Microsoft System Center 2012 Virtual Machine Manager 用 Dell Lifecycle Controller Integration バージョン 1.2

ユーザーズガイド

メモ、注意、警告

メモ: メモでは、コンピュータを使いやすくするための重要な情報を説明しています。

注意: 注意では、ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 警告では、物的損害、けが、または死亡の原因となる可能性があることを示しています。

2016 - 03

Rev. A00

目次

1

Microsoft System Center 2012 Virtual Machine Manager 用 Dell Lifecycle Controller Integration について

Microsoft System Center 2012 Virtual Machine Manager（SC2012 VMM）用 Dell Lifecycle Controller Integration（DLCI）は、ハードウェアの設定を可能にし、ファームウェアアップデートプロセスをシンプル化かつ改善するためのソリューション、およびデルサーバーでハイパーバイザーを導入するためのソリューションを提供します。このプラグインは、Integrated Dell Remote Access Controller（iDRAC）with Lifecycle Controller（LC）のリモート導入機能を使用してシームレスなユーザー体験を提供します。また、仮想環境を管理するために、Microsoft System Center コンソール経由でデルの付加価値を活用することができます。

Microsoft System Center Virtual Machine Manager についての情報は、Microsoft の文書を参照してください。

本リリースの新機能

本リリースの機能は次のとおりです。

- アップデートソース - Hypertext Transfer Protocol（HTTP）タイプのアップデートソースをサポートします。
- テスト接続 - アップデートソースを作成する前にアップデートソースの場所および資格情報を検証します。
- アップデートグループ - カスタムアップデートグループ上でファームウェアアップデートを作成、管理、および実行するために、サーバーをグループ化します。
- ポーリングと通知 - アップデートソース内で新しいカタログが使用可能になったらアラートを受信するように、通知を設定します。
- 保護ボールト - システム設定プロファイルを保存する場所。
- サーバープロファイルのエクスポート - 内部または外部の場所に対して、基本入出力システム（BIOS）、Redundant Array of Independent Disks（RAID）、ネットワークインタフェースコントローラ（NIC）、integrated Dell Remote Access Controller（iDRAC）、LC などのコンポーネント上のファームウェアイメージを含めます。
- サーバープロファイルのインポート - 既存のサーバープロファイルが破損しているとき、同じサーバーまたはサーバーグループの現在の RAID 設定を保持または除外します。
- フィルタ - **Maintenance Center**（メンテナンスセンター）で選択された基準に基づいて情報を表示するときに使用します。
- ダウングレードを許可 - 有効にすると、ファームウェアバージョンを以前のバージョンにダウングレードできます。
- クラスタ対応アップデート（CAU）- サーバーの可用性を維持しながら、クラスタアップデートグループ上で Microsoft の機能を使用してソフトウェアアップデートプロセスを自動化します。
- Dell Repository Manager（DRM）との統合 - 既存のサーバーのサーバーインベントリ情報をアプライアンスから DRM に提供します。

既存機能

SC2012 VMM 用 DLCI では、次の機能を引き続き利用することができます。

- 未割り当ての Dell サーバーの自動検出 - 工場から出荷された Dell サーバーをネットワークに接続し、サーバーの電源を投入してから、DLCI アプライアンスのプロビジョニングサーバー詳細を入力することによって、サーバーが自動的に検出されます。

  アプライアンスによって検出されたサーバーは、未割り当てサーバーとして認識され、これらのサーバーにハイパーバイザーの導入を行うことができます。
- 未割り当て Dell サーバーの手動検出 — 第 11、12、および 13 世代の PowerEdge サーバーを検出し、仮想環境にサーバーを導入します。
- 検出されたサーバーのインベントリの表示 — Dell サーバーに関する重要なインベントリ詳細が表示されます。
- サーバーコンプライアンスのチェック - アプライアンスで使用可能な機能を使用するには、必要なファームウェアバージョンの iDRAC、LC、および基本入出力システム（BIOS）が Dell サーバーに搭載されている必要があります。バージョン番号の詳細については、『DLCI for SC2012 VMM Release Notes』（SC2012 VMM 用 DLCI リリースノート）を参照してください。
- ゴールデン設定とも呼ばれる理想的なサーバー設定の準備 - 仮想環境に導入されるサーバーにこの設定を複製します。さらに、次の操作も実行できます。
  - 起動順序と BIOS に対するゴールデン設定を編集および変更します。
  - RAID のための専用ホットスペア（DHS）戦略をカスタマイズします。
- プロファイルとテンプレートを作成および維持します。
- Microsoft Windows プレインストール環境（WinPE）のカスタマイズ — 最新の Dell OpenManage Deployment Toolkit（DTK）ドライバで、カスタマズされた WinPE イメージを準備します。
- 工場から出荷された最新ドライバパック同梱の最新サーバーにおいて、LC ドライバインジェクション機能を使用します。

  LC のドライバインジェクション機能を使用した、または使用しないハイパーバイザーの導入 - アプライアンスから、ゴールデン設定に基づいたハイパーバイザーの導入を行います。
- DLCI コンソールから iDRAC コンソールを起動してインベントリ情報を表示し、トラブルシューティングを行います。
- ジョブの情報の表示 — アプライアンスで実行されたさまざまなジョブに関して記録された情報を表示します。
- 簡略化されたライセンス - ライセンスの管理に Dell Connections License Manager（DCLM）は必要なくなりました。ライセンスの詳細は、管理ポータルの **License Center**（ライセンスセンター）で参照できます。
- 新しい資格情報プロファイルタイプ：
  - デバイス資格情報プロファイル - iDRAC または Chassis Management Controller（CMC）へのログインに使用します。
  - Windows 資格情報プロファイル - Windows 共有にアクセスするために使用します。
  - FTP 資格情報プロファイル - FTP サイトにアクセスするために使用します。
  - プロキシサーバー資格情報 - プロキシ資格情報を提供するために使用します。

- 検出 - ホストがクラスタの一部である場合はクラスタの詳細情報と共に、ホストがモジュラーサーバーの場合はシャーシの詳細情報と共にサーバーを検出します。
- SCVMM との同期 - SCVMM 環境内にリストされているすべての Dell ホストシステムを SC2012 VMM 用 DLCI と同期します（ホストは SCVMM によって管理されている Hyper-V ホストです）。
  - 同期エラーの解決 - 前の試行時に同期されなかったホストサーバーを再同期します。
- サーバー管理 - SCVMM 環境内の Dell サーバーを管理し、最新のファームウェアとその他アップデートに基づいたデルの推奨に従ってサーバーを最新の状態に保ちます。第 11 世代から第 13 世代までの Dell PowerEdge サーバーのサーバー管理がサポートされています。
  - サーバー管理の主な機能は次のとおりです。
    * 比較レポートの表示 - アップデートソースから重要度で比較レポートを表示し、ベースラインバージョンを作成します。重要度は、アップデートがどの程度重要であるかを示します。
    * ファームウェアインベントリの更新とエクスポート - ファームウェアインベントリを更新し、インベントリの詳細情報を `xml` 形式でエクスポートします。
    * アップデートの適用 - ファームウェアアップデートを適用、またはアップデートをスケジュールします。
    * 特定のアップデートの適用 - 特定のコンポーネントアップデートのみを適用、または Dell FTP で使用可能な最新のアップデートを適用します。
    * オペレーティングシステム導入前のアップデートの適用 - オペレーティングシステムの導入前に、適切なアップデートソースを使用してファームウェアアップデートを適用します。
  - 次のコンポーネントの最新のファームフェアバージョンについてサーバーをリモートでアップデートします（1 対 1 または 1 対多）。
    * BIOS
    * NIC または LAN on Motherboard（LOM）
    * 第 12 世代 PowerEdge サーバー以降からの電源装置ユニット（PSU）
    * PowerEdge RAID コントローラ（PERC）またはシリアルアタッチド SCSI（SAS）
    * バックプレーン
    * iDRAC with LC（モジュラーおよびモノリシック）

      メモ: 使用可能なコンポーネントは Dell サーバーの下にリストされます。
- アップデートグループ - 検出されたサーバーは、すべて適切な事前定義されたアップデートグループに追加されます。
- アップデートソース - DRM を使用することにより、または FTP サイトに接続することによって、リポジトリを作成します。
  - DRM との統合 - SC2012 VMM 用 DLCI からシステムインベントリ情報を DRM にエクスポートし、DRM を使用してリポジトリを準備します。
  - FTP - Dell FTP（ローカルまたはオンライン）に接続し、最新の Dell オンラインカタログを取得します。

2

DLCI コンソールアドインのインストールとセットアップ

SC2012 VMM 用 DLCI コンソールアドインのインストールおよびセットアップには、次の作業が含まれます。

- システム要件を確認および完了し、**SC2012 VMM 用 DLCI コンソールアドイン** をインストールします。詳細については、「DLCI コンソールアドインのインストール」を参照してください。
- DLCI コンソールを VMM コンソールにインポートします。詳細については、「VMM コンソールへの DLCI コンソールのインポート」を参照してください。
- VMM コンソールで DLCI コンソールを表示します。詳細については、「DLCI コンソールの表示」を参照してください。
- DLCI コンソールをアンインストールします。詳細については、「DLCI コンソールのアンインストール」を参照してください。

DLCI コンソールアドインのインストール

アプライアンスでの作業を開始する前に、SC2012 VMM コンソールがインストールされているシステムに DLCI コンソールをインストールします。DLCI コンソールをインストールしたら、DLCI コンソールを SC2012 VMM コンソールにインポートすることができます。
前提条件：SC2012 VMM SP1 または SC2012 VMM R2 コンソールがインストールされていること。
DLCI コンソールを **Setup and Configuration**（セットアップと設定）から初めてインストールする場合は、手順 3 から開始します。それ以外の場合は、手順 1 から開始します。

DLCI コンソールをインストールするには、次の手順を実行します。

1. **DLCI Admin Portal - SC2012 VMM**（DLCI 管理ポータル - SC2012 VMM）で、**Downloads**（ダウンロード）をクリックします。
2. **DLCI Console Add-in for SC2012 VMM Installer**（SC2012 VMM 用 DLCI コンソールアドインインストーラ）から、**Download Installer**（インストーラをダウンロード）をクリックしてこの場所にファイルを保存します。
3. インストーラファイルを実行します。
4. **DLCI Console Add-in for SC2012 VMM**（SC2012 VMM 用 DLCI コンソールアドイン）の ようこそ ページで **Next**（次へ）をクリックします。
5. **License Agreement**（ライセンス契約）ページで、**I accept the terms in the license agreement**（ライセンス契約の条件に同意します）を選択してから、**Next**（次へ）をクリックします。
6. **Destination Folder**（宛先フォルダ）ウィンドウでは、インストール先フォルダがデフォルトで選択されています。場所を変更するには、**Change**（変更）をクリックし、変更を完了して **Next**（次へ）をクリックします。
7. **Ready to Install the Program**（プログラムインストールの準備完了）ウィンドウで、**Install**（インストール）をクリックします。

8. **InstallShield Wizard Completed**（InstallShield ウィザードを完了しました）ページが表示されたら、**Finish**（終了）をクリックします。

DLCI コンソールアドインの削除または修復

DLCI コンソールアドインを削除または修復するには、次の手順を実行します。

1. **SC2012 VMM 用 DLCI コンソールアドイン** インストーラを実行します。
2. **Program Maintenance**（プログラムメンテナンス）で、**Remove**（削除）または **Repair**（修復）を選択して **Next**（次へ）をクリックします。
3. **プログラムの修復または削除の準備完了** で、**インストール** をクリックします。
4. 削除または修復作業が完了したら、**完了** をクリックします。

VMM への DLCI コンソールアドインのインポート

DLCI アプライアンスで作業するには、DLCI コンソールを VMM コンソールにインポートします。

前提条件：アプライアンスとの接続を機能させるには、ウェブブラウザでプロキシ設定をクリアします。ただし、ウェブブラウザのプロキシが設定済みの場合は、プロキシ例外リストにアプライアンスの完全修飾ドメイン名（FQDN）を含めます。

VMM コンソールに DLCI コンソールをインポートするには、次の手順を実行します。

1. SC2012 VMM から **Settings**（設定）をクリックします。
2. **ホーム** リボンで、**コンソールのアドインをインポート** をクリックします。
3. **Import Console Add-in Wizard（コンソールのアドインのインポート ウィザード）→ Select an add-in to import（インポートするアドインの選択）** をクリックし、SC2012 VMM 用 DLCI コンソールアドイン（**DLCI_VMM_Console_Addin.zip**）を参照して選択してから、**Next**（次へ）をクリックします。
4. **設定の確認** で必要な設定が行われていることを確認してから、**終了** をクリックします。
   DLCI コンソールが VMM コンソールにインポートされ、**VM およびサービス → すべてのホスト** で利用できるようになりました。

DLCI コンソールアドインの表示

SC2012 VMM で DLCI コンソールを表示するには、次の手順を実行します。

1. SC2012 VMM コンソールで **Fabric**（ファブリック）を選択してから、**All Hosts Group**（すべてのホストグループ）を選択します。

   メモ: DLCI コンソールを起動するために、アクセス可能な任意のホストグループを選択できます。
2. **ホーム** リボンで **DLCI コンソール** を選択します。

DLCI コンソールアドインのアンインストール

DLCI コンソールをアンインストールするには、次の手順を実行します。

1. SC2012 VMM で、**設定** をクリックします。
2. **Settings → Console Add-ins（設定 > コンソールアドイン）**をクリックし、**DLCI Console Add-in for SC2012 VMM**（SC2012 VMM 用 DLCI コンソールアドイン）を選択します。

3. **ホーム** で **削除** をクリックします。

3

はじめに

管理システムは、SC2012 VMM 用 DLCI（アプライアンスとそのコンポーネントとも呼ばれる）がインストールされているシステムです。アプライアンスのコンポーネントは次のとおりです。

- SC2012 VMM 用 DLCI 統合ゲートウェイと呼ばれる、Microsoft System Center 2012 Virtual Machine Manager（SC2012 VMM）用 Dell Lifecycle Controller Integration（DLCI）統合ゲートウェイ。
- SC2012 VMM 用 DLCI コンソールアドインと呼ばれる、Microsoft System Center 2012 Virtual Machine Manager（SC2012 VMM）用 Dell Lifecycle Controller Integration（DLCI）コンソールアドイン。

DLCI 管理ポータル - SC2012 VMM へのログイン

DLCI 管理ポータル - SC2012 VMM にログインするには、次の手順を実行します。

1. アプライアンスで、DLCI 管理者ポータル - SC2012 VMM の URL をメモします。
2. ウェブブラウザで、URL：**https://<IP Address>** または **<FQDN>** にアクセスします。
   例：**192.168.20.30** または **DLCIforSC2012vmm.myorgdomain.com**。
3. アプライアンスの設定時に入力したユーザー資格情報を使用して DLCI 管理ポータル - SC2012 VMM にログインします。

