動化されたフェールバックは、次のターゲットプラットフォームに対してサポートされています。

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、11 上で実行される Xen
- Microsoft Hyper-V

5.7 高度なワークロード保護に関するトピック

- 71 ページのセクション 5.7.1「Windows クラスタの保護」
- 72 ページのセクション 5.7.2「Xen-on-SLES 上で並行仮想化された VM への Linux フェールバック」

5.7.1 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スケジュールが継続します。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 (59 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。

5.7.2 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 (xmps) 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。

- 72 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」
- 74 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 Linux ブート ISO をターゲットの Xen_SLES サーバにコピーします。90 ページの 表 7-2 「ターゲット物理マシン向けの ISO ブートイメージ」を参照してください。
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す*］オプションをインストールします。

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、ソースマシンと等しいか、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。70 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 PV

  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」をタイプし、<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
kjournald 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
kjournald 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るには

[DB]$ poweroff

7 XEN/SLES サーバに root としてログインし、PlateSpin Linux ブート ISO 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 Linux ブート ISO のマウントを解除します。

```
# 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 Linux ブート ISO をターゲットの Xen/SLES サーバにコピーします。90 ページの 表 7-2 「ターゲット物理マシン向けの ISO ブートイメージ」を参照してください。

2 XEN/SLES サーバに root としてログインして、次のとおり、PlateSpin Linux ブート ISO としてマウントします。

```
# 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/booxofxx2p.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す。

5 フェールバックプロシージャを完了してください。70 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、72 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。

物理マシンを操作するための補助ツール

6

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。

- 77 ページのセクション 6.1「PlateSpin アナライザを使用したワークロードの分析 (Windows)」
- 78 ページのセクション 6.2「デバイスドライバの管理」

6.1 PlateSpin アナライザを使用したワークロードの分析 (Windows)

ワークロードのフェールバックまたは操作を物理マシンに対して実行する前に、PlateSpin アナライザ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 6-1 *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 6-2 *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。

6.2 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。77 ページの「PlateSpin アナライザを使用したワークロードの分析 (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。

- 79 ページのセクション 6.2.1「Windows システム用のデバイスドライバのパッケージ化」
- 79 ページのセクション 6.2.2「Linux システム用のデバイスドライバのパッケージ化」
- 80 ページのセクション 6.2.3「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」

6.2.1 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。80 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

6.2.2 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、Linux の制御の取得 ISO ブートイメージに含まれているカスタムユーティリティを使用できます。90 ページの 表 7-2 「ターゲット物理マシン向けの ISO ブートイメージ」を参照してください。

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。80 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。

6.2.3 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。

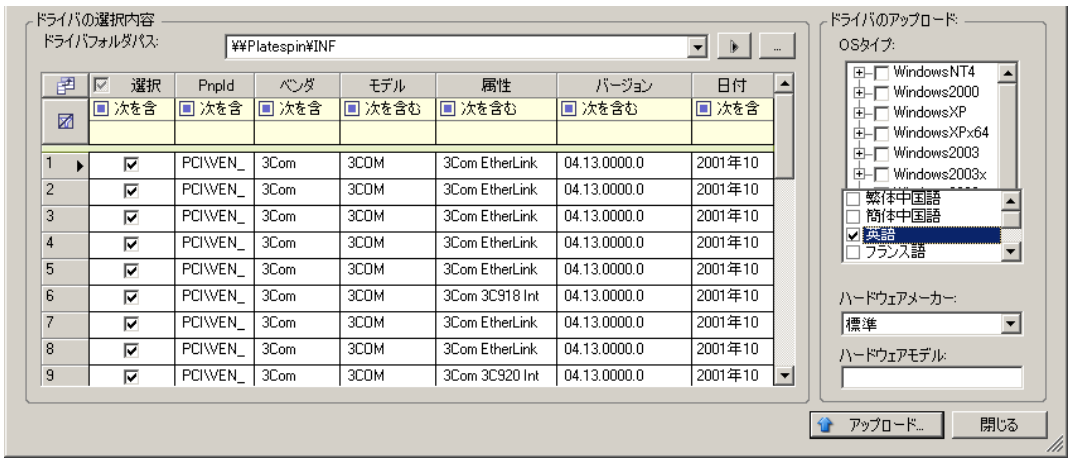
- 80 ページの 「デバイスドライバのアップロード手順 (Windows)」
- 81 ページの 「デバイスドライバのアップロード手順 (Linux)」

