OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager

Unified User's Guide

September 2020
Rev. A01

DELL EMC

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。

Contents

Chapter 1: はじめに : OMIMSSC 9
新機能 9

Chapter 2: OMIMSSC コンポーネント 10

Chapter 3: OMIMSSC のシステム要件 11
サポートマトリックス 11
アカウント権限 13
OMIMSSC の一般的なシステム要件 13
SCCM 用 OMIMSSC コンソール拡張機能のシステム要件 14
SCVMM 用 OMIMSSC コンソール拡張機能のシステム要件 14
ネットワーク要件 14

Chapter 4: 導入 OMIMSSC 15
Web からの OMIMSSC のダウンロード 15
OMIMSSC アプライアンスのセットアップ 15
複数の Microsoft コンソールの登録 16
OMIMSSC コンポーネントをダウンロードするための OMIMSSC 管理ポータルの起動 16
SCCM 用 OMIMSSC コンソール拡張機能のインストール 17
SCVMM 用 OMIMSSC コンソール拡張機能のインストール 17

Chapter 5: OMIMSSC のライセンス 18
ライセンスのアップロード後のオプション 18
強制 19
OMIMSSC へのライセンスのインポート 19
ライセンスの詳細情報の表示 19

Chapter 6: OMIMSSC での Microsoft コンソールの登録 21
登録済み Microsoft コンソールからの OMIMSSC の起動 21
ブラウザーでの OMIMSSC FQDN アドレスの追加 21
SCCM 用 OMIMSSC コンソール拡張機能の起動 22
SCVMM 用 OMIMSSC コンソール拡張機能の起動 22

Chapter 7: OMIMSSC とそのコンポーネントの管理 23
OMIMSSC アプライアンスの詳細情報の表示 23
OMIMSSC ユーザー管理の表示 23
登録済みコンソールの表示または更新 23
OMIMSSC アプライアンスのパスワードの変更 23
インストールツールの修復または変更 24
SCCM 用 OMIMSSC コンソール拡張機能の修復 24
SCVMM 用の OMIMSSC コンソール拡張機能の修復 24
OMIMSSC 管理ポータルでの SCCM および SCVMM アカウントの変更 24

Chapter 8: OMIMSSC アプライアンスのバックアップおよび復元 25

OMIMSSC アプライアンスのバックアップ....25
OMIMSSC アプライアンスの復元....25
OMIMSSC アプライアンスの復元....26

Chapter 9: OMIMSSC のアンインストール....27
OMIMSSC からの Microsoft コンソールの登録解除....27
SCCM 用 OMIMSSC コンソール拡張機能のアンインストール....27
SCVMM 用 OMIMSSC コンソール拡張機能のアンインストール....28
SCVMM 用 OMIMSSC コンソール拡張機能の削除....28
SCVMM での OMIMSSC コンソール拡張機能の削除....28
その他のアンインストール手順....28
アプライアンス固有の RunAsAccounts の削除....28
OMIMSSC アプリケーション プロファイルの削除....28
アプライアンス VM の削除....28

Chapter 10: SCVMM 用 OMIMSSC のアップグレード....29
Service Pack のアップデートについて....29
インストールの必要条件....30
Service Pack のアップグレード手順....30
Service Pack アップデートのリポジトリへのコピー....30
Service Pack アップデートのためのリポジトリ URL 情報の入力....31
Service Pack アップデートのインストール....31
SCCM 用 OMIMSSC コンソール拡張機能のアップグレード....32
SCVMM 用 OMIMSSC コンソール拡張機能のアップグレード....32

Chapter 11: OMIMSSC アプライアンスの再起動....33

Chapter 12: OMIMSSC アプライアンスからのログアウト....34

Chapter 13: プロファイルの管理....35
資格情報プロファイルについて....35
認定資格プロフィールの作成....35
資格情報プロファイルの変更....36
資格情報プロファイルの削除....36
ハイパーバイザープロファイルについて（SCVMM ユーザー用）....37
ハイパーバイザープロファイルの作成....37
ハイパーバイザープロファイルの変更....37
ハイパーバイザープロファイルの削除....38

Chapter 14: デバイスの検出および MSSC コンソールとサーバの同期....39
デバイスの検出： OMIMSSC....39
SCCM 用の OMIMSSC コンソール拡張機能でのデバイス検出....39
SCVMM 用の OMIMSSC コンソール拡張機能でのデバイス検出....39
管理対象システムのシステム要件....40
自動検出を使用したサーバーの検出....40
手動検出を使用したサーバの検出....40
手動検出を使用した MX7000 の検出....41
OMIMSSC コンソール拡張機能と登録された SCCM との同期....42
OMIMSSC コンソール拡張機能と登録された SCVMM との同期....42

登録された Microsoft コンソールとの同期 42
同期エラーの解決 42
システムロックダウンモードの表示 43
OMIMSSC からのサーバの削除 43
OMIMSSC からのモジュラーシステムの削除 43

Chapter 15: OMIMSSC のビュー 44
サーバビューの起動 44
モジュラー型システム ビューの起動 45
OpenManage Enterprise Modular コンソールの起動 46
入力 / 出力モジュール 46
クラスタビューの起動 46
iDRAC コンソールの起動 46
メンテナンスセンターの起動 47
ジョブとログセンターの起動 47

Chapter 16: Operational Template (運用テンプレート) 49
事前定義された Operational Template (運用テンプレート) 50
参照サーバの構成について 50
参照サーバからの Operational Template (運用テンプレート) の作成 50
SCCM 用の OMIMSSC コンソール拡張機能の Windows OS コンポーネント 52
SCVMM 用の OMIMSSC コンソール拡張機能の Windows コンポーネント 52
OMIMSSC コンソール拡張機能の Windows 以外のコンポーネント 52
参照モジュラー型システムからの Operational Template (運用テンプレート) の作成 53
Operational Template (運用テンプレート) の表示 53
Operational Template (運用テンプレート) の変更 54
複数サーバーでの運用テンプレートを使用したシステム固有値 (プール値) の設定 55
Operational Template (運用テンプレート) の削除 55
Operational Template (運用テンプレート) の割り当てとサーバの Operational Template (運用テンプレート) コンプライアンスの実行 55
サーバへの Operational Template (運用テンプレート) の導入 56
モジュラー型システムの Operational Template (運用テンプレート) の割り当て 57
モジュラー型システムへの Operational Template (運用テンプレート) の導入 57
Operational Template (運用テンプレート) の割り当て解除 58
参照モジュラー型システムの構成について 58

Chapter 17: オペレーティングシステムの導入の準備 59
WinPE イメージについて 59
SCCM 用の WIM ファイルの提供 59
SCVMM 用の WIM ファイルの提供 59
DTK ドライバの解凍 59
WinPE イメージのアップデート 60
SCCM コンソールでのオペレーティングシステム導入の準備 60
タスクシーケンス - SCCM 60
Lifecycle Controller 起動メディアのデフォルト共有場所の設定 62
タスクシーケンスメディアのブータブル ISO の作成 62
Windows 以外のオペレーティングシステムの導入の準備 63

Chapter 18: Operational Template (運用テンプレート) を使用したクラスタの作成 64

Storage Spaces Direct クラスター用の論理スイッチの作成 64
Storage Spaces Direct クラスターの作成 64

Chapter 19: OMIMSSC のファームウェアアップデート 66
アップデートグループについて 66
アップデートグループの表示 67
カスタムアップデートグループの作成 67
カスタムアップデートグループの変更 67
カスタムアップデートグループの削除 67
アップデートソースとは 68
ローカル FTP のセットアップ 69
ローカル HTTP のセットアップ 69
ローカル HTTPS のセットアップ 70
アップデートソースの表示 70
アップデートソースの作成 70
アップデートソースの変更 71
アップデートソースの削除 71
Dell EMC Repository Manager（DRM）との統合 71
DRM との統合： OMIMSSC 71
ポーリング頻度の設定 72
デバイスインベントリの表示と更新 72
フィルタの適用 74
フィルタの削除 74
アップデートの実行メソッドを使用したファームウェアバージョンのアップグレードとダウングレード 74
CAU を使用したアップデート 75

Chapter 20: OMIMSSC でのデバイスの管理 76
サーバのリカバリ 76
保護ボールト 76
サーバープロファイルのエクスポート 77
サーバプロファイルのインポート 77
交換したコンポーネントに対するファームウェアおよび構成設定の適用 78
サーバの LC ログの収集 79
LC ログの表示 80
ファイルの説明 80
インベントリのエクスポート 80
スケジュール済みジョブのキャンセル 81

