OpenManage Integration for Microsoft System Center バージョン 7.0

ユーザーズ ガイド

1

2021 年 5 月
Rev. A00

メモ、注意、警告

メモ: 製品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: **ハードウェアの損傷やデータの損失の可能性を示し、その危険を回避するための方法を説明しています。**

警告: **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。**

目次

1

はじめに

Microsoft System Center 向け OpenManage Integration (OMIMSSC) は System Center 製品スイートへの統合を実現し、Lifecycle Controller (LC) に統合されている Dell Remote Access Controller (iDRAC) を使用することで、Dell EMC サーバの完全なライフサイクル管理を可能にします。

OMIMSSC は、オペレーティングシステムの導入、ハードウェアへのパッチ適用、ファームウェアのアップデート、サーバメンテナンスを行います。OMIMSSC があれば、Microsoft System Center Configuration Manager (SCCM) と統合して、従来型のデータセンターで Dell EMC サーバを管理することも、Microsoft System Center Virtual Machine Manager (SCVMM) システムとの統合によって、仮想化されたクラウド環境で Dell EMC サーバを管理することもできます。

このガイドでは、製品の使い方に関する情報と、製品のさまざまな使用事例を示します。

SCCM と SCVMM の詳細については、Microsoft のマニュアルを参照してください。

トピック：

- OMIMSSC の機能

OMIMSSC の機能

表 1. このリリースでの機能

[特長]	[説明]
Windows 以外のオペレーティングシステム (OS) の導入	Windows 以外のオペレーティングシステム(ESXi および RHEL) の導入をサポートします。
第 14 世代 PowerEdge サーバ	第 14 世代の Dell EMC PowerEdge サーバの検出と管理をサポートします。
iDRAC ロックダウンモード	第 14 世代 PowerEdge サーバ向け iDRAC ロックダウンモードをサポートします。
マルチコンソール	複数の SCCM および SCVMM コンソールと単一の OMIMSSC アプライアンスとの統合をサポートします。
検出	第 11 世代以降の PowerEdge サーバを検出し、検出したサーバを Microsoft System Center (MSSC) 環境に導入します。
MSSC との同期	登録済みの SCCM または SCVMM 環境にリストされているすべての Dell EMC ホストシステムを OMIMSSC と同期します。
ライセンスセンター	管理ポータルから OMIMSSC ライセンスを管理します。
インベントリ	Dell EMC サーバに関する重要なインベントリの詳細情報を表示します。
ハードウェアの設定	ネットワークアダプタ、ファイバチャネル、および PowerEdge サーバの PCIe コンポーネントと SSD コンポーネントの設定をサポートします。
起動メディアの作成	タスクシーケンスのメディアからのゼロタッチ導入起動メディアをサポートします。
Operational Template (運用テンプレート)	ファームウェアアップデート、ハードウェア設定、およびオペレーティングシステム導入に、統一されたテンプレートを使用します。
運用テンプレートコンプライアンス	運用テンプレートに対するハードウェア設定コンプライアンスを検証します。

表 1. このリリースでの機能（続き）

Microsoft Cluster-Aware アップデート（CAU）	Microsoft の CAU 機能を通じて、ファームウェアアップデートプロセスを自動化します。
インベントリのエクスポート	サーバインベントリとアップデートソースを比較したあと、比較レポートを CSV ファイルまたは XML ファイルにエクスポートできます。
サーバープロファイルのエクスポート	サーバプロファイルを内部または外部の場所にエクスポートします。サーバプロファイルには、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）、iDRAC、LC といったコンポーネントのファームウェアイメージなどがあります。
サーバープロファイルのインポート	現在の RAID 設定を保持または除外することにより、サーバプロファイルをインポートします。
LifeCycle Controller（LC）ログメッセージの収集と表示	LC ログメッセージのエクスポート、表示、.CSV ファイへのダウンロード、検索を行います。
ポーリングと通知	アップデートソースで新しいカタログが使用可能になったときにアラートを受信するよう通知を設定します。

2

OMIMSSC のコンポーネントについて

次のリストは、本書で使用されている OMIMSSC のコンポーネントとその名前の一覧です。

- Microsoft System Center 向け OpenManage Integration アプライアンス仮想マシン。アプライアンスとも呼ばれ、CentOS ベースの仮想マシンとして Hyper-V でホストされ、次のタスクを実行します。
  - Web Services Management（WSMAN）コマンドを使用して、iDRAC 経由で Dell EMC サーバーと対話します。
  - 管理ポータル経由での OMIMSSC アプライアンスの管理を可能にします。
- OMIMSSC 統合ゲートウェイ。統合ゲートウェイ（IG）とも呼ばれる、Windows サーバーにインストールされたウェブサービスのセットで、次のタスクを実行します。
  - SCCM または SCVMM PowerShell コマンドを実行し、SCCM または SCVMM とアプライアンスの間の中間ゲートウェイとして機能します。
  - アプライアンス向けに WinPE をカスタマイズします。
- Microsoft System Center 向け OpenManage Integration コンソール。OMIMSSC コンソールとも呼ばれます。
  - SCCM 用 OMIMSSC コンソールプラグイン。SCCM 用 OMIMSSC コンソール拡張とも呼ばれます。
  - SCVMM 用 OMIMSSC コンソールアドイン。SCVMM 用 OMIMSSC コンソール拡張とも呼ばれます。

3

管理ポータルについて

管理ポータルを使用すると、管理者として OMIMSSC にログインし、さまざまなユーザによって OMIMSSC で開始されたすべてのジョブの表示、ライセンスやコンソールの詳細情報の表示、必要なコンポーネントのダウンロード、OMIMSSC のアップグレードなどができます。管理ポータルでの使用事例とライセンスについては、次で説明します。

トピック：

IG および SCCM または SCVMM アカウントの変更

このオプションを使用すると、OMIMSSC コンソールで SCCM、SCVMM、および IG アカウントのパスワードを変更できます。

管理ポータルから SCCM、SCVMM 管理者認証情報、および IG 認証情報を変更することができます。このプロセスは連続したアクティビティです。

- IG アカウントについては、OMIMSSC でアカウントを変更する前に、次の前提条件を実行します。
  1. Active Directory の認証情報を変更します。
  2. IG インストーラーの認証情報を変更します。
- SCCM または SCVMM アカウントについては、OMIMSSC でアカウントを変更する前に、Active Directory の認証情報を変更します。

インストーラーから OMIMSSC IG アカウントを変更するには、次の手順を実行します。

1. IG インストーラーを実行します。
2. [プログラム メンテナンス] で [変更] を選択してから、[次へ] をクリックします。
3. パスワードを変更して、[次へ] をクリックします。
4. [プログラムの変更] ダイアログ ボックスで [インストール] をクリックします。
5. 変更タスクが完了したら、[終了] をクリックします。

OMIMSSC 管理ポータルでの認証情報の変更

1. OMIMSSC 管理ポータルで、[設定]、[コンソールの登録] の順にクリックします。
   登録済みコンソールが表示されます。
2. 編集するコンソールを選択し、[編集] をクリックします。
3. 新しい詳細情報を入力し、[終了] をクリックして変更を保存します。

SCCM 用 OMIMSSC コンソール拡張機能の修復

OMIMSSC ファイルが破損した場合にファイルを修復するには、次の手順を実行します。

1. SCCM 用 OMIMSSC コンソール拡張機能のインストーラーを実行します。
   [[ようこそ]] 画面が表示されます。
2. [[次へ]] をクリックします。
3. [[プログラム メンテナンス]] で、[[修復]] を選択して [[次へ]] をクリックします。
   [[プログラム修正の準備完了]] 画面が表示されます。
4. [[インストール]] をクリックします。
   進行状況画面にインストールの進行状況が表示されます。インストールが完了すると、[[InstallShield ウィザード完了]] ウィンドウが表示されます。

5. [[終了]] をクリックします。

SCVMM 用の OMIMSSC コンソール拡張機能の修復

OMIMSSC ファイルが破損した場合にそのファイルを修復するには、次の手順を実行します。

1. **SCVMM 用の OMIMSSC コンソール拡張機能**インストーラーを実行します。
2. [[プログラム メンテナンス]] で、[[修復]] を選択して [[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、[[修復]] をクリックします。
4. 修復タスクが完了したら、[[終了]] をクリックします。

OMIMSSC IG の修復

このオプションを使用すると、削除されたファイルまたは破損したファイルを再インストールしたり、OMIMSSC IG に必要なフォルダーを再作成したりすることができます。

1. OMIMSSC IG インストーラーを実行します。
2. [プログラム メンテナンス] で、[修復] を選択して [次へ] をクリックします。
3. [修復の準備完了] で、IG ユーザー アカウントのパスワードを入力し、[インストール] をクリックします。
4. 修復タスクが完了したら、[終了] をクリックします。

4

登録済み MSSC コンソールからの OMIMSSC の起動

登録済み SCCM コンソールまたは SCVMM コンソールから OMIMSSC を起動します。

トピック：

ブラウザ設定

次の操作を実行するためには、OMIMSSC を起動する前に、前提条件として OMIMSSC の IP アドレスを **Local Intranet（ローカルイントラネット）** サイトのリストに追加します。

- ファームウェアインベントリのエクスポートと表示
- LC ログの表示
- Operational Template（運用テンプレート）でのプール値のエクスポート

.CSV ファイルをダウンロードする前に、次の手順を実行します。

1. [IE Settings（IE の設定）] をクリックし、[Internet Options（インターネットオプション）] をクリックします。
2. [Advanced（詳細設定）] をクリックし、[Settings（設定）] から [Security（セキュリティ）] セクションを探します。
3. [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）] オプションをクリアし、[OK] をクリックします。

SCCM 用 OMIMSSC コンソール拡張機能の起動

SCCM 用 OMIMSSC コンソール拡張機能へのログインに使用したものと同じ認証情報を使用して、Windows OS にログインします。

SCCM コンソールで、[アセットとコンプライアンス]、[概要]、[SCCM 用 OMIMSSC コンソール拡張機能] の順にクリックします。

メモ: SCCM コンソールへの接続にリモート デスクトップ プロトコル（RDP）を使用している場合は、RDP が閉じると OMIMSSC セッションがログアウトされることがあります。そのため、RDP セッションを再度開いて、再度ログインしてください。

SCVMM 用 OMIMSSC コンソール拡張機能の起動

1. SCVMM コンソールで、[ファブリック] を選択してから、[すべてのホスト] サーバー グループを選択します。

   メモ: OMIMSSC を起動するには、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、[OMIMSSC] を選択します。

5

使用事例

OMIMSSC と互換性のあるハードウェア設定を持つサーバにのみ、OS を導入できます。OS の導入前に、ファームウェアバージョンを `ftp.dell.com` または `downloads.dell.com` から入手できる最新バージョンにアップグレードしてから、OS の導入を続行するようにしてください。OMIMSSC コンソール拡張を使用するいくつかのシナリオを次に示します。

トピック：

SCCM 向け OMIMSSC コンソール拡張を使用した OS の導入

選択したサーバに OS を導入するには、次の手順を実行します。

1. 最新の Dell Deployment ToolKit（DTK）をダウンロードし、Windows プレインストール環境（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。
2. この .wim イメージを SCCM コンソールにインポートし、SCCM で起動イメージを作成します。詳細については、*Microsoft のマニュアル*を参照してください。
3. SCCM でタスクシーケンスを作成します。詳細については、「タスクシーケンスの作成」を参照してください。
4. SCCM でタスクシーケンスメディアイメージを作成します。詳細については、*Microsoft のマニュアル*を参照してください。
5. 無人の ISO イメージを生成します。詳細については、「LC 起動メディアの作成」を参照してください。
6. [Discovery（検出）] ページを使用して、参照サーバを検出します。詳細については、「手動検出を使用したサーバの検出」を参照してください。
7. Operational Template（運用テンプレート）を作成します。詳細については、「Operational Template（運用テンプレート）の作成」を参照してください。
8. Operational Template（運用テンプレート）を割り当てます。詳細については、「Operational Template（運用テンプレート）の割り当て」を参照してください。
9. Operational Template（運用テンプレート）を導入します。詳細については、「Operational Template（運用テンプレート）の導入」を参照してください。

   メモ: ホストサーバに OS を導入する前に、SCCM でサーバの [Client（クライアント）] ステータスが **No（いいえ）** になっているようにします。

   メモ: Windows OS を SCCM 環境に正常に導入した後、サーバは OMIMSSC でホストとしてリストされていません。サーバをホストタブに表示するには、SCCM でサーバの [Client（クライアント）] ステータスが SCCM で **YES（はい）** になっていることを確認してから、OMIMSSC を SCCM と同期します。

10. [Jobs and Logs Center（ジョブとログセンター）] ページで、ファームウェアアップデートと OSD のジョブステータスを表示します。詳細については、「OMIMSSC での情報の表示」を参照してください。

SCVMM 向け OMIMSSC コンソール拡張を使用した OS の導入

選択したサーバに OS を導入するには、次の手順を実行します。

1. 最新の Dell Deployment ToolKit（DTK）をダウンロードし、Windows プレインストール環境（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。
2. SCVMM で物理コンピュータプロファイルを作成します。詳細については、SCVMM のマニュアルを参照してください。
3. SCVMM でターゲットホストグループを作成します。詳細については、SCVMM のマニュアルを参照してください。
4. SCVMM 向け OMIMSSC コンソール拡張で、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。
5. [Discovery（検出）] ページを使用して、参照サーバを検出します。詳細については、「手動検出を使用したサーバの検出」を参照してください。
6. Operational Template（運用テンプレート）を作成します。詳細については、「Operational Template（運用テンプレート）の作成」を参照してください。
7. Operational Template（運用テンプレート）を割り当てます。詳細については、「Operational Template（運用テンプレート）の割り当て」を参照してください。
8. Operational Template（運用テンプレート）を導入します。詳細については、「Operational Template（運用テンプレート）の導入」を参照してください。

表 3. 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	Operational Template（運用テンプレート）の作成時には、すべての物理コンポーネントのチェックボックスをクリアします。

9. [Jobs and Logs Center（ジョブとログセンター）] ページで、ファームウェアアップデートと OSD のジョブステータスを表示します。詳細については、「OMIMSSC での情報の表示」を参照してください。

OMIMSSC コンソール拡張を使用した Windows 以外の OS の導入

Windows 以外の種類の OS を導入するには、次の手順を実行します。

1. Operational Template（運用テンプレート）を作成します。詳細については、「Operational Template（運用テンプレート）の作成」を参照してください。
2. Operational Template（運用テンプレート）を割り当てます。詳細については、「Operational Template（運用テンプレート）の割り当て」を参照してください。
3. Operational Template（運用テンプレート）を導入します。詳細については、「Operational Template（運用テンプレート）の導入」を参照してください。

メモ:

導入中に DHCP ルックアップが失敗すると、サーバはタイムアウトし、SCCM の [Managed Lifecycle Controller（ESXi）] コレクションには移動されません。

サーバ上でのアップデートの適用

次のアップデートソースを使用すると、選択したサーバまたはサーバ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 Dell Repository Manager（DRM）リポジトリ

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。アップデートソースの詳細については、「アップデートソース」を参照してください。アップデートソースが作成されているようにします。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。
2. サーバを検出するか、サーバを登録済み MSSC と同期します。詳細については、「デバイスの検出と同期」を参照してください。サーバのインベントリが最新であるようにします。詳細については、「設定と導入の起動」を参照してください。
3. 次のいずれかのオプションを使用して、サーバをアップデートします。

- 必要なサーバグループを選択し、アップデートを適用します。詳細については、「サーバ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。
- Operational Template（運用テンプレート）のファームウェアアップデートコンポーネントを使用します。詳細については、「Operational Template（運用テンプレート）の作成」を参照してください。

4. ポーリングと通知を使用して、最新のカタログのアップデートソースを変更します。詳細については、「ポーリングと通知」を参照してください。

交換したコンポーネントの設定

交換したサーバコンポーネントを、必要なファームウェアバージョンまたは古いコンポーネントの設定、あるいはその両方にアップデートする場合は、「ファームウェアおよび構成設定の適用」を参照してください。