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。

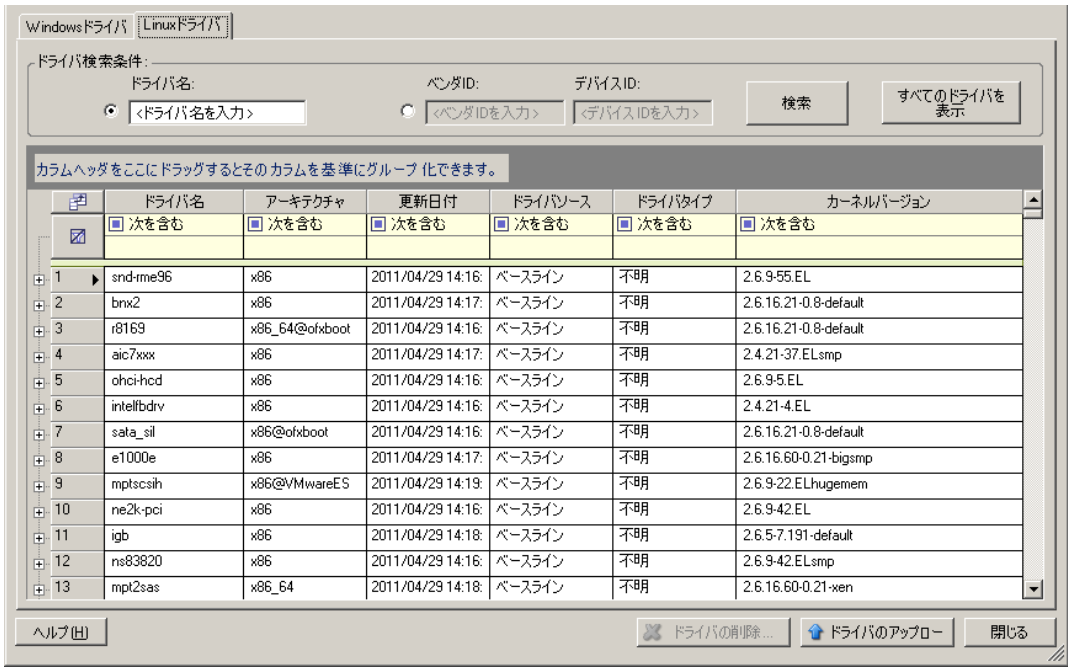
4 *[アップロード]* をクリックし、プロンプトが表示されたら選択内容を確認します。

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。

ワークロード保護の要点 7

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。

- 83 ページのセクション 7.1「ワークロードの資格情報向けのガイドライン」
- 84 ページのセクション 7.2「転送方法」
- 84 ページのセクション 7.3「保護ティア」
- 86 ページのセクション 7.4「復旧ポイント」
- 86 ページのセクション 7.5「初期レプリケーション方法 (フルおよび差分)」
- 87 ページのセクション 7.6「サービスおよびデーモンの制御」
- 88 ページのセクション 7.7「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)」
- 88 ページのセクション 7.8「ボリューム」
- 90 ページのセクション 7.9「ネットワーキング」
- 90 ページのセクション 7.10「フェールバック用に物理マシンを PlateSpin Forge に登録」

7.1 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 7-1 *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。 ◆ ドメインメンバーのマシン用 : *authority\principal* ◆ ワークグループメンバーのマシン用 : *hostname*
Windows クラスタ	ドメイン管理者の資格情報	クラスタの仮想 IP アドレスを使用します。個々の Windows クラスタノードの IP アドレスを使用すると、このノードは一般的な (クラスタ非対応) Windows ワークロードとして検出されます。
Linux のすべてのワークロード	ルートレベルのユーザ名とパスワード	ルート以外のアカウントは、sudo を使用できるよう適切に設定する必要があります。ナレッジベースの記事 7920711 (http://www.novell.com/support/viewContent.do?externalId=7920711) を参照してください。
VMware ESX 4.1	管理者の役割を持つ ESX アカウント。	ESX Server 4.1 が Windows ドメイン認証用に設定されている場合は、Windows ドメイン資格情報を使用することもできます。