Chapter 21: デバイスのプロビジョニングに使用： OMIMSSC 82
導入シナリオのワークフロー 82
SCCM 用の OMIMSSC コンソール拡張機能を使用した Windows OS の導入 83
SCVMM 用の OMIMSSC コンソール拡張機能を使用したハイパーバイザーの導入 84
Windows OS の再展開に使用： OMIMSSC 85
OMIMSSC コンソール拡張機能を使用した Windows 以外の OS の導入 85
事前定義された Operational Template（運用テンプレート）を使用した Storage Spaces Direct クラスターの作成 85
デバイスをメンテナンスするためのワークフロー 86
サーバおよび MX7000 デバイスのファームウェアのアップデート 86
交換したコンポーネントの設定 88

サーバプロファイルのエクスポートとインポート 88

Chapter 22: 設定と導入 89
使用例 89
運用テンプレートの作成 89
インストーラフォルダ 91
運用テンプレートの割り当て 91
運用テンプレートの導入 92
SCCM 用の OMIMSSC コンソール拡張機能用の Windows OS コンポーネント 92
SCVMM 用の OMIMSSC コンソール拡張機能用の Windows コンポーネント 93
SCCM/SCVMM 用の OMIMSSC コンソール拡張機能用の Windows 以外のコンポーネント 93
登録した MSSC での検出 93
サーバープロファイルのインポート 93
サーバープロファイルのエクスポート 94
LC ログの表示 94
LC ログの収集 94
部品交換 94
ポーリングと通知 94
iDRAC の起動 94
入力出力モジュールの起動 95
同期化エラーの解決 95
OMIMSSC と登録済み Microsoft コンソールの同期 95
割り当ておよび導入 95
アップデートの実行 95
Azure Stack HCI クラスターの導入 95

Chapter 23: トラブルシューティングのシナリオ 97
管理に必要なリソース： OMIMSSC 97
SCCM 用 OMIMSSC コンソール拡張機能を使用するためのアクセス権の検証 97
WMI へのユーザーアクセスの設定 98
SCVMM 用 OMIMSSC コンソール拡張機能を使用するための PowerShell 許可の検証 99
インストールおよびアップグレードのシナリオ： OMIMSSC 99
登録の失敗 100
テスト接続の失敗 100
SCVMM 用 OMIMSSC コンソール拡張機能の接続の失敗 100
SCVMM R2 のアップデート後のコンソール拡張機能へのアクセスエラー 100
OMIMSSC アプライアンスに IP アドレスが割り当てられていない 101
OMIMSSC コンソール拡張機能のインポート中に SCVMM がクラッシュ 101
OMIMSSC コンソール拡張機能へのログインに失敗 101
アップデート中の SC2012 VMM SP1 のクラッシュ 101
OMIMSSC 管理ポータルのシナリオ 101
Mozilla Firefox ブラウザから OMIMSSC 管理ポータルへのアクセス時のエラーメッセージ 101
OMIMSSC 管理ポータルに Dell EMC ロゴが表示されない 102
検出、同期、インベントリーのシナリオ： OMIMSSC 102
サーバの検出の失敗 102
検出されるサーバが すべての Dell Lifecycle Controller サーバ コレクションに追加されていない 102
正しくない資格情報によるサーバ検出の失敗 102
サーバ検出後の不正な VRTX シャーシグループの作成 102
ホスト サーバーは登録済み SCCM と同期できない 103

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....103
再検出されたサーバでのメンテナンス関連タスクの実行に失敗....103
一般的なシナリオ：OMIMSSC....103
CIFS 共有へのホスト名を使用したアクセスの失敗....103
コンソール拡張機能での ジョブおよびログ ページの表示の失敗....103
管理下システムでのオペレーションの失敗....103
OMIMSSC のオンラインヘルプの起動の失敗....104
ファームウェア アップデートのシナリオ：OMIMSSC....104
アップデートソースの作成の失敗....104
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....104
ローカルアップデートソースのテスト接続に失敗....104
DRM アップデートソースの作成に失敗....104
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....105
OMIMSSC のアップグレードまたは移行後に比較レポートを表示できない....105
クラスタのファームウェアアップデートに失敗....105
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....106
DRM アップデートソースの使用時のファームウェアアップデートの失敗....106
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....106
ファームウェアアップデート後に最新のインベントリ情報が表示されない....106
カスタムアップデートグループの削除の失敗....107
WinPE イメージのアップデートに失敗....107
頻度設定の変更後にポーリングと通知ベルの色が変わる....107
OMIMSSC でのオペレーティングシステム導入シナリオ....107
オペレーティングシステム導入の一般的なシナリオ....107
SCCM ユーザー用のオペレーティングシステム導入シナリオ....108
SCVMM ユーザー用のオペレーティングシステム導入シナリオ....108
SCVMM ユーザー用の S2D クラスタ作成シナリオ....109
OMIMSSC でのサーバプロファイルのシナリオ....110
サーバープロファイルのエクスポートの失敗....110
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....110
OMIMSSC での LC ログシナリオ....110
LC ログの .CSV 形式でのエクスポートの失敗....110
LC ログファイルのオープンに失敗....110
テスト接続の失敗....110

Chapter 24: 付録....111

Chapter 25: 付録 2....114

Chapter 26: Dell EMC サポートサイトからのドキュメントへのアクセス....115

1

はじめに：OMIMSSC

このドキュメントは、OMIMSSC の使用方法、インストール、ベスト プラクティスに関連するすべての情報が記載された統合ユーザーズ ガイドです。

Microsoft System Center 向け OpenManage Integration （ OMIMSSC ）は、アプライアンスベースの System Center スイートの製品に統合されています。 OMIMSSC は、Integrated Dell Remote Access Controller （ iDRAC ）with Lifecycle Controller （ LC ）を使用して、Dell EMC PowerEdge サーバーの完全なライフサイクル管理が行えるようにします。

OMIMSSC では、オペレーティング システムの導入、Storage Spaces Direct クラスターの作成、ハードウェアのパッチ、ファームウェア アップデート、サーバー型およびモジュラー型システムのメンテナンスが行えます。従来のデータ センターで OMIMSSC を Microsoft System Center Configuration Manager （ SCCM ）と統合して Dell PowerEdge サーバーを管理したり、仮想およびクラウド環境で OMIMSSC を Microsoft System Center Virtual Machine Manager （ SCVMM ）と統合して Dell PowerEdge サーバーを管理したりできます。

SCCM および 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。

メモ: 関連づけられている Dell EMC Deployment Tool Kit （ DTK ）バージョン 6.4 は、OMIMSSC パックでのみ使用されるように、最新の iDRAC9 X5 ベースの PowerEdge サーバーで使用可能になります。

メモ: DTK は、Dell EMC のサポート終了製品です。このバージョンの DTK は、OMIMSSC バージョン 7.2.1 でのみの使用がサポートされています。

トピック：

- 新機能

新機能

- System Center Configuration Manager （ SCCM ）バージョン 1910 のサポート。
- System Center Configuration Manager （ SCCM ）バージョン 2002 のサポート。
- System Center Virtual Machine Manager （ SCVMM ）2016 UR8 のサポート。
- System Center Virtual Machine Manager （ SCVMM ）2016 UR9 のサポート。
- System Center Virtual Machine Manager （ SCVMM ）2019 UR1 のサポート。
- ユーザー マニュアルの簡略化（ インストール ガイド、ユーザーズ ガイド、およびトラブルシューティング情報は、単一の統合ドキュメントに統合されました ）。
- より高速なアプライアンス ダウンロードをサポートするためのインストーラー ファイル サイズの削減。
- 不適切な認証、アプライアンスのログの情報開示、ハードコードされた暗号キーの使用の脆弱性に対するセキュリティの修正の実装。このセキュリティの修正の詳細については、https://www.dell.com/support/security を参照してください。
- 最新の iDRAC9 ベース PowerEdge サーバーのサポート。