サーバプロファイルのエクスポートとインポート

サーバプロファイルをエクスポートおよび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 設定を含むサーバプロファイルをエクスポートし、RAID 設定を含むサーバプロファイルをインポートします。詳細については、「リカバリ」を参照してください。

6

プロファイル

プロファイルによって、資格情報を管理し、導入に向けて WinPE イメージをカスタマイズできます。OMIMSSC では、次のタイプのプロファイルがサポートされています。

トピック：

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、ユーザの役割ベースの能力を認証することにより、ユーザ資格情報の使用と管理をシンプルにします。各資格情報プロファイルには、単一ユーザアカウントのユーザ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、ユーザの役割ベースの能力を認証します。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対象システムの 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ときは、iDRAC の工場出荷時のデフォルト設定が使用されます。デフォルトのユーザ名は `root` で、パスワードは `calvin` です。

  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。

  メモ: デフォルトの CMC プロファイルは、ユーザ名が `root`、パスワードが `calvin` で、モジュラーサーバ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。

  メモ: 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時に、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に使用されます。

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、FTP タイプの資格情報の事前定義された資格情報プロファイルで、[Username (ユーザ名)] と [Password (パスワード)] は [anonymous] です。これは編集できません。このプロファイルは、`ftp.dell.com` へのアクセスに使用されます。

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、サーバを管理するために、関連する **RunAsAccount** が [SCVMM] で作成され、その [RunAsAccount] の名前は `Dell_CredentialProfileName` になります。
- 自動検出中に、iDRAC で使用可能な資格情報プロファイルがないと、工場出荷時のデフォルトの iDRAC 設定が使用されます。デフォルトユーザ名は [root] で、パスワードは [calvin] です。

1. OMIMSSC で、次のいずれかを実行して資格情報プロファイルを開きます。
   - OMIMSSC ダッシュボードで [Create Credential Profile (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(プロファイル)] > [Credential Profile(資格情報プロファイル)] をクリックし、[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のタイプを選択します。

   OMIMSSC は 4 つのタイプの資格情報プロファイルをサポートし、定義済みの資格情報プロファイルが 1 つあります。次の 4 つのタイプの資格情報プロファイルが作成できます。
   - [Device Credential Profile (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)] を作成するときは、[iDRAC] を選択して、これを iDRAC のデフォルトプロファイルにするか、[CMC] を選択して、これを Chassis Management Controller (CMC) のデフォルトプロファイルにします。このプロファイルをデフォルトプロファイルとして設定しない場合は、[None(なし)] を選択します。

     - デバイスタイプ資格情報プロファイルが作成されると、サーバを管理するために、関連する **RunAsAccount** が **SCVMM** で作成され、そのアカウントの名前は **Dell_CredentialProfileName** になります。
       - **RunAsAccount** は編集または削除しないよう推奨されています。
     - デバイスタイプ資格情報プロファイルを削除すると、関連する **RunAsAccount** も SCVMM から削除されます。したがって、対応する資格情報プロファイルが OMIMSSC で表示されなくなります。
   - [Windows Credential Profile (Windows 資格情報プロファイル)] - このプロファイルは、Windows の共有フォルダへのアクセスのために使用します。
   - [FTP Credential Profile (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します。

     メモ: アプライアンスで使用できるデフォルトの FTP 資格情報プロファイルは、[System Default FTP (システムデフォルト FTP)] です。
   - [SYSTEM DEFAULT FTP (システムデフォルト FTP)] - 事前定義された、FTP 資格情報タイプの資格情報プロファイルです。このタイプでは、パスワードフィールドは必須ではありません。
   - [Proxy Server Credentials (プロキシサーバ資格情報)] - このプロファイルは、ファームウェアのアップデートで FTP サイトのプロキシ資格情報を入力するために使用します。
3. [Domain (ドメイン)] で Windows 資格情報のドメイン詳細を入力し、[Proxy Server URL (プロキシサーバ URL)] でプロキシサーバ URL を `http://hostname:port` 形式または `http://IPaddress:port` 形式で入力し、[Default Profile for (デフォルトプロファイル)] で、このプロファイルを iDRAC または CMC にログインするためのデフォルトプロファイルにするよう選択します。このプロファイルをデフォルトプロファイルとして設定しない場合は、[None (なし)] を選択します。

   メモ: [Default Profile for (デフォルトプロファイル)] オプションは、デバイスタイプ資格情報プロファイルにのみ適用されます。
4. プロファイルが作成されるよう、[Finish (終了)] をクリックします。

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。

- 作成後、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、他のフィールドは変更できます。変更を表示するには、画面を更新します。
- 使用中のデバイスタイプ資格情報プロファイルは変更できません。
- 使用中の資格情報プロファイルは変更できません。

1. 変更する資格情報プロファイルを選択し、[Edit (編集)] をクリックして、プロファイルをアップデートします。
2. 加えた変更を保存するために、[Save (保存)] をクリックします。

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 SCVMM から削除されます。
- SCVMM で **RunAsAccount** が削除されると、対応する資格情報プロファイルが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、まず SCVMM 環境に導入されたサーバを削除してから、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。

削除する資格情報プロファイルを選択し、[Delete (削除)] をクリックします。

ハイパーバイザープロファイルについて

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)、SCVMM から取得したホストグループとホストプロファイル、インジェクション用の LC ドライバが含まれています。

メモ: ハイパーバイザープロファイルは、SCVMM 向け OMIMSSC コンソール拡張にのみ適用できます。

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、そのプロファイルを使用してオペレーティングシステムをサーバに導入できます。

- ハイパーバイザープロファイルの作成中、必要な WinPE ISO が作成され、OMIMSSC IG の共有フォルダで入手可能になります。WinPE イメージのアップデートについては、「WinPE アップデート」を参照してください。
- SCVMM 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を作成します。

1. OMIMSSC、次のいずれかのタスクを実行します。
   - OMIMSSC ダッシュボードで、[Create Hypervisor Profiles (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。
   - 左のナビゲーションペインで、[Profiles (プロファイル)] > [Hypervisor Profiles (ハイパーバイザープロファイル)] > [Create (作成)] をクリックします。
2. [Hypervisor Profile Wizard (ハイパーバイザープロファイルウィザード)] > [Welcome (ようこそ)] > [Next (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. [SCVMM] 情報ページで、次の手順を実行します。
   a. [SCVMM Host Group Destination (SCVMM ホストグループ導入先)] で、ドロップダウンメニューから SCVMM ホストグループを選択し、ホストをこのグループに追加します。
   b. [SCVMM Host Profile/Physical Computer Profile (SCVMM ホストプロファイル / 物理コンピュータプロファイル)] で、サーバに適用する設定情報を含む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を SCVMM から選択します。
5. [WinPE Boot Image Source (WinPE 起動イメージソース)] で、次の手順を実行します。
   a. オペレーティングシステムとその関連設定にアクセスする方法を選択し、[Network WinPE ISO Name (ネットワーク WinPE ISO 名)] で次の手順を実行します。
   b. 使用するオペレーティングシステム ISO を選択し、[Next (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化にするには、次の手順を実行します。
   a. 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。
   b. [Enable LC Drivers Injection (LC ドライバインジェクションの有効化)] を選択します。
   c. [Hypervisor Version (ハイパーバイザーバージョン)] で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 名は変更できます。ただし、ISO イメージを変更することはできません。

1. 編集するプロファイルを選択し、[編集] をクリックします。
2. 詳細情報を入力し、[Finish (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

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。

7

設定と導入の起動

[Configuration and Deployment (設定と導入)] ページには、未割り当てのサーバとホストサーバがすべてリストされます。サーバのホスト名または IP アドレスを使用して、サーバの詳細情報 (iDRAC の IP アドレスまたはホスト名、サーバ識別子、クラスタ FQDN、シャーシサービスタグ、サーバモデル、サーバの世代、CPU、メモリ、コンプライアンスステータス) を表示できます。[Hardware Compatibility (ハードウェア互換性)] 列にマウスを重ねると、BIOS、iDRAC、LC、およびドライバパックのバージョンを見ることができます。

OMIMSSC コンソール拡張の起動前に、iDRAC System Lockdown Mode (iDRAC システムロックダウンモード) の設定を確認します。システムロックダウンモード設定は、第 14 世代 PowerEdge サーバの iDRAC で使用できます。この設定を有効にすると、ファームウェアアップデートを含むシステム設定がロックされます。システムロックダウンモードが有効になると、ユーザはどの構成設定も変更できません。この設定の目的は、意図しない変更からシステムを保護することです。システムロックダウンモードのステータスは、サーバの iDRAC IP アドレスの前にあるロック画像で表現されます。

- システムでこの設定が有効な場合、ロック画像がサーバの iDRAC IP の横に表示されます。
- システムでこの設定が無効な場合、ロック解除画像がサーバの iDRAC IP の横に表示されます。

iDRAC システムロックダウンモードの詳細については、`dell.com/support` にある iDRAC のマニュアルを参照してください。

メモ: 第 14 世代 PowerEdge サーバでは、iDRAC コンソールから、管理対象ホストサーバのシステムロックダウンモード設定を手動で無効にするようにしてください。

[Configuration and Deployment (設定と導入)] ページを使用して、次のタスクを実行します。

- サーバーの検出
- ページを更新して、アップデートされた情報を表示
- OMIMSSC からのサーバの削除
- 登録済み MSSC との同期
- 同期化エラーの解決
- Operational Template (運用テンプレート) の割り当てと Operational Template (運用テンプレート) コンプライアンスの実行
- Operational Template (運用テンプレート) の導入
- サーバが属するクラスタグループとシャーシへのホストサーバの関連付け
- iDRAC コンソールの起動

メモ: サーバがシャーシの一部でない場合、[Chassis Service Tag (シャーシサービスタグ)] は空白で表示されます。

メモ: ホストサーバがクラスタの一部である場合、サーバをそのクラスタグループに関連付けたり、シャーシ情報を調べたりするには、[Cluster FQDN (クラスタ FQDN)] 列と [Chassis Service Tag (シャーシサービスタグ)] 列を参照してください。

メモ: 前のバージョンの OMIMSSC アプライアンスで検出されたサーバを使用するには、それらのサーバを再検出してください。

メモ: 委任された管理者として OMIMSSC にログインすると、このユーザ固有でないすべてのホストサーバと未割り当てサーバを表示できます。したがって、サーバ上で何らかの操作を実行する前に、必要な権限を持っているようにします。

メモ: サーバが Operational Template (運用テンプレート) に準拠する場合は、割り当てられた Operational Template (運用テンプレート) に対し、チェック記号の付いた緑色のボックスが表示されます。

メモ: サーバが Operational Template (運用テンプレート) に準拠しない場合は、割り当てられた Operational Template (運用テンプレート) に対し、赤色の警告メッセージが表示されます。

サーバーを表示するには、次の手順を実行します。

OMIMSSC コンソール拡張で、[Configuration and Deployment (設定と導入)] をクリックします。

メモ: このページはユーザ固有ではないため、登録済み MSSC 内に存在するすべてのサーバグループが OMIMSSC にリストされます。これらのサーバ上で何らかの操作を実行するアクセス権を持っているようにします。

検出されたサーバまたは登録済み MSSC と同期されたサーバは、すべて［ Unassigned Servers（未割り当てサーバ）］タブまたは［ Hosts（ホスト）］タブにリストされます。

8

サーバの検出と MSSC コンソールとの同期

検出とは、サポートされている PowerEdge ベアメタルサーバとホストサーバを OMIMSSC に追加するプロセスであり、MSSC コンソールと同期して、SCCM または SCVMM コンソールのホストサーバを OMIMSSC に追加できます。

トピック：

参照サーバの設定について

優先起動順序、BIOS、RAID 設定、ハードウェア設定、ファームウェアアップデート属性、およびオペレーティングシステムパラメータを、組織にとって最適となるよう完璧に調整したサーバ設定は、参照サーバ設定と呼ばれます。

これらの設定を Operational Template (運用テンプレート) にキャプチャすることで参照サーバを検出し、同じハードウェア設定を持つさまざまなサーバに、その設定を同期します。

OMIMSSC でのサーバの検出

ホストと未割り当てサーバは OMIMSSC で検出できます。検出されたサーバの情報は、OMIMSSC データベースに保存されます。

サーバの検出後は次の点に注意してください。

- 検出されたサーバは、OMIMSSC の［Configuration and Deployment (設定と導入)］ページにある［Hosts (ホスト)］タブまたは［Unassigned (未割り当て)］タブに追加されます。
- 検出されたサーバに、OMIMSSC と連携するための LC ファームウェア、iDRAC、および BIOS の対応バージョンが含まれていれば、このサーバはハードウェア互換としてマークされます。対応バージョンの詳細については、『*Microsoft System Center 向け OpenManage Integration Release Notes* (OpenManage Integration for Microsoft System Center リリースノート)』を参照してください。
- 検出されたサーバには、ライセンスが 1 つ使用されます。

  ［License Center (ライセンスセンター)］ページにある［Licensed Nodes (ライセンスされたノード)］のカウントは、検出されたサーバの数だけ減ります。

- PowerEdge サーバが導入されているオペレーティングシステムで PowerEdge サーバを検出し、そのサーバがすでに SCCM コンソールまたは SCVMM コンソールに存在する場合、このサーバはホストサーバとして、検出ジョブが開始された OMIMSSC コンソール拡張の［Hosts (ホスト)］タブにリストされます。
  - ホストがモジュラーサーバの場合、そのサーバを含むシャーシのサービスタグも［Configuration and Deployment (設定と導入)］ページに表示されます。
- SCCM または SCVMM にリストされていない PowerEdge サーバを検出すると、そのサーバは未割り当てサーバとして、登録済みのすべての OMIMSSC コンソール拡張で［Unassigned (未割り当て)］タブにリストされます。

iDRAC IP アドレスを使用すると、次の方法で Dell EMC サーバを検出できます。

- 自動検出
- 手動検出

SCCM 向け OMIMSSC コンソール拡張でのサーバの検出

サーバの検出後、サーバは SCCM の事前定義グループまたはコレクションである、[Device Collections (デバイスコレクション)] で作成された [All Lifecycle Controller Lifecycle Controller Servers collection (すべての Lifecycle Controller サーバコレクション)] または [Import Dell Server collection (Dell サーバのインポート コレクション)] のいずれかに追加されます。

検出されたサーバが SCCM に存在しない場合、または事前定義グループまたはコレクションが SCCM にない場合は、事前定義コレクションが作成され、検出されたサーバが該当するグループに追加されます。

メモ: 検出されたサーバが、OMIMSSC と連携するために必要な LC ファームウェア、iDRAC、および BIOS の対応バージョンを持っていれば、このサーバはハードウェア互換としてマークされます。対応バージョンの詳細については、『*Microsoft System Center 向け OpenManage Integration Release Notes* (OpenManage Integration for Microsoft System Center リリースノート)』を参照してください。

SCVMM 向け OMIMSSC コンソール拡張でのサーバの検出

SCVMM 向け OMIMSSC コンソール拡張で、hyper-V ホスト、モジュラー hyper-V ホスト、未割り当てサーバを検出できます。

メモ: ホストがクラスタの一部である場合は、クラスタの完全修飾ドメイン名 (FQDN) が表示されます。

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、OMIMSSC を使用して管理されるシステムです。SCCM 向け OMIMSSC コンソール拡張または SCVMM 向け OMIMSSC コンソール拡張を使用してサーバを検出するときのシステム要件は、次のとおりです。

- SCVMM 向け OMIMSSC コンソール拡張は、第 11 世代以降の PowerEdge サーバ上でモジュラー型とモノリシック型のサーバモデルをサポートします。
- SCCM 向け OMIMSSC コンソール拡張は、第 11 世代以降の PowerEdge サーバ上で、モジュラー型、モノリシック型、およびタワー型のサーバ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。
- 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は、Collect System Inventory on Restart (CSIOR) を有効にしてください。詳細については、iDRAC のマニュアルを参照してください。

自動検出を使用したサーバーの検出

サーバを自動検出するには、PowerEdge サーバをネットワークに接続し、OMIMSSC 用のサーバの電源をオンにします。OMIMSSC では、未割り当ての Dell EMC サーバの自動検出に、iDRAC のリモート有効化機能が使用されます。OMIMSSC はプロビジョニングサーバとして機能し、Dell EMC サーバの自動検出には iDRAC のリファレンスが使用されます。