7.2 転送方法

転送方法とは、データがソース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。

- **ブロックレベル：** 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 はドライバを使用してソースワークロード上の変更を監視します。
  - **Windows システム：** Windows システムの場合、PlateSpin Forge は、Microsoft Volume Snapshot Service (VSS) を活用するブロックベースのコンポーネントを、VSS をサポートするアプリケーションやサービスとともに使用します。ブロックベースのコンポーネントの自動インストールでは、ソースワークロードの再起動を必要とします (ブロックレベルデータ転送をおこなう Windows クラスタを保護するときに、再起動は必要ありません)。ワークロード保護の詳細を設定する際に、コンポーネントのインストールの時期を選択できます。同様に、ワークロードを削除する場合、ブロックベースのコンポーネントをアンインストールするには再起動が必要になります。
  - **Linux システム：** Linux システムのブロックレベルの転送を行うために、PlateSpin Forge は、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可能な場合に使用します（これはデフォルトであり、推奨されるオプション）。ナレッジベースの記事 7005872 (http://www.novell.com/support/viewContent.do?externalId=7005872) を参照してください。

    PlateSpin Forge 配布に含まれる 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 配布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 (http://www.novell.com/support/viewContent.do?externalId=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、連続性の影響はなく、介入が必要ありません。
- **ファイルレベル：** データがファイルごとに複製されます (Windows のみ)。VSS の有無に関係なくサポートされます。

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。

7.3 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 Client 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、次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、この機能の実装を考慮してください。 ブラックアウト期間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。 **メモ：**ブラックアウト期間の開始時には、未完了のレプリケーションがあれば中止します。
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。14 ページの「データ圧縮」を参照してください。 次のいずれかのオプションを選択します。［*高速*］はソースの最小 CPU リソースを消費しますが、圧縮比率は下げ、［*最大*］はソースの最大 CPU リソースを消費しますが、圧縮比率は高くなります。［*最適*］は、中程度で、推奨オプションです。
帯域幅制限	これらの設定は、帯域幅制限を制御します。14 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。86 ページの 「復旧ポイント」を参照してください。値を 0 にすると、この機能が無効になります。
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。

7.4 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。

保護されたワークロードごとに、最大 32 個の復旧ポイントを保持できます。

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、44 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。

7.5 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。

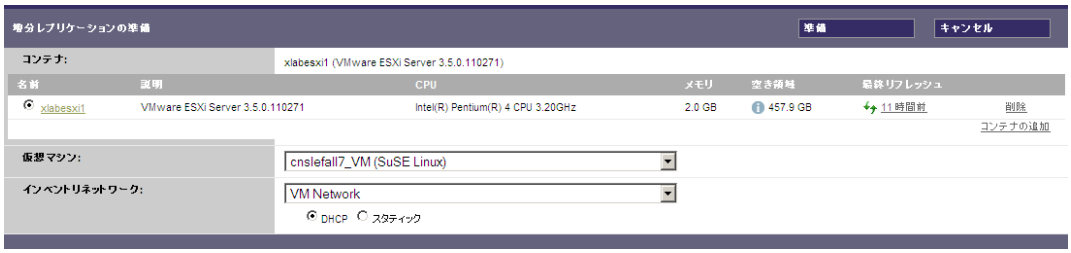
- **フル :** フルボリューム転送は、運用ワークロードからそのレプリカ (回復ワークロード) に対して、またはフェールオーバーワークロードからその元となる仮想インフラまたは物理的インフラに対して実施されます。
- **増分 :** 選択された操作のソースからターゲットに対して差分のみが転送されます。この時、ソースとターゲットは同様のオペレーティングシステムとボリュームプロファイルを使用している必要があります。
  - 保護時 : 運用ワークロードはアプライアンスホスト内の既存の VM と比較されます。既存の VM は次のうちの 1 つになります。
    - 以前に保護されたワークロードの回復 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)。
    - 運用サイトからリモート復旧サイトへとポータブルメディア上で物理的に移動されるワークロード VM など、アプライアンスホストに手動でインポートされる VM（VMware ESX 3.5 以降の場合のみ）。

      44 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（70 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、*［増分］*を選択すると、初期レプリケーション方法によって、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、準備することが要求されるため、