2

OMIMSSC コンポーネント

このガイドで使用されている OMIMSSC コンポーネントとその名前を以下にリストします。

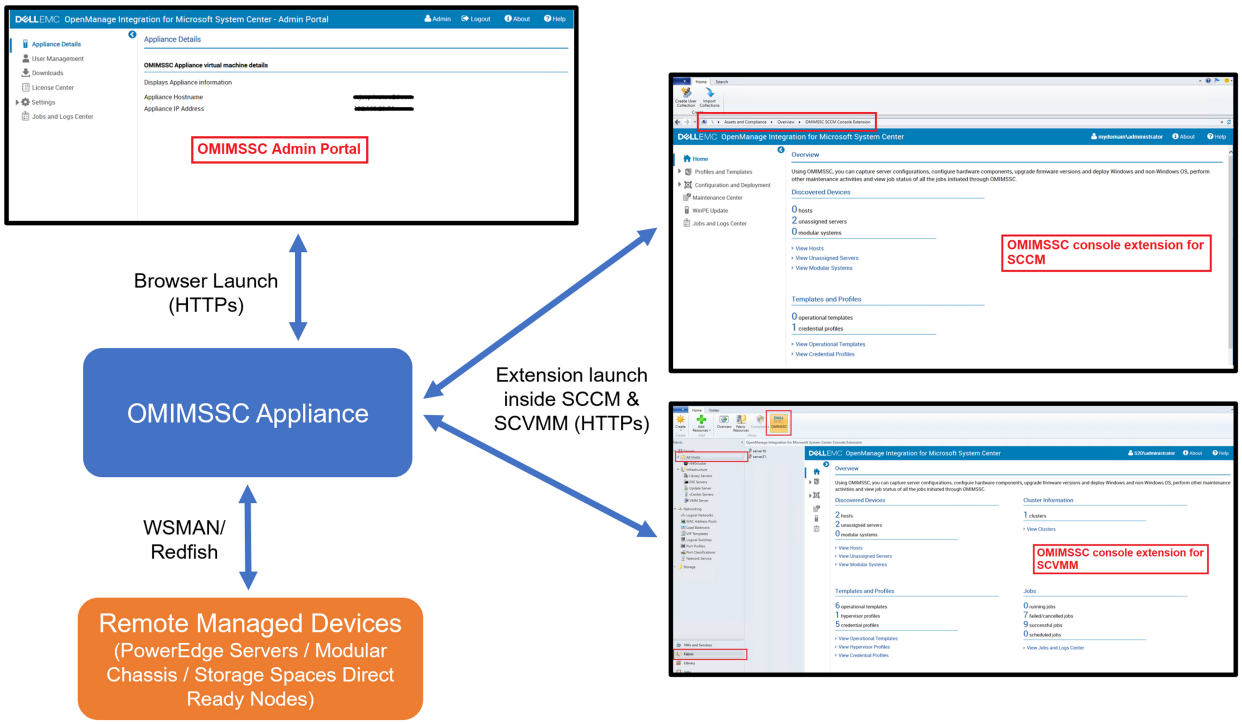
表 1. 含まれるコンポーネント OMIMSSC

コンポーネント	説明
Microsoft System Center 向け OpenManage Integration アプライアンス仮想マシン。OMIMSSC アプライアンスとも呼ばれます。	Hyper-V 上で OMIMSSC アプライアンスを CentOS に基づく仮想マシンとしてホストし、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 サーバと通信する。 • REST API コマンドを使用して、OpenManage Enterprise Module (OME モジュール型) 経由で Dell EMC PowerEdge MX7000 デバイスと通信する。 • OMIMSSC 管理ポータルから OMIMSSC アプライアンスの管理を可能にする。
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 コンソールと SCVMM コンソールで、次のように同じコンソール拡張機能が使用されます。 • OMIMSSC SCCM 用コンソール拡張機能 • OMIMSSC SCVMM 用コンソール拡張機能

管理システムとは、OMIMSSC とそのコンポーネントがインストールされているシステムです。

管理対象システムとは、OMIMSSC によって管理されているサーバーです。

OMIMSSC アーキテクチャ



3

OMIMSSC のシステム要件

トピック：

- サポートマトリックス
- アカウント権限
- OMIMSSC の一般的なシステム要件
- SCCM 用 OMIMSSC コンソール拡張機能のシステム要件
- SCVMM 用 OMIMSSC コンソール拡張機能のシステム要件
- ネットワーク要件

サポートマトリックス

OMIMSSC で使用可能なすべてのサポート マトリックスは、次のとおりです。

OMIMSSC **対応 System Center**

- Microsoft System Center Configuration Manager (SCCM) 2012 SP1
- Microsoft System Center Configuration Manager (SCCM) 2012 SP2
- Microsoft System Center Configuration Manager (SCCM) 2012 R2
- Microsoft System Center Configuration Manager (SCCM) 2012 R2 SP1
- Microsoft System Center Configuration Manager (SCCM) 1610
- Microsoft System Center Configuration Manager (SCCM) バージョン 1809
- Microsoft System Center Configuration Manager (SCCM) バージョン 1810
- Microsoft System Center Configuration Manager (SCCM) バージョン 1902
- Microsoft System Center Configuration Manager (SCCM) バージョン 1906
- Microsoft System Center Configuration Manager (SCCM) バージョン 1910
- Microsoft System Center Configuration Manager (SCCM) バージョン 2002
- Microsoft System Center Virtual Machine Manager (SCVMM) 2012 SP1
- Microsoft System Center Virtual Machine Manager (SCVMM) 2012 R2
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016 UR8
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016 UR9
- Microsoft System Center Virtual Machine Manager (SCVMM) 2019
- Microsoft System Center Virtual Machine Manager (SCVMM) 2019 UR1
- Microsoft System Center Virtual Machine Manager (SCVMM) SAC バージョン 1807

表 2. 対応デバイス

Dell EMC システム	対応バージョン
iDRAC 9 ベースの PowerEdge サーバー	• サポート AMD プラットフォーム向け OS ドライバー パック： ○ R6515、R7515、C6525、R6525 - 19.12.08 ○ R7525 - 19.12.07 • サポート AMD プラットフォーム向けの Lifecycle Controller バージョンと Integrated Dell EMC Remote Access Controller バージョン： **SCCM** ○ R6515 および R7515 - 3.40.40.40 以降 ○ C6525 および R6525 - 3.42.42.42 以降 ○ R7525 - 4.10.10.10 以降

表 2. 対応デバイス（続き）

Dell EMC システム	対応バージョン
	SCVMM ○ R6515、R7515、C6525、R6525、R7525 - 4.30.30.30 以降 ● Dell EMC OpenManage Deployment Tool kit バージョン 6.4 **メモ:** ESXi のオペレーティング システムの導入はサポートされていません。 **メモ:** vFlash から起動/vFLash からステージングする方式のオペレーティング システムの導入機能およびサーバープロファイルのバックアップ機能はサポートされていません。
PowerEdge サーバー第 14 世代	● OS ドライバー パック：17.05.21 ● Lifecycle Controller バージョン 3.00.00.00 以降 ● Integrated Dell EMC Remote Access Controller バージョン 3.00.00.00 以降 ● Dell EMC OpenManage Deployment Tool kit バージョン 6.3
PowerEdge サーバー第 13 世代	● OS ドライバー パック：16.08.13 ● Lifecycle Controller バージョン 2.40.40.40 以降 ● Integrated Dell Remote Access Controller バージョン 2.40.40.40 以降 ● Dell EMC OpenManage Deployment Tool kit バージョン 6.3
PowerEdge サーバー第 12 世代	● OS ドライバー パック：サーバー R220 および FM120 - 16.08.13 ● その他のサポート プラットフォーム OS ドライバー パック：15.07.07 ● Lifecycle Controller バージョン 2.40.40.40 以降 ● Integrated Dell Remote Access Controller バージョン 2.40.40.40 以降 ● Dell OpenManage Deployment Tool kit バージョン 6.3
Chassis Management Console（CMC）	● FX2 1.4 以降 ● M1000e 5.2 以降 ● VRTX 2.2 以降
Dell EMC OpenManage Enterprise-Modular	● PowerEdge MX7000 シャーシ 1.0

メモ: 第 11 世代 PowerEdge サーバーのサポートは、OMIMSSC バージョン 7.2.1 リリース以降では廃止されています。

表 3. 対応オペレーティング システム（導入）：

オペレーティングシステム	対応バージョン
Microsoft Windows	● Windows Server 2019 ● Windows Server 2016 ● Windows Server 2012 R2 ● Windows Server 2012 SP 1
Linux オペレーティング システム	● RHEL 7.3、7.4、7.5 ● RHEL 7.2 ● RHEL 6.9
VMWare ESXi	● ESXi 6.0 - A02 ● ESXi 6.0 U3 - A15 ● ESXi 6.5 - A03 ● ESXi 6.5 U1 - A11 ● ESXi 6.7 - A06

表 3. 対応オペレーティング システム (導入) : (続き)

オペレーティングシステム	対応バージョン
	メモ: https://www.dell.com/support/ からイメージをダウンロードします。OMIMSSC 対応バージョンに応じて、特定のサーバー モデルの [ドライバーおよびダウンロード] ページを参照してください。

OMIMSSC 対応クラスター

- SCVMM コンソール上の Windows 2016 および 2019 S2D 対応クラスターの作成と管理
- SCVMM コンソール上の Windows 2012 R2、2016、および 2019 Hyper-V ホスト クラスターの管理