1. OMIMSSC では、(iDRAC 資格情報を指定し、それをデフォルトにすることによって) Dell EMC サーバのデバイスタイプ資格情報プロファイルが作成されます。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. Dell EMC サーバを自動検出するには、次のタスクを実行します。
   a. iDRAC 内の既存の管理者アカウントを無効にします。

メモ: 自動検出が失敗した場合に備えて、iDRAC にログインするためのオペレータ権限付きゲストユーザアカウントを持つことが推奨されています。

b. ターゲットサーバの自動検出を有効にするには、[Remote Enablement (リモート有効化)] の [iDRAC Settings (iDRAC 設定)] で、[Enable Auto-Discovery (自動検出の有効化)] 機能の [Enabled (有効)] オプションを選択します。
c. 自動検出を有効にしてから、プロビジョニングサーバの IP アドレス (OMIMSSC がインストールされているサーバの IP アドレス) を入力し、サーバを再起動します。

手動検出を使用したサーバの検出

IP アドレスまたは IP 範囲を使用して、PowerEdge サーバを手動で検出できます。サーバを検出するには、iDRAC IP アドレスとサーバのデバイスタイプ資格情報を指定します。IP 範囲を使用してサーバを検出するときは、開始と終了の範囲を含む IP (IPv4) 範囲 (サブネット内) を指定します。

1. OMIMSSC コンソールで、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 [Configuration and Deployment (設定と導入)] をクリックし、[Discover (検出)] をクリックします。
2. [Discover (検出)] ページで、必要なオプションを選択します。
   - [Discover Using an IP Address (IP アドレスを使用して検出)] - IP アドレスを使用してサーバを検出します。
   - [Discover Using an IP Range (IP 範囲を使用して検出)] - IP 範囲内のすべてのサーバを検出します。
3. 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)] をクリックしてデバイスタイプ資格情報プロファイルを作成します。

   選択したプロファイルが、すべてのサーバに適用されます。
4. [Dell iDRAC IP address (Dell iDRAC IP アドレス)] に、検出するサーバの IP アドレスを入力します。
5. [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 Address Start Range (IP アドレス開始範囲)] と [IP Address End Range (IP アドレス終了範囲)] に、指定する IP アドレス範囲の開始範囲と終了範囲を入力します。
   - IP アドレス範囲を除外する場合は [Enable Exclude Range (除外範囲を有効にする)] を選択し、[IP Address Start Range (IP アドレス開始範囲)] と [IP Address End Range (IP アドレス終了範囲)] に、除外する範囲を入力します。
6. 固有のジョブ名を入力し、[Finish (終了)] をクリックします。
7. (オプション) このジョブを追跡するには、[Go to the Job List (ジョブリストに移動)] オプションを選択します。

   [Jobs and Logs Center (ジョブとログセンター)] ページが表示されます。[Running (実行中)] タブで検出ジョブを展開すると、ジョブの進行状況が表示されます。

OMIMSSC コンソール拡張と登録済み SCCM の同期

すべての PowerEdge サーバ (ホストおよび未割り当て) は SCCM から OMIMSSC に同期できます。

PowerEdge サーバを OMIMSSC コンソール拡張と、登録済み SCCM または SCVMM コンソールと同期する前に、次の要件が満たされているようにします。

- サーバのデフォルト iDRAC 資格情報プロファイルの詳細情報が必要です。
- OMIMSSC を SCCM と同期する前に、**Dell Default Collection (Dell デフォルトコレクション)** をアップデートします。ただし、未割り当てサーバが SCCM で検出された場合は、そのサーバが **Import Dell server collection (Dell サーバコレクションのインポート)** に追加されます。このサーバを **Dell Default Collection (Dell デフォルトコレクション)** に追加するには、サーバの iDRAC IP アドレスを OOB ページに追加します。

OMIMSSC を SCCM と同期した後、サーバが SCCM に存在しない場合は、[Device Collections (デバイスコレクション)] に [All Dell Lifecycle Controller Servers (すべての Dell Lifecycle Controller サーバ)] コレクションと [Import Dell server (Dell サーバのインポート)] コレクションが作成され、サーバがそれぞれ該当するグループに追加されます。

OMIMSSC コンソール拡張と登録済み SCVMM の同期

SCVMM コンソールにある Dell EMC Hyper-V ホスト、Hyper-V ホストクラスタ、モジュラー Hyper-V ホスト、未割り当てサーバはすべて、SCVMM 向け OMIMSSC コンソール拡張と同期できます。また、同期後には、サーバの最新ファームウェアインベントリ情報が得られます。

OMIMSSC を SCVMM と同期する前に、次の点に注意してください。

- 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。
- ホストサーバのベースボード管理コントローラ(BMC)で iDRAC IP アドレスが設定されていないと、ホストサーバを OMIMSSC と同期できません。このため、SCVMM で BMC を設定してから (詳細については、`technet.microsoft.com` にある MSDN の記事を参照)、OMIMSSC を SCVMM と同期してください。
- SCVMM R2 は環境内で多数のホストをサポートしているため、同期は長時間かかるタスクです。同期は次のように行われます。
  - SCVMM 環境に登録されているホストが、OMIMSSC アプライアンスの [Hosts (ホスト)] タブに追加されます。
  - サーバが未割り当てサーバとしてリストされていて、SCVMM に手動で追加された場合、そのサーバは同期後に OMIMSSC アプライアンスの [Hosts (ホスト)] タブに追加されます。
  - ホストサーバが Hyper-V クラスタに属している場合、クラスタの詳細情報は [Hosts (ホスト)] タブにあります。ホストサーバ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、この情報を [Maintenance Center (メンテナンスセンター)] ページで見ることができます。
  - ホストがモジュラーサーバの場合、そのモジュラーサーバを含むシャーシのサービスタグは [Hosts (ホスト)] タブに追加されます。モジュラーサーバが Hyper-V クラスタに属していない場合、ホストサーバが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。この情報は [Maintenance Center (メンテナンスセンター)] ページで見ることができます。
  - ホストインベントリの詳細情報 (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) に対する変更は、いずれも [Hosts (ホスト)] タブでアップデートされます。
  - 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。

登録済み MSSC との同期

OMIMSSC で [Configuration and Deployment (設定と導入)] をクリックしてから、登録済み MSSC にリストされているすべてのホストを OMIMSSC アプライアンスと同期するために、[Synchronize with OMIMSSC (OMIMSSC と同期)] をクリックします。

同期エラーの解決

OMIMSSC と同期されなかったサーバは、iDRAC IP アドレスとホスト名と共にリストされます。

メモ: 無効な資格情報や iDRAC IP アドレス、接続などの問題によって同期されないすべてのサーバについては、まず問題を解決してから同期するようにしてください。

メモ: 再同期中に、登録済み MSSC 環境から削除されたホストサーバは、OMIMSSC コンソール拡張の **Unassigned Servers (未割り当て)** タブに移動されます。サーバが廃止された場合は、そのサーバを未割り当てサーバのリストから削除します。

資格情報プロファイルの問題があるサーバを再同期するには、次の手順を実行します。

1. OMIMSSC で、[Configuration and Deployment (設定と導入)] をクリックしてから [Resolve Sync Errors (同期エラーの解決)] をクリックします。
2. 再同期するサーバを選択し、資格情報プロファイルを選択するか、資格情報プロファイルを作成するために [Create New (新規作成)] をクリックします。
3. ジョブ名を入力します。必要であれば、[Go to the Job List (ジョブリストに移動)] オプションを選択すると、ジョブが送信されたときに自動的にジョブのステータスが表示されます。
4. [Finish (終了)] をクリックしてジョブを送信します。

OMIMSSC からのサーバの削除

サーバを削除すると、使用されていたライセンスが解放されます。

OMIMSSC にリストされているサーバを次の基準に基づいて削除できます。

- [Unassigned servers (未割当サーバ)] タブにリストされている未割り当てサーバ。
- 登録済み SCCM または SCVMM でプロビジョニングされ、OMIMSSC の [Hosts (ホスト)] タブに存在するホストサーバを削除するには、最初に SCCM または SCVMM でサーバを削除し、さらに OMIMSSC からそのサーバを削除します。

1. OMIMSSC コンソール拡張で、[Configuration and Deployment (設定と導入)] をクリックします。
   - 未割り当てサーバを削除するには - [Unassigned Servers (未割り当てサーバ)] タブでサーバを選択し、[Delete (削除)] をクリックします。
   - ホストサーバを削除するには - [Host Servers (ホストサーバ)] タブでサーバを選択し、[Delete (削除)] をクリックします。
2. 確認ダイアログボックスで、[Yes (はい)] をクリックします。

iDRAC コンソールの起動

[Configuration and Deployment (設定と導入)] の [Unassigned Servers (未割り当てサーバ)] タブまたは [Hosts (ホスト)] タブで、サーバの [iDRAC IP] アドレスをクリックします。

メモ: Windows 2012 OS および iDRAC 2.40.40.40 以降のファームウェアバージョンを使用する場合、 iDRAC コンソールを起動するには Web ブラウザに基づき TLS 1.1 以降用のサポートを有効にします。

9

OMIMSSC のライセンス

OMIMSSC には、次の 2 種類のライセンスがあります。

- 評価ライセンス — ライセンスの試用版です。インストール後に自動インポートされる 5 つのサーバ (ホストまたは未割り当て) 用の評価ライセンスが含まれています。このライセンスは、第 11 世代以降の Dell EMC サーバにのみ適用されます。
- 実稼働ライセンス — OMIMSSC によって管理するサーバの数が制約されないようにするには、Dell EMC から実稼働ライセンスを購入してください。このライセンスには、製品サポートと OMIMSSC アプライアンスのアップデートが含まれています。

ライセンスを購入すると、.XML ファイル (ライセンスキー) を、Dell Digital ストアからダウンロードできるようになります。ライセンスキーをダウンロードできない場合は、www.dell.com/support/softwarecontacts に掲載されている、地域および製品ごとのデルサポートの電話番号までお問い合わせください。

OMIMSSC では、ライセンスファイルを 1 つ使用すればサーバを検出できます。サーバが OMIMSSC で検出されると、ライセンスが使用されます。サーバが削除された場合は、ライセンスが解除されます。次のアクティビティが行われると、OMIMSSC のアクティビティログにエントリが作成されます。

- ライセンスファイルがインポートされる
- サーバが OMIMSSC から削除され、ライセンスが解除される
- ライセンスは、サーバの検出後に使用されます。

評価ライセンスから実稼働ライセンスにアップグレードすると、評価ライセンスは実稼働ライセンスによって上書きされます。[Licensed Nodes (ライセンスされたノード)] のカウントは、購入した実稼働ライセンスの数と同じです。

トピック：

ライセンスアップロード後のオプション

OMIMSSC のライセンス機能でサポートされているオプションは次のとおりです。

新しく購入された製品のライセンスファイル

新しいライセンスを注文すると、注文の確認に関する電子メールがデルから送信され、Dell Digital ストアからライセンスファイルをダウンロードできます。ライセンスは .xml 形式です。ライセンスが .zip 形式の場合は、.xml ファイルのライセンスを .zip ファイルから抽出してからアップロードします。

ライセンスのスタッキング

複数の実稼働ライセンスをスタックし、サポートされるサーバの数をアップロードされたライセンス内のサーバの合計数まで増やすことができます。評価ライセンスはスタックできません。サポートされるサーバの数は、スタッキングでは増加できず、複数のアプライアンスを使用する必要があります。

すでに複数のライセンスがアップロードされている場合、サポートされるサーバの数は、最後のライセンスがアップロードされた時点でのライセンス内のサーバの合計数となります。

ライセンスの交換

ご注文に問題がある場合、あるいは変更されたファイルや壊れたファイルをアップロードしようとした場合は、それに関するエラーメッセージが表示されます。別のライセンスファイルを Dell Digital ストアに要求できます。交換用のライセンスを受け取った場

合、交換用のライセンスの資格 ID は前のライセンスと同じになります。交換用のライセンスをアップロードするとき、同じ資格 ID のライセンスがすでにアップロードされていると、そのファイルは置き換えられます。

ライセンスの再インポート

同じライセンスファイルのインポートを試行すると、エラーメッセージが表示されます。新しいライセンスを購入し、新しいライセンスファイルをインポートしてください。

複数ライセンスのインポート

別の資格 ID を持つ複数のライセンスファイルをインポートして、OMIMSSC で検出および維持するサーバの数を増やすことができます。

強制

ライセンスのアップグレード

サポートされているすべてのサーバ世代向けの既存のライセンスファイルが、OMIMSSC に使用できます。ライセンスファイルが最新のサーバ世代をサポートしていない場合は、新しいライセンスを購入してください。

評価用ライセンス

評価ライセンスの有効期限が切れると、いくつかの主要な領域の動作が停止し、エラーメッセージが表示されます。

サーバ検出後の OMIMSSC でのライセンス使用

ホストの追加またはベアメタルサーバの検出を試みると、使用状況について警告されます。次のような状況では、新規ライセンスを購入することが推奨されています。

- ライセンスされたサーバの数が、購入したライセンスの数を超えている場合
- 検出したサーバの数が、購入したライセンスの数と同じ場合
- 購入したライセンスの数を超えるので、猶予ライセンスが与える場合
- 購入したライセンスの数を超えていて、そのすべてが猶予ライセンスの場合

メモ: 猶予ライセンスの数は、購入したライセンス合計の 20 パーセントです。したがって、OMIMSSC で実際に使用できるライセンスの数は、購入したライセンス数と猶予ライセンス数を足し合わせた数となります。

OMIMSSC へのライセンスのインポート

ライセンスを購入したら、次の手順を実行して OMIMSSC にインポートします。

1. 管理ポータルで [License Center (ライセンスセンター)] をクリックします。
2. [Import License (ライセンスのインポート)] をクリックし、Dell Digital ストアからダウンロードしたライセンスファイルを参照して選択します。

   メモ: 有効なライセンスファイルのみインポートできます。ファイルが破損または改ざんされている場合は、それに応じたエラーメッセージが表示されます。Dell Digital ストアからファイルを再度ダウンロードするか、Dell の担当者に問い合わせて有効なライセンスファイルを入手してください。

ライセンスの詳細情報の表示

1. ブラウザーを開き、OMIMSSC アプライアンスの URL を入力します。

OMIMSSC 管理ポータルのログイン ページが表示されます。

2. [[ライセンス センター]] をクリックします。

   ページに次の情報が表示されます。

   [[ライセンス概要]] : OMIMSSC のライセンスの詳細情報が表示されます。
   - [[ライセンスされたノード]] : 購入したライセンスの総数
   - [[使用中ノード]] : 検出され、ライセンスを使用しているサーバーの数
   - [[使用可能ノード]] : OMIMSSC で検出できる残りのライセンスされたノード

   [[ライセンスの管理]] : インポートされた各ライセンス ファイルを、その詳細情報 (資格 ID、製品の説明、ライセンス ファイルをインポートした日付、ライセンス ファイルの有効期間の開始日、ライセンスによってサポートされるすべての世代のサーバーのリストなど) とともに表示します。

10

Operational Template（運用テンプレート）

Operational Template（運用テンプレート）は、MSSC 環境内の PowerEdge サーバにオペレーティングシステムを導入し、ファームウェアバージョンをアップデートします。

参照サーバからサーバ設定全体をキャプチャし、これに基づいて、Operational Template（運用テンプレート）でハードウェア構成、ファームウェアアップデート属性、OS パラメータを設定し、このテンプレートを各サーバに適用します。また、割り当てられた運用テンプレートに対してサーバのコンプライアンスステータスをチェックし、その違いをサマリページに表示します。参照サーバの詳細については、「参照サーバ設定について」を参照してください。

次の表に、運用テンプレートがサポートしているすべての機能を示します。

表 4. OMIMSSC の機能

[コンポーネント]	[設定と導入]	[ファームウェアアップデート]	[インベントリの表示]	[運用テンプレートのコンプライアンスステータス]
BIOS	有	有	有	有
iDRAC	有	有	有	有
NIC/CNA	有	有	有	有
RAID	有	有	有	有
FC	有	有	有	有
Windows	[有]	-	無	-
RHEL	[有]	-	無	-
ESXI	[有]	-	無	-