DLCI 管理ポータル - SC2012 VMM

DLCI 管理ポータル - SC2012 VMM のユーザーインタフェースには、次のオプションがあります。

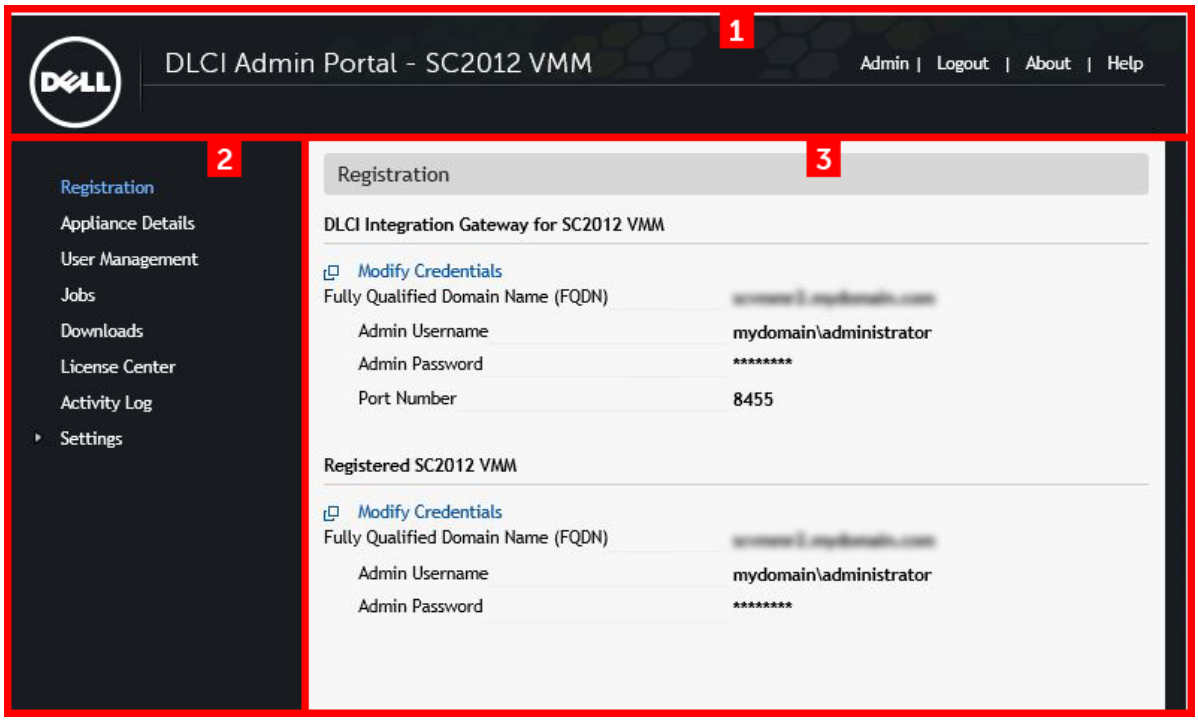


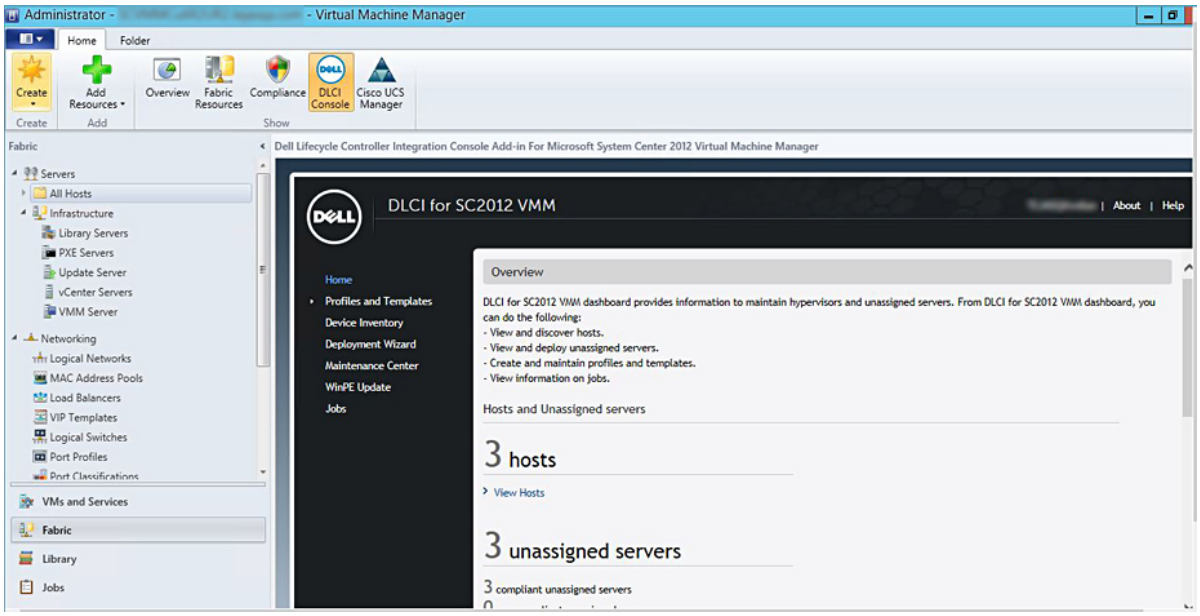
図 1. DLCI 管理ポータル - SC2012 VMM

1. 見出しバナーには、製品名および次のオプションが表示されます。
   - **Admin**（管理）- SC2012 VMM 用 DLCI - 管理ポータルにログインしているユーザーの情報が表示されます。
   - **Logout**（ログアウト）- SC2012 VMM 用 DLCI 管理ポータルからログアウトできます。
   - **About**（バージョン情報） - SC2012 VMM 用 DLCI のバージョン情報が表示されます。
   - **ヘルプ** — 状況依存オンラインヘルプを起動します。
2. ナビゲーションペインには、次のオプションが含まれています。各オプションの詳細については、オンラインヘルプを参照してください。
   - **登録**
   - **アプライアンス詳細**
   - **ユーザー管理**
   - **ジョブ**
   - **Downloads（ダウンロード）**
   - **ライセンスセンター**
   - **Activity Log（アクティビティログ）**
   - **設定**
     - **サービスパックアップデート**
     - **ログ**
3. コンソールエリアには、ナビゲーションペインで選択したオプションの情報が表示されます。

SC2012 VMM 用 DLCI コンソールアドインへのログイン

SC2012 VMM 用 DLCI コンソールアドインにログインするには、次の手順を実行します。

1. SC2012 VMM で、**ファブリック** を選択し、**すべてのホスト** を選択します。
2. **ホーム** リボンで **DLCI コンソール** を選択します。



SC2012 VMM 用 DLCI コンソールアドイン

DLCI コンソールアドインのユーザーインタフェースには次のオプションがあります。

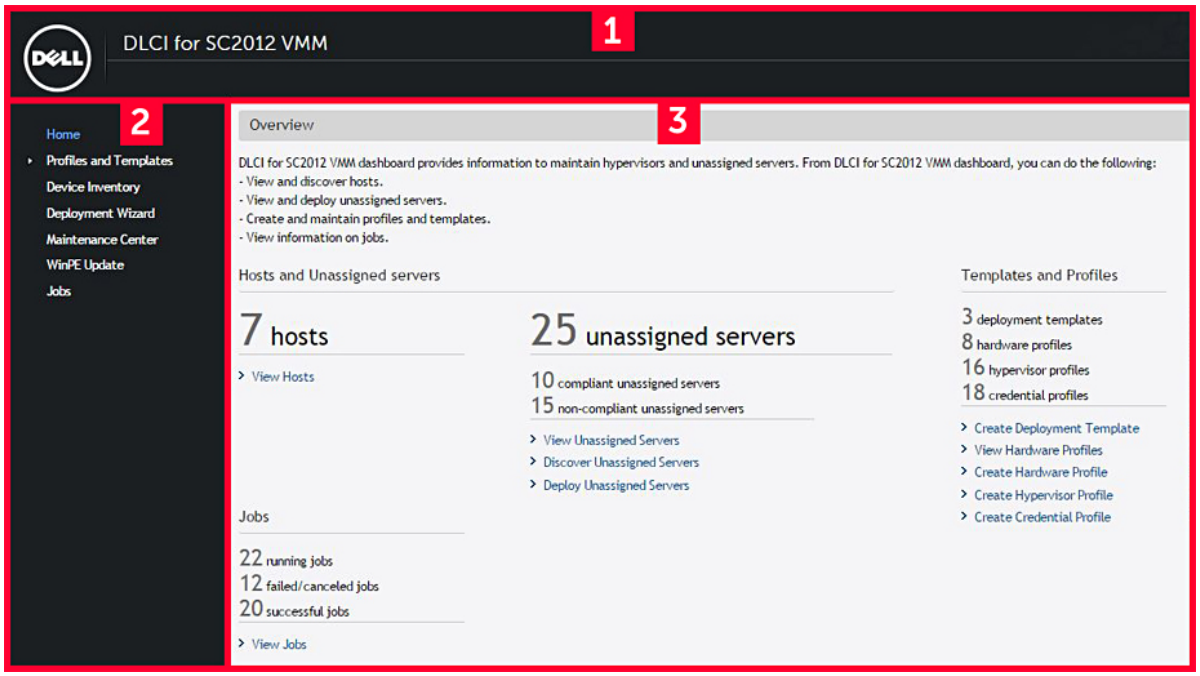


図 2. SC2012 VMM 用 DLCI コンソールアドイン

1. 見出しバナーには、製品名および次のオプションが表示されます。
   - **<Domain>\adminstrator** - SC2012 VMM 用 DLCI にログインしているユーザーに関する情報が表示されます。
   - **About**（バージョン情報）- SC2012 VMM 用 DLCI のバージョン情報が表示されます。
   - **Help**（ヘルプ）- 状況依存オンラインヘルプを起動します。
2. ナビゲーションペインには、次のオプションがあります。
   - **ヘルプ**（ホーム）- SC2012 VMM 用 DLCI のダッシュボードが表示されます。
   - **プロファイルとテンプレート**
     - **展開テンプレート**
     - **ハードウェアプロファイル**
     - **ハイパーバイザープロファイル**
     - **資格情報プロファイル**
   - **デバイスインベントリ**
   - **導入ウィザード**
   - **Maintenance Center**（メンテナンスセンター）
   - **WinPE のアップデート**
   - **ジョブ**
3. コンソールエリアには、ナビゲーションペインで選択したオプションの情報が表示されます。

メモ: SC2012 VMM 用 DLCI コンソールでは、たとえばハードウェアプロファイルのウィザードを使用している間に SC2012 VMM コンソール内の他のタブまたはリンクに移動して、再度 SC2012 VMM 用 DLCI コンソールアドインを表示させた場合、移動前に入力した情報は保存されず、DLCI コンソールにはホームページが表示されます。

4

ワークフロー

本項には、以下の操作のためのワークフローが記載されています。

- ゴールデン設定の作成
- 資格情報プロファイルの作成と管理
- アップデートソースの作成と管理
- カスタムアップデートグループの作成と管理
- サーバーまたはサーバーグループ上でのアップデートの適用
- ハイパーバイザー導入
- 保護ボールトの作成、管理、および削除
- サーバープロファイルのエクスポート
- サーバープロファイルのインポート
- サーバーの削除

ゴールデン設定について

優先起動順序、BIOS、および RAID の設定が組織に理想的に適合しているサーバー設定は、ゴールデン設定と呼ばれます。これらの設定はハードウェアプロファイルに集められ、ハイパーバイザー導入中に同一のサーバー上に導入されます。

ゴールデン設定の作成

ゴールデン設定を準備し、使用するには、次の手順を実行します。

1. 理想的な設定が行われたサーバーが検出済みで、使用可能であることを確認します。サーバー検出の詳細については、要件に応じて「自動検出を使用したサーバーの検出」または「手動検出を使用したサーバーの検出」を参照してください。
2. サーバーのインベントリが最新の状態であることを確認します。詳細については、「ファームウェアインベントリの表示と更新」を参照してください。
3. 理想的な設定を記録するには、ハードウェアプロファイルを作成します。ハードウェアプロファイルを作成するには、「ハードウェアプロファイルの作成」を参照してください。
4. 設定を変更する場合は、「ハードウェア構成プロファイルの変更」を参照してください。

資格情報プロファイルの作成、管理、および削除

資格情報プロファイルを作成するには、「資格情報プロファイルの作成」を参照してください。

資格情報プロファイルを管理するには、「資格情報プロファイルの変更」を参照してください。

資格情報プロファイルを削除するには、「資格情報プロファイルの削除」を参照してください。

アップデートソースの作成、管理、および削除

アップデートソースを作成するには、「アップデートソースの作成」を参照してください。
アップデートソースを管理するには、「アップデートソースの変更」を参照してください。

アップデートソースを削除するには、「アップデートソースの削除」を参照してください。

カスタムアップデートグループの作成、管理、および削除

カスタムアップデートグループを作成するには、「カスタムアップデートグループの作成」を参照してください。

カスタムアップデートグループを管理するには、「カスタムアップデートグループの変更」を参照してください。

カスタムアップデートグループを削除するには、「カスタムアップデートグループの削除」を参照してください。

サーバーまたはサーバーグループ上でのアップデートの適用

次のソースを使用して、選択したサーバーまたはサーバーグループをアップデートできます。

- オンライン FTP およびローカル FTP ソース
- オンライン HTTP およびローカル HTTP
- ローカル DRM リポジトリ

選択したサーバーまたはサーバーグループ上でアップデートを適用するには、次の手順を実行します。

1. アップデートを開始する前に、アップデートソースとアップデートグループに関する情報を表示します。詳細については、「アップデート管理」を参照してください。
2. サーバーを検出します。詳細については、「自動検出を使用したサーバーの検出」、または「手動検出を使用したサーバーの検出」を参照してください。
3. SCVMM 環境内に存在するサーバーを SC2012 VMM 用 DLCI と同期します。同期化の詳細については、「SCVMM との同期化」を参照してください。
4. サーバーのインベントリが最新の状態であることを確認します。詳細については、「デバイスインベントリの表示」を参照してください。
5. アップデートソースが作成されていることを確認します。詳細については、「アップデートソースの作成」を参照してください。
6. アップデートソースがポーリングと通知を使用して定期的に最新のカタログで更新されることを確認します。詳細については、「ポーリングと通知」を参照してください。
7. アップデートを適用するために必要なサーバーグループが選択されていることを確認します。詳細については、「サーバー上でのアップデートの適用」を参照してください。

   メモ: コンポーネントのファームウェアバージョンをダウングレードするには、**Allow Downgrade**（ダウングレードを許可）を選択します。

保護ボールトの作成、管理、および削除

1. 保護ボールトを作成するには、「保護ボールトの作成」を参照してください。
2. 保護ボールトを管理するには、「保護ボールトの変更」を参照してください。
3. 保護ボールトを削除するには、「保護ボールトの削除」を参照してください。

サーバープロファイルのエクスポート

サーバー設定をエクスポートするには、次の手順を実行します。

1. 保護ボールトを作成します。詳細については、「保護ボールトの作成」を参照してください。
2. サーバープロファイルをすぐにエクスポートするか、後日にするようにスケジュールします。詳細については、「エクスポートジョブの作成」を参照してください。

サーバープロファイルのインポート

サーバープロファイルをインポートするには、次の手順を実行します。

1. 保護ボールトを作成します。詳細については、「保護ボールトの作成」を参照してください。
2. サーバープロファイルをエクスポートします。詳細については、「エクスポートジョブの作成」を参照してください。
3. RAID 設定を含めて、または除外して、エクスポートされたサーバープロファイルをインポートします。詳細については、「サーバープロファイルのインポート」を参照してください」を参照してください。

ハイパーバイザー導入

アプライアンスを使用して、ファームウェアアップデートおよびハイパーバイザー導入をゴールデン設定に基づいて実行できます。最新のドライバパックと共に工場から出荷されたサーバーに対しては、LC ドライバインジェクション機能を使用できます。また、ドライバパックをアップデートし、ハイパーバイザー導入およびファームウェアアップデート時における最新ドライバのインストールと同様の効果を得ることができます。

表 1. ハイパーバイザー導入のためのさまざまなシナリオ

工場出荷時の最新のドライバおよび帯域外ドライバが必要な場合	ハイパーバイザープロファイルの作成中に、LC（Lifecycle Controller）ドライバの挿入を有効にします。
既存のハードウェア構成を保持する場合	導入テンプレートの作成中に、ハイパーバイザープロファイルのみを選択します。

ハイパーバイザー導入の作業には、次を参照してください。

1. 導入について
2. 資格情報プロファイルの作成
3. アップデートソースの作成
4. ハードウェアプロファイルの作成
5. ハイパーバイザープロファイルの作成

6. 導入テンプレートの作成
7. （オプション）カスタムアップデートグループの作成
8. （オプション）サーバー上でのアップデートの適用
9. ハイパーバイザーの導入

サーバーの削除

アプライアンスでサーバーを削除する方法については、「DLCI コンソールからのサーバーの削除」を参照してください。

5

ハイパーバイザー導入のための環境のセットアップ

ハイパーバイザー導入のための環境をセットアップするには、次の手順を実行します。

1. ゴールデン設定を準備します。
2. 物理コンピュータプロファイルを SC2012 VMM に作成します。詳細については、SC2012 VMM のマニュアルを参照してください。
3. ターゲットホストグループを SC2012 VMM に作成します。詳細については、SC2012 VMM のマニュアルを参照してください。
4. 最新の Dell Deployment ToolKit（DTK）をダウンロードして Windows Preinstallation Environment（WinPE）ブート ISO イメージを作成します。詳細については、「WinPE アップデート」を参照してください。
5. 自動検出のためにシステムをセットアップします。詳細については、「自動検出を使用したサーバーの検出」を参照してください。
6. アップデートソースを作成します。詳細については、「アップデートソースの作成」を参照してください。
7. （オプション）カスタムアップデートグループを作成します。詳細については、「カスタムアップデートグループの作成」を参照してください。
8. （オプション）ハードウェアプロファイルを作成します。詳細については、「ハードウェアプロファイルの作成」を参照してください。
9. ハイパーバイザープロファイルを作成します。詳細については、「ハイパーバイザープロファイルの作成」を参照してください。
10. 導入テンプレートを作成します。詳細については、「導入テンプレートの作成」を参照してください。
11. システムが検出され、アプライアンス内で使用可能になった後、ファームウェアアップデートを実行（オプション）してから、ハイパーバイザー導入を実行します。アップデートの適用についての詳細は、「サーバー上でのアップデートの適用」を参照してください。ハイパーバイザーの導入についての詳細は、「ハイパーバイザーの導入」を参照してください。
12. ファームウェアアップデートと導入のジョブステータスを表示します。詳細については、「ジョブステータスの表示」を参照してください。

6

サーバー検出

未割り当ての Dell サーバーの帯域外検出を実行し、Dell サーバーに関する情報をアプライアンスにインポートできます。サーバーを検出するために、Dell サーバーをネットワークに接続し、サーバーの電源を入れ、iDRAC にログインし、プロビジョニングサーバーの IP を DLCI アプライアンスの IP に更新し、DLCI アプライアンスの管理者アカウントを無効にして、サーバーを自動的に検出します。サーバーの設定方法の詳細については、Integrated Dell Remote Access Controller のマニュアルを参照してください。