アカウント権限

OMIMSSC を使用するために必要なすべてのアカウント権限は、次のとおりです。

SCCM 用 OMIMSSC コンソール拡張機能のアカウント権限とは、ユーザーが SCCM の次のグループのメンバーであることです。

表 4. 必要な権限のあるユーザーアカウント

ユーザー	権限 / 役割
登録時	• OMIMSSC への SCCM コンソールの登録に使用するアカウントは、SCCM の管理者またはフル管理者である必要があります。 • OMIMSSC への SCVMM コンソールの登録に使用するアカウントは、SCVMM の管理者役割のメンバーである必要があります。 • ドメイン ユーザー。 • システム センター マシンのローカル管理者グループのメンバー。
コンソール拡張機能へのログイン時	• OMIMSSC への SCCM コンソールの登録に使用するアカウントは、SCCM の管理者またはフル管理者である必要があります。 • OMIMSSC への SCVMM コンソールの登録に使用するアカウントは、SCVMM の委任管理者または管理者である必要があります。 • ドメイン ユーザー。 • システム センター マシンのローカル管理者グループのメンバー。

OMIMSSC の一般的なシステム要件

OMIMSSC をインストールする前に、リストにある 3 つの OMIMSSC コンポーネントに基づき、次のソフトウェア前提条件をインストールしてください。

- OMIMSSC アプライアンス :
  - Windows Server をインストールして、Hyper-V 役割を有効にする。
  - OMIMSSC がマルチコンソール登録をサポートするようになったため、任意の数の SCCM または SCVMM コンソールを 1 台の OMIMSSC アプライアンスに登録できるようになりました。登録コンソール数に応じたハードウェア要件は次のとおりです。

表 5. ハードウェア要件

コンポーネント	SCCM または SCVMM コンソール 1 台の場合	SCCM または SCVMM コンソール N 台の場合
RAM	8 GB	8 GB x N
プロセッサー数	4	4 x N

- 次の Windows オペレーティングシステムのいずれかをインストール：
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- OMIMSSC 管理ポータル：

  次のいずれかのサポート対象ブラウザをインストール：
  - Internet Explorer 10 以降
  - Mozilla Firefox 30 以降
  - Google Chrome 23 以降
  - Microsoft Edge

次の特定の OMIMSSC システム要件を満たすには、使用するコンソールに応じて次のリンクの説明にある要件に従ってください。
- SCCM 用 OMIMSSC コンソール拡張機能のシステム要件
- SCVMM 用 OMIMSSC コンソール拡張機能のシステム要件

SCCM 用 OMIMSSC コンソール拡張機能のシステム要件

SCCM 用 OMIMSSC コンソール拡張機能をインストールするには、次の手順を実行します。
- 同じバージョンの SCCM 管理コンソールと SCCM サイトサーバをインストールしてください。

SCVMM 用 OMIMSSC コンソール拡張機能のシステム要件

SCVMM 用 OMIMSSC コンソール拡張機能をインストールするには、次の手順を実行します。
- 同じバージョンの SCVMM 管理コンソールと SCVMM サーバをインストールします。
- SCVMM サーバのフェイルオーバークラスタリング機能を有効にします。
- 登録済みユーザーには、SCVMM サーバーでの管理者権限が必要です。
- 登録済みユーザーには、管理下クラスターでの管理者権限が必要です。

ネットワーク要件

OMIMSSC アプライアンスが使用するポート：

さまざまな OMIMSSC コンポーネントが次のリストのポートを使用します。これらのポートはファイアウォールの例外リストにも入っています。

表 6. ポート情報

使用状況	プロトコル	ポート番号
iDRAC 通信	WSMan	—
モジュラーシステム	REST	—
自動検出	HTTPS	—
iDRAC — これらのポートは、インストールツールまたはユーザーによって作成された CIFS 共有に iDRAC がアクセスできるように有効化されています。	HTTPS	135 から 139、および 445

4

導入 OMIMSSC

トピック：

- Web からの OMIMSSC のダウンロード
- OMIMSSC アプライアンスのセットアップ
- 複数の Microsoft コンソールの登録
- OMIMSSC コンポーネントをダウンロードするための OMIMSSC 管理ポータルの起動

Web からの OMIMSSC のダウンロード

OMIMSSC を https://www.dell.com/support からダウンロードするには、次の手順を実行します。

1. **すべてのプロダクトのブラウズ** > **ソフトウェア** > **エンタープライズシステム管理** > **Microsoft システム用 OpenManage Integration** の順にクリックします。
2. 必要なバージョンの OMIMSSC を選択します。
3. **ドライバおよびダウンロード** タブをクリックします。
4. OMIMSSC VHD ファイルをダウンロードします。
5. VHD ファイルを抽出し、OMIMSSC アプライアンスをセットアップします。
   VHD ファイルのサイズは約 5 GB になります。そのため、導入には 5～10 分程度かかります。
6. ファイルの解凍先とする場所を指定し、[解凍] ボタンをクリックしてファイルを解凍します：
   - **OMIMSSC_v7.2.1.2610_for_VMM_and_ConfigMgr**
   - **DellEMC_OpenManage_Deployment_Toolkit_Windows_6.4.0**

     メモ: DTK バージョン 6.4 は、OMIMSSC バージョン 7.2.1 でのみの使用がサポートされています。

OMIMSSC アプライアンスのセットアップ

OMIMSSC アプライアンスをセットアップする Hyper-V が、次の要件を満たしていることを確認してください。

- 仮想スイッチ が設定済みであり、使用可能である。
- 登録する Microsoft コンソール数に応じたメモリーが、OMIMSSC アプライアンス VM に割り当てられている。詳細については、「一般的な要件」を参照してください。

OMIMSSC アプライアンスをセットアップするには、次の手順を実行します。

1. 次の手順に従って、OMIMSSC アプライアンス VM を導入します。
   a. **Windows サーバ** の **Hyper-V マネージャ** の **アクション** メニューで、**新規** を選択して **Virtual Machine Manager** を選択します。
      仮想マシンの新規作成ウィザード が表示されます。
   b. **開始する前に** で **次へ** をクリックします。
   c. **名前と場所の指定** では、仮想マシンの名前を入力します。
      仮想マシンを別の場所に格納する場合は、**別の場所に仮想マシンを格納** を選択し、**ブラウズ** をクリックして、新しい場所をスキャンします。
   d. **世代の指定** で、**第 1 世代** を選択してから、**次へ** をクリックします。
   e. **メモリの割り当て** で、前提条件で示されるメモリ容量を割り当てます。
   f. **ネットワークの設定** の **接続** で、使用するネットワークを選択して、**次へ** をクリックします。
   g. [**仮想ハード ディスクの接続**] で [**既存の仮想ハード ディスクを使用**] を選択し、**OMIMSSC_v7.2.1_for_VMM_and_ConfigMgr** VHD ファイルがある場所をスキャンして、そのファイルを選択します。
      VHD ファイルのサイズは約 5 GB になります。そのため、導入には 5～10 分程度かかります。
   h. **概要** で指定した詳細を確認し、**完了** をクリックします。

i. **仮想プロセッサの数** の値を 4 に設定します。デフォルトでは、プロセッサの数が 1 に設定されています。

プロセッサ数を設定するには次のようにします。

i. OMIMSSC アプライアンスを右クリックして、[**設定**] を選択します。
ii. **設定** で **プロセッサ** を選択し、**仮想プロセッサの数** を **4** に設定します。

2. OMIMSSC アプライアンス VM を起動して、次のタスクを実行します。
3. OMIMSSC アプライアンスが起動したら、次のタスクを実行します。

メモ: すべてのサービスが開始されるように、5 分間待ってから **Admin** としてログインすることを推奨します。

a. **localhost ログイン** に admin と入力します。
b. **新しい管理者パスワードを入力** にパスワードを入力します。

メモ: Dell EMC では、アプライアンスの admin ユーザーとコンソール拡張機能を認証するために、強固なパスワードを設定して使用することを推奨します。

c. **新しい管理者パスワードを確認してください** にパスワードを再入力し、**Enter** を押して続行します。
d. リストされたオプションで、**ネットワークの設定** を選択して **Enter** キーを押し、次のサブステップを実行します。
   - **NetworkManagerTUI** で、[**システム ホスト名の設定**] を選択し、OMIMSSC アプライアンス名を入力して、[**OK**] をクリックします。

     例： `Hostname.domain.com`

     メモ: [**ネットワークの設定**] オプションを選択して、OMIMSSC アプライアンスの IP アドレスを変更します。これ以降、OMIMSSC アプライアンスの IP アドレスあるいはホスト名を変更することはできません。
   - 固定 IP アドレスを指定する場合は、**接続の編集**、**Ethernet0** の順に選択します。

     IPv4 設定 で **手動** を選択して、**表示** をクリックします。IP 設定アドレス、ゲートウェイアドレス、DNS サーバ IP を指定して、**OK** をクリックします。

e. OMIMSSC アプライアンスの OMIMSSC 管理ポータルの URL をメモしておいてください。

メモ: OMIMSSC アプライアンスの IP と FQDN を DNS の 前方参照ゾーン および 逆引き参照ゾーン に追加します。

メモ: アプライアンス ログは、管理者以外のユーザーがアクセスできます。ただし、これらのログには機密情報は記録されません。回避策として、アプライアンスの URL を保護してください。