Operational Template（運用テンプレート）を導入するときは、次の点に注意してください。

- 設定用のハードウェアコンポーネント（BIOS、RAID NIC/CNA、FC、iDRAC）を選択するときは、同じモデルのサーバを選択するようにしてください。
- ファームウェアコンポーネントを選択する場合は、任意のサーバにわたってファームウェアをアップデートできます。

トピック：

- 導入の準備
- Operational Template（運用テンプレート）の管理

導入の準備

Operational Template（運用テンプレート）を導入する前に、WinPE イメージ、タスクシーケンス、Operational Template（運用テンプレート）を作成します。

WinPE ISO イメージの作成

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。WinPE ISO イメージの作成には、PreExecution Environment（PXE）サーバが必要です。WinPE ISO は、WinPE イメージおよび Dell OpenManage Deployment Toolkit（DTK）から作成されます。WinPE ISO イメージを作成したら、PXE サーバを停止します。オペレーティングシステム関連のドライバパックが Lifecycle Controller にインストールされているようにします。WinPE ISO イメージの作成に DTK の最新バージョンを使用している場合は、DTK ファイルの WinPE バージョンを使用します。DTK ファイルには、オペレーティングシステムの導入先のサーバに必要な必須ファームウェアバージョンが含まれています。

メモ: WinPE ISO イメージの作成に DTK の最新バージョン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の導入先のシステムに必要な必須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。

1. PXE サーバを OMIMSSC アプライアンスに追加します。
2. PXE サーバを追加した後、`boot.wim` ファイルを PXE サーバから OMIMSSC IG の SCVMM 共有 WIM フォルダにコピーします。`boot.wim` は、次のパスにあります。`C:\RemoteInstall\DCMgr\Boot\Windows\Images`

   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 ドライバの抽出

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 ドライバを抽出するために、フォルダ (`C:\DTK501` など) を選択します。
3. 抽出した DTK フォルダを IG の DTK 共有フォルダにコピーします。例えば、`\\OMIMSSC IG Share\DTK\DTK501` です。

   メモ: SCVMM SP1 SCVMM から SCVMM R2 にアップグレードしている場合は、Windows PowerShell 4.0 にアップグレードし、WinPE ISO イメージを作成します。

WinPE イメージのアップデート

1. OMIMSSC で [WinPE Update (WinPE アップデート)] を選択し、[Image Source (イメージソース)] の [Custom WinPE Image Path (カスタム WinPE イメージパス)] で、WinPE イメージのパスを入力します。
   たとえば、`\\OMIMSSC 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。
   例えば、`\\OMIMSSC IG Share\DTK\DTK501` です。
3. ファイルについて、次のいずれかを入力します。
   - SCCM 用の WIM ファイル名
   - SCVMM 用の ISO ファイル名
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、`\\OMIMSSC IG Share\ISO` の下に作成されます。

タスクシーケンス

タスクシーケンスは、オペレーティングシステムイメージのキャプチャや SCCM コンソールへのオペレーティングシステムの導入に使用されます。

Operational Template (運用テンプレート) を作成する前に、次の前提条件を満たすことが推奨されています。

- Configuration Manager において、システムが検出されて [Assets and Compliance (資産およびコンプライアンス)] > [Device Collections (デバイスコレクション)] > [All Dell Lifecycle Controller Servers (すべての Dell Lifecycle Controller サーバ)] に存在しているようにします。詳細については、「サーバの検出」を参照してください。
- システムに最新の BIOS バージョンをインストールします。
- システムに Lifecycle Controller の最新バージョンをインストールします。
- システムに iDRAC ファームウェアの最新バージョンをインストールします。

メモ: Configuration Manager コンソールは常に管理者権限を使用して起動します。

タスクシーケンスの作成

タスクシーケンスは次の 2 つの方法で作成でき、サーバの設定に使用されます。

- OMIMSSC 導入テンプレートを使用して、Dell 固有のタスクシーケンスを作成する。
- カスタムタスクシーケンスを作成する。

タスクシーケンスは、コマンドの成功または失敗に関わらず、次のタスクシーケンスの手順に進みます。

Dell 固有のタスクシーケンスの作成

[OMIMSSC Server Deployment Template (OMIMSSC サーバ導入テンプレート)] を使用して Dell 固有のタスクシーケンスを作成するには、次の手順を実行します。

1. Configuration Manager を起動します。
   Configuration Manager コンソール画面が表示されます。
2. 左ペインで、[ソフトウェアライブラリ] > [概要] > [オペレーティングシステム] > [タスクシーケンス] の順に選択します。
3. [Task Sequences (タスクシーケンス)] を右クリックし、[OMIMSSC Server Deployment (OMIMSSC サーバ導入)] > [Create OMIMSSC Server Deployment Template (OMIMSSC サーバ導入テンプレートの作成)] をクリックします。
   [OMIMSSC Server Deployment Task Sequence Wizard (OMIMSSC サーバ導入タスクシーケンスウィザード)] が表示されます。
4. [Task Sequence Name] (タスクシーケンス名) フィールドにタスクシーケンスの名前を入力します。
5. ドロップダウンリストから使用する起動イメージを選択します。

   メモ: 作成した Dell カスタムブートイメージの使用が推奨されます。

6. [Operating System Installation (オペレーティングシステムのインストール)] で、オペレーティングシステムのインストールタイプを選択します。このオプションは次のとおりです。
   - [OS WIM イメージを使用]
   - [スクリプトによる OS インストール]
7. [Operating system package to use] (使用するオペレーティングシステムパッケージ) ドロップダウンメニューから、オペレーティングシステムパッケージを選択します。
8. 使用するパッケージに [unattend.xml] が含まれている場合は、[Package with unattend.xml info (unattend.xml 情報を含むパッケージ)] メニューからそれを選択してください。それ以外の場合は、[<do not select now> (今は選択しない)] を選択します。
9. [作成] をクリックします
   [Task Sequence Created] (作成されたタスクシーケンス) ウィンドウが、作成したタスクシーケンスの名前と共に表示されます。
10. 表示される確認メッセージボックスで、[Close] (閉じる) をクリックします。

カスタムタスクシーケンスの作成

1. Configuration Manager を起動します。
   Configuration Manager コンソールが表示されます。
2. 左ペインで、[ソフトウェアライブラリ] > [概要] > [オペレーティングシステム] > [タスクシーケンス] の順に選択します。
3. [タスクシーケンス] を右クリックし、[タスクシーケンスの作成] をクリックします。
   [タスクシーケンスの作成] ウィザードが表示されます。
4. [新しいカスタムタスクシーケンスの作成] を選択してから、[次へ] をクリックします。
5. [タスクシーケンス名] テキストボックスにタスクシーケンスの名前を入力します。
6. 作成した Dell 起動イメージを指定し、[次へ] をクリックします。
   [設定の確認] 画面が表示されます。
7. 設定内容を確認して [次へ] をクリックします。
8. 表示される確認メッセージボックスで、[Close] (閉じる) をクリックします。

タスクシーケンスの編集

メモ: SCCM 2016 でタスクシーケンスを編集するとき、欠落しているオブジェクト参照メッセージで **Setup windows and ConfigMgr (Windows および ConfigMgr のセットアップ)** パッケージがリストされません。パッケージを追加してタスクシーケンスを保存します。

1. Configuration Manager を起動します。
   Configuration Manager 画面が表示されます。
2. 左ペインで、[ソフトウェアライブラリ] > [オペレーティングシステム] > [タスクシーケンス] の順に選択します。
3. 編集するタスクシーケンスを右クリックし、[編集] をクリックします。
   [タスクシーケンスエディタ] ウィンドウが表示されます。
4. [追加] > [Dell 展開] > [Dell Lifecycle Controller からドライバを適用] をクリックします。
   Dell サーバ導入のカスタムアクションがロードされます。これで、タスクシーケンスに変更を加えられるようになりました。

   メモ: タスクシーケンスを初めて編集する際には、[Setup Windows, and Configuration Manager (Windows および Configuration Manager のセットアップ)] というエラーメッセージが表示されます。このエラーを解決するには、Configurations Manager Client Upgrade package (Configuration Manager クライアントのアップグレードパッケージ) を作成して選択します。パッケージの作成に関する詳細については、**technet.microsoft.com** にある Configuration Manager のマニュアルを参照してください。

Lifecycle Controller 起動メディアの作成

この機能を使用して、タスクシーケンスメディアからゼロタッチ導入用の起動メディアを作成します。

メモ: この機能は、SCCM 向け OMIMSSC コンソール拡張にのみ適用できます。

1. OMIMSSC を起動し、[Boot Media Creation (起動メディアの作成)] をクリックします。
2. [Image Source (イメージソース)] で、オペレーティングシステムイメージを含む ISO ファイルを指定します。

   詳細については、「タスクシーケンスメディアのブータブル ISO の作成」を参照してください。
3. [Output File (出力ファイル)] で、ISO ファイル (無人用 ISO ファイル) の名前を入力します。
4. (オプション) ジョブの開始後に [Jobs and logs (ジョブとログ)] ページに移動するために、[Go to the Job List (ジョブリストに移動)] チェックボックスを選択します。
5. [Update (アップデート)] をクリックして、出力ファイルを ISO 共有に保存します。

Lifecycle Controller 起動メディアのデフォルト共有場所の設定

Lifecycle Controller 起動メディアのデフォルト共有場所を設定するには、次の手順を実行します。

1. Configuration Manager で [Administration (管理)] > [Site Configuration (サイト設定)] > [Sites (サイト)] を選択します。
2. [<site server name> (<サイトサーバ名>)] を右クリックして、[Configure Site Components (サイトコンポーネントの設定)] を選択してから、[Out of Band Management (帯域外管理)] を選択します。
   [帯域外管理コンポーネントプロパティウィンドウ] が表示されます。
3. [Lifecycle Controller] タブをクリックします。
4. [Default Share Location for Custom Lifecycle Controller Boot Media](カスタム Lifecycle Controller 起動メディアのデフォルト共有場所) の下で [Modify] (変更) をクリックして、カスタム Lifecycle Controller 起動メディアのデフォルト共有場所を変更します。
5. [[Modify Share Information (共有情報の変更)]] ウィンドウで、新しい共有名と共有パスを入力します。
6. [OK] をクリックします。

タスクシーケンスメディアのブータブル ISO の作成

1. [Software Library (ソフトウェアライブラリ)] の Configuration Manager で、[Task Sequences (タスクシーケンス)] を右クリックしてから、[Create Task Sequence Media (タスクシーケンスメディアの作成)] を選択します。

   メモ:
   - このウィザードを開始する前に、すべての配布ポイントで起動イメージの管理とアップデートを行います。

- OMIMSSC : OMIMSSC は、タスクシーケンスメディアの作成で、スタンドアロンメディアを使用した方法をサポートしていません。

2. [タスクシーケンスメディアウィザード] から、[起動可能なメディア] を選択し、[次へ] をクリックします。
3. [CD/DVD セット] を選択し、[参照] をクリックして、ISO イメージの保存場所を選択します。
4. [Next](次へ) をクリックします。
5. [パスワードでメディアを保護する] チェックボックスをオフにし、[次へ] をクリックします。
6. [PowerEdge Server Deployment Boot Image] を参照して選択します。

   メモ: DTK を使用して作成された起動イメージのみ使用します。

7. ドロップダウンメニューから配布ポイントを選択し、[子サイトからの配布ポイントを表示する] チェックボックスをオンにします。
8. [Next](次へ) をクリックします。
   タスクシーケンスメディア情報が記載された [サマリ] 画面が表示されます。
9. [Next](次へ) をクリックします。
   プログレバーが表示されます。
10. 作業が完了したら、ウィザードを閉じます。

Windows 以外のオペレーティングシステムの導入作業について

ターゲットシステムへの Windows 以外のオペレーティングシステムの導入ついては、以下の点に留意するようにしてください。

- Windows 以外の ISO ファイルは、読み取り書き込みアクセス権のある Network File System Version (NFS) 共有または Common Internet File System (CIFS) 共有で使用できます。
- ターゲットシステムで仮想ディスクが使用可能であることを確認します。
- ESXi OS の導入後、サーバは SCCM の [Managed Lifecycle Controller (ESXi)] コレクションに移動されます。
- Windows 以外のどのような種類の OS を導入した場合でも、サーバは [Default Non-Windows Host Update Group (デフォルトの Windows 以外のホストアップデートグループ)] に移動されます。
- ネットワークアダプタは、オペレーティングシステムが導入されているサーバ内のネットワークポートに接続することが推奨されています。

Operational Template (運用テンプレート) の管理

OMIMSSC で、Operational Template (運用テンプレート) を作成、編集、削除できます。

Operational Template (運用テンプレート) の作成

Operational Template (運用テンプレート) を作成する前に、次のタスクを完了しておいてください。

- [Discovery (検出)] ページを使用して、参照サーバを検出します。詳細については、「手動検出を使用したサーバの検出」を参照してください。
- (オプション) 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。
- (オプション) SCCM については、OMIMSSC で以下を実行します。
  - タスクシーケンスを作成します。

    詳細については、「タスクシーケンスの作成」を参照してください。

  - Windows 以外のオペレーティングシステムを導入するには、デバイスタイプ資格情報プロファイルが必要です。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。
  - 無人起動メディアを作成します。詳細については、「LC 起動メディアの作成」を参照してください。
- (オプション) SCVMM については、OMIMSSC で以下を実行します。
  - ハイパーバイザープロファイルを作成します。ハイパーバイザープロファイルの作成に関する詳細は、「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。
  - Windows を導入する場合は、デバイスタイプ資格情報プロファイルが必要です。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。

参照サーバの設定をキャプチャすることによって、Operational Template (運用テンプレート) を作成できます。設定をキャプチャしたら、テンプレートを直接保存することも、アップデートソース、ハードウェア設定、Windows コンポーネントの属性を必要に

応じて編集することもできます。これでテンプレートを保存できます。保存したテンプレートは、他の同種の PowerEdge サーバに使用できます。

1. OMIMSSC で、次のいずれかを実行し、Operational Template（運用テンプレート）を開きます。
   - OMIMSSC ダッシュボードで、[Create Operational Template（運用テンプレートの作成）] をクリックします。
   - ナビゲーションペインで、[Profiles（プロファイル）] > [Operational Template（運用テンプレート）] をクリックし、[Create（作成）] をクリックします。

   [Operational Template（運用テンプレート）] ウィザードが表示されます。
2. テンプレートの名前と説明を入力します。また、参照サーバの IP アドレスを入力し、[Next（次へ）] をクリックします。

   メモ: iDRAC 2.0 以降を使用している参照サーバの設定がキャプチャできます。
3. [Server Components（サーバコンポーネント）] で、利用可能な属性とその値を表示するコンポーネントをクリックします。
   コンポーネントには次のものがあります。
   - ファームウェアアップデート
   - RAID、NIC、BIOS といったハードウェアコンポーネント
   - オペレーティングシステム — Windows、ESXi、RHEL のいずれかを選択します。
4. （オプション）必要であれば、利用可能な属性の値を編集します。
5. 選択したコンポーネントの選択したコンポーネント設定だけが適用されるので、キャプチャしたすべての設定に Operational Template（運用テンプレート）を適用するときは、各コンポーネントでチェックボックスを選択してください。

   [Operating System（オペレーティングシステム）] コンポーネントでは、必要に応じて、以下のいずれかの手順を実行します。
   - SCCM で Windows OS を導入する場合は、「SCCM 向け OMIMSSC コンソール拡張の Windows コンポーネント」を参照してください。
   - SCVMM で Windows OS を導入する場合は、「SCVMM 向け OMIMSSC コンソール拡張の Windows コンポーネント」を参照してください。
   - OMIMSSC
   - Windows 以外の OS を導入する場合は、「OMIMSSC コンソール拡張の Windows 以外のコンポーネント」を参照してください。
6. プロファイルが保存されるよう、[Finish（終了）] をクリックします。