1. *［ワークロードの追加］*または *［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 Client によって［増分レプリケーションの準備］ページが表示されます。



4 必要なコンテナ、仮想マシン、および VM との通信に使用するインベントリネットワークを選択します。

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、ソース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すでにポーリングされたデータに依存します。

7.6 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、ソースワークロードを回復ワークロードにより一貫した状態で転送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。88 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 :** ターゲットワークロード上のサービス / 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ほう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。

7.7 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 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 (87 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。値がしていされない場合、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

7.8 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 Client 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、RAID、および 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非ボリュームストレージが複製され、回復ワークロードに割り当てられます。

- 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 7-1 *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*

次の図は、EVMS レイアウトが保存され、回復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 OES2 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 7-2 *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)*

7.9 ネットワーキング

PlateSpin Forge では、回復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) 回復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回復ワークロードに適用するネットワーク設定です。

7.10 フェールバック用に物理マシンを PlateSpin Forge に登録

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適切な 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。

ブート ISO イメージを使用するには、Novell ダウンロードの PlateSpin Forge エリア (http://download.novell.com/Download?buildid=C3BckY0Hp0s) からダウンロードしてください。ご使用のターゲットマシンに適したイメージを使用します。

表 7-2　ターゲット物理マシン向けの ISO ブートイメージ

ファイル名	備考
WindowsFailback.zip (WindowsFailback.iso を含む)	Windows
LinuxFailback.zip (LinuxFailback.iso を含む)	Linux システム
WindowsFailback-Cisco.zip (WindowsFailback-Cisco.iso を含む)	Cisco のハードウェア上の Windows システム
WindowsFailback-Dell.zip (WindowsFailback-Dell.iso を含む)	Dell のハードウェア上の Windows システム
WindowsFailback-Fujitsu.zip (WindowsFailback-Fujitsu.iso を含む)	Fujitsu のハードウェア上の Windows システム

必要なファイルをダウンロードしたら、ISO ファイルを解凍し、生成されたファイルを保存します。

- 91 ページのセクション 7.10.1「ターゲットの物理マシンの登録」

7.10.1 ターゲットの物理マシンの登録

1. 適切なイメージを、ターゲットをブートできるような CD に書き込むか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。

   Windows バージョンのブート CD イメージは、*[自動ネゴシエート全二重]* のみをサポートし、これによりデュプレックス設定に競合がないようにします。
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。

   (Windows のみ)［*REGISTERMACHINE*］と［*回復オプション*］コマンドボックスが開くのを待ちます。REGISTERMACHINE コマンドボックスを使用します。Recovery Console ユーティリティの詳細については、91 ページの 「Recovery Tool コマンドラインユーティリティの使用 (Windows)」を参照してください。
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、次の URL を入力してください。

   http://<*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。
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. SSL を有効化している場合は *[はい]* と入力します。有効化していない場合は *[いいえ]* と入力します。

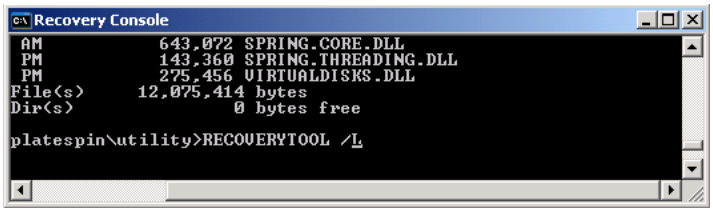
しばらくすると、物理マシンが PlateSpin Forge Web Client のフェールバックの設定で利用可能になります。

Recovery Tool コマンドラインユーティリティの使用 (Windows)

Recovery Console コマンドラインユーティリティは、物理ターゲット全体の登録プロセスを再開する必要なく、Windows デバイスドライバをターゲットの物理マシンに動的に設定することができるようにします。

このユーティリティは、Windows ブートイメージからブーツを初めて行うときに表示される 2 番目のコマンドボックスにロードされます (91 ページのステップ 3 を参照)。

Recovery Tool を使用するために、Recovery Console ウィンドウでコマンド名「RECOVERYTOOL」の後に適切なパラメータを入力します。