複数の Microsoft コンソールの登録

OMIMSSC に複数の Microsoft コンソールが登録されている場合は、OMIMSSC アプライアンスのリソースを管理します。

OMIMSSC アプライアンスに登録する Microsoft コンソール数に応じて、ハードウェア要件を満たしていることを確認してください。詳細については、「OMIMSSC の一般的なシステム要件」を参照してください。

複数の Microsoft コンソールのリソースを設定するには、次の手順を実行します。

1. OMIMSSC アプライアンスを起動してログインします。
2. **登録パラメーターの設定** に移動し、**Enter** キーをクリックします。
3. OMIMSSC アプライアンスに登録するコンソール数を入力します。
   必要なリソースの一覧が表示されます。

OMIMSSC コンポーネントをダウンロードするための OMIMSSC 管理ポータルの起動

1. ブラウザーを起動し、OMIMSSC アプライアンスへのログインに使用したのと同じ認証情報で OMIMSSC 管理ポータルにログインします

   フォーマット： `https://<IP address or FQDN>`

メモ: OMIMSSC 管理ポータルの URL を [**ローカル イントラネット サイト**] に追加します。詳細については、「ブラウザーでの OMIMSSC IP アドレスの追加」を参照してください

2. **ダウンロード**、**インストール ツールのダウンロード** の順にクリックして、必要なコンソール拡張機能をダウンロードします。

SCCM 用 OMIMSSC コンソール拡張機能のインストール

- SCCM 管理コンソールを使用する前に、SCCM サイトサーバに OMIMSSC をインストールするようにしてください。
- SCCM 用 OMIMSSC コンソール拡張機能のインストール、アップグレード、アンインストールを行う前に、Configuration Manager を閉じておくことを推奨します。

1. `OMIMSSC_SCCM_Console_Extension.exe` をダブルクリックします。
   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. **ライセンス契約** ページで、**ライセンス契約の条件に同意します** を選択してから、**次へ** をクリックします。
4. **インストール先フォルダ** ページには、デフォルトのインストールフォルダが選択されています。場所を変更するには、**変更** をクリックし、新しい場所をスキャンして、**次へ** をクリックします。
5. **プログラムインストールの準備完了** ページで、**インストール** をクリックします。

   コンソール拡張機能をインストールすると、次のフォルダが作成されます。
   - ログ—このフォルダは、コンソール関連のログ情報で構成されます。
6. **インストールが完了しました** で、**終了** をクリックします。

SCVMM 用 OMIMSSC コンソール拡張機能のインストール

- SCVMM 管理サーバーおよび SCVMM コンソールに OMIMSSC コンソール拡張機能をインストールします。OMIMSSC コンソールのインストールが完了したら、SCVMM にコンソール拡張機能をインポートしてください。

1. `OMIMSSC_SCVMM_Console_Extension.exe` をダブルクリックします。
   [**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. **ライセンス契約** ページで、**ライセンス契約の条件に同意します** を選択してから、**次へ** をクリックします。
4. **インストール先フォルダ** ページには、デフォルトのインストールフォルダが選択されています。場所を変更するには、**変更** をクリックし、新しい場所をスキャンして、**次へ** をクリックします。
5. **プログラムインストールの準備完了** ページで、**インストール** をクリックします。

   コンソール拡張機能をインストールすると、次のフォルダが作成されます。
   - ログ—このフォルダは、コンソール関連のログ情報で構成されます。
   - OMIMSSC_UPDATE - Cluster Aware Update (CAU) に必要なすべてのアクティビティーが入ったフォルダーです。このフォルダには、CAU 操作専用の読み取り / 書き込み権限があります。このフォルダには、Windows Management Instrumentation (WMI) 権限が設定されています。詳細については、Windows のマニュアルを参照してください。
6. **InstallShield ウィザードを完了しました** ページで、**終了** をクリックします。
7. SCVMM 用 OMIMSSC コンソール拡張機能を SCVMM コンソールにインポートします。詳細については、「SCVMM 用 OMIMSSC コンソール拡張機能のインポート」を参照してください。

5

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。

- 評価版ライセンス：インストールすると自動的にインポートされる、サーバ（ホストまたは未割り当て）5 台分の評価版ライセンスからなる評価版のライセンスです。第 11 世代以降の Dell EMC サーバにのみ適用されます。
- 本番ライセンス：OMIMSSC で管理するサーバ数に応じて、Dell EMC から本番ライセンスを購入できます。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も含まれています。

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 Locker 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、`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。

ライセンスファイルが 1 つあれば、OMIMSSC でサーバの検出を行うことができます。OMIMSSC でサーバが検出されると、ライセンスが使用されます。サーバが削除されると、ライセンスは解放されます。次のアクティビティは、OMIMSSC のアクティビティログに記録されます。

- ライセンスファイルがインポートされた。
- OMIMSSC からサーバが削除され、ライセンスが譲渡された。
- サーバが検出され、ライセンスが使用された、

評価版ライセンスから本番ライセンスにアップグレードすると、評価版ライセンスは本番ライセンスで上書きされます。**ライセンスノード** 数は、購入した本番ライセンス数と同一です。

トピック：

- ライセンスのアップロード後のオプション
- 強制
- OMIMSSC へのライセンスのインポート
- ライセンスの詳細情報の表示

ライセンスのアップロード後のオプション

以下は、OMIMSSC のライセンス機能にサポートされるオプションです。

新しく購入した製品のライセンスファイル

新規ライセンスを注文すると、注文確認の電子メールがデルから届き、Dell Digital ストアから新しい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、ライセンスの XML ファイルを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

本番ライセンスを複数スタックしておき、アップロードしたライセンスの合計サーバ数までサポート対象サーバ数を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。スタックでサポート対象サーバ数を増やすことはできません。複数の OMIMSSC 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、サポート対象ホスト数は最後にライセンスをアップロードした時点のライセンスの合計サーバ数です。

ライセンスの交換

注文に問題がある場合、あるいは変更または破損したファイルをアップロードしようとすると、同じエラーメッセージが表示されます。Dell Digital Locker から別のライセンスファイルをリクエストできます。受け取った交換用ライセンスには、以前の

ライセンスと同じ使用資格 ID が入っています。交換用のライセンスをアップロードする際、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、そのライセンス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をインポートしようとすると、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て、インポートしてください。

複数ライセンスのインポート

異なる登録 ID が入ったライセンスファイルを複数インポートして、OMIMSSC で検出およびメンテナンスするサーバ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、次の手順に従い OMIMSSC にインポートします。

1. OMIMSSC 管理ポータルで、**ライセンスセンター** をクリックします。
2. **ライセンスのインポート** をクリックして、Dell Digital Store 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: インポートできるのは、有効なライセンスファイルだけです。ファイルが破損または改ざんされている場合は、それに応じてエラーメッセージが表示されます。Dell Digital Store からファイルを再度ダウンロードするか、デルの担当者に連絡し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。

6

OMIMSSC での Microsoft コンソールの登録

- SCCM ユーザーの場合は、SCCM コンソール用の OMIMSSC コンソール拡張機能がインストールされていること。
- SCVMM ユーザーの場合は、SCVMM 用 OMIMSSC コンソール拡張機能がインストールされていること。

次の情報が利用できるように準備しておいてください。

- Microsoft がセットアップされているシステムのユーザー資格情報。「必要なアカウント特権」を参照してください。
- SCCM の FQDN または SCVMM の FQDN。

SCCM または SCVMM コンソールを OMIMSSC に登録するは、次の手順を実行します。

1. ブラウザを開き、OMIMSSC アプライアンスの URL を入力します。
   OMIMSSC 管理ポータルページが表示されます。
2. **設定**、**コンソール登録**、**登録** の順にクリックします。
   コンソール登録 ページが表示されます。
3. コンソールの名前と説明を入力します。
4. SCCM サイトサーバまたは SCVMM サーバの FQDN と資格情報を入力します。
5. （オプション）**新規作成** をクリックして、SCCM または SCVMM コンソールにアクセスするための Windows タイプの資格情報プロファイルを作成します。
   - [**Windows 資格情報プロファイル**] として [**資格情報プロファイル タイプ**] を選択します。
   - プロファイル名および説明を指定します。
   - **資格情報** で、ユーザー名とパスワードを指定します。
   - ドメインの詳細を [**ドメイン**] に入力します。