SCCM 向け OMIMSSC コンソール拡張の Windows OS コンポーネント

Operational Template（運用テンプレート）を作成するときは、Windows コンポーネントについて次の手順を実行します。

1. タスクシーケンスと導入方法を選択します。

   メモ: コレクションに導入されたタスクシーケンスだけがドロップダウンメニューにリストされます。

   タスクシーケンスの詳細については、「タスクシーケンス」を参照してください。
2. [Deployment method（導入方法）] で、次のいずれかのオプションを選択します。
   - [Boot to Network ISO（ネットワーク ISO からの起動）] - 指定した ISO を再起動します。
   - [Stage ISO to vFlash and Reboot（ISO を vFlash にステージングして再起動）] - ISO を vFlash にダウンロードして再起動します。
   - [Reboot to vFlash（vFlash から再起動）] - vFlash から再起動します。ISO が vFlash にあることを確認します。

     メモ: [Reboot to vFlash（vFlash から再起動）] オプションを使用するには、vFlash 上に作成されたパーティションのラベル名が [ISOIMG] である必要があります。
3. （オプション）vFlash にあるイメージが壊れている場合に、ネットワーク共有にあるイメージを使用するには、[Use Network ISO as Fallback（ネットワーク ISO を予備として使用）] オプションを選択します。
4. LC 起動メディアイメージファイルを指定し、（オプションで）[Enable LC Drivers Injection（LC ドライバインジェクションを有効にする）] を使用します。LC 起動メディアイメージの作成の詳細については、「LC 起動メディアの作成」を参照してください。
5. OS に必要なドライバを選択します。

SCVMM 向け OMIMSSC コンソール拡張の Windows コンポーネント

Operational Template（運用テンプレート）を作成するときは、Windows コンポーネントについて次の手順を実行します。

[Hypervisor Profile (ハイパーバイザープロファイル)]、[Credential Profile (資格情報プロファイル)]、[Server IP from (次のサーバ IP から)] の順に選択します。

メモ: [Host Name (ホスト名)] と [Server Management NIC (サーバ管理 NIC)] は、常にプール値です。

[Server IP from (次のサーバ IP から)] で [Static (静的)] を選択した場合は、SCVMM で論理ネットワークが設定してあるようにします。次のフィールドはプール値です。

- [Console Logical Network (コンソール論理ネットワーク)]
- [IP サブネット]
- [静的 IP アドレス]

OMIMSSC コンソール拡張の Windows 以外のコンポーネント

Operational Template (運用テンプレート) を作成するときは、Windows 以外のコンポーネントについて次の手順を実行します。

Windows 以外の OS、OS バージョン、共有フォルダのタイプ、ISO ファイル名、ISO ファイルの場所、OS のルートアカウントのパスワードを指定します。

(オプション) CIFS 共有にアクセスするために、Windows タイプの資格情報プロファイルを選択します。

[Host name (ホスト名)] はプール値で、DHCP オプションを無効にした場合、次のフィールドはプール値になります。

- [IP アドレス]
- [サブネットマスク]
- [Default Gateway (デフォルトゲートウェイ)]
- [プライマリ DNS]
- [セカンダリ DNS]

メモ: Windows 以外の OS の導入では、共有タイプとして Network File System (NFS) と Common Internet File System (CIFS) がサポートされています。

Operational Template (運用テンプレート) の表示

Operational Template (運用テンプレート) テンプレートを表示するには、次の手順を実行します。

OMIMSSC コンソールで [Profiles and Templates (プロファイルとテンプレート)] をクリックし、[Operational Template (運用テンプレート)] をクリックします。作成されたすべての Operational Template (運用テンプレート) テンプレートがここに表示されます。

Operational Template (運用テンプレート) の編集

Operational Template (運用テンプレート) を編集して、アップデートソース、ハードウェア設定、および参照サーバのオペレーティングシステムコンポーネントを変更できます。

メモ: 一部の属性が、他の属性値に依存している場合があります。これらの属性がアップデートされないと、ハードウェア設定の適用が失敗する可能性があります。このため、リファレンス設定を編集しないことが推奨されています。

メモ: SCCM 2016 でタスクシーケンスを編集するとき、欠落しているオブジェクト参照メッセージで **Setup windows and ConfigMgr (Windows および ConfigMgr のセットアップ)** パッケージがリストされません。パッケージを追加してタスクシーケンスを保存します。

1. 編集するテンプレートを選択し、[Edit (編集)] をクリックします。
   Operational Template (運用テンプレート) ページが表示されます。
2. 必要に応じてテンプレートの名前と説明を編集し、[Next (次へ)] をクリックします。
3. 使用可能な属性とその値を [Server Components (サーバコンポーネント)] に表示するために、コンポーネントをクリックします。
4. 必要であれば、利用可能な属性の値を編集します。

   メモ: Operational Template (運用テンプレート) の適用時には、選択したコンポーネント設定だけがターゲットシステムに適用されるので、各コンポーネントでチェックボックスを選択してください。

   メモ: 各コンポーネントにおけるチェックボックスの選択モードとは無関係に、すべての設定がテンプレートにキャプチャされます。

5. OS コンポーネントの場合は、要件に応じて次のいずれかのタスクを実行します。
   - SCCM で Windows OS を導入する場合は、「SCCM 向け OMIMSSC コンソール拡張の Windows コンポーネント」を参照してください。
   - SCVMM で Windows OS を導入する場合は、「SCVMM 向け OMIMSSC コンソール拡張の Windows コンポーネント」を参照してください。
   - Windows 以外の OS を導入する場合は、「OMIMSSC コンソール拡張の Windows 以外のコンポーネント」を参照してください。
6. プロファイルが保存されるよう、[Finish (終了)] をクリックします。

SCCM 向け OMIMSSC コンソール拡張の Windows コンポーネント

Operational Template (運用テンプレート) を編集するときは、「SCCM 向け OMIMSSC コンソール拡張の Windows OS コンポーネント」に記載されている次の手順を実行します。

SCVMM 向け OMIMSSC 拡張コンソールの Windows コンポーネント

Operational Template (運用テンプレート) を編集するときは、「SCVMM 向け OMIMSSC コンソール拡張の Windows OS コンポーネント」に記載されている次の手順を実行します。

OMIMSSC コンソール拡張の Windows 以外のコンポーネント

Operational Template (運用テンプレート) を編集するときは、「OMIMSSC コンソール拡張の Windows OS 以外のコンポーネント」に記載されている次の手順を実行します。

Operational Template (運用テンプレート) の削除

Operational Template (運用テンプレート) を削除するには、次の手順を実行します。

Operational Template (運用テンプレート) を削除する前に、次のことを確保します。

- 選択した Operational Template (運用テンプレート) が、どのサーバとも関連付けられていないこと。サーバに関連付けられている場合は、テンプレートの割り当てを解除してから、テンプレートを削除します。
- Operational Template (運用テンプレート) に関連付けられたジョブが実行されていないこと。

削除するテンプレートを選択し、[Delete (削除)] をクリックします。確認するために [Yes (はい)] をクリックします。

Operational Template (運用テンプレート) の割り当てと Operational Template (運用テンプレート) コンプライアンスの実行

Operational Template (運用テンプレート) をサーバに割り当て、Operational Template (運用テンプレート) コンプライアンスを実行します。Operational Template (運用テンプレート) をサーバに割り当てた後にのみ、その Operational Template (運用テンプレート) コンプライアンスステータスを表示できます。テンプレートをサーバに割り当てることで、サーバ設定を Operational Template (運用テンプレート) と比較できます。Operational Template (運用テンプレート) を割り当てるとコンプライアンスジョブが実行され、完了時に Operational Template (運用テンプレート) ステータスが表示されます。

1. OMIMSSC で [Configuration and Deployment (設定と導入)] をクリックします。必要なサーバを選択し、[Assign Operational Template and Run Compliance (運用テンプレートの割り当てとコンプライアンスの実行)] をクリックします。

   [Assingn] **Operational Template (運用テンプレート) and Run Compliance (運用テンプレートの割り当てとコンプライアンスの実行)** ページが表示されます。
2. **Operational Template (運用テンプレート)** ドロップダウンメニューからテンプレートを選択し、ジョブ名を入力して [Assign (割り当て)] をクリックします。

   サーバがテンプレートに準拠する場合は、[green (緑色)] のチェックマークが表示されます。

   サーバがテンプレートに準拠しない場合は、テンプレート名のリンクをクリックすればサマリレポートを表示できます。テンプレートとサーバ設定の違いを示すサマリレポートが **Operational Template (運用テンプレート)** [Compliance-Summary Report (運用テンプレートコンプライアンス - サマリレポート)] ページに表示されます。

   詳細なレポートを表示するには、次の手順を実行します。

a. [View Detailed Compliance (詳細なコンプライアンスの表示)] をクリックします。これで、割り当てたテンプレートと違う属性値を持つコンポーネントが表示されます。色によって、Operational Template (運用テンプレート) コンプライアンスの状態の違いが示されます。
   - 黄 - サーバの設定がテンプレート値と一致しないことを表します。
   - 赤 - コンポーネントがサーバ上に存在していることを表します。

Operational Template (運用テンプレート) の導入

Windows OS と Windows 以外の OS (ESXi および RHEL) を導入できます。

メモ: Windows 2016 OS を第 12 世代の PowerEdge サーバに導入後、デバイスマネージャに黄色い警告が表示された場合は、`Dell.com/support` から適切なドライバをダウンロードしてインストールします。

1. OMIMSSC で [Configuration and Deployment (設定と導入)] をクリックします。テンプレートを導入するサーバを選択してから、[Deploy] **Operational Template (運用テンプレート)** をクリックします。
   [Deploy] **Operational Template (運用テンプレート)** ページが表示されます。
2. (オプション) 選択したテンプレートでプール値としてマークされたすべての属性を .CSV ファイルにエクスポートするときは [Export Pool Attributes (プール属性のエクスポート)] をクリックし、それ以外の場合は手順 3 に進みます。

   メモ: プール値をエクスポートする前に、OMIMSSC コンソール拡張がインストールされているサーバの IP アドレスをローカルイントラネットサイトに追加します。IE ブラウザで IP アドレスを追加する方法の詳細については、「ブラウザ設定」を参照してください。

   メモ: プール値をエクスポートした場合は、プール値としてマークされたすべての属性のすべての値を .CSV ファイルに入力し、ファイルを保存します。[Attribute Value Pool (属性値プール)] で、インポートするこのファイルを選択します。

   メモ: 適切なすべての属性を含む .CSV ファイルを選択し、iDRAC IP または iDRAC 資格情報がテンプレートによって変更されないようにします。その理由は、iDRAC IP または iDRAC 資格情報が変更されると、ジョブは OMIMSSC によって追跡されないため、ジョブが iDRAC で正常に終了しても失敗とみなされるからです。

   メモ: Windows 2016 OS を第 12 世代の PowerEdge サーバに導入後、デバイスマネージャに黄色い警告が表示された場合は、`Dell.com/support` から適切なドライバをダウンロードしてインストールします。

3. 一意のジョブ名と、ジョブの説明を入力し、[Deploy (導入)] をクリックします。ジョブを表示するために、[Go to the Job List (ジョブリストに移動)] をクリックします。

Operational Template (運用テンプレート) の割り当て解除

1. OMIMSSC で [Configuration and deployment (設定と導入)] をクリックします。
2. テンプレートの割り当てを解除するサーバを選択してから、[Assign] **Operational Template (運用テンプレート)** [and Run Compliance (運用テンプレートの割り当てとコンプライアンスの実行)] をクリックします。
   [Assign] **Operational Template (運用テンプレート) and** [Run Compliance (運用テンプレートの割り当てとコンプライアンスの実行)] ページが表示されます。
3. [ ] Operational Template (運用テンプレート) ドロップダウンメニューから [Unassign (割り当て解除)] を選択し、[Assign (割り当て)] をクリックします。

11

Dell Repository Manager（DRM）との統合

OMIMSSC は DRM バージョン 2.2 以降と統合し、既存サーバのサーバインベントリ情報を OMIMSSC アプライアンスから DRM に提供します。このインベントリ情報を使用して DRM でカスタムリポジトリを作成し、これを OMIMSSC アプライアンスでアップデートソースに指定すると、サーバやサーバグループでファームウェアのアップデートジョブを実行できます。DRM でのリポジトリの作成の詳細については、『*Dell Repository Manager*』マニュアルを参照してください。

メモ: OMIMSSC をアップグレードしたら、DRM を OMIMSSC アプライアンスと再統合し、サーバに関する最新情報を表示します。

DRM を使用して OMIMSSC 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）] を `https:// IP address of appliance/genericconsolerepository/` という形式で入力し、[Next（次へ）] をクリックします。
4. OMIMSSC アプライアンスで使用した [UserName（ユーザ名）] と [Password（パスワード）] を入力し、[Ok] をクリックし、さらに [Ok] をクリックします。

12

メンテナンス

[Maintenance Center (メンテナンスセンター)] ページを使用すると、サーバインベントリをエクスポートできます。また、サーバをアップグレードする、前の設定をインポートしてサーバを以前の状態に復元する、古いコンポーネントと同じ設定を置き換え後のコンポーネントに適用する、トラブルシューティング用に LC をエクスポートするなどのジョブをスケジュールできます。

トピック：

ファームウェアアップデートについて

推奨に従って、Dell EMC サーバコンポーネントのファームウェアバージョンを最新に維持できます。ファームウェアアップデートを実行するには、アップデートソースとカスタムアップデートグループを作成するか、事前定義されたアップデートグループを使用します。ファームウェアアップデート用のジョブを作成してスケジュールできます。また、アップデートソースで新規カタログが使用可能になったときにアラートを受け取るよう通知をスケジュールすることも可能です。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作成されます。この情報に基づいて、インベントリファイルを作成できます。また、アップデートのタイプ、サーバコンポーネント、サーバモデルに基づいて情報をフィルタすることもできます。iDRAC アップデートは、サポートされている最低限のバージョン以降でしか使用できないため、ハードウェアの互換性があるサーバにのみアップデートを実行できます。

メモ: OMIMSSC の最新バージョンにアップグレード後、`ftp.dell.com` または `downloads.dell.com` への接続に失敗すると、デフォルトの Dell オンライン FTP アップデートソースまたは Dell HTTP アップデートソースがカタログファイルをダウンロードできないため、比較レポートは作成されません。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 アップデートソースまたは 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てから、[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で同じものを選択します。アップデートのソースの編集に関する詳細については、「アップデートソースの変更」を参照してください。

OMIMSSC の [Maintenance center (メンテナンスセンター)] ページには、次のアップデートアクションがあります。

- Downgrade (ダウングレード) - 使用可能な以前のバージョンがアップデートソースにあり、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。
- No Action Required (必要なアクションなし) - 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。
- No Update Available (使用可能なアップデートなし) - コンポーネントに使用できるファームウェアアップデートがありません。
- Upgrade - Optional (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。
- Upgrade - Urgent (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。
- Upgrade - Recommended (アップグレード - 推奨) - OMIMSSC でバグフィックスまたは機能を強化を行うアップデートです。また、他のファームウェアアップデートとの互換性の修正も含まれています。

OMIMSSC には、ファームウェアアップデートを実行する次の方法があります。

- **Update using DRM repository (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。インベントリ情報のエクスポートに関する詳細については、「インベントリのエクスポート」を参照してください。
  - DRM でリポジトリを作成した後、関連するサーバを選択し、サーバの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ときは、他の要素 (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 アドバイザリなど) も考慮してください。リポジトリの作成に関する詳細については、**Dell.com/support/home** にある『*Dell Repository Manager*』マニュアルを参照してください。
- **Update using FTP or HTTP (FTP または HTTP を使用したアップデート)** - 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て、コンポーネントをアップデートします。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。

- Integration with Dell Online Catalog（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は、Dell FTP に接続して、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` に接続して、これ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。

- **Referencing firmware inventory and comparison（ファームウェアインベントリと比較の参照）** - 選択したサーバまたはサーバグループのファームウェアインベントリを含む参照インベントリファイルを作成します。作成後、アプライアンス内に存在するサーバ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できます。参照サーバ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からのインベントリ情報や、タイプまたはモデルが異なる複数のサーバを含めることができます。