次を使用することができます。

- /L - ターゲット OS にインストールされた任意のドライバサービスを一覧にします
- /J - ターゲット OS にドライバを設定します

PlateSpin Forge Server またはローカルパスのいずれからドライバをダウンロードすることを指定できます。ローカルパスを使用する場合、同じデバイスに対して複数のドライバをまとめる必要があります。PlateSpin Forge Server からドライバをダウンロードする場合、ユーティリティでは、使用するドライバの指定を求められます(ドライバが複数ある場合)。

PlateSpin ブートイメージへのドライバの挿入 (Linux)

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. 必要な *.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 ファイルに含まれるカーネル 2.6.16.21-0.8-default に対して有効で、ターゲットのアーキテクチャに適していることを確認します。

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 (unmount < *マウントポイント* > コマンドを実行)。
4. 必要なドライバファイル用に別の作業ディレクトリを作成し、それらのファイルをそのディレクトリに保存します。
5. rebuildiso.shスクリプトを保存したディレクトリで、次のコマンドをルートで実行します。

   ./rebuildiso.sh –i <*ISO ファイル*> -d < *ドライバのディレクトリ* > -m i586|x86_64

   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。

トラブルシューティング 8

- 93 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)」
- 97 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)」
- 97 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)」
- 98 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」
- 99 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」
- 100 ページのセクション 8.6「保護後のワークロードのクリーンアップ」

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
The domain in the credentials is invalid or blank	このエラーは資格情報のフォーマットが不正な場合に発生します。 hostname\LocalAdmin という資格情報のフォーマットでローカル管理者アカウントを使用して検出してみてください。 または、domain\DomainAdmin という資格情報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。
Unable to connect to Windows server...Access is denied	ワークロードを追加しようとする際に、非管理者アカウントが使用されました。管理者アカウントを使用するか、このユーザを管理者グループに追加して再試行します。 このメッセージは、WMI 接続性に障害が発生したことを示す場合もあります。次の考えられる解決策について、それぞれ試してみてから 95 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。 ◆ 95 ページの 「DCOM の接続性のトラブルシューティング」 ◆ 95 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」
Unable to connect to Windows server...The network path was not found	ネットワークの接続性の障害です。94 ページの 「接続性テストの実行」で、テストを実行します。このテストが失敗した場合は、PlateSpin Forge とワークロードが同じネットワーク上にあることを確認します。ネットワークを再設定して再試行してください。

問題またはメッセージ	解決方法
"Discover Server Details {hostname}" Failed Progress: 0% Status: NotStarted	このエラーには複数の原因があり、それぞれに固有の解決策があります。 ◆ 認証を有効にしたローカルプロキシを使用している環境では、プロキシをバイパスするか適切な権限を追加します。詳細については、ナレッジベースの記事 7920339 (http://www.novell.com/support/viewContent.do?externalId=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 (http://www.novell.com/support/viewContent.do?externalId=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 Could not find file output.xml または Network path not found または (Windows クラスタの検出試行時に) Inventory failed to discover. Inventory result returned nothing.	「output.xml ファイルが見つかりませんでした」というエラーにはいくつかの理由があります。 ◆ ソース上のウイルス対策ソフトウェアが検出を妨げている場合があります。ウイルス対策ソフトウェアを無効にし、これが問題の原因かどうか判断します。96 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C$共有またはAdmin$共有(あるいはその両方)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。96 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。 ◆ \Program Files\PlateSpin Portability Suite Server\Web フォルダ内の web.config ファイルのフラグ ForceMachineDiscoveryUsingService を true に変更します。 ◆ サーバまたはワークステーションのサービスが実行されていない可能性があります。実行されていない場合は、それらを有効にし、起動モードを自動に設定します。 ◆ Windows リモートレジストリサービスが無効です。サービスを開始し、起動タイプを自動に設定します。

8.1.1 接続性テストの実行

- 94 ページの 「ネットワークの接続性テスト」
- 95 ページの 「WMI の接続性テスト」
- 95 ページの 「DCOM の接続性のトラブルシューティング」
- 95 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。

42 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 42 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 NT/2000 サーバマシン上で、［DCOM 設定］ダイアログが表示されます。*［規定のプロパティ］*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 Server 2003 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。*［規定のプロパティ］*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
- ハードウェアファイアウォール