   メモ: コンソール登録のための資格情報プロファイルの作成時に、ドメイン名とトップレベルドメイン（TLD）の詳細情報を指定します。

   たとえば、ドメイン名が `mydomain` で TLD が `com` の場合は、資格情報プロファイルのドメイン名に `mydomain.com` と指定します。
6. OMIMSSC アプライアンスと Microsoft コンソールの間の接続を確認するには、**テスト接続** をクリックします。
7. テスト接続の完了後、コンソールを登録するには、**登録** をクリックします。

   メモ: 登録が完了すると、OMIMSSC は **OMIMSSC SCVMM コンソール拡張機能登録プロファイル** という名前で、SCVMM にアカウントを作成します。このプロファイルを削除しないようにしてください。削除すると、OMIMSSC で一切の操作が実行できなくなります。

   メモ: SCCM 管理コンソールで、OMIMSSC コンソール拡張機能を使用するように SCCM サイトサーバを登録します。

トピック：

- 登録済み Microsoft コンソールからの OMIMSSC の起動

登録済み Microsoft コンソールからの OMIMSSC の起動

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

ブラウザーでの OMIMSSC FQDN アドレスの追加

OMIMSSC を起動する前に、次の手順を実行して、前提条件として OMIMSSC の FQDN アドレスを [**ローカル イントラネット**] サイト リストに追加します。

1. **IE の設定** をクリックし、**インターネットオプション** をクリックします。
2. **詳細設定** をクリックして、**設定** で **セキュリティ** セクションを探します。

3. **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て、**OK** をクリックします。

SCCM 用 OMIMSSC コンソール拡張機能の起動

「アカウント権限」に記述されているユーザー権限テーブルが表示されます。

SCCM コンソールで、**情報およびコンプライアンス**、**概要**、**SCCM 用 OMIMSSC コンソールの拡張機能** 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

SCVMM 用 OMIMSSC コンソール拡張機能を起動するには、次の手順を実行します。

1. SCVMM にコンソール拡張機能をインポートします。詳細については、「SCVMM 用 OMIMSSC コンソール拡張機能のインポート」を参照してください。
2. SCVMM でコンソール拡張機能を起動します。詳細については、「SCVMM からの OMIMSSC コンソール拡張機能の起動」を参照してください。

SCVMM 用 OMIMSSC コンソール拡張機能のインポート

SCVMM 用 OMIMSSC コンソール拡張機能をインポートするには、次の手順を実行します。

1. 管理者権限または委任管理者権限を使用して、SVMM コンソールを起動します。
2. **設定**、**コンソールアドインのインポート** の順にクリックします。
   コンソールアドインのインポートウィザード が表示されます。
3. **ブラウズ** をクリックし、`C:\Program Files\OMIMSSC\VMM Console Extension` で .zip ファイルを選択して、**次へ**、**完了** の順にクリックします。
   アドインが有効なことを確認します。

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** サーバグループを選択します。

   メモ: OMIMSSC の起動には、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、**DELL EMC OMIMSSC** をリボンから選択します。

7

OMIMSSC とそのコンポーネントの管理

トピック：

- OMIMSSC アプライアンスの詳細情報の表示
- OMIMSSC ユーザー管理の表示
- 登録済みコンソールの表示または更新
- OMIMSSC アプライアンスのパスワードの変更
- インストールツールの修復または変更
- OMIMSSC 管理ポータルでの SCCM および SCVMM アカウントの変更

OMIMSSC アプライアンスの詳細情報の表示

1. ブラウザから OMIMSSC 管理ポータルを起動します。
2. OMIMSSC アプライアンス VM へのログイン時に使用した資格情報と同じ資格情報を使用して OMIMSSC 管理ポータルにログインし、**アプライアンスの詳細情報** をクリックします。OMIMSSC アプライアンスの IP アドレスとホスト名が表示されます。

OMIMSSC ユーザー管理の表示

1. ブラウザから OMIMSSC 管理ポータルを起動します。
2. OMIMSSC アプライアンス VM へのログイン時に使用した資格情報と同じ資格情報を使用して OMIMSSC 管理ポータルにログインし、**OMIMSSC ユーザー管理** をクリックします。前回 SCCM または SCVMM にログインしたユーザーのステータスが表示されます。

登録済みコンソールの表示または更新

次の手順を実行すると、OMIMSSC に登録されているすべての Microsoft コンソールが表示されます。

1. OMIMSSC 管理ポータルで、**設定**、**コンソール登録** の順にクリックします。
   登録されているすべてのコンソールが表示されます。
2. 登録されているコンソールの最新のリストを表示するには、**更新** をクリックします。

OMIMSSC アプライアンスのパスワードの変更

OMIMSSC アプライアンス VM のパスワードを変更するには、次の手順を実行します。

1. OMIMSSC アプライアンス VM を起動し、古い認証情報を使用してログインします。
2. **管理者パスワードの変更** に移動して、**Enter** キーを押します。
   パスワードを変更する画面が表示されます。
3. 現在のパスワードを入力し、リストされている条件を満たす新しいパスワードを入力します。新しいパスワードを再度入力し、**Enter** キーを押します。
   パスワード変更後のステータスが表示されます。
4. ホームページに戻るには、**Enter** キーを押します。

メモ: パスワードを変更すると、アプライアンスは再起動します。

インストールツールの修復または変更

インストールツールファイルのいずれかを修復するには、次の説明を参照してください。

- SCCM 用 OMIMSSC コンソール拡張機能の修復
- SCVMM 用 OMIMSSC コンソール拡張機能の修復

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 管理ポータルでの SCCM および 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 と SCVMM アカウントのパスワードを変更できます。

OMIMSSC 管理ポータルから、SCCM および SCVMM 管理者パスワード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。

1. Active Directory の SCCM または SCVMM 管理者アカウントのパスワードを変更します。
2. OMIMSSC でパスワードを変更します。

OMIMSSC で SCCM または SCVMM 管理者アカウントを変更するには、次の手順を実行します。

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. 新しいパスワードを入力し、**終了** をクリックして変更を保存します。

パスワードの更新後、新しい資格情報を使用して Microsoft コンソールと OMIMSSC コンソール拡張機能を再起動してください。

8

OMIMSSC アプライアンスのバックアップおよび復元

OMIMSSC アプライアンスの [**バックアップ アプライアンス データ**] オプションを使用して、登録 Microsoft コンソール、検出デバイス、プロファイル、アップデート ソース、運用テンプレート、ライセンス、完了ジョブなどの OMIMSSC 情報を OMIMSSC コンソール拡張機能に保存します。

トピック：

- OMIMSSC アプライアンスのバックアップ
- OMIMSSC アプライアンスの復元

OMIMSSC アプライアンスのバックアップ

この機能により、OMIMSSC アプライアンス データベースと重要な設定をバックアップすることができます。バックアップ ファイルは、ユーザーが入力した暗号化されたパスワードを使用して CIFS 共有パスに格納されます。アプライアンス データは定期的にバックアップすることをお勧めします。

前提条件：

- アクセス資格情報を使用して CIFS 共有を作成し、読み取りと書き込みアクセス権を許可していることを確認します。
- バックアップと復元の両方で同じ暗号化パスワードが使用されていることを確認します。暗号化パスワードを回復することはできません

CIFS 共有上の OMIMSSC アプライアンス データをバックアップするには、次の手順を実行します。

メモ: この機能は OMIMSSC バージョン 7.2.1 以降で使用可能であり、黒のコンソールでは使用できません。

1. OMIMSSC 管理ポータルで、 [**設定**]、 [**アプライアンスのバックアップ**] の順にクリックします。
2. [**バックアップの設定と詳細**] ページで、バックアップのための CIFS 共有パスを *<IP address or FQDN>* *<folder name>*形式で入力します。
3. ドロップダウン メニューから [**CIFS 共有の認定資格プロフィール**] を選択します。
4. [**パスワード**] フィールドと [**パスワードの再入力**] フィールドに暗号化パスワードを入力します。
5. [**接続のテスト**] をクリックして、OMIMSSC アプライアンスと CIFS 共有の間の接続を確認します。
   前述したバックアップ フォルダーが存在し、アクセス可能であることを確認します
6. [**バックアップ**] をクリックして、OMIMSSC アプライアンスのデータをバックアップします。

次の手順

バックアップが成功したかどうかを確認するには、バックアップ フォルダーに移動します。バックアップ フォルダーには、次の形式で作成された 2 つのファイルがあります。

- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz
- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz.sum

メモ: バックアップ ファイルに表示される日付と時刻は、バックアップが実行された日時を示します。バックアップ ファイルの名前は変更しないでください。

OMIMSSC アプライアンスの復元

アプライアンスの復元を行う前に、OMIMSSC バージョン 7.2.1 のコンソール拡張機能をインストールしてください。「OMIMSSC コンポーネントをダウンロードするための OMIMSSC 管理ポータルの起動」セクションを参照してください。