サーバ上でのアップデートの適用

サーバ上でアップデートを適用する前に、次の条件が満たされているようにします。

- サーバ上でアップデートを実行するために、Dell オンラインの FTP または HTTP サイト、ローカルの FTP または HTTP サイト、あるいは Dell Repository Manager（DRM）で、アップデートソースが使用可能である。
- アップデートが適用されるサーバ上で、アップデートの適用前に IDRAC ジョブキューがクリアされている。
- IG ユーザ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。
- ファームウェアリポジトリの作成のために、FTP サーバには OMIMSSC がホストされている場所から到達できるようになっており、ネットワークに問題がなく、ファームウェアアップデートジョブの作成で正しい資格情報を入力する。

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。

メモ: サーバまたはサーバグループに適用できる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は、そのサーバ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。

メモ: 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。

メモ: ファームウェアアップデートジョブを作成することで、サーバまたはサーバグループに対し、アップデートをすぐに適用することも、アップデートをスケジュールすることもできます。アップデートのために作成されたジョブは、[Jobs and Logs Center（ジョブとログセンター）] ページにリストされます。

メモ: OMIMSSC アプライアンスから直接 CMC ファームウェアをアップデートすることはできませんが、CMC にあるモジュラーサーバ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）の項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）の項を、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）の項をそれぞれ参照してください。

メモ: [Allow Downgrade（ダウングレードを許可）] を選択すると、推奨されているバージョンにファームウェアバージョンをダウングレードできます。このオプションを選択しないと、ファームウェアのダウングレードが必要なコンポーネントで何も起こりません。

1. OMIMSSC で [Maintenance Center（メンテナンスセンター）] をクリックし、サーバまたはサーバ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。
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として、[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）] のいずれかを選択し、[Finish（終了）] をクリックします。
   - **Agent-free staged updates（エージェントフリーステージドアップデート）** - 直接適用可能なファームウェアおよびシステムの再起動が不要なファームウェアが、すぐに適用されます。残りのアップデートは、システムの再起動時に適用されます。アップデートは iDRAC を介して実行されます。iDRAC がアップデートの成功を報告すると、OMIMSSC アプライアンス

はアップデートが成功したものとみなします。アップデートの適用後、OMIMSSC アプライアンスはサーバとはやり取りしません。この操作が 1 つのサーバで失敗するだけでも、アップデートジョブ全体が失敗となります。

- **Agent-free updates (エージェントフリーアップデート)** - 必要な場合、ファームウェアアップデートは、即時再起動をともなう帯域外アップデートとなります。

メモ: クラスタアップデートグループのアップデートは、IG がインストールされているシステムと同じ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ます。[Update Method (アップデート方法)] ドロップダウンメニューでの選択とは無関係に、アップデートジョブは Microsoft Cluster-Aware-Update (CAU) 機能に送信されます。詳細については、「CAU を使用したアップデート」を参照してください。

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、OMIMSSC アプライアンスはジョブのステータスについて iDRAC とやり取りし、管理ポータルの **Jobs and Logs (ジョブとログ)** ページにステータスアップデートを表示します。iDRAC では、OMIMSSC アプライアンスによって追跡されたジョブのステータスアップデートを表示しないことがあります。OMIMSSC アプライアンスは最大 6 時間待ち、iDRAC から応答がない場合は、ファームウェアアップデートジョブのステータスを失敗とみなします。

CAU を使用したアップデート

サーバ上でのアップデートは、IG がインストールされているのと同じ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、中断やサーバダウンタイムを最小限に抑えることができ、ワークロード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は影響を及ぼしません。CAU の詳細については、`technet.microsoft.com` にある「Cluster-Aware Updating Overview (クラスタ対応更新の概要)」セクションを参照してください。

クラスタアップデートグループに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確認します。

- 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、Windows Server 2012 R2、または Windows 2016 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。
- 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の準備状況を確認します。CAU の詳細については、`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。
- 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 PowerEdge サーバ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) のファームウェアバージョンはアップグレードできません。

メモ: CAU 方法を適用するためのレポートには、重大なエラーおよび警告が記載されていないようにしてください。

アップデートの適用方法については、「アップデートの実行」を参照してください。

ポーリングと通知

ユーザ選択の事前定義されたデフォルトのアップデートソースに、入手可能な新しいカタログががあるときにアラートを受け取るポーリング通知を設定できます。入手可能な新しいカタログがアップデートソースにあると、通知ベルの色がオレンジ色に変わります。アップデートソースで入手可能なカタログをローカルにキャッシュして置き換えるには、ベルアイコンをクリックします。古いカタログを最新のカタログに置き換えると、ベルの色が緑に変わります。

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. OMIMSSC で [Maintenance Center (メンテナンスセンター)] 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. ポーリングの実行頻度を選択します。
   - [Never (行わない)] - デフォルトでは、このオプションが選択されています。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。

アップデートソースの概要

アップデートソースによって、Dell のアップデートソースからアップデートを選択して適用できるようになります。アップデートソースの作成、表示、管理ができます。サポートされているアップデートソースのタイプには、DRM リポジトリ、FTP、HTTP があります。DRM、HTTP、または FTP の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にすることができます。

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、ドライバパック) を含む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が付属します。

アップデートソースにあるインベントリ情報を、選択したサーバまたはサーバグループ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できます。また、アップデートソースを変更して、サーバまたはサーバ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にあるバージョン情報と比較することもできます。

セキュリティ強化、バグ修正、および新機能の要求を使用するために、最新のファームウェアにアップグレードすることが推奨されています。デルは、四半期に 1 回のペースで Dell FTP に投稿される PDK カタログを通じて、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)] は事前定義された FTP タイプのアップデートソースであり、新規インストールまたはアップグレード後の OMIMSSC アプライアンスで使用できます。事前定義されたアップデートソースの削除や名前の変更はできません。

[DELL ONLINE HTTP CATALOG (DELL ONLINE HTTP カタログ)] はデフォルトのアップデートソースであり、新規インストールまたはアップグレード後の OMIMSSC アプライアンスで使用できます。このデフォルトアップデートソースの削除や名前の変更はできません。ただし、別のアップデートソースを作成し、それをデフォルトのアップデートソースに指定することはできます。

メモ: OMIMSSC をインストールしたら、[DELL ONLINE CATALOG (DELL ONLINE カタログ)] アップデートソースと [DELL ONLINE HTTP CATALOG (DELL ONLINE HTTP カタログ)] アップデートソースのプロキシ詳細情報を追加し、それを保存します。

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

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。
   例えば、[baseLocation] を `downloads.dell.com` からホスト名または IP アドレス (`hostname.com` など) 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

1. [OMIMSSC] 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。
   作成されたすべてのアップデートソースが、その説明、ソースタイプ、場所、および資格情報プロファイル名と共に表示されます。

アップデートソースの作成

- アップデートソースのタイプに基づいて、Windows または FTP の資格情報プロファイルが使用できるようにします。
- DRM アップデートソースを作成する場合は、DRM がインストール済みで管理者役割が設定されているようにします。

1. OMIMSSC コンソールで、[Maintenance Center (メンテナンスセンター)] をクリックしてから [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)] ページで、[Create New (新規作成)] をクリックし、アップデートソースの名前と説明を入力します。
3. [Source Type (ソースタイプ)] ドロップダウンメニューで、アップデートソースのタイプとして次のいずれかを選択します。
   - FTP Sources (FTP ソース) - オンラインまたはローカルの FTP アップデートソースを作成するときに選択します。
     メモ: 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。
   - HTTP Sources (HTTP ソース) - オンラインまたはローカルの HTTP アップデートソースを作成するときに選択します。
     メモ: 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。
   - DRM Repository (DRM リポジトリ) - ローカルリポジトリアップデートソースを作成するときに選択します。DRM がインストールされているようにします。
     メモ: DRM ソースを作成する場合は、Windows 資格情報を入力し、Windows の共有場所にアクセスできるようにします。場所のフィールドには、カタログファイルのフルパスを、ファイル名も含めて入力します。
   - Inventory Output files (インベントリ出力ファイル) - 参照サーバ設定に対するファームウェアインベントリを表示するときに選択します。
     メモ: 比較レポートは、アップデートソースとして Inventory Output files (インベントリ出力ファイル) を使用することによってのみ、1 つのサーバのインベントリ情報を他のすべてのサーバと比較したものを表示できます。
4. [Location (場所)] で、FTP または HTTP ソースのアップデートソースの URL を入力し、DRM の Windows 共有場所の URL を入力します。

   メモ: ローカル FTP サイトでは、オンライン FTP が複製される必要があります。

   メモ: ローカル HTTP サイトでは、オンライン HTTP が複製される必要があります。

   メモ: FTP ソースの URL については、HTTP または HTTPS の入力は必須ではありません。

5. アップデートソースにアクセスするには、必要な資格情報プロファイルを [Credentials (資格情報)] で選択します。
6. FTP または HTTP ソースへのアクセスにプロキシが必要な場合は、必要なプロキシ資格情報を [Proxy Credentials (プロキシ資格情報)] で選択します。
7. (オプション) 作成したアップデートソース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。
8. 入力した資格情報を使用してアップデートソースの場所にアクセスできるかどうかを確認するには、[Test Connection (テスト接続)] をクリックしてから [Save (保存)] をクリックします。

メモ: アップデートソースは、テスト接続が正常に行われた後でのみ作成できます。

アップデートソースの変更

アップデートソースの変更時は、次の点を理解して留意するようにしてください。

- 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が、進行中のジョブや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や、導入テンプレートによって使用されている場合でも、そのアップデートソースの変更はできます。使用中のアップデートソースを変更した際には、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ます。
- アップデートソースでカタログファイルが更新されても、ローカルにキャッシュされたカタログファイルは自動的には更新されません。キャッシュに保存された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いったん削除して再作成します。

変更するアップデートソースを選択し、[Edit (編集)] をクリックしてから、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

アップデートソースは、次の場合には削除できません。

- 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の [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。

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、同じようなアップデート管理を必要とするサーバのグループです。アップデートグループには、次の 2 つのタイプがあります。

- 事前定義されたアップデートグループ - このグループのサーバは、表示だけができます。

  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、削除することはできません。

- カスタムアップデートグループ - このグループのサーバは、作成して維持できます。

メモ: サーバグループはユーザ固有ではないため、SCVMM 内に存在するすべてのサーバグループが OMIMSSC にリストされます。これらのサーバ上で何らかの操作を実行するアクセス権を持っているようにします。

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。

[Generic update groups (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で構成されます。

[All update groups (すべてのアップデートグループ)] - このグループは、すべてのサーバグループで構成されます。OMIMSSC に存在するどのグループも、すべてのアップデートグループのメンバーです。このグループのタイプは、汎用アップデートグループです。

[Default unassigned server update group (デフォルトの未割り当てサーバアップデートグループ)] - このグループは、他のどのグループにも属さないすべての未割り当てサーバで構成されます。このグループのタイプは、汎用アップデートグループです。次のことが行われた後、サーバはデフォルトの未割り当てサーバ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。
- 同期または再同期 (SCVMM から削除されたが、OMIMSSC アプライアンス内に存在している場合)。

[Cluster update group (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。モジュラーサーバがクラスタに属している場合、そのサーバ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、OMIMSSC にリストされているすべてのサーバのホスト名とクラスタ FQDN が表示される [Configutation and Deployment (設定と導入)] ページを参照します。

[Host update group (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で構成され、1 回のセッションでアップデートが適用されます。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が一度にアップデートされます。

[Default host update group (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。このグループのタイプは、ホストアップデートグループです。

[Chassis update group (シャーシアップデートグループ)] - シャーシに属し、クラスタグループの一部ではないモジュラーサーバは、シャーシアップデートグループに分類されます。第 12、13 世代の PowerEdge サーバは、その CMC 情報と共に検出されます。デフォルトでは、グループは `Chassis-Service-tag-of-Chassis-Group` という命名形式で作成されます。例えば、`Chassis-GJDC4BS-Group` のように入力します。モジュラーサーバがクラスタアップデートグループから削除されると、そのサーバは 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が 1 つもない場合でも、シャーシ内のすべてのモジュラーサーバ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ますが、表示されるのは CMC 情報のみです。

[Default Non-Windows Host Update group (デフォルトの Windows 以外のホストアップデートグループ)] - このグループは、Windows 以外の OS を持つサーバで構成されます。

カスタムアップデートグループ

このグループでは、アップデートグループを作成、変更、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、[Default unassigned update groups (デフォルトの未割り当てアップデートグループ)] と [Default host update groups (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を追加すると、そのサーバ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を追加するには、サービスタグを使用して必要なサーバを検索します。

メモ: サーバを MSSC から削除した後、OMIMSSC を登録済み MSSC と同期すると、そのサーバがカスタムアップデートグループから削除され、事前定義された適切なグループに移動されます。

アップデート方法

OMIMSSC と互換性のあるハードウェアを持つサーバグループを選択し、アップデートを適用できます。

- 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。
  - **Agent-free staged updates (エージェントフリーのステージングアップデート)** - 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が不要なファームウェアアップデートは直ちに適用されます。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一括で実行されます。バッチサイズは、アップデートの実行時に決定されます。すべてのアップデートが適用されているかどうかを確認するには、インベントリを更新します。この操作が 1 つのサーバで失敗するだけでも、アップデートジョブ全体が失敗となります。
  - **Agent-free updates (エージェントフリーのアップデート)** - これは、サーバがすぐに再起動される帯域外アップデートです。
  - **Cluster-Aware Updating (CAU) (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に Windows CAU 機能を使用することで、サーバの可用性を維持しながらアップデートプロセスを自動化します。CAU の詳細については、「CAU を使用したアップデート」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. [OMIMSSC] で、[[メンテナンス センター]] をクリックし、[[メンテナンス設定]] をクリックします。
2. [[メンテナンス設定]] で、[[アップデート グループ]] をクリックします。
   作成されたすべてのカスタム グループが、名前、グループ タイプ、グループ内のサーバー数とともに表示されます。

カスタムアップデートグループの作成

1. OMIMSSC コンソールで、[Maintenance Center (メンテナンスセンター)] をクリックしてから [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. グループ名と説明を入力します。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のサーバのみ持つことができます。

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

また、2 つのタイプのサーバグループの組み合わせにすることもできます。

4. サーバ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を検索し、サーバを［Servers Included in the Update Group（アップデートグループに含まれるサーバ）］表に追加するために、右矢印をクリックします。
5. カスタムアップデートグループを作成するために、［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。
  1. サーバを既存のカスタムアップデートグループから削除します。そうすることにより、サーバ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。
  2. そのサーバを追加するよう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を検索します。

1. ［OMIMSSC］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。
- サーバがアップデートグループに存在していても、そのアップデートグループを削除できます。ただし、そのようなアップデートグループを削除した後、サーバは事前定義されたそれぞれのアップデートグループに移動されます。
- サーバグループを削除する前に、カスタムアップデートグループに関連するスケジュール済みのジョブを削除します。

1. ［OMIMSSC］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。

フィルタの適用

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。

OMIMSSC アプライアンスでは、カテゴリのフィルタとして次の 3 つ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（サーバモデル）］- フィルタを適用し、選択されたサーバ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。

OMIMSSC 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て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。

OMIMSSC 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。

ファームウェア インベントリの表示と更新

サーバまたは特定のサーバグループのファームウェアインベントリを表示および更新できます。

選択したアップデートソースに対し、サーバや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て、変更後のアップデートソースに対する、選択したサーバ、サーバグループ、またはシャーシのインベントリ情報の比較レポートを表示できます。

サーバ、サーバグループ、シャーシのファームウェアインベントリを更新し、最新情報を表示できます。サーバのコンポーネント情報を更新すると、サーバのインベントリ情報全体がアップデートされます。

メモ: 作成時に、カタログファイルのローカルコピーが OMIMSSC にキャッシュされます。このため、カタログファイルをアップデートして最新の比較レポートを表示します。カタログファイルを更新するには、アップデートソースを編集して保存するか、アップデートソースをいったん削除してから再作成します。