未割り当ての Dell サーバーは、次のオプションを使用して検出することもできます。

- 未割り当てサーバーの自動検出。
- IP アドレスに基づいた手動検出。

未割り当てサーバーと一緒に Hyper-V ホスト、モジュラー Hyper-V ホストを検出することができます。検出後、それらのサーバーは事前定義された対応するアップデートグループに追加されます。グループの分類の詳細については、「アップデート管理」を参照してください。

サーバー検出についてのメモ：

- オペレーティングシステムが導入済みで、SCVMM に存在する Dell PowerEdge サーバーを検出した場合、そのサーバーはホストサーバーとしてリストされ、準拠または非準拠のマークが付けられます。
  - アプライアンスと連携するために必要な最低限のバージョンの LC ファームウェア、iDRAC、および BIOS が搭載されている場合、そのホストサーバーは準拠になります。
  - ホストがモジュラーサーバーの場合、そのサーバーが収容されているシャーシのサービスタグが表示されます。ホストがクラスタの一部の場合、クラスタの完全修飾ドメイン名（FQDN）が表示されます。
- SCVMM 荷リストされていない Dell PowerEdge サーバーを検出した場合、そのサーバーは未割り当てサーバーとしてリストされ、適合または非適合のマークが付けられます。
- 誤った資格情報を入力してしまった場合、iDRAC のバージョンに応じて次の解決策を使用できます。
  - iDRAC バージョン 2.10.10.10 以降を搭載した第 12 世代の Dell PowerEdge サーバーを検出しているとき、ログイン時に資格情報プロファイルの誤った詳細情報を入力すると、次の動作を伴ってサーバー検出が失敗します。
    * 初回試行の場合、サーバーの IP アドレスはブロックされません。
    * 2 回目の試行、サーバーの IP アドレスが 30 秒間ブロックされます。
    * 3 回目以降の試行では、サーバーの IP アドレスが 60 秒間ブロックされます。

    IP アドレスのブロックが解除されたら、正しい資格情報プロファイルの詳細情報を使用してサーバー検出を再試行できます。
  - 2.10.10.10 より前のバージョンの iDRAC を搭載した第 11 世代または第 12 世代の PowerEdge サーバーを検出しているとき、誤った資格情報プロファイルの詳細情報を入力してサーバー検出の試行が失敗した場合は、正しい資格情報プロファイルの詳細情報を使用してサーバーを再検出します。
  - 2.10.10.10 より前のバージョンの iDRAC では、IP アドレスのブロックは設定可能です。詳細については、**dell.com/support/home** にある iDRAC のマニュアルを参照してください。要件に基づいて、IP

アドレスのブロックを無効にすることもできます。また、**iDRAC.IPBlocking.BlockEnable** 機能が iDRAC で有効になっているかどうかを確認することもできます。

– サーバーがデフォルトの資格情報プロファイルを使用して検出され、アプライアンスに追加された後、デフォルトの iDRAC 資格情報プロファイルを変更すると、そのサーバー上でアクティビティを一切実行できなくなります。そのサーバーで作業するには、新しい資格情報プロファイルでサーバーを再検出してください。

管理対象システムのシステム要件

管理対象システムとは、アプライアンスを使用して管理されるシステムのことです。アプライアンスで管理対象システムを検出する場合、システム要件は次のとおりです。

- 第 11、第 12、および第 13 世代の Dell PowerEdge サーバーの場合、アプライアンスはモジュラー型およびモノリシック型のサーバーモデルをサポートします。
- ソース設定と宛先設定については、同じタイプのディスク（ソリッドステートドライブ（SSD）のみ、SAS またはシリアル ATA（SATA）ドライブのみ）を使用してください。
- ハードウェアプロファイルの RAID クローニングを正常に行うため、宛先ディスクシステムでは、ソースに存在するディスクのサイズまたは数と同じ、またはそれらを超えるサイズまたは数のディスクを使用します。
- RAID スライスされた仮想ディスクはサポートされていません。
- 共有 LOM 装備の iDRAC はサポートされていません。
- UEFI（Unified Extensible Firmware Interface）起動モードはサポートされていません。
- 外部コントローラ上の RAID 構成はサポートされていません。
- 管理対象システムで Collect System Inventory on Start（CSIOR）を有効にします。詳細については、「管理対象システムでの CSIOR の有効化」を参照してください。

管理対象システムでの CSIOR の有効化

第 12 および第 13 世代の Dell PowerEdge サーバーに対して CSIOR を有効にするには、次の手順を実行します。

1. POST 中に **F2** を押して **セットアップユーティリティ** を起動します。
2. **iDRAC 設定** を選択し、**Lifecycle Controller** をクリックします。
3. **Collect system inventory on Restart (CISOR)** に対して、オプションを **Enabled**（有効）に設定します。

第 11 世代の PowerEdge サーバーに対して CSIOR を有効にするには、次の手順を実行します。

1. システムを再起動します。
2. パワーオンセルフテスト（POST）中に iDRAC ユーティリティを起動するよう求めるプロンプトが表示されたら、**CTRL + E** を押します。
3. 使用可能なオプションから、**System Services**（システムサービス）を選択し、**Enter** を押します。
4. **Collect System Inventory on Restart** を選択し、右または下矢印キーを押して **有効** に設定します。

自動検出を使用したサーバーの検出

Dell サーバーをネットワークに接続し、サーバーの電源をオンにして、DLCI アプライアンスによるサーバーの自動検出を行います。アプライアンスは iDRAC の Remote Enablement 機能を使用して、未割り当ての

Dell サーバーを自動検出します。アプライアンスはプロビジョニングサーバーとして機能し、Dell サーバーの自動検出には iDRAC 参照を使用します。

Dell サーバーでの自動検出を実行するには、次の手順を実行します。

1. アプライアンスで、Dell サーバー用のデバイスタイプ資格情報プロファイルを作成します（iDRAC 資格情報を指定して、それにデフォルトとしてマークを付けます）。詳細については、「資格情報プロファイルの作成」を参照してください。
2. 自動検出する Dell サーバーで、次の手順を実行します。
   a. iDRAC 内の既存の管理者アカウントを無効にします。
   b. iDRAC 設定の Remote Enablement で、自動検出を有効にします。
   c. 自動検出を有効にした後、プロビジョニングサーバー（DLCI アプライアンス）の IP アドレスを使用してサーバーを再起動します。

手動検出を使用したサーバーの検出

サーバーは IP アドレスまたは IP 範囲を使用して手動で検出することができます。サーバーを検出するには、サーバーの iDRAC IP およびサーバーのデバイスタイプ資格情報を入力します。IP 範囲を使用してサーバーを検出する場合は、IP（IPv4）範囲（サブネット内）を指定します。

Dell サーバーを手動で検出するには、次の手順を実行します。

1. SC2012 VMM 用 DLCI コンソールアドイン で、次のいずれかを実行します。
   - ダッシュボードで、**未割り当てのサーバーを検出** をクリックします。
   - ナビゲーションペインで、**デバイスのインベントリ** をクリックして、**インベントリ** で **検出** をクリックします。
2. **検出** で、必要なオプションを選択します。
   - **IP アドレスを使用して検出**
   - **IP 範囲を使用して検出**
3. 必要なデバイスタイプ資格情報プロファイルを選択するか、**Create New**（新規作成）をクリックして資格情報プロファイルを作成します。
4. **Discover Using an IP Address or IP Address Range**（IP アドレスまたは IP アドレスの範囲を使用した検出）で、次のいずれかを実行します。
   - **IP アドレスを使用した検出** を選択した場合は、検出したいサーバーの IP アドレスを入力します。
   - **IP 範囲を使用した検出** を選択した場合は IP アドレス範囲を指定し、IP アドレス範囲を除外する必要がある場合は **除外範囲を有効にする** を選択して、除外する範囲を指定します。
5. **ジョブオプション** でこのジョブを追跡するにはジョブ名を指定し、ジョブを表示するには **終了後にジョブリストに移動する** を選択します。
6. **終了** をクリックします。

DLCI コンソールからのサーバーの削除

未割り当てサーバーおよびホストサーバーを次の条件に基づいて削除することができます。

- アプライアンスにリストされている未割り当てサーバーを削除できます。
- ホストサーバーが SCVMM でプロビジョニングされており、アプライアンス内に存在する場合は、先に SCVMM 内でそのサーバーを削除してから、そのサーバーをアプライアンスから削除します。

  DLCI コンソールで、次の手順を実行します。

- 未割り当てサーバーを削除する場合、**Unassigned Servers**（未割り当てサーバー）でサーバーを選択して **Delete**（削除）をクリックし、確認メッセージが表示されたら **Yes**（はい）をクリックします。
- ホストサーバーを削除するには、**Host Servers**（ホストサーバー）でサーバーを選択して **Delete**（削除）をクリックし、確認メッセージが表示されたら **Yes**（はい）をクリックします。

デバイスインベントリの表示

Device Inventory（デバイスインベントリ）ページには、未割り当てサーバーとホストサーバーがリストされます。サーバーのホスト名または IP アドレスを使用して、適合ステータスやファームウェアバージョンなどのサーバー詳細を確認できます。
デバイスインベントリ ページからは、以下の操作を実行できます。

- サーバーの検出
- サーバー情報の更新
- DLCI コンソールからのサーバーの削除
- SC2012 VMM との同期化
- 同期化エラーの解決
- サーバーが所属するクラスタグループとシャーシへのホストサーバーの関連付け
- iDRAC コンソールの起動

未割り当てサーバーがモジュラーサーバーの場合、そのモジュラーサーバーが収容されているシャーシのシャーシサービスタグがインベントリ詳細に追加されます。

ホストサーバーがクラスタの一部の場合、サーバーをそのクラスタグループに関連付ける、およびシャーシ情報を調べるには、クラスタ FQDN とシャーシサービスタグを参照してください。

前のバージョンのアプライアンスで検出されたサーバーを操作するには、それらのサーバーを再検出してください。

サーバを表示するには、次の手順を実行します。

DLCI コンソールで **デバイスインベントリ** をクリックします。

SC2012 VMM との同期化

SC2012 VMM 環境内のすべての Dell Hyper-V ホスト、Hyper-V ホストクラスタ、およびモジュラー Hyper-V ホストをアプライアンスと同期できます。また、同期化後にサーバーの最新のファームウェアインベントリを取得することもできます。

同期化についてのメモ：

- 同期化には、サーバーのデフォルト iDRAC 資格情報プロファイルの詳細情報が使用されます。
- SC2012 VMM でホストサーバーのベースボード管理コントローラ（BMC）に iDRAC IP アドレスが設定されていない場合、ホストサーバーをアプライアンスと同期することはできません。したがって、SC2012 VMM で BMC を設定してから（詳細については、`technet.microsoft.com` にある MSDN 記事を参照）、アプライアンスを SC2012 VMM と同期します。

- SC2012 VMM R2 は環境内で多数のホストをサポートするため、同期化は長い時間がかかるタスクです。同期化は次のように実行されます。

  a. SC2012 VMM 環境に登録されているホストが、アプライアンスの **Host**（ホスト）タブに追加されます。

  b. SC2012 VMM 環境から削除されたホストサーバーが再同期されると、ホストサーバーは再同期化中にアプライアンスの **Unassigned**（未割り当て）タブに移動されます。サーバーが廃止される場合は、そのサーバーを未割り当てサーバーのリストから削除します。

  c. サーバーが未割り当てサーバーとしてリストされており、SCVMM に手動で追加されると、そのサーバーは同期化後にアプライアンスの **hosts**（ホスト）タブに追加されます。

  d. ホストサーバーが Hyper-V クラスタに属している場合、クラスタの詳細情報をデバイスインベントリで使用できます。このホストサーバーは、クラスタアップデートグループに追加または移動されます。

  e. ホストがモジュラーサーバーの場合、そのモジュラーサーバーが収容されているシャーシのサービスタグがデバイスインベントリページに追加されます。モジュラーサーバーが Hyper-V クラスタに属していない場合、そのホストサーバーはシャーシアップデートグループに追加または移動されます。

  f. ホスト名、iDRAC IP アドレス、メモリ、クラスタメンバーシップなどのホストインベントリの詳細情報に対する変更は、いずれもデバイスインベントリでアップデートされます。

  g. SCVMM 用 DLCI は、最新のファームウェアインベントリ情報を提供することができます。デフォルトのアップデートソースが提供されると、ファームウェアインベントリがアップデートソースと比較され、最新の情報がアップデートグループに追加されます。

SCVMM とのアプライアンスの同期

同期を実行するには、次の手順を実行します。

DLCI for SC2012 VMM（C2012 VMM 用 DLCI）で、**Device Inventory**（デバイスインベントリ）をクリックしてから **Synchronize with SCVMM**（SCVMM との同期化）をクリックします。

同期化エラーの解決

アプライアンスと同期されなかったサーバーは、iDRAC IP アドレスとホスト名と共にリストされます。

同期化エラーを解決するときには、次の点に注意してください。

- サーバーが、資格情報、iDRAC、接続、またはその他の問題により同期されない場合は、先に問題を解決し、その後で再同期します。

サーバーを再同期するには、次の手順を実行します。

1. SC2012 VMM 用 DLCI コンソールアドインで、**Device Inventory**（デバイスインベントリ）をクリックし、**Resolve Sync Errors**（同期化エラーの解決）をクリックします。
2. 同期するサーバーを選択し、資格情報プロファイルを選択、または新しい資格情報プロファイルを作成します。
3. ジョブ名を入力し、**Go to the Job List**（ジョブリストに移動）を選択してジョブステータスを表示し、**Finish**（終了）をクリックします。

iDRAC コンソールの起動

iDRAC コンソールを起動するには、次の手順を実行します。

Device Inventory（デバイスインベントリ）の **Unassigned Servers**（未割り当てサーバー）または **Hosts**（ホスト）で、**iDRAC IP** をクリックします。

7

アプライアンスのライセンス

SC2012 VMM 用 DLCI では、エージェントフリーの設定、導入、およびファームウェアアップデート機能がライセンスされています。5 つのライセンスを評価のために追加料金なしで使用することができます。この 5 つのライセンスをダウンロードするには、`marketing.dell.com/software-download-DLCISCVMM` にアクセスしてください。ライセンス付与の詳細については、Dell TechCenter ウェブサイトに移動し、OpenManage Integration Suite for Microsoft System Center wiki ページにアクセスしてください。

ライセンスの詳細を表示するには、**DLCI Admin Portal — SC2012 VMM**（DLCI 管理ポータル - SC2012 VMM）から **License Center**（ライセンスセンター）を起動します。

8

サーバー管理

Maintenance Center（メンテナンスセンター）を使用して、Dell アップデートの管理に関連するすべてのタスクを SCVMM 環境内で実行することができます。デルの推奨に従った Dell サーバーコンポーネントの最新ファームウェアバージョンを維持することができます。

保護ボールト、アップデートソース、カスタムグループを表示、作成、および維持したり、事前定義されたアップデートグループを表示したりできます。ファームウェアアップデートのジョブを作成およびスケジュールしたり、アップデートソースで新しいカタログが入手可能なときにアラートを受信するための通知をスケジュールしたりできます。既存のファームウェアバージョンとベースラインバージョンの比較レポートが提供され、この情報に基づいて、インベントリファイルを作成し、サーバープロファイルをインポートおよびエクスポートできます。また、アップデート、サーバーコンポーネント、およびサーバーモデルのタイプに基づいて情報をフィルタリングすることもできます。

iDRAC アップデートは最小適合バージョン以降でしか使用できないため、アップデートを実行できるのは適合サーバー上のみです。

メモ:

- SC2012 VMM 用 DLCI バージョン 1.1 からバージョン 1.2 にアップグレードした後、以前に検出されたすべてのサーバーが**デフォルトの未割り当てアップデートグループ**または**デフォルトのホストアップデートグループ**に追加されます。これらのサーバーをそれぞれの事前定義されたアップデートグループに追加するには、サーバーを再検出してください。
- SC2012 VMM 用 DLCI バージョン 1.2 にアップグレードした後、**ftp.dell.com** または **downloads.dell.com** への接続が失敗する場合、デフォルトの Dell オンライン FTP、または Dell HTTP アップデートソースは、カタログファイルをダウンロードできず、したがって、比較レポートは使用できません。比較レポートを表示するには、デフォルトの Dell オンライン FTP、または Dell HTTP アップデートソースを編集し、プロキシ資格情報を作成し、**Select Update Source**（アップデートソースの選択）ドロップダウンメニューから同じものを選択します。アップデートソースの編集方法の詳細については、「アップデートソースの変更」を参照してください。
- SC2012 VMM 用 DLCI バージョン 1.2 にアップグレードした後、**ftp.dell.com** または **downloads.dell.com** への接続が失敗する場合、デフォルトの Dell オンライン FTP、および Dell HTTP アップデートソースは、カタログファイルをダウンロードできず、したがって、比較レポートは使用できません。比較レポートを表示するには、新しいアップデートソースを作成し、**Select Update Source**（アップデートソースの選択）ドロップダウンメニューから同じものを選択します。アップデートソースの作成方法の詳細については、「アップデートソースの作成」を参照してください。