次のいずれかのシナリオの場合に、OMIMSSC アプライアンスのデータを復元します。

- 次へアップグレードする前：新バージョンの OMIMSSC
- 次へ移行する前：特定の OMIMSSC アプライアンスから別の OMIMSSC アプライアンスへ

OMIMSSC アプライアンスの復元

前提条件：

新しい OMIMSSC アプライアンスで操作を実行する前に、忘れずにデータを復元してください。

古い OMIMSSC アプライアンスのデータを新しい OMIMSSC アプライアンスに復元するには、次の手順を実行します。

1. OMIMSSC 管理ポータルで、[**設定**]、[**アプライアンスの復元**] の順にクリックします
2. アプライアンス データの復元には、2 つのオプションを使用できます。
   - `Option 1: Restore using IP address`

     OMIMSSC バージョン 7.1、7.1.1、および 7.2 からデータを復元するには、このオプションを使用する必要があります。

     IP アドレスに古い OMIMSSC アプライアンスの IP アドレスを指定して、[復元] をクリックします。

     メモ: データは新しい OMIMSSC アプライアンスに復元されます。
   - オプション 2：カスタム CIFS 共有を使用した復元

     7.2.1 リリース以降からデータを復元するには、このオプションを使用する必要があります

     メモ: CIFS 共有アクセス資格情報は、認定資格プロフィールとしてデータベースに格納されています。セキュリティ対策を追加するには、バックアップされたファイルを復号化するために暗号化パスワードを指定する必要があります。

   a. CIFS 共有の場所のパスを`\\<IP address or FQDN>\<folder name>\<filename>.tar.gz` 形式で指定します。
   b. ドロップダウン メニューから CIFS 共有の認定資格プロフィールを選択します。
   c. ファイルの暗号化パスワードを入力し、[復元] をクリックします。

   [**復元**] ページは、自動的にログアウトされます。
3. OMIMSSC アプライアンスの再起動後に復元のステータスを表示するには、次の手順を実行します。

   すべてのサービスが開始されるように、ログインする前に数分間待ってからログインすることを推奨します。

   a. OMIMSSC 管理ポータルにログインします。
   b. **設定** を展開して、**ログ** をクリックします。
   c. `dlciappliance_main.log` ファイルをダウンロードし、次のメッセージを検索して復元に成功したかどうかを確認します。

   ```
   Successfully restored OMIMSSC Appliance
   ```

古い OMIMSSC アプライアンスの復元が終了したら、次の手順を実行します。

- 古い OMIMSSC アプライアンスの復元後、スケジュール ジョブを作成し直すことをお勧めします。
- 以前のバージョンの OMIMSSC からエクスポートしたハイパーバイザー プロフィールの場合は、そのプロフィールを編集してから、ISO ファイル パスと Windows 認定資格プロフィールを指定するようにしてください。

9

OMIMSSC のアンインストール

OMIMSSC をアンインストールするには、次の手順を実行します。

1. OMIMSSC 管理ポータルから、OMIMSSC コンソールの登録を解除します。詳細については、「OMIMSSC コンソールの登録解除」を参照してください。
2. 登録されている Microsoft コンソールの OMIMSSC コンソール拡張機能をアンインストールします。詳細については、「SCCM 用 OMIMSSC コンソール拡張機能のアンインストール」または「SCVMM 用 OMIMSSC コンソール拡張機能のアンインストール」を参照してください。
3. OMIMSSC アプライアンス VM を削除します。詳細については、「OMIMSSC アプライアンス VM の削除」を参照してください。
4. アプライアンス固有のアカウントを削除します。詳細については、「その他のインストールタスク」を参照してください。

トピック：

- OMIMSSC からの Microsoft コンソールの登録解除
- SCCM 用 OMIMSSC コンソール拡張機能のアンインストール
- SCVMM 用 OMIMSSC コンソール拡張機能のアンインストール
- その他のアンインストール手順
- アプライアンス VM の削除

OMIMSSC からの Microsoft コンソールの登録解除

1 台の OMIMSSC アプライアンスに Microsoft コンソールを複数登録している場合は、コンソール登録を 1 つ解除しても OMIMSSC での操作を継続できます。完全なアンインストールについては、『*OpenManage Integration for Microsoft System Center Installation Guide*』(Microsoft System Center 用 OpenManage Integration インストールガイド) を参照してください。

Microsoft コンソールの登録を解除するには、次の手順を実行します。

1. OMIMSSC で **コンソール登録** をクリックします。
   OMIMSSC アプライアンスに登録されているすべてのコンソールが表示されます。
2. コンソールを選択し、[**登録解除**] をクリックして、アプライアンスへのコンソールの登録を削除します。
3. コンソール プラグインをアンインストールします。

   メモ:
   - コンソールを登録解除してアンインストールすると、コンソールに関連付けられていたホスト サーバーは OMIMSSC の未割り当てサーバー リストに移動します。

4. (オプション) コンソールにアクセスできない場合、コンソールを強制的に登録解除するプロンプトが表示されたら、**はい** をクリックします。
   - 登録解除時に OMIMSSC コンソールがすでに開いている場合は、Microsoft コンソールを閉じてから登録を解除するようにしてください。
   - SCVMM ユーザーの場合：
     - SCVMM サーバにアクセスできない場合に、SCVMM コンソールを OMIMSSC から強制的に登録解除するには、SCVMM で **アプリケーションプロファイル** を手動で削除してください。

SCCM 用 OMIMSSC コンソール拡張機能のアンインストール

`OMIMSSC_SCCM_Console_Extension.exe` をダブルクリックし、[**削除**] を選択して画面の指示に従います。

SCVMM 用 OMIMSSC コンソール拡張機能のアンインストール

SCVMM 用 OMIMSSC コンソール拡張機能をアンインストールするには、次の手順を実行します。

1. **プログラムのアンインストール** からコンソール拡張機能を削除します。
2. SCVMM コンソールからコンソール拡張機能を削除します。

SCVMM 用 OMIMSSC コンソール拡張機能の削除

1. **コントロール パネル** で **プログラム** をクリックし、**プログラムのアンインストール** をクリックします。
2. **SCVMM 用 コンソール アドイン** を選択し、**アンインストール** をクリックします。

SCVMM での OMIMSSC コンソール拡張機能の削除

1. SCVMM コンソールで **設定** をクリックします。
2. **OMIMSSC** を右クリックして、**削除** を選択します。

その他のアンインストール手順

OMIMSSC コンソール拡張機能を SCVMM から削除するには、次のアカウントとプロファイルを削除します。

- アプライアンス固有の RunAsAccounts
- OMIMSSC アプリケーション プロファイル

アプライアンス固有の RunAsAccounts の削除

アプライアンス固有の RunAsAccounts を SCVMM コンソールから削除するには、次の手順を実行します。

1. SCVMM コンソールで [**設定**] をクリックします。
2. **RunAsAccounts** をクリックします。
3. アカウントのリストから、アプライアンス固有のアカウントを削除します。
   アプライアンス固有のアカウントには、先頭に「`Dell_`」が付加されています。

OMIMSSC アプリケーション プロファイルの削除

1. SCVMM コンソールで、[**ライブラリー**]、[**プロファイル**] の順にクリックして、[**アプリケーション プロファイル**] をクリックします。
   SCVMM で使用されているすべてのアプリケーション プロファイルが表示されます。
2. **OMIMSSC Registration Profile** を選択して、削除します。

アプライアンス VM の削除

アプライアンス VM を削除するには、次の手順を実行します。

1. **Windows Server** の **Hyper-V マネージャー** でアプライアンス VM を右クリックし、**オフにする** をクリックします。
2. アプライアンス VM を右クリックし、**削除** をクリックします。

10

SCVMM 用 OMIMSSC のアップグレード

OMIMSSC のインストールおよび設定後、利用できるサービス パックのアップデートがある場合は、OMIMSSC の Service Pack Update 機能を使用して最新のアップデートをインストールできます。

メモ: 旧バージョンの OMIMSSC から OMIMSSC v7.2 または v7.2.1 へのサービス パック アップグレードは利用できません。

OMIMSSC の旧バージョンからアップグレードするには、現在のバージョンのデータをバックアップし、OMIMSSC バージョン 7.2 または 7.2.1 アプライアンスで復元します。

OMIMSSC アプライアンスのバックアップと復元の詳細については、「OMIMSSC アプライアンスのバックアップ」セクションおよび「OMIMSSC アプライアンスの復元」セクションを参照してください。

トピック：

- Service Pack のアップデートについて
- SCCM 用 OMIMSSC コンソール拡張機能のアップグレード
- SCVMM 用 OMIMSSC コンソール拡張機能のアップグレード