メモ: インベントリを更新しても、**Driver Pack Version（ドライバパックバージョン）**や **Drivers Available For OS（OS で使用可能なドライバ）**などのサーバ詳細情報は、SCCM コンソールにあるサーバの［Dell Out of Band Controllers（OOB）］プロパティではアップデートされません。OOB ページをアップデートするには、OMIMSSC を SCCM と同期します。

メモ: このバージョンの OMIMSSC 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には最新情報が表示されません。最新のサーバ情報と正しい比較レポートを表示するには、サーバを再検出します。

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. ［OMIMSSC］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 OMIMSSC 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）］のサーバグループをサーバレベル、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 サーバについての NIC 関連の情報は次のように表示されます。

   - ［Nature of Update（アップデートの性質）］が［Urgent（緊急）］のとき、これに基づいてフィルタを適用すると、緊急アップデートのコンポーネントだけを含む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）］リストのすべてのインターフェースに 1 つのエントリだけが表示されます。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。
   - 既存の NIC カードと一緒に NIC カードを追加すると、新たに追加した NIC カード は、別のインスタンスとして［Component Information（コンポーネント情報）］リストに表示されます。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。

リカバリ

サーバプロファイルをエクスポートして保護ボールトに保存しておき、そのプロファイルを同じサーバにインポートすると、以前の状態に復旧できます。

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 つのサーバーまたはサーバーグループを 1 つの保護ボールトのみ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

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。

1. [OMIMSSC] で、[[メンテナンス センター]] をクリックし、[[メンテナンス設定]] をクリックします。
2. [[メンテナンス センター]] で、[[保護ボールト]] をクリックし、[[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、詳細情報を入力します。
   - [ネットワーク共有] タイプの保護ボールトを作成している場合は、プロファイルの保存場所、そ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。

     メモ: 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。

1. [OMIMSSC] で、[Maintenance Center (メンテナンスセンター)] > [Maintenance Settings (メンテナンス設定)] > [Protection Vault (保護ボールト)] をクリックします。
2. ボールトを変更するには、ボールトを選択して [Edit (編集)] をクリックします。

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。

  このような場合に保護ボールトを削除するには、当該のサーバーまたはサーバー グループを削除してから、保護ボールトを削除します。
- 保護ボールトに関連付けられたジョブがスケジュールされている。このような場合に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. [OMIMSSC] で、[[メンテナンス センター]] > [[メンテナンス設定]] > [[保護ボールト]] をクリックします。
2. 削除する保護ボールトを選択し、[[削除]] 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プロファイルをエクスポートできます。OMIMSSC 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。サーバまたはサーバグループの設定プロファイルは、すぐにエクスポートすることも、後日エクスポートするようスケジュールすることもできます。また、サーバ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、1 つのサーバグループについて一度に 1 つのみスケジュールできます。設定プロファイルをエクスポート中のサーバまたはサーバグループには、他のアクティビティを実行できません。

[BIOS Settings (BIOS 設定)] で [F1/F2 Prompt on Error (エラー時に F1/F2 プロンプト)] オプションを無効にします。

メモ: iDRAC で [Automatic Backup (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ようにします。

メモ: フィルタを適用したら、サーバプロファイルをエクスポートすることはできません。サーバプロファイルをエクスポートするには、適用されているフィルタをすべてクリアします。

メモ: サーバプロファイルをエクスポートするには、iDRAC Enterprise ライセンスが必要です。

メモ: サーバプロファイルをエクスポートする前にサーバの IP アドレスが変更されないようにします。他の操作によって IP アドレスが変更された場合は、OMIMSSC でこのサーバを再検出し、サーバ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。

1. OMIMSSC で [Maintenance Center (メンテナンスセンター)] をクリックします。エクスポートするプロファイルを持つサーバを選択し、[Export Server Profile (サーバプロファイルのエクスポート)] をクリックします。

2. [Export Server Profile (サーバプロファイルのエクスポート)] ウィンドウでジョブの詳細を入力し、保護ボールトを選択します。

   保護ボールトの詳細については、「保護ボールトの作成」を参照してください。

   [Schedule Export Server Profile (サーバプロファイルのエクスポ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)] - 選択したサーバまたはサーバグループのサーバ設定をすぐにエクスポートします。
   - [ ] Schedule (スケジュール) - 選択したサーバグループのサーバ設定をエクスポートするためのスケジュールを設定します。
     - [Never (行わない)] - スケジュール期間中に 1 回だけサーバ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 回のペースでサーバ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 回のペースでサーバ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 回のペースでサーバプロファイルをエクスポートする場合に選択します。

サーバプロファイルのインポート

サーバまたはサーバグループから以前にエクスポートされたサーバプロファイルを、同じサーバまたはサーバグループにインポートできます。サーバプロファイルのインポートは、サーバの設定とファームウェアを、プロファイルに保存された状態に復元する際に役立ちます。このような場合、以前にエクスポートしておいたサーバプロファイルを、同じサーバまたはサーバグループにインポートすることで、現在のサーバプロファイルを置換できます。

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。

- サーバプロファイルのクイックインポート - サーバからエクスポートした最新のサーバプロファイルを、同じサーバに自動的にインポートできます。この操作を行うサーバごとに、個々のサーバプロファイルを選択する必要はありません。
- サーバプロファイルのカスタムインポート - 選択した個々のサーバごとにサーバプロファイルをインポートできます。例えば、サーバ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、そのサーバの保護ボールト内の使用可能なサーバプロファイルのリストから、インポートする特定のサーバ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：

- サーバにインポートできるサーバプロファイルは、そのサーバから以前にエクスポートしたサーバプロファイルだけです (リストから選択)。同じサーバプロファイルを別のサーバまたはサーバグループにインポートすることはできません。別のサーバまたはサーバグループのサーバプロファイルをインポートしようとすると、サーバプロファイルのインポートジョブが失敗します。
- 特定のサーバまたはサーバグループのサーバプロファイルイメージが使用できない場合、そのサーバまたはサーバグループに対してサーバプロファイルのインポートジョブが試行されると、サーバプロファイルを持たないこれらの特定のサーバへのサーバプロファイルのインポートジョブは失敗します。失敗の詳細を含むログメッセージが、アクティビティログに追加されます。
- サーバプロファイルのエクスポート後、いずれかのコンポーネントがサーバから削除され、その後でプロファイルのインポートジョブが開始された場合は、削除されたコンポーネントを除くすべてのコンポーネント情報が復元されます。この情報は、OMIMSSC のアクティビティログでは利用できません。欠落したコンポーネントの詳細を把握するには、iDRAC の [LifeCycle Log (LifeCycle ログ)] を参照してください。
- フィルタの適用後は、サーバプロファイルをインポートできません。サーバプロファイルをインポートするには、適用されているフィルタをすべてクリアします。
- サーバプロファイルをインポートするには、iDRAC Enterprise ライセンスが必要です。

1. OMIMSSC 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を選択し、[Import Server Profile (サーバプロファイルのインポート)] をクリックします。
2. 詳細情報を入力し、必要な [Import Server Profile Type (サーバプロファイルのインポートタイプ)] を選択します。

   メモ: [Preserve Data (データの保持)] がデフォルトで選択され、サーバの既存の RAID 設定が保持されます。サーバプロファイルに保存されている RAID 設定を適用する場合は、チェックボックスをクリアします。

3. サーバプロファイルをインポートするために、[Finish (終了)] をクリックします。

ファームウェアと構成設定の適用

部品交換機能は、交換したサーバコンポーネントを、必要なファームウェアバージョンや古いコンポーネントの設定、またはその両方に自動的にアップデートします。このアップデートは、部品交換後のシステム再起動時に自動的に行われます。

部品交換用のパラメータを設定するには：

1. OMIMSSC で［Maintenance Center（メンテナンスセンター）］をクリックし、サーバまたはサーバグループを選択して、［Configure Part Replacement（部品交換の設定）］をクリックします。
   ［Part Replacement Configuration（部品交換設定）］ウィンドウが表示されます。
2. ［CSIOR］、［Part Firmware Update（部品ファームウェアアップデート）］、および［Part Configuration Update（部品設定アップデート）］に、次のいずれかのオプションを設定し、［Finish（終了）］をクリックします。
   - Collect System Inventory On Restart（CSIOR）- 再起動時にすべてのコンポーネントを収集します。
     - ［Enabled（有効）］- サーバーコンポーネントのソフトウェアおよびハードウェアインベントリの情報はシステムの再起動時に自動的に更新されます。
     - ［Disabled（無効）］- サーバーコンポーネントのソフトウェアおよびハードウェアインベントリの情報は更新されません。
     - ［Do not change the value on the server（サーバーの値を変更しない）］- 既存のサーバー設定が保持されます。
   - 部品ファームウェアアップデート - 選択モードに基づいて、コンポーネントのファームウェアバージョンを復元、アップグレード、またはダウングレードします。
     - ［Disabled（無効）］- 部品ファームウェアアップデートが無効になり、交換したコンポーネントに同じものが適用されます。
     - ［Allow version upgrade only（バージョンのアップグレードのみ許可）］- 新しいコンポーネントのファームウェアバージョンが既存のバージョンよりも古い場合に、アップグレードされたファームウェアバージョンが、交換したコンポーネントに適用されます。
     - ［Match firmware of replaced part（交換部品のファームウェアを一致させる）］- 新しい部品のファームウェアバージョンを元のコンポーネントのファームウェアバージョンに一致させます。
     - ［Do not change the value on the server（サーバーの値を変更しない）］- コンポーネントの既存の設定が保持されます。
   - 部品設定アップデート - 選択モードに基づいて、コンポーネントの設定を復元またはアップグレードします。
     - ［ ］［Disabled（無効）］- 部品設定のアップデートが無効になり、古いコンポーネントの保存済み設定は交換したコンポーネントに適用されません。
     - ［Apply always（常に適用）］- 部品設定のアップデートが有効になり、古いコンポーネントの保存済み設定が、交換したコンポーネントに適用されます。
     - ［Apply only if firmware matches（ファームウェアが一致する場合にのみ適用）］- 古いコンポーネントの保存済み設定は、ファームウェアバージョンが一致する場合にのみ、交換したコンポーネントに適用されます。
     - ［Do not change the value on the server（サーバーの値を変更しない）］- 既存の設定が保持されます。

LC ログの収集

LC ログは、管理対象システムでの過去のアクティビティの記録を提供します。これらのログファイルには、推奨アクションに関する詳細情報やトラブルシューティングの際に役立つテクニカル情報が含まれているので、サーバ管理者にとって有益です。LC ログからさまざまなタイプの情報を入手できます。アラート関連、システムのハードウェアコンポーネントの設定変更、アップデートやダウングレードによるファームウェアの変更、交換済み部品、温度警告、アクティビティの開始時刻を示す詳細なタイムスタンプ、アクティビティの重大度などです。

LC ログを収集するための 2 つのオプションがあります：

- アクティブ LC ログ - 最新の LC ログファイルです。これらのログファイルの表示や検索、アプライアンスへのエクスポートが可能です。LC ログをアプライアンスまたはネットワーク共有に収集するジョブをスケジュールすることができます。また、ログファイルのバックアップをネットワーク共有上に保存できます。
- LC 完了ログ - アクティブおよびアーカイブされた LC ログファイルが含まれます。これらのファイルは大きいため、`.gz` 形式に圧縮され、CIFS ネットワーク共有上の指定された場所にエクスポートされます。

1. OMIMSSC で［Maintenance Center（メンテナンスセンター）］をクリックします。サーバまたはサーバグループを選択し、［Collect LC Logs（LC ログの収集）］をクリックします。
2. ［LC Log Collection（LC ログの収集）］で次のいずれかを選択し、［Finish（終了）］をクリックします。
   - ［Export Complete LC Logs（.gz）(LC 完了ログのエクスポート（.gz））］- Windows の資格情報を入力して、アクティブおよびアーカイブされた LC ログを CIFS ネットワーク共有にエクスポートします。

     たとえば、`20160720103001O597.xml.gz` は LC ファイル名で、このファイル名には作成された日付と時刻が含まれています。

メモ: これらのファイルは大きいため、LC 完了ログを保存するための十分なスペースが共有フォルダにあるようにします。

メモ: LC 完了ログのエクスポートは、第 11 世代の PowerEdge サーバではサポートされません。

メモ: LC ログは、`<YYYYMMDDHHMMSSSSS>.<file format>` というフォーマットで保存されます。

- [Export Active Logs (Run now) (アクティブログのエクスポート (今すぐ実行))] - アクティブログをすぐにアプライアンスにエクスポートするときに選択します。
  - (オプション) [Back up LC logs on the network share (LC ログをネットワーク共有にバックアップ)] オプションを有効にすると、Windows の資格情報を入力して、LC ログのバックアップを CIFS ネットワーク共有に保存できます。
    メモ: 第 11 世代の PowerEdge サーバ用のアクティブ LC ログをエクスポートする前に、iDRAC および LC を最新バージョンにアップデートするようにしてください。
- [Schedule LC Log Collection (LC ログ収集のスケジュール)] - 日付、時刻、および頻度を選択して、アクティブ LC ログをエクスポートします。
  - (オプション) [Back up LC logs on the network share (LC ログをネットワーク共有にバックアップ)] オプションを有効にすると、Windows の資格情報を入力して、LC ログのバックアップを CIFS ネットワーク共有に保存できます。

  LC ログの収集を行う頻度を決定するために使用できる頻度のスケジュールのオプションは次のとおりです :
  - [Never (行わない)] - スケジュール期間中に 1 回だけ LC ログをエクスポートする場合に選択します。
  - [Daily (日次)] - スケジュール期間中に LC ログを毎日エクスポートする場合に選択します。
  - [Once a week (週に一度)] - スケジュール期間中に週に 1 回 LC ログをエクスポートする場合に選択します。
  - [Once every 4 weeks (4 週間に一度)] - スケジュール期間中に 4 週間に 1 回 LC ログをエクスポートする場合に選択します。

メモ: エクスポートされた LC ログファイルは、特定サーバーのサービスタグのフォルダ名内に保存されます。

LC ログの表示

LC ログの表示機能を使用して、すべてのアクティブな LC ログの表示、詳細説明の検索、および CSV 形式でのログのダウンロードができます。

「ブラウザ設定」での説明に従って、ブラウザ設定を行います。

1. OMIMSSC で [Maintenance Center (メンテナンスセンター)] をクリックします。サーバまたはサーバグループを選択し、[View LC Logs (LC ログの表示)] をクリックします。
2. 選択したグループのすべてのサーバー、および LC ログが収集されるサーバーが、それらの LC ログファイルと一緒にリストされます。ファイル名をクリックすると、そのサーバに固有の LC ログファイルに含まれるログエントリがすべて表示されます。詳細については、「ファイルの説明」を参照してください。
3. (オプション) すべてのログファイルから説明を検索したり、CSV 形式でファイルをエクスポートするには、検索ボックスを使用します。

   LC ファイル内のメッセージの説明を検索するには、次の 2 つの方法があります。
   - ファイル名をクリックして LC ログファイルを開き、検索ボックスで説明を検索します。
   - 検索ボックスに説明のテキストを入力し、このテキストのインスタンスを含むすべての LC ファイルを表示します。

   メモ: LC ログメッセージの説明が長い場合、メッセージは 80 文字に切り捨てられます。

   メモ: LC ログメッセージに表示される時間は、iDRAC のタイムゾーンに従います。

   メモ: LC ログをダウンロードする前に、アプライアンスをローカルイントラネットサイトに追加します。

   アプライアンスを [Internet Explorer] の [Local intranet (ローカルイントラネット)] サイトに追加するには、次の手順を実行します。
   a. ブラウザを起動して [Tools (ツール)] をクリックし、[Internet Options (インターネットオプション)] をクリックします。
   b. [Security (セキュリティ)] > [Local intranet (ローカルイントラネット)] > [Sites (サイト)] をクリックします。

      [Local intranet (ローカルイントラネット)] ページが表示されます。
   c. [Advanced (詳細設定)] をクリックし、**アプライアンス URL** を入力して [Add (追加)] をクリックします。

ファイルの説明

このウィンドウを使用して、推奨アクションに関する詳細情報と、特定のサーバの追跡やアラート対応に役立つ他のテクニカル情報を表示します。

ファイルの内容を表示するには、ファイル名をクリックします。

- 特定のメッセージの説明を検索できます。
- ウィンドウ内にログファイルを表示したり、ファイルをダウンロードして追加のログメッセージを表示したりすることができます。
- アクティビティ用にユーザが入力したコメントを表示できます。