SC2012 VMM 用 DLCI は、次のアップデート処置を提供します。

- ダウングレード - アップデートソースには使用可能な以前のバージョンが存在し、ファームウェアをこのバージョンにダウングレードできます。
- 必要な処置なし - ファームウェアバージョンはリポジトリ内のものと同レベルです。
- 使用可能なアップデートなし - コンポーネントに対して使用できるファームウェアアップデートはありません。
- アップグレード（オプション）- オプションの新機能または特定の設定アップグレードで構成されたアップデートです。

- アップグレード（緊急）- BIOS などのコンポーネントにおけるセキュリティ、パフォーマンス、または破損時補償状況を解決するために使用される重要なアップデートです。
- アップグレード（推奨）- 製品のバグ修正または機能拡張を提供するアップデートで、他のファームウェアアップデートとの互換性修正も含まれています。

SC2012 VMM 用 DLCI は、ファームウェアアップデートを実行するために次の方法を提供します。

- **DRM リポジトリを使用したアップデート** - DRM のリポジトリを準備するために、検出されたサーバーのインベントリ情報をアプライアンスからエクスポートします。
  - xml ファイルをエクスポートした後で DRM にリポジトリを作成するには、**My Repositories**（マイリポジトリ）で **New**（新規）をクリックし、その後 **Dell Modular Chassis inventory**（Dell モジュラーシャーシインベントリ）をクリックします。**Modular Chassis Inventory**（モジュラーシャーシインベントリ）で、エクスポートされた xml ファイルをアプライアンスから選択します。DRM にリポジトリを作成する方法の詳細については、Dell Repository Manager のマニュアルを参照してください。
  - リポジトリが作成されたら、関連するサーバーを選択して、そのサーバー上でアップデートを開始します。必要なアップデートを準備するには、テスト環境でのテスト、セキュリティアップデート、アプリケーションの推奨事項、Dell による勧告などのその他の要因を考慮してください。
- **FTP または HTTP を使用したアップデート** - 任意の特定のコンポーネントに FTP または HTTP サイト上で提供されている最新のアップデートを適用します。Dell IT は、年 4 回のペースでリポジトリをご用意しています。
  - Dell オンラインカタログとの統合 - FTP アップデートソースの場合、Dell FTP に接続し、カタログファイルをキャッシュディレクトリにダウンロードします（HTTP アップデートソースの場合は、`downloads.dell.com` に接続します）。その後、そのファイルを参照インベントリにします。
  - アップデートソースとの比較レポートを表示し、関連するサーバーまたはサーバーコンポーネントを選択して、それらのサーバー上でアップデートを開始します。
- **ファームウェアインベントリと比較の参照** - 選択したサーバーまたはサーバーグループのファームウェアインベントリが格納されている参照インベントリファイルを作成すると、後でアプライアンス内に存在するサーバーのインベントリ情報を、保存された参照インベントリファイルと比較することができます。参照サーバーインベントリファイルには、タイプまたはモデルが同じ単一サーバーからのインベントリ情報を含めたり、タイプまたはモデルが異なる複数のサーバーを含めたりすることができます。

DRM との統合

SC2012 VMM 用 DLCI は、DRM バージョン 2.2 以降と統合され、既存のサーバーのサーバーインベントリ情報をアプライアンスから DRM に提供します。インベントリ情報を使用して、カスタムリポジトリを DRM で作成し、それを、サーバーまたはサーバーグループ上でファームウェアアップデートジョブを実行するためのアップデートソースとしてアプライアンスで設定できます。DRM でのリポジトリの作成の詳細については、Dell Repository Manager のドキュメントを参照してください。

メモ: SC2012 VMM 用 DLCI バージョン 1.2 にアップグレードした後、サーバーの再検出を実行して、DRM によって消費されているインベントリ情報を更新します。

DRM を使用してアプライアンスのリポジトリを作成するには、次の手順を実行します。

1. **Dell Repository Manager Data Center** バージョンを起動します。
2. **My Repositories**（マイリポジトリ）をクリックし、**New**（新規）をクリックし、**Dell Console Integration**（Dell コンソール統合）をクリックします。
3. **URL (Rest API)** に `https:// IP address of appliance/genericconsolerepository/` の形式で URL を入力し、**Next**（次へ）をクリックします。

4. アプライアンスで使用した **UserName**（ユーザー名）と **Password**（パスワード）を入力し、**Ok** をクリックし、**Ok** をクリックします。

フィルタ

フィルタを適用して選択された情報を比較レポートで表示します。
アプライアンスでは、次の 3 つのカテゴリのフィルタがサポートされます。

- **Nature Of Update**（アップデートの性質）- フィルタを適用し、サーバー上の選択されたタイプのアップデートのみを表示する場合に選択します。
- **Component Type**（コンポーネントタイプ）- フィルタを適用し、サーバー上の選択されたコンポーネントのみを表示する場合に選択します。
- **Server Model**（サーバーモデル）- フィルタを適用し、選択されたサーバーモデルのみを表示する場合に選択します。

メモ: フィルタが適用されている場合、サーバープロファイルをエクスポートおよびインポートすることはできません。

フィルタを適用するには、次の手順を実行します。

DLCI コンソールアドインで、**Maintenance Center**（メンテナンスセンター）をクリックし、フィルタドロップダウンメニューをクリックし、フィルタを選択します。

フィルタを削除するには、次の手順を実行します。

DLCI コンソールアドインで、**Maintenance Center**（メンテナンスセンター）をクリックしてから、**Clear Filters**（フィルタのクリア）をクリックするか、選択されているチェックボックスをクリアします。

アップデートソースの概要

アップデートソースでは、デルのアップデートソースからアップデートを選択し、適用できます。アップデートソースを作成、表示、および管理することができます。サポートされているアップデートソースのタイプは、DRM リポジトリ、FTP、および HTTP です。DRM、HTTP、または FTP アップデートソースを作成し、それをデフォルトのアップデートソースとして設定できます。

アップデートソースには、Dell アップデート（BIOS、ファームウェア、アプリケーション、ドライバ、およびドライバパック）が含まれているカタログファイルがあり、Dell Update Packages（DUP）と呼ばれる自己完結型実行可能ファイルを提供します。カタログファイルのローカルコピーは、作成時にアプライアンスにキャッシュされます。カタログファイルがアップデートソース内でアップデートされるときは、ローカルにキャッシュされているカタログファイルが自動ではアップデートされません。キャッシュに保存されているカタログファイルをアップデートするには、アップデートソースを編集するか、アップデートソースを削除して再作成します。

アップデートソースで使用可能なインベントリ情報を、選択したサーバーまたはサーバーグループインベントリ情報のインベントリ情報と比較して、ベースラインバージョンを作成することができます。また、アップデートソースを変更して、サーバーまたはサーバーグループのインベントリ情報を、選択したアップデートソースから使用できるバージョン情報と比較することもできます。

セキュリティ修正、バグ修正、および新機能の要求を使用するため、デルでは最新のファームウェアへのアップグレードをお勧めします。デルは、月に 1 回のペースで Dell FTP に投稿される PDK カタログによって次のアップデートを公開しています。

- サーバー BIOS とファームウェア

- デル認証のオペレーティングシステムドライバパック（オペレーティングシステム導入用）

事前定義されたデフォルトのアップデートソース

DELL ONLINE CATALOG（Dell Online カタログ）は、新規インストールまたはアップグレードの後にアプライアンスで使用可能な FTP タイプの事前定義されたアップデートソースです。事前定義されたアップデートソースの名前を削除、または変更することはできません。

DELL ONLINE HTTP CATALOG（Dell Online HTTP カタログ）は、新規インストールまたはアップグレードの後にアプライアンスで使用可能なデフォルトのアップデートソースです。このデフォルトアップデートソースの名前を削除または変更することはできません。ただし、別のアップデートソースを作成し、それをデフォルトアップデートソースに設定することができます。

メモ:

- SC2012 VMM 用 DLCI をインストールした後、**DELL ONLINE CATALOG**（Dell Online カタログ）と **DELL ONLINE HTTP CATALOG**（Dell Online HTTP カタログ）のアップデートソースのプロキシ詳細を追加し、それを保存します。
- SC2012 VMM 用 DLCI バージョン 1.2 へのアップグレード後、**DELL ONLINE HTTP CATALOG**（Dell Online HTTP カタログ）をデフォルトアップデートソースとして設定します。

テスト接続

アップデートソースの作成時に参照した資格情報を使用することにより、**Test Connection**（テスト接続）を使用して、アップデートソースの場所が到達可能であるかどうかを検証します。

入力した資格情報でカタログの場所にアクセス可能であることを確認できた場合にのみ、アップデートソースを作成できます。

ローカル FTP のセットアップ

ローカル FTP をセットアップするには、次の手順を実行します。

1. ローカル FTP にオンライン FTP **ftp.dell.com** と全く同一のフォルダ構造を作成します。
2. オンライン FTP から **catalog.xml.gz** ファイルをダウンロードし、ファイルを解凍します。
3. **catalog.xml** ファイルを開き、**baseLocation** をお使いのローカル FTP URL に変更して、そのファイルを **.gz** 拡張子で圧縮します。

   たとえば、**baseLocation** を `ftp.dell.com` から **ftp.yourdomain.com** に変更します。
4. カタログファイルと DUP ファイルを **ftp.dell.com** と同じ構造でローカル FTP フォルダ内に配置します。

ローカル HTTP のセットアップ

ローカルシステム上の HTTP サーバーをセットアップするには、次の手順を実行します。

1. ローカル HTTP に **downloads.dell.com** と全く同一のフォルダ構造を作成します。
2. **http://downloads.dell.com/catalog/catalog.xml.gz** のオンライン HTTP から **catalog.xml.gz** ファイルをダウンロードし、ファイルを解凍します。
3. **catalog.xml** ファイルを解凍し、**baseLocation** をお使いのローカル HTTP URL に変更して、そのファイルを **.gz** 拡張子で圧縮します。

   たとえば、**baseLocation** を **downloads.dell.com** から **hostname.com** に変更します。

4. 変更したカタログファイルを含むカタログファイル、および DUP ファイルを、**downloads.dell.com** と同じ構造でローカル HTTP フォルダ内に配置します。

アップデートソースの表示

アップデートソースを表示するには、次の手順を実行します。

1. **DLCI for SC2012 VMM**（SC2012 VMM 用 DLCI）で **Maintenance Center**（メンテナンスセンター）をクリックします。
2. **Maintenance Center**（メンテナンスセンター）で **Maintenance Settings**（メンテナンス設定）をクリックし、次に **Update Source**（アップデートソース）をクリックします。

アップデートソースの作成

前提条件：

- アップデートソースタイプに基づいて、Windows または FTP の資格情報プロファイルが必要です。
- DRM アップデートソースを作成する場合は、DRM がインストールされ、管理者役割が設定されていることを確認します。

アップデートソースを作成するには、次の手順を実行します。

1. **DLCI Console Add-in for SC2012 VMM**（SC2012 VMM 用 DLCI コンソールアドイン）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Maintenance Settings**（メンテナンス設定）をクリックします。
2. **Update Source**（アップデートソース）で **Create New**（新規作成）をクリックし、必要な情報を入力します。
   - FTP ソースを作成している場合は、FTP 資格情報を入力します。FTP サイトへの到達にプロキシ資格情報が必要な場合は、プロキシ資格情報も入力します。
   - DRM ソースを作成している場合は、Windows 資格情報を入力して Windows 共有の場所へのアクセスを確保します。場所フィールドにカタログファイルの完全なパスをファイル名も含めて入力します。

     メモ: DRM 内のアップデートソースの作成には、32 ビットの DUP のみを使用してください。
   - タイプ HTTP のアップデートソースを作成している場合は、カタログの完全なパスをカタログ名とプロキシ資格情報と一緒に入力して、アップデートソースにアクセスします。
3. （オプション）これをデフォルトのアップデートソースにするには、**Make this as default source**（デフォルトソースにする）を選択します。
4. **Test Connection**（テスト接続）をクリックしてアップデートソースの場所を検証してから、**Save**（保存）をクリックします。

   メモ: 場所が検証されたら、アップデートソースを作成することができます。

アップデートソースの変更

アップデートソースを変更する際には、次の点に注意してください。

- アップデートソースの作成後、そのアップデートソースのタイプと場所を変更することはできません。
- アップデートソースは、進行中またはスケジュールされたジョブによって使用中であっても、または導入テンプレートで使用されている場合でも、変更することができます。使用中のアップデートソースを変更しているときは警告メッセージが表示されます。**Confirm**（確認）をクリックして変更を続行してください。

アップデートソースを変更するには、次の手順を実行します。

変更するアップデートソースを選択し、**Edit**（編集）をクリックして、必要に応じてソースをアップデートします。

アップデートソースの削除

次の状況でアップデートソースを削除することはできません。

- アップデートソースが、事前定義されたアップデートソース - **Dell Online Catalog**（Dell Online カタログ）と **DELL ONLINE HTTP CATALOG**（Dell Online HTTP カタログ）である場合。
- アップデートソースが導入テンプレートで使用されている場合。
- アップデートソースが、進行中のジョブ、またはスケジュールされたジョブによって使用されている場合。
- アップデートソースがデフォルトアップデートソースである場合。

アップデートソースを削除するには、次の手順を実行します。

削除するアップデートソースを選択し、**Delete**（削除）をクリックします。

アップデートグループ

アップデートグループは、類似したアップデート管理を要求するサーバーのグループです。事前定義されたアップデートグループとカスタムアップデートグループの 2 種類のアップデートグループを使用できます。事前定義されたグループは表示することができます。カスタムアップデートグループは、作成およびメンテナンスすることができます。

メモ: SC2012 VMM 用 DLCI バージョン 1.1 からバージョン 1.2 にアップグレードした後、以前に検出されたすべてのサーバーが**汎用アップデートグループ**または**ホストアップデートグループ**に追加されます。これらのサーバーをそれぞれの事前定義されたアップデートグループに追加するには、サーバーを再検出してください。

事前定義されたアップデートグループ

事前定義されたアップデートグループの説明および挙動は次のとおりです。

- **汎用アップデートグループ**
  - **すべてのアップデートグループ**
  - **デフォルトの未割り当てサーバーアップデートグループ**
- **クラスタアップデートグループ**
- **ホストアップデートグループ**
  - **デフォルトのホストアップデートグループ**
- **シャーシアップデートグループ**

汎用アップデートグループ - このグループは、単一のセッションでアップデートされるホストと未割り当てサーバーで構成されます。

すべてのアップデートグループ - このグループは、すべてのサーバーグループで構成されます。アプライアンス内に存在するすべてのグループがこのすべてのアップデートグループのメンバーになります。このグループは、汎用アップデートグループに分類されます。

デフォルトの未割り当てサーバーアップデートグループ - このグループは、他のいずれのグループにも属していないすべての未割り当てサーバーで構成されます。このグループは、汎用アップデートグループに分類

されます。サーバーは、次の操作の後でデフォルトの未割り当てサーバーアップデートグループに追加されます。

- ベアメタルサーバーの新規検出または再検出。
- 同期化または再同期化（SCVMM から削除された後もアプライアンス内に存在している場合）。

クラスタアップデートグループ - このグループは、Windows Server フェールオーバークラスタで構成されます。モジュラーサーバーがクラスタに属している場合、そのサーバーはクラスタアップデートグループに追加されます。第 12 世代または第 13 世代の Dell PowerEdge モジュラーサーバーがクラスタに属している場合は、**Maintenance Center**（メンテナンスセンター）ページのインベントリに CMC 情報も追加されます。

サーバーが属しているクラスタアップデートグループを調べるには、アプライアンスにリストされているすべてのサーバーのホスト名とクラスタ FQDN が表示される デバイスインベントリ ページを参照します。

ホストアップデートグループ - このグループはホストサーバーで構成され、アップデートが 1 回のセッションで適用されます。つまり、1 回のセッションでグループ内のすべてのサーバーが一度にアップデートされます。

デフォルトのホストアップデートグループ - このグループは、検出されたホストのうち、他のどのアップデートグループにも属していないすべてのホストで構成されます。このグループは、ホストアップデートグループに分類されます。

シャーシアップデートグループ - シャーシに属していて、どのクラスタグループにも属さないモジュラーサーバーは、シャーシアップデートグループとして分類されます。第 12 世代、または第 13 世代の Dell PowerEdge サーバーは、それらの CMC 情報と共に検出されます。デフォルトで、グループは **Chassis-Service-tag-of-Chassis-Group** の命名形式で作成されます（たとえば、`Chassis-GJDC4BS-Group` です）。モジュラーサーバーがクラスタアップデートグループから削除されると、サーバーはその CMC 情報と共にシャーシアップデートグループに追加されます。対応するシャーシアップデートグループにモジュラーサーバーが 1 つも存在しない場合でも、シャーシ内のすべてのモジュラーサーバーはクラスタアップデートグループ内にあるため、シャーシアップデートグループは存続しても、表示されるのは CMC 情報のみです。

カスタムアップデートグループ

カスタムアップデートグループを作成、修正、および削除できます。ただし、カスタムアップデートグループには、**デフォルトの未割り当てアップデートグループ**と**デフォルトのホストアップデートグループ**からのみサーバーを追加できます。カスタムアップデートグループにサーバーを追加した後、そのサーバーは事前定義されたアップデートグループから削除されます。このサーバーはカスタムアップデートグループ内でのみ使用可能です。カスタムアップデートグループにサーバーを追加するには、サービスタグを使用してサーバーを検索します。