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（23 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 は OFX コントローラ、およびブロックレベルのレプリケーションが必要な場合は、専用のブロックベースのコンポーネントを正常に展開し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 コンピューター*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 C$ および Admin$ が表示されるはずです。

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。

   42 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*>\C$」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。	このメッセージにはさまざまな原因があります。 ◆ ワークロードに到達できません。 ◆ ワークロードで SSH が実行されていません。 ◆ ファイアウォールがオンで、必要なポートが開いていません。 ◆ ワークロードの特定のオペレーティングシステムがサポートされません。 ワークロードのネットワークとアクセス要件については、23 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。
`Access denied`	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、83 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。

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。	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。98 ページの 「グループポリシーおよびユーザ権限」を参照してください。
.NET Framework がインストールされているかどうか判別できません (例外 : このワークステーションとプライマリドメインの間の信頼性のある関係が設定されていません)。	ソースのリモートレジストリサービスが有効であり、開始されているかどうかを確認してください。93 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

gpudate /force (Windows 2003/XP の場合) または secedit /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。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。

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

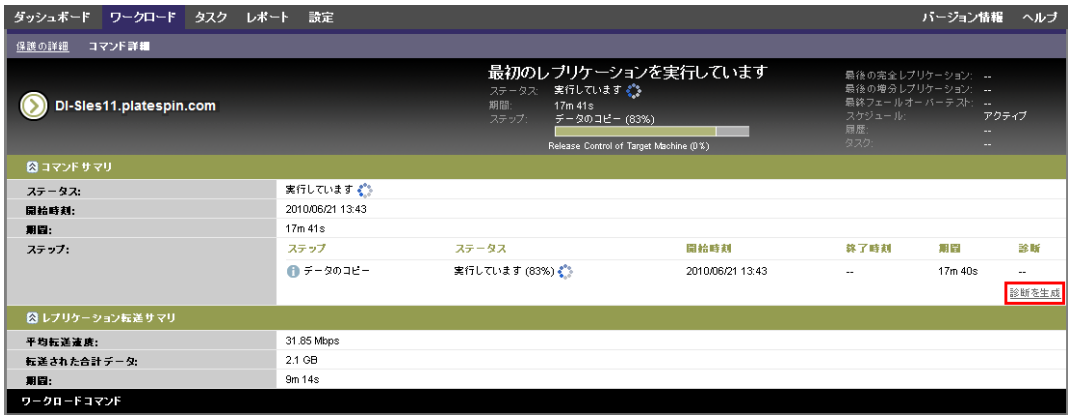
問題またはメッセージ	解決方法
ワークロード問題でユーザの介入が必要 *[仮想マシンのスナップショット取得のスケジュール]* または *[開始前に仮想マシンをスナップショットに戻すようにスケジュールする]* のいずれかのレプリケーション中に回復可能なエラーが発生しました。	この問題は、サーバに負荷がかかっているため、プロセスの処理に予想よりも時間がかかっている場合に発生します。 解決策としては、レプリケーションが終了するまで待ちます。
ディスク領域が不足しているので、すべてのワークロードが回復可能なエラーになっています。	空き領域を確認します。より多くの領域が必要な場合は、ワークロードを削除します。
ネットワーク速度が 1MB 未満で遅い。	ソースマシンのネットワークインタフェースカードがデュプレックス設定でオンになっており、接続先のスイッチの設定と整合していることを確認します。つまり、スイッチが自動に設定されている場合、ソースを 100MB には設定できません。
ネットワーク速度が 1MB 超で遅い。	ソースワークロードから次のコマンドを実行して遅延時間を測定します。 ping *ip*–t（*ip* は、Forge VM の IP アドレスで置き換え）。 50 回反復して実行するようにし、平均値が遅延時間を示します。 も参照してください。30 ページの 「WAN 接続を使用した転送を最適化するパラメータ」