メモ: 検索オプションを使用すると、検索結果だけが CSV ファイルにエクスポートされます。

メモ: メッセージの説明が長い場合、メッセージは 80 文字に切り捨てられます。

メモ: [Message ID (メッセージ ID)] をクリックすると、メッセージに関する詳細情報が表示されます。

インベントリのエクスポート

OMIMSSC では、選択したサーバまたはサーバグループのインベントリを XML または CSV フォーマットのファイルにエクスポートできます。この情報は、Windows 共有ディレクトリまたは管理システムに保存します。

メモ: この XML ファイルを DRM にインポートし、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、リファレンス設定を作成します。

「ブラウザ設定」の説明に従って、ブラウザ設定を行います。

メモ: サーバーのコンポーネント情報のみを選択して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。

1. [OMIMSSC] で [Maintenance Center (メンテナンスセンター)] をクリックします。
2. インベントリをエクスポートしたいサーバーを選択し、[インベントリのエクスポート] ドロップダウンメニューから形式を選択します。

   エクスポートされたファイルは、サーバグループ、サーバのサービスタグ、ホスト名または IP アドレス、デバイスモデル、コンポーネント名、そのコンポーネントの現在のファームウェアバージョン、アップデートソースからのファームウェアバージョン、そのコンポーネントでのアップデートアクションなどの詳細情報で構成されています。

XML ファイルをエクスポートした後、DRM でリポジトリを作成するには、次の手順を実行します。

1. [My Repositories (マイリポジトリ)] > [New (新規)] > [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。
2. [Base Repository (ベースリポジトリ)] セクションで名前と説明を入力し、[Next (次へ)] をクリックします。
3. アプライアンスからエクスポートされたインベントリファイルを選択するために、[Modular Chassis Inventory (モジュラーシャーシインベントリ)] セクションで [Browse (参照)] をクリックしてから、[Next (次へ)] をクリックします。

   リポジトリの作成の詳細については、**Dell.com/support/home** にある『*Dell Repository Manager*』マニュアルを参照してください。

13

OMIMSSC での情報の表示

OMIMSSC で開始されたアクティビティに関するすべての情報は、ジョブの進行状況やそのサブタスクと共に、[Jobs and logs center (ジョブとログセンター)] ページ経由で表示できます。また、特定のカテゴリのジョブをフィルタして表示できます。ジョブは、OMIMSSC 管理ポータルおよび OMIMSSC コンソール拡張から表示できます。

- 管理ポータル - 開始されたジョブをすべての OMIMSSC ユーザについて表示
- OMIMSSC コンソール - 1 人のユーザや 1 つのコンソールに固有のジョブを表示

ジョブ名は、ユーザが入力するか、システムによって生成されます。サブタスクは、管理対象サーバの IP アドレスまたはホスト名に基づいて名前が付けられます。ジョブのアクティビティログを表示するには、そのサブタスクを展開します。ジョブには次の 4 つのカテゴリがあります。

- 実行中 - 現在実行中のすべてのジョブ (つまり、進行中の状態のジョブ) が表示されます。
- 履歴 - 過去に実行されたすべてのジョブがそのジョブのステータスとともに表示されます。
- スケジュール済み - 将来の日時がスケジュールされたすべてのジョブが表示されます。スケジュール済みのジョブは、キャンセルすることもできます。
- 汎用ログ - サブタスクまたはその他のアクティビティに固有でない、OMIMSSC アプライアンス固有の一般的なログメッセージを、ユーザ名とコンソール FQDN を指定しているすべてのユーザについて表示します。
  - アプライアンスログメッセージ - OMIMSSC アプライアンス固有のログメッセージ (OMIMSSC アプライアンスの再起動など) をすべて表示します。このカテゴのメッセージは、管理ポータルからのみ表示できます。
  - 汎用ログメッセージ - [実行中]、[履歴]、および [スケジュール] タブでリストされるジョブを通じて共通のすべてのログメッセージが表示されます。これらのログは、コンソールまたはユーザに固有です。

    例えば、サーバグループのファームウェアアップデートジョブが進行中の場合、そのジョブのサーバアップデートユーティリティ (SUU) リポジトリの作成に属するログメッセージがタブに表示されます。

OMIMSSC アプライアンスでは、ジョブの状態が次のように定義されています。

- キャンセル - ジョブは、ユーザによって手動でキャンセルされたか、または OMIMSSC アプライアンスの再起動時にキャンセルされました。
- 成功 - ジョブは正常に完了しました。
- 失敗 - ジョブは成功しませんでした。
- 進行中 - ジョブは実行中です。
- スケジュール - ジョブは将来の時刻にスケジュールされました。

  メモ: 複数のジョブが同時に同じサーバに送信されると、そのジョブは失敗します。したがって、異なる時間にジョブが実行されるようにスケジュールしてください。
- 待機中 - ジョブは実行を開始するまでキュー内にあります。
- 定期的なスケジュール - 一定の間隔で反復するジョブです。

トピック：

ジョブの表示

OMIMSSC で作成されたすべてのジョブを、そのステータス情報と共に表示できます。

1. OMIMSSC で [Jobs and Logs Center (ジョブとログセンター)] をクリックします。
2. [Scheduled (スケジュール済み)]、[History (履歴)]、[Generic (汎用)] など、特定のカテゴリのジョブを表示するには、該当するタブをクリックします。

   ジョブを展開して、ジョブに含まれているすべてのサーバを表示します。さらに展開して、そのジョブのログメッセージを表示します。

   メモ: すべてのジョブに関連する一般的なログメッセージは、[汎用] タブにはリストされますが、[実行中] または [履歴] タブにはリストされません。

3. （オプション）別カテゴリのジョブを表示するには、フィルタを適用すると、そのステータスを［Status（ステータス）］列に表示されます。

ジョブの管理

ジョブが［Scheduled（スケジュール済み）］状態であるようにします。

1. OMIMSSC で、次のいずれかを実行します。
   - ナビゲーションペインで、［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。
   - ナビゲーションペインで、［Jobs and Log Center（ジョブとログセンター）］をクリックし、［Scheduled（スケジュール）］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、確認として［Yes（はい）］をクリックします。

14

トラブルシューティング

トピック：

導入オプションがタスクシーケンスに表示されない

SCCM 向け OMIMSSC コンソール拡張をアンインストールして再インストールした後に、[Deploy（導入）] オプションが既存のタスクシーケンスに表示されません。

回避策として、タスクシーケンスを編集用に開き、[Apply（適用）] オプションを再度有効にしてから、[OK] をクリックします。[Deploy（導入）] オプションが再び表示されます。

[Apply] (適用）オプションを再度有効にするには、次の手順を実行します。

1. タスクシーケンスを右クリックして、[Edit]（編集）を選択します。
2. [Restart in Windows PE（Windows PE で再起動）] を選択します。[Description（説明）] セクションで任意の文字を入力し、変更が保存されないようにその文字を削除します。
3. [OK] をクリックします。

これで [Apply]（適用）プションが再度有効になります。

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が VRTX シャーシに追加されて検出されると、そのモジュラーサーバは前のシャーシサービスタグ情報を引き続き使用し、重複する VRTX シャーシグループをアプライアンス内に作成します。

これを解決するには、次の手順を実行します。

1. 1 つのシャーシからモジュラーサーバを削除し、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 Enclosure オーナーズマニュアル）』のサーバ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` にある『*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。

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

アプライアンスでクラスタグループが検出されると、クラスタアップデートグループにリストされているすべてのサーバを含む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）] で作成されます。その後、SCVMM を通じてこのクラスタのすべてのサーバを削除し、自動検出操作または SCVMM との同期操作を実行しても、**Maintenance Center（メンテナンスセンター）**で空のクラスタアップデートグループが削除されません。

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。

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。

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。

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。

第 11 世代サーバーのファームウェアアップデートの失敗

第 11 世代の PowerEdge サーバで開始されるファームウェアアップデートジョブは、iDRAC と LC の互換性のないバージョンによって、次のエラーが表示されて失敗することがあります。`WSMan command failed to execute on server with iDRAC IP <IP address>`

この問題を回避するには、iDRAC および LC を最新バージョンにアップグレードしてから、ファームウェアアップデートジョブを開始します。

DRM をアップデートソースの使用中にファームウェアアップデートの失敗

共有フォルダへのアクセスが不十分な状態で DRM アップデートソースを使用している場合、ファームウェアアップデートジョブが失敗する場合があります。DRM アップデートソースの作成中に提供された Windows 資格情報プロファイルがドメイン管理者グループまたはローカル管理者グループの一部ではない場合、次のエラーメッセージが表示されます：`Local cache creation failure`。

回避策として、次の手順を実行します。

1. DRM からリポジトリを作成した後、フォルダを右クリックし、[セキュリティ] タブをクリックしてから、[Advanced （ 詳細設定)] をクリックします。
2. [Enable inheritance(継承を有効にする)]をクリックし、[Replace all child object permission entries with inheritable permission entries from this object (すべての子オブジェクトのアクセス許可エントリをこのオブジェクトの継承可能なアクセス許可エントリと置き換える)] オプションを選択し、[Everyone （ 全員)] に読み取り / 書き込みアクセス許可を与えてフォルダを共有します。

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。

Operational Template (運用テンプレート) の適用の失敗

選択したサーバで Operational Template (運用テンプレート) の [Deploy (導入)] ジョブを送信した後、選択した .CSV ファイルの属性または属性値が適切でなくとも、iDRAC IP または iDRAC 資格情報がテンプレートによって変更されると、iDRAC のジョブは成功します。ただし、.CSV ファイルが無効であると、OMIMSSC 内のこのジョブのステータスが不成功 / 失敗と表示され、ターゲットサーバで iDRAC が変更されるため、ジョブを追跡することができません。

回避策として、選択した .CSV ファイルに含まれる属性と属性値がすべて適切であるようにして、iDRAC IP または資格情報がテンプレートによって変更されることがないようにしてください。

ホスト名を使用した CIFS 共有へのアクセスの失敗

モジュラーサーバが、OMIMSSC で任意のジョブを実行するために、ホスト名を使用して CIFS 共有にアクセスすることができない場合があります。

回避策として、CIFS 共有があるサーバの IP アドレスを指定します。

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 Catalog（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に、FTP サイトへのアクセスに失敗することがあります。

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。

回避策として、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到達できるようになっており、ネットワークに問題がないようにして、ファームウェアアップデートジョブの作成で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。

ジョブとログ表示の失敗

[Jobs and Logs Center（ジョブとログセンター）] が OMIMSSC コンソール拡張に表示されません。

回避策として、コンソールを再登録します。

CSV 形式での LC ログのエクスポートの失敗

LC ログを表示しているときに、ログファイルを CSV 形式でダウンロードしようとすると、ダウンロード操作が失敗します。

回避策として、アプライアンス FQDN をブラウザのローカルイントラネットサイトに追加します。ローカルイントラネットへのアプライアンスの追加に関する詳細については、「LC ログの表示」の項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。

OMIMSSC 管理ポータルにおける Dell EMC ロゴ表示の失敗

OMIMSSC 管理ポータルを Windows 2016 のデフォルト IE ブラウザで起動すると、管理ポータルに Dell EMC ロゴが表示されません。

回避策として、次のいずれかを行ってください。

- IE ブラウザを最新バージョンにアップグレードします。
- 閲覧履歴を削除し、ブラウザのお気に入りリストに管理ポータルの URL を追加します。

LC ログの表示の失敗

LC ログを収集した後、サーバー の LC ログファイルを表示すると、次のエラーメッセージが表示されます。"`Failed to perform the requested action. For more information see the activity log`"。

この問題を回避するには、iDRAC をリセットしてから、LC ログの収集と表示を行います。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

同一サーバ上の同じコンポーネントが、個々のサーバで行われたコンポーネントの選択とは無関係に、ファームウェアの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 ライセンスを有する第 12、13 世代の PowerEdge サーバで発生します。

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。

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: ""`
- **Information**: `Successfully deleted drivers from library share sttig.tejasqa.com for <server uuid>`
- **Error**: `Deleting staging share (drivers) for <server uuid> failed.`

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となり発生することがあります。再試行するか、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. SCVMM コンソールから、[Library (ライブラリ)] > [Library Servers (ライブラリサーバ)] の順に選択し、ライブラリサーバとして追加された IG サーバを選択します。
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 IG 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。

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

Active Directory のユーザ資格情報を使用したとき、第 11 世代 PowerEdge ブレードサーバでのハイパーバイザーの導入が失敗します。第 11 世代 PowerEdge ブレードサーバは、Intelligent Platform Management Interface (IPMI) プロトコルを使用して通信します。しかし、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。

検出中の誤った資格情報

- 検出時に誤った資格情報を入力した場合、iDRAC バージョンに応じて次の解決策を用いることができます。
  - 2.10.10.10 以降の iDRAC バージョンを搭載した第 12 世代の PowerEdge サーバを検出するときに、資格情報プロファイルに誤った詳細情報が提供された場合、サーバの検出は次の動作を伴って失敗します。
    - 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により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 よりも前の iDRAC バージョンでは、IP アドレスのブロックを設定できます。詳細については、**Dell.com/idracmanuals** にある iDRAC のマニュアルを参照してください。要件に応じて、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チェックできます。
  - サーバが検出され、アプライアンスに追加された後にデフォルトの iDRAC 資格情報プロファイルが変更された場合、サーバ上ではアクティビティを実行できません。サーバを使用するには、新しい資格情報プロファイルを使用してサーバを再検出してください。

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。

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 PowerEdge サーバ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ら、サーバを再起動するようにしてください。インベントリの更新の詳細については、「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 SCVMM エラー 21119

Active Directory にサーバーを追加しているとき、次のような SCVMM 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>.`」

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. SCVMM にサーバーを追加します。
4. SCVMM にサーバーが追加されたら、SCVMM 用 OMIMSSC コンソール拡張機能でサーバーを再検出します。
   サーバーが [ホスト] タブの下に表示されます。

15

付録

16

Dell EMC サポート サイトからのサポート コンテンツへのアクセス

直接リンクを使用して Dell EMC サポート サイトに移動するか、検索エンジンを使用して、一連のシステム管理ツールに関連するサポート コンテンツにアクセスします。

- 直接リンク：
  - Dell EMC エンタープライズ システム管理および Dell EMC リモート エンタープライズ システム管理：https://www.dell.com/esmmanuals
  - Dell EMC 仮想化ソリューション：https://www.dell.com/SoftwareManuals
  - Dell EMC OpenManage：https://www.dell.com/openmanagemanuals
  - iDRAC：https://www.dell.com/idracmanuals
  - Dell EMC OpenManage Connections エンタープライズ システム管理：https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Dell EMC Serviceability Tools：https://www.dell.com/serviceabilitytools
- Dell EMC サポート サイト：
  1. https://www.dell.com/support にアクセスします。
  2. [すべての製品の参照] をクリックします。
  3. [すべての製品] ページで [ソフトウェア] をクリックして、次に必要なリンクをクリックします。
  4. 必要な製品をクリックして、必要なバージョンをクリックします。

検索エンジンを使用する場合は、検索ボックスにドキュメントの名前とバージョンを入力します。

トピック：

- デルへのお問い合わせ

デルへのお問い合わせ

メモ: お使いのコンピュータがインターネットに接続されていない場合は、購入時の納品書、出荷伝票、請求書、またはデルの製品カタログで連絡先をご確認ください。

デルでは、オンラインまたは電話によるサポートとサービスのオプションを複数提供しています。サポートやサービスの提供状況は国や製品ごとに異なり、国 / 地域によってはご利用いただけないサービスもございます。デルのセールス、テクニカルサポート、またはカスタマーサービスへは、次の手順でお問い合わせいただけます。

1. **Dell.com/support** にアクセスします。
2. サポートカテゴリを選択します。
3. ページの下部にある [国 / 地域の選択] ドロップダウンリストで、お住まいの国または地域を確認します。
4. 必要なサービスまたはサポートのリンクを選択します。