アップデート方法

選択したアップデートを、それに対応している選択したサーバーグループに適用できます。

- サーバーグループ上では次のアップデートを実行できます。
  - **エージェントフリーのステージングされたアップデート** - これは、ファームウェアアップデートのステージングです。すぐに適用可能で再起動を必要としないファームウェアアップデートはただちに適用されます。システムの再起動を必要とする残りのアップデートは、サーバーの再起動時に適用されます。アップデートは、iDRAC を使用して、スケジュールされた時刻にバッチで実行されます。バッチサイズは、アップデートが行われるときに決定されます。アプライアンスは、iDRAC からアップ

デートの成功が報告されると、アップデートが成功したとみなします。ジョブが iDRAC に送信された後、アップデートのステータスはアプライアンスに記録されません。そのため、インベントリを更新して、すべてのアップデートが適用されたかどうかを確認してください。アップデートジョブは、1 つのサーバーで操作が失敗するだけでも、全体が失敗となります。

- **エージェントフリーのアップデート** - これは、サーバーの即時再起動を伴う帯域外アップデートです。
- **クラスタ対応アップデート（CAU）** - クラスタアップデートグループ上で Windows CAU 機能を利用することにより、アップデート処理を自動化してサーバーの可用性を維持します。サーバー上のアップデートは、統合ゲートウェイ（IG）がインストールされている同一システム上に存在するクラスタアップデートコーディネータを介して行われ、iDRAC を経由しません。アップデートはステージングされず、すぐに適用されます。CAU を使用すると、中断やサーバーダウンタイムを最小限に抑えることができ、作業負荷への継続的な対応を可能にします。したがって、クラスタグループが提供するサービスに影響することはありません。CAU の詳細については、`technet.microsoft.com` にある「Cluster-Aware Updating Overview」（クラスタ対応更新を使って可用性を維持したままフェールオーバークラスタを更新する：シナリオの概要）セクションを参照してください。

アップデートグループについてのメモ

- 事前定義されたアップデートグループを手動で作成、変更、または削除することはできません。
- アプライアンスから CMC ファームウェアを直接アップデートすることはできません。ただし、CMC 内に存在するモジュラーサーバーのファームウェアはアップデートできます。CMC ファームウェアのアップデートについては、『Dell PowerEdge M1000e Chassis Management Controller Firmware User's Guide』（Dell PowerEdge M1000e Chassis Management Controller Firmware ユーザーズガイド）の「Updating CMC firmware」（CMC ファームウェアのアップデート）を参照してください。VRTX での CMC ファームウェアのアップデートについては、『Dell Chassis Management Controller for Dell PowerEdge VRTX User's Guide』（Dell Chassis Management Controller for Dell PowerEdge VRTX ユーザーズガイド）の「Updating firmware」（ファームウェアのアップデート）を参照してください。FX2 での CMC ファームウェアのアップデートについては、『Dell Chassis Management Controller for Dell PowerEdge FX2 User's Guide』（Dell Chassis Management Controller for Dell PowerEdge FX2 ユーザーズガイド）の「Updating firmware」（ファームウェアのアップデート）を参照してください。

アップデートグループの表示

アップデートグループを表示するには、次の手順を実行します。

1. **DLCI for SC2012 VMM**（SC2012 VMM 用 DLCI）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Maintenance Settings**（メンテナンス設定）をクリックします。
2. **Maintenance Settings**（メンテナンス設定）で、**Update Groups**（アップデートグループ）をクリックします。

カスタムアップデートグループの作成

カスタムアップデートグループを作成するには、次の手順を実行します。

1. **DLCI for SC2012 VMM**（SC2012 VMM 用 DLCI）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Maintenance Settings**（メンテナンス設定）をクリックします。
2. **Maintenance Settings**（メンテナンス設定）で、**Update Groups**（アップデートグループ）をクリックし、**Create**（作成）をクリックします。

   Firmware Update Group（ファームウェアアップデートグループ）ページが表示されます。
3. 詳細を入力し、作成するアップデートグループのタイプを選択します。

   カスタムアップデートグループは、次のアップデートグループタイプを形成するサーバーのみを持つことができます。

   - 汎用ホストアップデートグループ - デフォルトの未割り当てアップデートグループとホストアップデートグループのサーバーで構成されます。

- ホストアップデートグループ - デフォルトのホストアップデートグループのサーバーで構成されます。

4. サーバーをアップデートグループに追加するには、サービスタグを使用してサーバーを検索し、**Save**（保存）をクリックします。

カスタムアップデートグループの変更

カスタムアップデートグループを変更する際には、次の点に注意してください。

- アップデートグループは、作成後にタイプを変更することはできません。
- カスタムアップデートグループのサーバーを別のカスタムアップデートグループに移動させるには、次の手順を実行します。
  - 既存のカスタムアップデートグループからそのサーバーを削除します。その後、そのサーバーは、事前定義されたアップデートグループに自動的に追加されます。
  - 次に、そのサーバーを追加するようにカスタムグループを編集し、サービスタグを使用してそのサーバーを検索します。

カスタムアップデートグループを変更するには、次の手順を実行します。

1. **DLCI for SC2012 VMM**（SC2012 VMM 用 DLCI）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Maintenance Settings**（メンテナンス設定）をクリックします。
2. **Maintenance Settings**（メンテナンス設定）で、**Update Groups**（アップデートグループ）をクリックし、アップデートグループを選択し、**Edit**（編集）をクリックしてアップデートグループを変更します。

カスタムアップデートグループの削除

次のような状況でカスタムアップデートグループを削除する場合は、次の点に注意してください。

- ジョブがスケジュール済み、進行中、または待機中の場合は、アップデートグループを削除することはできません。
- サーバーがアップデートグループ内に存在する場合でも、アップデートグループを削除することができます。ただし、そのようなアップデートグループを削除した後、サーバーは、それぞれの事前定義されたアップデートグループに移動されます。

カスタムアップデートグループを削除するには、次の手順を実行します。

1. **DLCI for SC2012 VMM**（SC2012 VMM 用 DLCI）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Maintenance Settings**（メンテナンス設定）をクリックします。
2. **Maintenance Settings**（メンテナンス設定）で、**Update Groups**（アップデートグループ）をクリックし、アップデートグループを選択し、**Delete**（削除）をクリックしてアップデートグループを削除します。

サーバー上でのアップデートの適用

ファームウェアアップデートジョブを作成することにより、サーバーまたはサーバーグループ上でアップデートを即時適用またはスケジュールすることができます。アップデート用に作成されたジョブは、**Job Viewer**（ジョブビューア）の下で一覧表示されます。また、**Allow Downgrade**（ダウングレードを許可）を選択することにより、ファームウェアバージョンを、提案されたバージョンにダウングレードすることもできます。このオプションが選択されていない場合は、ファームウェアのダウングレードを必要とするコンポーネントに対して何も実行しません。

メモ:

- サーバーの単一コンポーネント上で、または環境全体に対して、ファームウェアアップデートを適用することができます。
- サーバーまたはサーバーのグループに対して適用可能なアップグレードまたはダウングレードが存在しない場合、そのサーバーまたはサーバーのグループ上でファームウェアアップデートを実行しても、何も起こりません。
- コンポーネントレベルの情報をアップデートしているときに、既存のファームウェアバージョンがアップデートソースのファームウェアバージョンと同じである場合は、そのコンポーネントに対する処置は何も実行されません。

前提条件：

- サーバー上でアップデートを実行するには、Dell オンライン FTP サイト、ローカル FTP サイト、HTTP、または Dell Repository Manager（DRM）上で利用可能なアップデートソースが必要です。
- アップデートを適用する前に、アップデートが適用されるサーバー上で iDRAC ジョブキューをクリアします。
- IG ユーザーがすべてのクラスタノード上でローカル管理者権限を持っていることを確認します。
- クラスタアップデートグループ上でアップデートを適用する前に、クラスタ準備レポートで次の点をチェックします。
  - アップデートソースへの接続性。
  - フェールオーバークラスタの可用性。
  - Windows Server 2012 または Windows Server 2012 R2 OS がすべてのフェールオーバークラスタノードにインストールされていて CAU 機能をサポートしていることを確認します。
  - 自動アップデートの設定が、いずれのフェールオーバークラスタノード上でもアップデートを自動的にインストールするようになっていないこと。
  - フェールオーバークラスタ内の各ノード上のリモートシャットダウンを許可するファイアウォールルールの有効化。
  - 設定されている更新実行オプションを検証します。詳細については、**technet.microsoft.com** にある「Requirements and Best Practices for Cluster - Aware Updating」（クラスタ対応更新の要件とヒント集）セクションを参照してください。
  - クラスタグループには、少なくとも 2 つのノードが必要です。
  - クラスタアップデート準備をチェックします。CAU に関する詳細については、**technet.microsoft.com** にある「Requirements and Best Practices for Cluster - Aware Updating」（クラスタ対応更新の要件とヒント集）セクションを参照してください。

メモ: CAU 方法を適用するためのレポート内に重大なエラーおよび警告がないことを確認してください。

サーバー上でアップデートを適用するには、次の手順を実行します。

1. SC2012 VMM 用 DLCI コンソールアドインで、**Maintenance Center**（メンテナンスセンター）をクリックし、サーバーまたはサーバーグループとアップデートソースを選択して、**Run Update**（アップデートの実行）をクリックします。

   メモ:

   - コンポーネントレベルのアップデートの場合、サーバーグループをコンポーネントレベルに展開し、**Run Update**（アップデートの実行）をクリックします。
   - 第 11 世代の Dell PowerEdge サーバー用のファームウェアアップデートを実行するときに、電源装置ユニット（PSU）ファームウェアバージョンをアップグレードすることはできません。

2. **Update Details**（アップデート詳細）で、ファームウェアアップデートジョブの名前と説明を入力します。

3. **Schedule Update**（アップデートのスケジュール）で、次のいずれかを選択します。
   - **Run Now**（今すぐ実行） - アップデートを今すぐ適用します。
   - 日付と時刻を選択して、今後のファームウェアアップデートをスケジュールします。
4. アップデートの方法を **Agent-free Update**（エージェントフリーアップデート）または **Agent-free Staged Update**（エージェントフリーステージドアップデート）を使用して選択し、**Finish**（終了）をクリックします。

   メモ: ファームウェアアップデートジョブを iDRAC に送信した後、アプライアンスは、そのジョブのステータスについて iDRAC と通信し、管理コンソールの **Jobs**（ジョブ）と **Activity Log**（アクティビティログ）でステータスアップデートを提供します。iDRAC は、アプライアンスによって追跡されているジョブに関してステータスアップデートを提供しないことがあります。アプライアンスは最大 6 時間待機し、それでも iDRAC から応答がなければ、そのファームウェアアップデートジョブのステータスは失敗と見なされます。

ポーリングと通知

システム生成時に新しいカタログが使用可能になっているときの通知と、デフォルトのアップデートソースを受信できます。

使用可能な新しいカタログファイルがアップデートソースに存在する場合、通知ベルの色はオレンジ色に変化します。ベルアイコンをクリックすると、ローカルにキャッシュされている、アップデートソースで使用可能なカタログが置き換えられます。最新のカタログが古いカタログと置き換えられると、ベルの色は緑色に変化します。

通知の設定

ポーリングの頻度を設定するには、次の手順を実行します。

1. **SC2012 VMM 用 DLCI** で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Maintenance Settings**（メンテナンス設定）をクリックし、**Polling and Notification**（ポーリングと通知）をクリックします。
2. ポーリングの発生頻度を選択します。
   - **Never**（行わない）- デフォルトでは、このオプションが選択されます。アップデートソースから入手可能な新しいカタログに関するアップデートを、スケジュールされた時間に一度だけ受信する場合に選択します。
   - **Once a week**（1 週間に 1 回）- アップデートソースから入手可能な新しいカタログに関するアップデートを 1 週間に 1 回受信する場合に選択します。
   - **Once every 2 weeks**（2 週間に 1 回）- アップデートソースから入手可能な新しいカタログに関するアップデートを 2 週間に 1 回受信する場合に選択します。
   - **Once a month**（1 ヶ月に 1 回）- アップデートソースから入手可能な新しいカタログに関するアップデートを 1 ヶ月に 1 回受信する場合に選択します。

保護ボールト

保護ボールトは、サーバーまたはサーバーグループのサーバープロファイルをエクスポートおよびインポートできるセキュアな場所です。このサーバープロファイルは、外部ボールトを作成することによってネットワーク内の共有の場所に、あるいは内部ボールトを作成することによって vFlash SD カードに保存することができます。1 つのインスタンスにおいて、1 つのサーバーまたはサーバーグループのみを 1 つの保護ボールトに関連付けることができます。ただし、1 つの保護ボールトを複数のサーバーまたはサーバーグループに関連付けることができます。

保護ボールトの作成

前提条件：ボールトの場所がアクセス可能であることを確認してください。
保護ボールトを作成するには、次の手順を実行します。

1. **DLCI for SC2012 VMM**（SC2012 VMM 用 DLCI）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Maintenance Settings**（メンテナンス設定）をクリックします。
2. **Maintenance Center**（メンテナンスセンター）で、**Protection Vault**（保護ボールト）をクリックし、**Create**（作成）をクリックします。
3. 使用する保護ボールトのタイプを選択し、必要な詳細を入力します。
   - **Network Share**（ネットワーク共有）タイプの保護ボールトを作成する場合は、プロファイルを保存する場所、この場所にアクセスするための資格情報、およびプロファイルを保護するためのパスフレーズを入力します。このタイプの保護ボールトは、Common Internet File System（CIFS）タイプのファイル共有をサポートしています。
   - **vFlash** タイプの保護ボールトを作成する場合は、プロファイルを保護するためのパスフレーズを入力します。

保護ボールトの変更

保護ボールトを変更するときには、次の点に注意してください。

- 保護ボールトの名前、説明、タイプ、およびパスフレーズを変更することはできません。

保護ボールトを変更するには、次の手順を実行します。

1. **DLCI for SC2012 VMM**（SC2012 VMM 用 DLCI）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Maintenance Settings**（メンテナンス設定）をクリックします。
2. **Maintenance Center**（メンテナンスセンター）で、**Protection Vault**（保護ボールト）をクリックし、**Edit**（編集）をクリックしてボールトを変更します。

保護ボールトの削除

次の状況で保護ボールトを削除することはできません。

- 保護ボールトがサーバーまたはサーバーグループに関連付けられている。
- 保護ボールトに関連付けられているスケジュールされたジョブが存在する。このような保護ボールトを削除するには、スケジュールされたジョブを削除してから、保護ボールトを削除します。

1. **DLCI for SC2012 VMM**（SC2012 VMM 用 DLCI）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Maintenance Settings**（メンテナンス設定）をクリックします。
2. **Maintenance Center**（メンテナンスセンター）で、**Protection Vault**（保護ボールト）をクリックし、**Delete**（削除）をクリックしてボールトを削除します。

インベントリのエクスポート

SC2012 VMM 用 DLCI では、選択したサーバーおよびサーバーグループのインベントリを `inventory.xml` ファイルにエクスポートすることができます。この情報は、Windows 共有ディレクトリ内、または管理システム上に保存できます。また、このインベントリファイルを DRM にインポートし、そのインベントリファイルに基づいてリポジトリを作成して、参照設定を作成することも可能です。

Internet Explorer バージョン 10 以降の使用中にサーバー、またはサーバーグループのファームウェアインベントリをエクスポートするには、コンソールアドインの IP アドレスを **Local Intranet**（ローカルイントラネ

ット）サイトに追加します。インベントリファイルをエクスポートするには、**IE Settings（IE 設定）** → **Internet Options（インターネットオプション）** → **Advanced（詳細設定）** → **Security（セキュリティ）**に移動し、**Do not save encrypted pages to disk**（暗号化されたページをディスクに保存しない）オプションの選択を外します。

サーバーのコンポーネント情報をエクスポートすると、サーバーの完全なインベントリ情報がエクスポートされます。

検出されたサーバーのインベントリをエクスポートするには、次の手順を実行します。

DLCI Console Add-in for SC2012 VMM（SC2012 VMM 用 DLCI コンソールアドイン）の **Maintenance Center**（メンテナンスセンター）で、インベントリをエクスポートするサーバーを選択し、**Export Inventory**（インベントリのエクスポート）をクリックします。

メモ: XML ファイルをエクスポートした後、DRM にリポジトリを作成するには、**My Repositories**（マイリポジトリ）で **New**（新規）をクリックし、**Dell Modular Chassis inventory**（Dell モジュラーシャーシインベントリ）をクリックします。**Modular Chassis Inventory**（モジュラーシャーシインベントリ）で、エクスポートされた XML ファイルをアプライアンスから選択します。リポジトリ作成の詳細については、**dell.com/support/home** で入手可能な Dell Repository Manager のマニュアルを参照してください。

ファームウェア インベントリの表示と更新

サーバーまたは特定のサーバーグループを選択した後で、Dell 準拠サーバーのファームウェアインベントリを表示および更新することができます。

選択したアップデートソースに対するサーバーまたはシャーシインベントリの比較レポートを表示できます。アップデートソースを変更し、選択したサーバー、サーバーグループ、またはシャーシのインベントリ情報について変更後のアップデートソースとの比較レポートを表示できます。