問題またはメッセージ	解決方法
`The file transfer cannot begin - port 3725 is already in use`	ポートが開いてリッスンしていることを確認します。
または	ワークロード上で netstat -ano を実行します。
`3725 unable to connect`	ファイアウォールを確認します。 レプリケーションを再試行します。
`Controller connection not established` レプリケーションが *[仮想マシンの制御の取得]* 手順で失敗する。	このエラーは、レプリケーションのネットワーク情報が無効な場合に発生します。DHCP サーバが利用できないか、レプリケーションの仮想ネットワークが Forge VM にルートできません。 レプリケーション IP をスタティック IP に変更するか、DHCP サーバを有効にします。 レプリケーションに対して選択されている仮想ネットワークが Forge VM にルートできることを確認します。
レプリケーションジョブが開始しない (0% でスタック)	このエラーには複数の原因があり、それぞれに固有の解決策があります。 ◆ 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 (http://www.novell.com/support/viewContent.do?externalId=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 (http://www.novell.com/support/viewContent.do?externalId=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。98 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 Client では、コマンドを実行した後に、その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。



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 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。

8.6.1 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 (http://www.novell.com/support/viewContent.do?externalId=7005616) を参照してください。
サードパーティのブロックベースの転送コンポーネント (提供中止)	1. Windows の［プログラムの追加と削除］アプレット (appwiz.cpl) を使用し、コンポーネントを削除します。ソースに応じて、次のいずれかのバージョンが存在します。 ◆ SteelEye Data Replication for Windows v6 Update2 ◆ SteelEye DataKeeper For Windows v7 2. マシンを再起動します。
ファイルベースの転送コンポーネント	保護されているボリュームごとのルートレベルで、PlateSpinCatalog*.dat という名前のすべてのファイルを削除します。
ワークロードインベントリソフトウェア	ワークロードの Windows ディレクトリで次を実行します。 ◆ 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。

コンポーネント	削除手順
コントローラソフトウェア	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。 ◆ \Program Files\platespin* (32 ビットシステムの場合) ◆ \Program Files (x86)\platespin (64 ビットシステムの場合) 2. 次のコマンドを実行します。 ofxcontroller.exe /uninstall 3. platespin* ディレクトリを削除します。

8.6.2 Linux ワークロードのクリーンアップ

コンポーネント	削除手順
コントローラソフトウェア	◆ 次のプロセスを終了します。 ◆ pkill -9 ofxcontrollerd ◆ pkill -9 ofxjobexec ◆ 次のように、OFX コントローラ RPM パッケージを削除します。 rpm -e ofxcontrollerd ◆ ソース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。

ブロックレベルのデータ転送ソフトウェア	1. ドライバがアクティブであるかどうかを確認します。
	`lsmod | grep blkwatch`
	ドライバが引き続きメモリにロードされている場合、結果には以下と類似する行が含まれるはずです。
	`blkwatch_7616  70924  0`
	2. (条件付き) ドライバがロードされている場合、メモリからそれを削除してください。
	`rmmod blkwatch_7616`
	3. 次のブートシーケンスからドライバを削除します。
	`blkconfig -u`
	4. 次のディレクトリを内容と共に削除することにより、ドライバファイルを削除します。
	`/lib/modules/`*`[Kernel_Version]`*`/Platespin`
	5. 次のファイルを削除します。
	`/etc/blkwatch.conf`

LVM スナップショット	1. ジョブビューで、失敗したジョブに関するジョブレポートを生成し、スナップショットの名前を書き留めます。 2. 次のコマンドを使用してスナップショットデバイスを削除します。 lvremove *snapshot_name*

コンポーネント	削除手順
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

8.6.3 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を通じて以前保護されていた Windows ワークロードに対して、PlateSpin Forge Web Client では、ブロックベースのコンポーネントも削除するかどうかを指定するように求められます。次のとおり選択できます。

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

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。

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
回復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 Forge Server メッセージのことです。

failback (フェールバック)
PlateSpin Forge 内で一時的な回復ワークロードのビジネス機能が必要でなくなった場合に、失敗したワークロードのビジネス機能を元の環境で復元する操作のことです。

failover (フェールオーバー)
失敗したワークロードのビジネス機能が、PlateSpin Forge の VM コンテナ内の回復ワークロードによって引き継がれる操作のことです。

増分
1. (名詞) 保護されたワークロードとそのレプリカ (回復ワークロード) 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回復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。

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。

回復ワークロード
保護ワークロードのブート可能な仮想レプリカです。

レプリケーション
1. ワークロードの初期のベースコピーを作成する操作です (*初期レプリケーション*)。

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、コンテナ内の回復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回復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、回復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回復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、ユーザが回復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。