サーバー、サーバーグループ、またはシャーシのファームウェアインベントリを更新して、最新の情報を表示することができます。サーバーのコンポーネント情報を更新すると、サーバーの完全なインベントリ情報が更新されます。

メモ:

- SC2012 VMM 用 DLCI バージョン 1.2 には、事前定義された FTP および HTTP アップデートソースの以前のバージョンの比較レポートを表示するカタログが同梱されています。したがって、最新の比較レポートを表示するには、最新のカタログをダウンロードしてください。
- SC2012 VMM 用 DLCI をこのバージョンにアップグレードすると、前のバージョンで検出されたサーバーに対して最新の情報が表示されません。最新のサーバー情報と正しい比較レポートを表示するには、それらのサーバーを再検出してください。

サーバーまたはサーバーグループのファームウェアインベントリを表示または更新するには、次の手順を実行します。

1. **DLCI Console Add-in for SC2012 VMM**（SC2012 VMM 用 DLCI コンソールアドイン）の **Maintenance Center**（メンテナンスセンター）で、**Select Update Group**（アップデートグループの選択）からアップデートグループを選択します。
2. （オプション）アップデートソースを変更するには、**Select Update Source**（アップデートソースの選択）からアップデートソースを選択します。
3. 現在のバージョンとベースラインバージョンのファームウェア情報、およびアプライアンスによって推奨されるアップデートアクションを表示するには、**Device Group/Servers**（デバイスグループ / サーバー）のサーバーグループをサーバーレベル、コンポーネントレベルへと順番に展開します。

メモ:
コンポーネントレベルの情報を表示しているとき、第 11 世代の PowerEdge サーバーに対する NIC 関連の情報は次のように表示されます。

- **Urgent**（緊急）の **Nature of Update**（アップデートの性質）に基づいたフィルタを適用した後は、緊急アップデートのコンポーネントのみが含まれるレポートが表示されます。このレポートがエクスポートされると、重要アップデートが後に続くダウングレードアクションを含むコンポーネントもエクスポートされます。
- 単一の NIC カードで複数のネットワークインタフェースが使用可能な場合、**Component Information**（コンポーネント情報）リストには、それらすべてのインタフェースに対して 1 つのエントリのみが存在します。ファームウェアアップデートが適用されると、それらすべての NIC カードがアップグレードされます。
- NIC カードが既存のカードと一緒に追加された場合、新たに追加された NIC カードは、**Component Information**（コンポーネント情報）リストに別のインスタンスとして表示されます。ファームウェアアップデートが適用されると、すべての NIC カードがアップグレードされます。

4. 更新するサーバーまたはサーバーグループを選択し、**Refresh Inventory**（インベントリの更新）をクリックします。

サーバープロファイルのエクスポート

BIOS、RAID、NIC、iDRAC、Lifecycle Controller などの各種コンポーネント上にインストールされたファームウェアイメージとそれらのコンポーネントの設定を含む、サーバープロファイルをエクスポートできます。アプライアンスは、すべての設定が含まれるファイルを作成します。このファイルは、vFlash SD カードまたはネットワーク共有に保存することができます。このファイルを保存するために、任意の保護ボールトを選択します。サーバーまたはサーバーグループの設定プロファイルをすぐにエクスポートしたり、後日にスケジュールしたりすることができます。また、サーバープロファイルがエクスポートされる頻度について、関連する反復オプションを選択することもできます。設定のエクスポートジョブは、サーバーグループに対して一度に 1 つしかスケジュールできません。設定プロファイルをエクスポート中のサーバーまたはサーバーグループに対して他のアクティビティを実行することはできません。

メモ:

- iDRAC で**自動バックアップ**ジョブが同じ時間にスケジュールされていないことを確認します。
- フィルタを適用してからサーバープロファイルをエクスポートすることはできません。サーバープロファイルをエクスポートするには、適用されているすべてのフィルタをオフにします。

エクスポートジョブの作成

サーバー設定をエクスポートするには、次の手順を実行します。
前提条件：**BIOS Settings**（BIOS 設定）で **F1/F2 Prompt on Error**（エラー時に F1/F2 プロンプト）を無効にしてください。

1. **DLCI Console Add-in for SC2012 VMM**（SC2012 VMM 用 DLCI コンソールアドイン）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Export Server Profile**（サーバープロファイルのエクスポート）をクリックします。
2. **Export Profile**（プロファイルのエクスポート）で、ジョブの詳細を入力し、保護ボールトを選択します。

   Export Server Profile（サーバープロファイルのエクスポート）で、次を選択します。

   - **Run Now**（今すぐ実行）- 選択したサーバーまたはサーバーグループのサーバー設定をすぐにエクスポートします。

- **Schedule**（スケジュール）- 選択したサーバーグループのサーバー設定をエクスポートするためのスケジュールを提供します。
  - **Never**（行わない）- スケジュールされた時間中に一度だけサーバープロファイルをエクスポートする場合に選択します。
  - **Once a week**（1 週間に 1 回）- 1 週間に 1 回でサーバープロファイルをエクスポートする場合に選択します。
  - **Once every 2 weeks**（2 週間に 1 回）- 2 週間に 1 回でサーバープロファイルをエクスポートする場合に選択します。
  - **Once every 4 weeks**（4 週間に 1 回）- 4 週間に 1 回でサーバープロファイルをエクスポートする場合に選択します。

サーバー設定のエクスポートジョブのキャンセル

エクスポートジョブをキャンセルするには、次の手順を実行します。

1. **DLCI Console Add-in for SC2012 VMM**（SC2012 VMM 用 DLCI コンソールアドイン）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Manage Jobs**（ジョブの管理）をクリックします。
2. フィルタから **Export and Import Jobs**（エクスポートおよびインポートジョブ）を選択し、キャンセルするジョブを選択し、ジョブが **Scheduled**（スケジュール済み）状態であることを確認します。
3. **Cancel**（キャンセル）をクリックし、**Yes**（はい）をクリックします。

サーバープロファイルのインポート

すでに同じサーバーまたはサーバーグループに対してエクスポートされたサーバープロファイルをインポートすることができます。サーバープロファイルのインポートは、プロファイルに保存されている状態にサーバーの設定およびファームウェアを復元する際に役立ちます。そのような場合、そのサーバーまたはサーバーグループの以前にエクスポートしたサーバープロファイルをインポートして、そのサーバーまたはサーバーグループのサーバープロファイルを置き換えることができます。

サーバープロファイルは次の 2 つの方法でインポートできます。

- サーバープロファイルのクイックインポート - そのサーバーの最新のエクスポートされたサーバープロファイルを自動的にインポートできます。この操作では、個々のサーバーの個別のサーバープロファイルを選択する必要はありません。
- サーバープロファイルのカスタムインポート - 個別選択したサーバーのそれぞれのサーバープロファイルをインポートできます。たとえば、サーバープロファイルのエクスポートがスケジュールされていて、サーバープロファイルが毎日エクスポートされる場合、この機能により、そのサーバーの保護ボールト内の使用可能なサーバープロファイルのリストから、インポートされる特定のサーバープロファイルを選択できます。

サーバープロファイルのインポートのメモ：

- そのサーバーのエクスポートされたサーバープロファイルのリストからのみサーバープロファイルをインポートできます。別のサーバーまたはサーバーグループの同じサーバープロファイルをインポートすることはできません。別のサーバーまたはサーバーグループのサーバープロファイルをインポートしようとすると、そのサーバープロファイルのインポートジョブは失敗します。
- 特定のサーバーまたはサーバーグループのサーバープロファイルイメージが使用できない場合、その特定のサーバーまたはサーバーグループに対してサーバープロファイルのインポートジョブが試行されると、それを実行する、サーバープロファイルを持たないそれらの特定のサーバーに対してサーバープロファイルのインポートジョブは失敗し、ログメッセージが失敗の詳細とともにアクティビティログに追加されます。
- サーバープロファイルをエクスポートした後、いずれかのコンポーネントがサーバーから削除され、その後にプロファイルのインポートジョブが開始されると、欠落しているコンポーネント情報がスキップされ

ることを除けば、すべてのコンポーネント情報が復元されます。スキップされた情報は、SC2012 VMM 用 DLCI のアクティビティログでは入手できません。欠落しているコンポーネントについて詳細を知るには、iDRAC の **LifeCycle Log**（LifeCycle ログ）を参照してください。

- フィルタを適用してからサーバープロファイルをインポートすることはできません。サーバープロファイルをインポートするには、適用されているすべてのフィルタをオフにします。

サーバープロファイルのインポート

検出されたサーバーのインベントリをインポートするには、次の手順を実行します。

1. **DLCI for SC2012 VMM**（SC2012 VMM 用 DLCI）の **Maintenance Center**（メンテナンスセンター）で、インポートするプロファイルを持つサーバーを選択し、**Import Server Profile**（サーバープロファイルのインポート）をクリックします。
2. 必要な詳細を入力し、**Import Server Profile Type**（サーバープロファイルのインポートタイプ）で必要なタイプを選択し、**Finish**（終了）をクリックします。

   メモ: サーバーの現在の RAID 設定を保存する必要がない場合は、**Preserve Data**（データを保存する）オプションをクリアしてください。

ジョブの管理

ファームウェアアップデート、サーバー設定のエクスポートおよびインポートのすべてのジョブがそれらのステータス情報とともに一覧表示されます。また、スケジュールされているジョブはキャンセルすることもできます。

ファームウェアアップデートジョブのキャンセル

前提条件：ジョブが **Scheduled**（スケジュール済み）状態であることを確認してください。
スケジュールされたファームウェアアップデートジョブをキャンセルするには、次の手順を実行します。

1. **DLCI for SC2012 VMM**（SC2012 VMM 用 DLCI）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Manage Jobs**（ジョブの管理）をクリックします。
2. キャンセルするジョブを選択し、**Cancel**（キャンセル）をクリックし、**Yes**（はい）をクリックします。

9

プロファイルとテンプレート

資格情報プロファイルについて

資格情報プロファイルは、ユーザーの役割ベースの機能を認証することにより、ユーザー資格情報の使用と管理を簡素化します。各資格情報プロファイルには、単一ユーザーアカウントのユーザー名とパスワードが含まれています。資格情報プロファイルは、ユーザーの役割ベースの機能を認証します。アプライアンスは、資格情報プロファイルを使用して管理下システムの iDRAC に接続します。

また、資格情報プロファイルは、FTP サイトや Windows 共有で使用可能なリソースへのアクセスに使用したり、iDRAC のさまざまな機能を操作する際に使用することができます。

資格情報プロファイルには、4 つのタイプのプロファイルを作成することができます。

- デバイス資格情報プロファイル - このプロファイルは、iDRAC または Chassis Management Controller（CMC）へのログインに使用されます。

  メモ:

  – デフォルトプロファイルが作成または選択されていない場合は、デフォルトの iDRAC 工場出荷時設定が使用されます。デフォルトのユーザー名には `root`、パスワードには `calvin` が使用されます。

  * デフォルトの iDRAC プロファイルは、サーバーの検出時、または同期化の実行時にサーバーにアクセスするために使用されます。

  – デフォルトの CMC プロファイルには、ユーザー名に `root`、パスワードに `calvin` があり、モジュラーサーバーにアクセスしてシャーシに関する情報を取得するために使用されます。

  – デバイスタイプ資格情報プロファイルは、サーバーの検出、CMC へのログイン、同期化問題の解決、およびオペレーティングシステムの導入を行うために使用します。
- Windows 資格情報プロファイル - このプロファイルは、DRM アップデートソースの作成中、Windows 共有へのアクセスのために使用されます。
- FTP 資格情報プロファイル - このプロファイルは、FTP サイトへのアクセスのために使用されます。
- プロキシサーバー資格情報 - このプロファイルは、アップデート用の FTP サイトにアクセスするためのプロキシ資格情報を提供するため使用されます。

事前定義された資格情報プロファイル

SYSTEM DEFAULT FTP（システムデフォルト FTP）アカウントは、**Username**（ユーザ名）と **Password**（パスワード）が **anonymous**（匿名）の FTP 資格情報タイプの事前定義された資格情報プロファイルです。このアカウントは編集できません。このプロファイルは、`ftp.dell.com` にアクセスするために使用されます。

資格情報プロファイルの作成

資格情報プロファイルを作成するときには、次の点に注意してください。

- デバイスタイプ資格情報プロファイルが作成されると、サーバーを管理するために **SC2012 VMM** で関連する **RunAsAccount** が作成され、その RunAsAccount の名前は `Dell_CredentialProfileName` になります。
  - （推奨）**RunAsAccount** を編集または削除しないでください。
- 資格情報プロファイルが作成されておらず、iDRAC 用のデフォルトの資格情報プロファイルがない場合、iDRAC の工場出荷時にデフォルトで設定される資格情報プロファイルが自動検出時に使用されます。デフォルトのユーザー名には **root**、パスワードには **calvin** が使用されます。

資格情報プロファイルを作成するには、以下を行います。

1. SC2012 VMM 用 DLCI コンソールアドイン で、次のいずれかを実行します。
   - ダッシュボードで、**資格情報プロファイルの作成** をクリックします。
   - ナビゲーションペインで、**Profiles and Templates → Credential Profile（プロファイルとテンプレート > 資格情報プロファイル）**とクリックして、**Create**（作成）をクリックします。
2. **Credential Profile**（資格情報プロファイル）で使用する資格情報プロファイルタイプを選択し、ユーザー資格情報の詳細を入力してから **Finish**（終了）をクリックします。

   メモ: Device Credential Profile（デバイス資格情報プロファイル）を作成している場合、**iDRAC** を選択して iDRAC 用のデフォルトプロファイルにする、または **CMC** を選択して Chassis Management Controller（CMC）用のデフォルトにします。このプロファイルをデフォルトプロファイルに設定しない場合は、**None**（なし）を選択します。

資格情報プロファイルの変更

資格情報プロファイルを変更するときには、次の点に注意してください。

- 一度作成されると、資格情報プロファイルのタイプを変更することはできません。ただし、他のフィールドを変更することは可能です。変更結果を確認するには、画面を更新してください。
- ハイパーバイザー導入に使用されるデバイスタイプ資格情報プロファイルを変更することはできません。

資格情報プロファイルを変更するには、以下を行います。

変更する資格情報プロファイルを選択し、**編集** をクリックして、必要に応じてプロファイルをアップデートします。

資格情報プロファイルの削除

資格情報プロファイルを削除するときには、次の点に注意してください。

- デバイスタイプ資格情報プロファイルが削除されると、関連付けられている **RunAsAccount** も SC2012 VMM から削除されます。
- SCV2012 VMM で **RunAsAccount** が削除されると、それに対応する資格情報プロファイルがそのアプライアンスで使用不可となります。
- サーバー検出で使用される資格情報プロファイルを削除するには、検出されたサーバー情報を削除してから、資格情報プロファイルを削除します。
- 導入に使用されるデバイスタイプ資格情報プロファイルを削除するには、最初に、SCVMM 環境に導入されたサーバーを削除し、その後に資格情報プロファイルを削除します。
- アップデートソースで使用されている資格情報プロファイルを削除することはできません。

資格情報プロファイルを削除するには、次の手順を実行します。

削除するプロファイルを選択し、**Delete**（削除）をクリックします。

ハードウェアプロファイルの作成

ゴールデン設定を持つサーバーを使用することによってハードウェアプロファイルを作成し、そのプロファイルを使用して、管理下システムにハードウェア構成を適用することができます。

ハードウェア構成を管理下システムに適用する前に、管理下システムが次のパラメーターについてゴールデン設定を持つサーバーと一致していることを確認します。

- 使用できるコンポーネント
- サーバーのモデル
- RAID コントローラ
- ディスク：
  - ディスクの数
  - ディスクのサイズ
  - ディスクのタイプ

メモ: SC2012 VMM 用 DLCI をバージョン 1.0.1 からバージョン 1.2 へアップグレードしたら、SC2012 VMM 用 DLCI バージョン 1.2 で作成したハードウェアプロファイルをサーバーに適用する前に、それらを編集および保存してください。

ハードウェアプロファイルを作成するには、以下を実行します。

1. SC2012 VMM 用 DLCI コンソールアドインページで、次のいずれかを実行します。
   - ダッシュボードで、**ハードウェアプロファイルの作成** をクリックします。
   - ナビゲーションペインで、**Profiles and Templates → Hardware Profile（プロファイルとテンプレート > ハードウェアプロファイル）**とクリックして、**Create**（作成）をクリックします。
2. **ハードウェアプロファイル** のようこそ画面で、**次へ** をクリックします。
3. **Profile**（プロファイル）で、プロファイルの名前と説明、および参照サーバーの iDRAC IP を入力し、**Next**（次へ）をクリックします。

   参照サーバーのハードウェア詳細が収集され、必要なプロファイルとして保存されます。導入時に、このプロファイルがサーバーに適用されます。
4. **Profile Details**（プロファイル詳細）で、BIOS、起動、および RAID 設定を選択し、要件に基づいて DHS をカスタマイズしてから **Next**（次へ）をクリックします。

   メモ:

   ハードウェアプロファイルの作成中は、選択したプリファランスに関わらず、すべての情報が収集されます。ただし、導入中はプリファランスのみが適用されます。

   たとえば、RAID 設定を選択した場合、BIOS、起動、および RAID 設定についてのすべての情報が収集されますが、導入中は、RAID 設定のみが適用されます。
5. **概要** で **終了** をクリックします。

   このハードウェアプロファイルを使用して、これを必要な管理下システムに適用することができます。

ハードウェア構成プロファイルの変更

ハードウェア構成プロファイルを変更するときには、次の点に注意してください。

- BIOS 設定と起動順序を変更することができます。
- 第 11 世代および第 12 世代の PowerEdge サーバーの場合、RAID の DHS を **One**（1）または **None**（なし）に変更できます。第 13 世代の PowerEdge サーバーの場合、保持できるのはサーバーの既存の RAID 設定のみです。

ハードウェア構成プロファイルを変更するには、次の手順を実行します。

1. SC2012 VMM 用 DLCI コンソールで、**ハードウェアプロファイル** をクリックします。
2. 編集するプロファイルを選択し、**編集** をクリックします。
3. 必要な変更を行い、**終了** をクリックします。

ハードウェアプロファイルの削除

ハードウェアプロファイルを削除するときには、次の点に注意してください。

- ハードウェアプロファイルを削除すると、このハードウェアプロファイルに関連付けられている導入テンプレートがアップデートされます。

ハードウェア構成プロファイルを削除するには、次の手順を実行します。

1. SC2012 VMM 用 DLCI コンソールで、**ハードウェアプロファイル** をクリックします。
2. 削除するハードウェアプロファイルを選択し、**削除** をクリックします。

ハイパーバイザープロファイルの作成

ハイパーバイザープロファイルを作成し、このプロファイルを使用して、サーバーにハイパーバイザーを導入することができます。ハイパーバイザープロファイルには、カスタマイズされた WinPE ISO（WinPE ISO はハイパーバイザー導入に使用されます）、SC2012 VMM から取得されたホストグループとホストプロファイル、およびインジェクション用の LC ドライバが含まれています。

前提条件：

- 必要な WinPE ISO が作成済みであり、SC2012 VMM 用 DLCI 統合ゲートウェイの共有フォルダで使用可能になっている。WinPE イメージをアップデートするには、「WinPE イメージアップデート」を参照してください。
- SC2012 VMM で、ホストグループ、ホストプロファイル、または物理コンピュータプロファイルが作成されている。

ハイパーバイザープロファイルを作成するには、次の手順を実行します。

1. SC2012 VMM 用 DLCI コンソールアドイン で、次のいずれかを実行します。
   - ダッシュボードで、**ハイパーバイザープロファイルの作成** をクリックします。
   - 左側のナビゲーションペインで、**プロファイルとテンプレート** をクリックし、**ハイパーバイザープロファイル** をクリックして、**作成** をクリックします。
2. **ハイパーバイザープロファイルウィザード** の **ようこそ** ページで、**次へ** をクリックします。
3. **Hypervisor Profile**（ハイパーバイザープロファイル）で、プロファイルの名前と説明を入力し、**Next**（次へ）をクリックします。
4. **SC2012 VMM** 情報ページで、**SC2012 VMM ホストグループ導入先** および **SC2012 VMM ホストプロファイル / 物理コンピュータプロファイル** 情報を入力します。

5. **WinPE ブートイメージソース** で、**<Network WinPE ISO file name>.iso** 情報を入力し、**次へ** をクリックします。
6. （オプション）LC ドライバインジェクションを有効にする： 有効な場合は、関連ドライバがピックアップされるように、導入するオペレーティングシステムを選択します。**LC ドライバインジェクションの有効化** を選択し、**ハイパーバイザーバージョン** で必要なハイパーバイザーバージョンを選択します。
7. **概要** で **終了** をクリックします。

ハイパーバイザープロファイルの変更

ハイパーバイザープロファイルを変更するときには、次の点に注意してください。

- Lifecycle Controller からのホストプロファイル、ホストグループ、およびドライバを変更することができます。
- WinpE ISO 名も変更できますが、ISO を変更することはできません。

ハイパーバイザープロファイルを変更するには、次の手順を実行します。

1. SC2012 VMM 用 DLCI コンソールアドインの **ハイパーバイザープロファイル** で、変更するプロファイルを選択し、**編集** をクリックします。
2. 詳細を入力し、**終了** をクリックします。

ハイパーバイザープロファイルの削除

ハイパーバイザープロファイルを削除するときには、次の点に注意してください。

- ハイパーバイザープロファイルが削除されると、そのハイパーバイザープロファイルに関連付けられている導入テンプレートも削除されます。

ハイパーバイザープロファイルを削除するには、以下を行います。

SC2012 VMM 用 DLCI コンソールの **ハイパーバイザプロファイル** で削除するプロファイルを選択し、**削除** をクリックします。

WinPE のアップデート

SC2012 VMM の PXE（PreExecution Environment）サーバーは、WinPE イメージを作成するために必要です。WinPE ISO は、WinPE イメージおよび Dell OpenManage Deployment Toolkit（DTK）から作成されます。

メモ: WinPE ISO イメージの作成に最新バージョンの DTK を使用している場合は、**Dell OpenManage Deployment Toolkit for Windows** ファイルを使用します。**Dell OpenManage Deployment Toolkit for Windows** ファイルには、オペレーティングシステムを導入しているシステムに必須とされる必要なファームウェアバージョンが含まれています。最新バージョンのファイルを使用し、WinPE アップデート用の **Dell OpenManage Deployment Toolkit Windows Driver Cabinet** ファイルは使用しないでください。

WinPE ISO イメージを作成するには、次の手順を実行します。

1. アプライアンスに PXE サーバーを追加します。
2. PXE サーバーの追加後、**boot.wim** ファイルを PXE サーバーから SC2012 VMM 用 DLCI 統合ゲートウェイ共有 WIM フォルダにコピーします。**boot.wim** は次のパス、**C:\RemoteInstall\DCMgr\Boot\Windows\Images** にあります。

メモ: boot.wim ファイルのファイル名は変更しないでください。

DTK は自己解凍型の実行ファイルです。

DTK を使用して作業するには、次の手順を実行します。

1. DTK 実行可能ファイルをダブルクリックします。
2. DTK のドライバを抽出するには、フォルダ（例：C:\DTK501）を選択します。
3. 展開された DTK フォルダを統合ゲートウェイの DTK 共有フォルダにコピーします。たとえば \\DLCI IG Share\DTK\DTK501。

メモ: SC2012 VMM SP1 から SC2012 VMM R2 にアップグレードする場合は、Windows PowerShell 4.0 アップグレードして WinPE ISO イメージを作成する必要があります。

WinPE イメージをアップデートするには、次の手順を実行します。

1. DLCI コンソールで、**WinPE Update**（WinPE アップデート）を選択し、**Image Source**（イメージソース）の下で、**Custom WinPE Image Path**（カスタム WinPE イメージパス）に WinPE イメージパスを入力します。
   たとえば、\\DLCI IG Share\WIM\boot.wim です。
2. **DTK Path**（DTK パス）の下で、**DTK Drivers Path**（DTK ドライバパス）に、Dell Deployment Toolkit ドライバの場所を入力します。
   たとえば、\\DLCI IG Share\DTK\DTK501 です。
3. ISO 名を入力します。
4. ジョブのリストを表示するには、**ジョブリストに移動** を選択します。
   各 Windows プレインストール環境（WinPE）アップデートに、固有のジョブ名が割り当てられています。
5. **Update**（アップデート）をクリックします。
   前の手順で指定された名前の WinPE ISO は、\\DLCI IG Share\ISO の下に作成されます。

ハイパーバイザー導入について

ハイパーバイザー導入は、プロファイルベースのワークフローです。このワークフローでは、ハードウェア設定、ハイパーバイザー設定、SC2012 VMM 設定、およびファームウェアアップデートのアップデートソースを指定できます。また、ハイパーバイザー導入は、ファームウェアアップデートが失敗しても続行できます。なお、選択したサーバーまたはサーバーグループのすべてのコンポーネントは、ハイパーバイザー導入中にアップデートされます。このワークフローは、アプライアンス内のハイパーバイザー導入用のハードウェア設定とともに、ハイパーバイザープロファイルの作成時に必要な SCVMM で利用可能な論理ネットワークとホストプロファイルを使用します。ハイパーバイザー導入は、1 対 1 および 1 対多の導入をサポートしています。

導入テンプレートの作成

必要なハードウェアとハイパーバイザープロファイル、およびアップデートソースで導入テンプレートを作成し、その導入テンプレートを未割り当てサーバーに適用することができます。導入テンプレートは、一度作成すれば、何度でも使用することができます。
導入テンプレートを作成するには、次の手順を実行します。

1. アプライアンスで、次の操作のいずれかを実行します。
   - アプライアンスダッシュボードで、**導入テンプレートの作成** をクリックします。

- アプライアンスナビゲーションペインで、**プロファイルとテンプレート** をクリックしてから、**導入テンプレート** をクリックします。

2. **Deployment Template**（導入テンプレート）で、テンプレートの名前と説明を入力し、ハイパーバイザープロファイル、ハードウェアプロファイル、およびアップデートソースを選択します。
3. （オプション）アップデートソース、ハードウェアプロファイルを選択し、ファームウェアアップデートが失敗しても導入を続行するように、**Continue OSD even if firmware update fails**（ファームウェアアップデートに失敗しても OSD を続行する）を選択します。

   メモ: デフォルトでは、ダウングレードはサポートされません。
4. （オプション）ハードウェア / ハイパーバイザープロファイルが作成されていない場合は、**Create New**（新規作成）をクリックしてプロファイルを作成します。

導入テンプレートの変更

メモ: ハイパーバイザープロファイル、ハードウェアプロファイル、およびアップデートソースの名前、説明、および選択を変更することができます。

導入テンプレートを変更するには、次の手順を実行します。

1. SC2012 VMM 用 DLCI コンソールアドインで、**導入テンプレート** をクリックします。
2. 変更する導入テンプレートを選択し、**変更** をクリックします。
3. 必要な変更を行い、**終了** をクリックします。

導入テンプレートの削除

メモ: 導入テンプレートの削除は、関連付けられているハードウェア、ハイパーバイザープロファイル、およびアップデートソースには影響しません。

展開テンプレートを削除するには、以下を行います。

1. SC2012 VMM 用 DLCI コンソールアドインで、**導入テンプレート** をクリックします。
2. 削除する導入テンプレートを選択し、**削除** をクリックします。

10

ハイパーバイザーの導入

オペレーティングシステムは、適合しているサーバーにのみ導入されます。

ハイパーバイザー導入の前に、ファームウェアバージョンを ftp.dell.com または downloads.dell.com で使用可能な最新バージョンにアップグレードすることを検討してください。その後、ハイパーバイザー導入を続行します。

サーバーに導入するには、次の手順を実行します。

1. アプライアンスで、次の作業を実行します。
   - アプライアンスダッシュボードで、**Deploy Unassigned Servers**（未割り当てサーバーの導入）をクリックします。
   - アプライアンスナビゲーションペインで、**Deployment Wizard**（導入ウィザード）をクリックします。
2. **ようこそ** で、**次へ** をクリックします。
3. **サーバーの選択** で、導入先となるサーバーを選択し、使用可能なライセンスをチェックしてから、**次へ** をクリックします。
4. **Select Template and Profile**（テンプレートとプロファイルの選択）で、適切な導入テンプレート、および関連するデバイスタイプ資格情報プロファイルを選択します。

   メモ: 複数の資格情報のプロファイルを複数のサーバーに割り当てることができます。

   導入テンプレートおよび資格情報プロファイルを作成することもできます。
5. **サーバー ID** でサーバーを選択し、ホスト名、MAC アドレス、およびサーバーに適用するネットワーク情報（静的または DHCP のいずれか）を選択してから、**次へ** をクリックします。
6. **ジョブ詳細** で、ジョブを追跡するためのジョブ名、および導入状態を入力し、**次へ** をクリックします。
7. **Summary**（概要）で、入力した導入オプションを確認し、**Finish**（終了）をクリックします。
8. **確認** メッセージで **はい** をクリックします。

11

アプライアンスでの情報の表示

ジョブステータスの表示

ログされたメッセージの中から特定のアップデートジョブに関するログを素早く検索して表示するには、アップデートジョブログメッセージのタイムスタンプを参照します。ジョブは、DLCI 管理ポータル - SC2012 VMM と SC2012 VMM 用 DLCI コンソールアドインから表示することができます。

1. 左側のナビゲーションペインで、**Jobs**（ジョブ）をクリックします。
2. フィルタから、表示するジョブに基づいて、**Deployments**（導入）、**Firmware Update**（ファームウェアアップデート）、**Discovery Jobs**（検出ジョブ）、**WinPE Creation Jobs**（WinPE 作成ジョブ）、**Sync Jobs**（同期ジョブ）、または **Export and Import Jobs**（エクスポートおよびインポートジョブ）を選択します。

管理対象ジョブの表示

ファームウェアアップデートジョブを表示するには、次の手順を実行します。

DLCI for SC2012 VMM（SC2012 VMM 用 DLCI）で、**Maintenance Center**（メンテナンスセンター）をクリックし、**Manage Jobs**（ジョブの管理）をクリックします。

アクティビティログの表示

アプライアンスは、アプライアンス内で発生したすべてのアクティビティに関する情報をアクティビティログに記録します。ジョブ内で何台の、およびどのサーバーが保留になっているかなど、ジョブの詳細なステータスを表示することができます。失敗したジョブに関する情報を確認するためには、アクティビティログを表示することができます。
アクティビティログを表示するには、次の手順を実行します。

1. DLCI 管理ポータル - SC2012 VMM で、**アクティビティログ** をクリックします。
2. ページの表示を最新のアクティビティに更新するには、**Refresh**（更新）をクリックします。

アプライアンスログの表示

SC 2012 VMM 用 DLCI で実行されたアクティビティに関するログ情報が含まれているファイルのリストをウェブページで表示します。
アプライアンスログを表示するには、次の手順を実行します。

DLCI 管理ポータル - SC2012 VMM で、**Settings（設定）→ Logs（ログ）** をクリックします。

メモ: `lifecyclecontrollerlogs dir` の下にファームウェア アップデート LC ログを表示できます。ただし、第 11 世代の Dell PowerEdge サーバーの場合、iDRAC でのファームウェアアップデートジョブについては LC ログ内にエントリが存在しません。

12

トラブルシューティング

SC2012 VMM でのアカウント削除

SC2012 VMM は、**DLCI-VMM Addin Registration Profile** という名前でアプライアンスのアカウントを作成します。このプロファイルが削除されると、そのアプライアンスでの作業ができなくなります。

このアカウントは削除しないことをお勧めしますが、このアカウントが削除された場合は、アプライアンスを再インストールしてください。

比較レポートがメンテナンスセンターに表示されない

64 ビット DUP を使用してアップデートソースを作成し、そのアップデートソースを比較レポートの生成に利用すると、64 ビット DUP を使用したアップデートソースの作成に対するサポートがないため、その比較レポートは **Maintenance Center**（メンテナンスセンター）で表示できません。

回避策として、アップデートソースの作成に 32 ビット DUP を使用します。

アプライアンスと ADK の互換性の問題

互換性のないバージョンの ADK を含むソフトウェアをインストールした後、SC2012 VMM 用 DLCI の既存の機能が失敗することがあります。

この問題を回避するには、『Dell Lifecycle Controller Integration for Microsoft System Center 2012 Virtual Machine Manager Installation Guide』（Microsoft System Center 2012 Virtual Machine Manager 用 Dell Lifecycle Controller Integration インストールガイド）に記載されている前提条件に従って ADK のバージョンをアップグレードします。

空のクラスタアップデートグループが自動検出または同期化中に削除されない

クラスタグループがアプライアンスで検出されると、クラスタアップデートグループが **Maintenance Center**（メンテナンスセンター）内に作成され、すべてのサーバーがそのクラスタアップデートグループ内にリストされます。その後、SCVMM を介してすべてのサーバーをこのクラスタから削除して自動検出する、または SCVMM で同期化する場合でも、その空のクラスタアップデートグループは**メンテナンスセンター**から削除されません。

回避策として、空のサーバーグループを削除するために、サーバーを再検出します。

検出ジョブが送信されない

Backspace キーを押して検出画面上のエラーメッセージを無視すると、後続の検出ジョブがバックエンド処理に送信されません。

回避策として、現在の検出画面を閉じ、**インベントリ** ページから検出画面を再起動します。必要な情報を入力した後、新しい検出ジョブを送信します。

重複した VRTX シャーシグループが作成される

以前別のシャーシに存在したモジュラーサーバーが VRTX シャーシに追加され、検出された場合、そのモジュラーサーバーは前のシャーシサービスタグ情報を引き続き使用し、アプライアンス内に重複する VRTX シャーシグループを作成します。

これを解決するには、次の手順を実行します。

1. モジュラーサーバーをひとつのシャーシから取り外してから、別のシャーシに追加します。詳細については、『Dell PowerEdge VRTX Enclosure Owner's Manual』（Dell PowerEdge VRTX エンクロージャオーナーズマニュアル）の「Server modules」（サーバーモジュール）の項を参照してください。
2. CMC を設定します。詳細については、**dell.com/support /home** から入手可能な『Chassis Management Controller Version 2.1 for Dell PowerEdge VRTX User's Guide』（Chassis Management Controller Version 2.1 for Dell PowerEdge VRTX ユーザーズガイド）の「Installing and Setting Up CMC」（CMC のインストールとセットアップ）を参照してください。

上記のタスクを実行した後で重複したシャーシグループエントリが存在する場合は、回避策として次の手順を実行します。

1. CSIOR を有効にし、新しく追加されたモジュラーサーバー上の iDRAC をリセットします。
2. VRTX シャーシグループ内のすべてのサーバーを手動で削除し、それらのサーバーを再検出します。

IP アドレスが変更された後の別のサーバーの構成プロファイルのエクスポート

サーバー上の**サーバープロファイルのエクスポート**ジョブがスケジュールされた後、このサーバーの IP アドレスが別のサーバーに割り当てられると、アプライアンスは、この新しいサーバーのサーバープロファイルをエクスポートします。

この問題を回避するには、**サーバープロファイルのエクスポート**ジョブをキャンセルし、IP アドレスが変更されたサーバーを再検出してから、このサーバー上で**サーバープロファイルのエクスポート**ジョブをスケジュールします。

ネットワーク設定の変更後のアプライアンスへのアクセスエラー

アプライアンスをセットアップした後、ネットワーク設定が変更されても、その変更がアプライアンスに反映されないことがあります。

回避策として、これらの変更を適用するために、アプライアンスを再起動します。

SCVMM R2 のアップデート後のプラグインへのアクセスエラー

SC2012 VMM 用 DLCI プラグインがインストールされている状態で SC2012 R2 VMM 用のアップデートロールアップ 8 を適用すると、セキュリティ上の理由から、SCVMM によってエラーが表示されます。結果として、SC2012 VMM 用 DLCI プラグインにアクセスすることはできません。

回避策として、次の手順を実行します。

1. デフォルトパスにあるフォルダ **C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\<username>** を削除します。
2. SCVMM を閉じて開きなおします。
3. 『Dell Lifecycle Controller Integration for Microsoft System Center 2012 Virtual Machine Manager Installation Guide』（Microsoft System Center 2012 Virtual Machine Manager 用 Dell Lifecycle Controller Integration インストールガイド）の記載内容に従って、コンソールアドインをアンインストールし、再インポートします。

サーバーへの接続の失敗

SCVMM 環境で SC2012 VMM 用 DLCI コンソールアドインをインストールした後、DLCI コンソールアイコンをクリックすると、「`Connection to server failed`」というエラーが表示されます。

回避策として、次の手順を実行します。

- アプライアンスの IP と FQDN を信頼済みサイトとして追加します。
- アプライアンスの IP と FQDN を DNS の **Forward Lookup Zones**（前方参照ゾーン）および **Reverse Lookup Zones**（逆引き参照ゾーン）に追加します。
- **C:\ProgramData\VMMLogs\AdminConsole** ファイルにエラーメッセージがないか確認します。

アップデートソースの作成の失敗

アプライアンスの Domain Name System（DNS）ネットワーク設定が変更されると、HTTP または FTP タイプのアップデートソースの作成は失敗します。

この問題を回避するには、アプライアンスを再起動し、その後に、HTTP または FTP タイプのアップデートソースを作成します。

クラスタアップデートグループ上でのファームウェアアップデートの失敗

クラスタアップデートグループ上でファームウェアアップデートジョブをスケジュールした後、IG に到達不能、クラスタグループが応答しない、進行中のジョブのために CAU でファームウェアアップデートジョブがキャンセルされたなどのさまざまな理由でファームウェアアップデートジョブが失敗すると、DUP がダウンロードされ、クラスタグループに属している各サーバークラスタノードに配置されます。すべての DUP ファイルは Dell という名前のフォルダの下に配置され、メモリを消費します。

この問題を回避するには、Dell フォルダ内のすべてのファイルを削除してから、ファームウェアアップデートジョブをスケジュールします。

アップデートグループのスケジュールされたジョブの失敗

アップデートグループに対してジョブをスケジュールした後、そのアップデートグループからすべてのサーバーが移動され、そのアップデートグループ内にサーバーが存在しなくなると、スケジュールされたジョブは失敗します。
この問題を回避するには、スケジュールされたジョブをキャンセルし、サーバーを別のアップデートグループに追加し、そのアップデートグループに対してジョブをスケジュールします。

満杯のジョブキューによるファームウェアアップデートの失敗

アプライアンスから iDRAC に送信されたファームウェアアップデートジョブが失敗し、アプライアンスメインログに `JobQueue Exceeds the size limit. Delete unwanted JobID(s)`（ジョブキューがサイズ上限を超過しています。不要なジョブ ID を削除してください）というエラーが表示されます。

回避策として、iDRAC 内の完了したジョブを手動で削除し、ファームウェアアップデートジョブを再試行します。iDRAC 内のジョブを削除する方法の詳細については、**dell.com/support/home** にある iDRAC のマニュアルを参照してください。

システムデフォルトアップデートソースを使用した FTP への接続の失敗

アプライアンスをセットアップ、設定、またはアップグレードした後、システムによって作成されたアップデートソース **Dell Online カタログ**を使用すると、プロキシ資格情報が必要な場合は、FTP サイトへのアクセスに失敗します。

Dell Online カタログ をアップデートソースにとして使用して FTP サイトにアクセスするには、編集してプロキシ資格情報を追加してください。

ファームウェアアップデート中におけるリポジトリの作成の失敗

ファームウェアアップデート中におけるリポジトリの作成は、ネットワーク問題、不適切な資格情報、到達不能なサーバーなどが原因で失敗する場合があります。

解決策として、ファームウェアアップデート中に、アプライアンスがホストされている場所から FTP サーバーに到達できること、ネットワーク問題が発生していないことを確認し、正しい資格情報を入力してください。

カスタムアップデートグループの削除の失敗

カスタムアップデートグループに属するサーバー上でジョブをスケジュールした後、そのサーバーが SCVMM から削除され、同期が完了すると、そのサーバーは、カスタムアップデートグループから削除され、適切な事前定義されたグループに移動します。このようなカスタムアップデートグループは、スケジュールされたジョブと関連付けられているため、削除することができません。

回避策として、このカスタムアップデートグループを削除するには、スケジュールされているジョブをジョブページから削除し、その後にカスタムアップデートグループを削除します。

サーバープロファイルのエクスポートの失敗

サーバープロファイルのエクスポートジョブをスケジュールした後、サーバープロファイルがエクスポートされず、「The selectors for the resource are not valid」（リソースのセレクタが有効ではありません）というエラーメッセージが表示されます。

この問題を回避するには、iDRAC をリセットしてから、サーバープロファイルのエクスポートジョブをスケジュールします。詳細については、**dell.com/support** にある iDRAC のマニュアルを参照してください。

一部のコンポーネントで選択とは無関係にファームウェアアップデートが行われる

全く同じサーバー上にある同じコンポーネントは、それぞれのサーバー上で行われたコンポーネントの選択に関わらず、ファームウェアアップデート中にアップデートされます。この動作は、iDRAC の Enterprise ライセンスを持つ第 12 および第 13 世代の Dell PowerEdge サーバーで見られます。

回避策として、次のいずれかを行ってください。

- 同一サーバー上で無関係なアップデートが行われることを防ぐため、同一サーバー上に共通コンポーネントを適用してから、特定のコンポーネントを個々のサーバー上で別々に適用します。
- 必要なファームウェアアップデートに対応するため、停止時間が計画されているステージングされたアップデートを実行してください。

インストーラの複数のインスタンスを同じサーバー上で実行したときに発生する IG インストールの問題

IG のインストールを開始した後、IG の別のインスタンスを実行しようとすると、エラーメッセージが表示されます。OK をクリックした後、別の IG MSI ファイルを保存するかどうかを確認するメッセージが表示されます。

この問題を回避するには、このファイルを保存せず、最初のインストールを続行します。

2 時間後にサーバープロファイルのインポートジョブがタイムアウト

アプライアンスでサーバープロファイルのインポートジョブを送信した後、2 時間後にそのジョブがタイムアウトすることがあります

この問題を回避するには、次の手順を実行します。

1. F2 を押し、**BIOS Settings**（BIOS 設定）を起動します。
2. **System Setup**（セットアップユーティリティ）をクリックし、**Miscellaneous Settings**（その他の設定）を選択します。
3. **F1/F2 Prompt on Error**（エラー時に F1/F2 プロンプト）を無効にします。

次の手順を実行した後、サーバープロファイルのエクスポートジョブをスケジュールし、同じものを使用してサーバープロファイルのインポートジョブを正常に完了させます。

ハイパーバイザー導入の失敗

ハイパーバイザ導入が失敗し、アクティビティログに `Error New-SCVMHost failed with following error : An out of band operation (SMASH) for the BMC <IP ADDRESS> failed on IDRAC IP : <IP ADDRESS>`（エラー 新規 SCVM ホストが次のエラーで失敗しました： BMC <IP アドレス> の帯域外操作（SMASH）が、IDRAC IP : <IP アドレス> で失敗しました）というエラーが表示される。

このエラーは、次のいずれかの理由で発生する可能性があります。

- Dell Lifecycle Controller の状態が不良。

  解決方法として、iDRAC ユーザーインタフェースにログインして Lifecycle Controller をリセットします。

  Lifecycle Controller のリセット後、問題が解決しない場合は、次の代替手段を行います。
- アンチウイルスまたはファイアウォールにより、**WINRM** コマンドの正常実行が制限されることがあります。

  回避策については、**support.microsoft.com/kb/961804** にある KB 記事を参照してください。

ライブラリ共有内で維持されているドライバファイルを起因とするハイパーバイザー導入の失敗

ハイパーバイザ導入が失敗し、そのアクティビティログに次のエラーが表示されます。

- **Error**: `Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""`（エラー：ハイパーバイザプロファイルのホスト `<IP アドレス>` への適用中にエラーが発生しました。エラーで失敗：入力文字列：`""`）
- **Information**: `Successfully deleted drivers from library share sttig.tejasqa.com for <server uuid>`（情報：<サーバー `UUID>` のライブラリ共有 `sttig.tejasqa.com` からドライバを正常に削除しました）
- **Error**: `Deleting staging share (drivers) for <server uuid> failed.`（エラー： `<サーバー UUID>` のステージング共有（ドライバ）の削除に失敗しました。）

これらのエラーは、VMM コマンドレット `GET-SCJOB status` によって出力された例外と、ライブラリ共有内で維持されているドライバファイルが原因で発生することがあります。再試行する、または別のハイパーバイザー導入を実行する前に、これらのファイルをライブラリ共有から削除する必要があります。

ライブラリ共有からファイルを削除するには、次の手順を実行します。

1. SC2012 VMM コンソールから、**Library（ライブラリ） → Library Servers（ライブラリサーバー）**の順に選択し、ライブラリサーバーとして追加された統合ゲートウェイサーバーを選択します。
2. ライブラリサーバーで、ライブラリ共有を選択して削除します。
3. ライブラリ共有が削除された後、**\\<Integration Gateway server>\LCDriver** を使用して統合ゲートウェイ共有に接続します。
4. ドライバファイルの入ったフォルダを削除します。

これで、オペレーティングシステムを導入できるようになりました。

ファームウェアアップデート後も最新のインベントリ情報が表示されない

第 11 世代の Dell PowerEdge サーバー上でファームウェアアップデートジョブが完了していても、アプライアンスのインベントリには最新のファームウェアバージョンが表示されません。
アプライアンスでは、インベントリの更新がファームウェアアップデートジョブ完了直後に実行されるアクティビティです。ファームウェアアップデートは、PowerEdge サーバーの CSIOR アクティビティがまだ完了していなくても完了するので、以前のファームウェアインベントリ情報が表示されることになります。

回避策として、PowerEdge サーバーで CSIOR アクティビティが完了していることを確認してから、アプライアンスでファームウェアインベントリを更新します。また、エージェントフリーのステージングされたアップデートを適用した後は、サーバーの再起動も行うようにしてください。インベントリの更新方法の詳細については、「ファームウェアインベントリの表示と更新」を参照してください。

CSIOR の詳細については、**dell.com/support/home** で入手可能な『Dell Lifecycle Controller GUI User's Guide』(Dell Lifecycle Controller GUI ユーザーズガイド) 最新バージョンのトラブルシューティングの項を参照してください。

Active Directory へのサーバー追加中の SC2012 VMM エラー 21119

Active Directory にサーバーを追加している間、SC2012 VMM エラー 21119 が表示されます。`Error 21119: The physical computer with <SMBIOS GUID> did not join Active Directory in time. The comptuer was expected to join Active Directory using the computer name <host.domain>.` (エラー 210119：物理コンピュータ <SMBIOS GUID> が時間内に Active Directory に参加しませんでした。コンピュータはコンピュータ名 <ホスト.ドメイン> で Active Directory に参加する必要がありました。)
回避策として、次の手順を実行します。

1. しばらく待ってから、サーバーが Active Directory に追加されたかを確認します。
2. Active Directory にサーバーが追加されていない場合は、Active Directory にサーバーを手動で追加します。
3. SC2012 VMM にサーバーを追加します。
4. SC2012 VMM にサーバーが追加されたら、DLCI コンソールでサーバーを再検出します。
   サーバーは **ホスト** タブの下に表示されます。

アプライアンスと統合ゲートウェイ間の接続喪失

統合ゲートウェイがインストールされているサーバーを再起動すると、アプライアンスと統合ゲートウェイ間における接続が失われます。これは、ユーザーに対する統合ゲートウェイの実行ポリシーがアクティブになっていないことが原因です。統合ゲートウェイユーザーアカウントを使用して統合ゲートウェイサーバーにログインし、実行ポリシーをアクティブにします。ただし、ログイン後も、次の手順を完了するまでは接続が回復されません。
PowerShell 実行ポリシーを設定するには、次の手順を実行します。

1. ローカルシステムの PowerShell 実行ポリシーを `RemoteSigned` に設定し、**統合ゲートウェイサービスアカウント** を `Unrestricted` に設定します。

ポリシー設定の詳細に関しては、次の MSDN 記事を参照してください。

- **PowerShell 実行ポリシー**： technet.microsoft.com/en-us/library/hh847748.aspx
- **PowerShell グループポリシー**： technet.microsoft.com/library/jj149004

2. 実行ポリシーが設定されたら、統合ゲートウェイを再起動します。

Active Directory 使用時の第 11 世代 PowerEdge ブレードサーバーに対するハイパーバイザー導入の失敗

Active Directory ユーザー資格情報を使用する時に、第 11 世代の PowerEdge ブレードサーバー上でのハイパーバイザ導入に失敗します。第 11 世代 PowerEdge ブレードサーバーは、Intelligent Platform Management Interface（IPMI）プロトコルを使用して通信します。ただし、Active Directory セットアップからの資格情報の使用に対しては、IPMI 規格がサポートされていません。
これらのサーバー上でオペレーティングシステムを導入するための回避策として、サポートされている資格情報プロファイルを使用してください。

RAID10 での仮想ディスクの RAID 設定失敗

5 台以上の物理ディスクを使用して、コントローラ H200 用に RAID レベル 10 で仮想ディスクを作成すると、RAID 設定に失敗します。
5 台以上の物理ディスクを使用した RAID 10 は失敗します。

回避策として、その RAID レベルに必要な最小数の物理ディスクを使用します。

ソフトウェア RAID S130 でのホットスペアの設定に起因する RAID の設定障害

グローバルホットスペア（GHS）と DHS を含む 4 つ以上のホットスペアを RAID に設定しようとすると、ソフトウェア RAID コントローラ S130 での RAID 設定に失敗します。
回避方法：

- プロファイルに適用するホットスペア（DHS および GHS）は 3 つまでにします。
- PowerEdge RAID コントローラ（PERC）カードを使用します。

13

デルサポートサイトからの文書へのアクセス

必要なドキュメントにアクセスするには、次のいずれかの方法で行います。

- 次のリンクを使用します。
  - すべての Enterprise システム管理マニュアル — Dell.com/SoftwareSecurityManuals
  - OpenManage マニュアル — Dell.com/OpenManageManuals
  - リモートエンタープライズシステム管理マニュアル — Dell.com/esmmanuals
  - OpenManage Connection エンタープライズシステム管理マニュアル — Dell.com/OMConnectionsEnterpriseSystemsManagement
  - Serviceability Tool マニュアル — Dell.com/ServiceabilityTools
  - OpenManage Connections クライアントシステム管理マニュアル — Dell.com/DellClientCommandSuiteManuals
- Dell サポートサイトから、
  a. Dell.com/Support/Home に移動します。
  b. **製品の選択** セクションで、**ソフトウェアとセキュリティ** をクリックします。
  c. **ソフトウェアとセキュリティ** グループボックスで、次の中から必要なリンクをクリックします。
     - **エンタープライズシステム管理**
     - **リモートエンタープライズシステム管理**
     - **Serviceability Tools**
     - **Dell Client Command Suite**
     - **接続クライアントシステム管理**
  d. ドキュメントを表示するには、必要な製品バージョンをクリックします。
- 検索エンジンを使用します。
  - 検索 ボックスに名前および文書のバージョンを入力します。