Service Pack のアップデートについて

OMIMSSC のリリース以後、既存の OMIMSSC アプライアンスに対するアップグレードまたは拡張機能として使用可能な、重要な欠陥の修正または機能の追加を共有する必要があります。Service Pack と OMIMSSC アプライアンスオペレーティングシステムおよび OMIMSSC に対するその他のアップデートのアップデートを行うことができます。

- Service Pack ファイルは、任意の HTTP サーバーに配置して、Service Pack のファイルを使用してアップデートを行なうことができます。
- これらの Service Pack を段階的に適用することができます。ただし、一度適用した後に元に戻すことはできません。
- この Service Pack は累積的です。つまり、最新の Service Pack では以前のすべてのリリースからの修正が含まれています。

OMIMSSC による Service Pack には、次の 2 つのタイプがあります。

- OMIMSSC アプライアンス Service Pack
- インフラストラクチャ Service Pack

サービス パック アップデートは、次の 2 つの方法で適用できます。

- オフライン パッケージを使用。
- ***linux.dell.com を使用。***

オフライン パッケージを使用して Service Pack アップデートを適用するには、次の手順を実行します。

1. ウェブから Service Pack をダウンロードします。詳細については、「」を参照してください。ウェブからの OMIMSSC のダウンロード
2. Service Pack アップデートの前提条件のリストを確認します。詳細については、「サービス パックのアップグレード手順」を参照してください。
3. ダウンロードした Service Pack アップデートをリポジトリにコピーします。詳細については、「Service Pack アップデートのリポジトリへのコピー」を参照してください。
4. OMIMSSC 管理ポータルで、リポジトリの URL 情報を入力します。詳細については、「リポジトリの URL 情報の入力」を参照してください。
5. Service Pack アップデートをインストールします。詳細については、「Service Pack アップデートのインストール」を参照してください。

オンライン パッケージを使用してサービス パック アップデートを適用するには、次の手順を実行します。

1. OMIMSSC 管理ポータルで、リポジトリの URL 情報を入力します。詳細については、「リポジトリの URL 情報の入力」を参照してください。
2. Service Pack アップデートをインストールします。詳細については、「Service Pack アップデートのインストール」を参照してください。

インストールの必要条件

- SCCM および SCVMM 向け OMIMSSC バージョン 7.2.1 にアップグレードする前に、SCCM および SCVMM 向け OMIMSSC バージョン 7.1 またはバージョン 7.1.1 またはバージョン 7.2 が導入されていることを確認します
- 実行中のジョブがないことを確認します。実行中の場合は、そのジョブが完了するまで待ちます。
- OMIMSSC アプライアンス データをバックアップします。

メモ: バックアップ手順の詳細については、「**OMIMSSC アプライアンスのバックアップ**」セクションを参照してください。

Service Pack のアップグレード手順

OMIMSSC を旧バージョンからアップグレードするには、現在のバージョンのデータをバックアップしてから、サービス パックを使用してアップデートします。

1. OMIMSSC 管理ポータルで、[**設定**] > [**Service Pack アップデート**] をクリックします。
2. [**リポジトリー URL**] ボックスに、次のアップデート方法のどちらを使用するかに応じて、Service Pack リポジトリーの場所の URL を入力します。
   a. オフライン パッケージを使用してアップデートするには、[**リポジトリー URL**] ボックスに、サービス パックが保存されている場所の URL 情報を「http://<ホスト名または IP アドレス>/OMIMSSC_v7.2_SP/RPM_Repository」の形式で入力します。
   b. linux.dell.com を使用してアップデートするには、[**リポジトリー URL**] ボックスに、URL 情報を「http://linux.dell.com/repo/omimssc-sccm-scvmm/<サービス パック バージョン>」の形式で入力し、必要に応じてプロキシ サーバーの詳細情報とプロキシ サーバーにアクセスするための認証情報を入力して、[**保存**] をクリックします。
3. [**アップデートを自動的にチェック**] チェック ボックスを選択します現在のバージョンの OMIMSSC および Service Pack が表示されます。
4. [**適用**]、[**OK**] の順にクリックします。
5. upgradelogs ディレクトリーで、[**設定**] > [**ログ**] の順に移動します。サービス パック アップグレードのログ ファイルを表示またはダウンロードするには、<サービス パック バージョン番号>ディレクトリー (たとえば、<フォルダー名>ディレクトリー) を選択して、サービス パック アップグレードのログ ファイルを表示またはダウンロードします。
6. **管理ポータル** にログインして、ブラウザー キャッシュの履歴を削除します。
7. Service Pack のアップデートが完了したら、アプライアンスを手動で再起動します。

Service Pack アップデート リポジトリー作成の詳細については、「Service Pack のアップデートについて」セクションを参照してください。

Service Pack アップデートのリポジトリへのコピー

- ダウンロードした Service Pack をリポジトリに保存します。
- サーバパックのすべてのファイル形式が HTTP サーバでサポートされていることを確認してください。サポートされていない場合は、HTTP 管理者に問い合わせてサポートを追加してください。次のファイル形式がサポートされています。
  - .RPM
  - .XML
  - .TXT
  - .BZ2

.BZ2 ファイル形式を有効にするには、次の手順を実行します。

1. repo ファイルが保存されているサーバーで、IIS マネージャを開きます。
2. ホスト名を展開します。**サイト**、**デフォルト Web サイト** の順にクリックします。
3. **アクション** ペインで、**追加**をクリックします。
   [MIME タイプを追加] ウィンドウが表示されます。
4. **ファイル名の拡張子** に **.BZ2** を、**MIME タイプ** に **APP/BZ2** を設定して、**OK** をクリックします。

リポジトリの準備

1. サービスパックファイルを直接 HTTP サーバーに配置します。
2. ダウンロードした Service Pack をダブルクリックして、指定した場所にファイルを解凍します。
3. HTTP サイトに解凍したファイルをコピーします。

Service Pack アップデートのためのリポジトリ URL 情報の入力

OMIMSSC をアップデートするには、Service Pack アップデートがある URL 情報を入力します。

Service Pack アップデートを使用して OMIMSSC を更新するには、次の手順を実行します。

1. **OMIMSSC** で、**設定 Service Pack アップデート** を選択します。
2. オフライン パッケージを使用してアップデートするには、[**リポジトリー URL**] に、「`http://<サーバー名>:<ポート名>/<リポジトリー パス>`」形式で URL 情報を入力し、必要に応じてプロキシー サーバーの詳細情報とサーバーにアクセスするための認証情報を入力して、[**保存**] をクリックします。

   メモ: URL 内に入力するホスト名にはアンダースコア (_) が含まれないように注意してください。

   linux.dell.com を使用してアップデートするには、[**リポジトリー URL**] に、「`http://linux.dell.com/repo/omimssc-sccm-scvmm/<Service Pack バージョン>`」形式で URL 情報を入力し、必要に応じてプロキシー サーバーの詳細情報とサーバーにアクセスするための認証情報を入力して、[**保存**] をクリックします。

Service Pack アップデートのインストール

リポジトリの URL 情報が使用可能であり、**Service Pack アップデート** ページに含まれていることを確認します。詳細に関しては、「リポジトリ URL 情報の入力」を参照してください。

Service Pack アップデートをインストールするには、次の手順を実行します。

1. Service Pack が HTTP サイトに置かれたら、**OMIMSSC 管理ポータル** > **設定** > **Service Pack アップデート** の順に移動して、[**アップデートのチェック**] をクリックします。

   OMIMSSC の場合は、既存のバージョンとリポジトリで使用可能な Service Pack バージョンが表示されます。

   必要に応じて、リリースノートを表示することができます。
2. **適用**、**OK** の順にクリックします。
3. アップグレードアクティビティが完了したら、OMIMSSC 管理ポータルにログインし、次にブラウザのキャッシュ履歴をクリアします。

インストール後の手順：

Service Pack のアップデートを確認するには、次の手順を実行します。

1. OMIMSSC 管理ポータルの **バージョン情報** に、Service Pack アップデートのバージョンの詳細が表示されます。
2. 詳細については、OMIMSSC 管理ポータルで **設定** > **ログ** を選択します。
3. **upgradelogs** ディレクトリで Service Pack アップグレードのログファイルを表示またはダウンロードするには、**<Service Pack バージョン番号>** ディレクトリ (たとえば 1.2.0.207 ディレクトリ) を選択して表示するか、Service Pack アップグレードのログファイルをダウンロードします。
4. Service Pack アップデートに失敗した場合は、**dell.com/support** にお問い合わせください。
5. アプライアンスを手動で再起動します。

   メモ: Service Pack のアップデートが完了したら、次の操作を行います。
   - SCCM 用 OMIMSSC コンソール拡張機能のアップグレード
   - SCVMM 用 OMIMSSC コンソール拡張機能のアップグレード

SCCM 用 OMIMSSC コンソール拡張機能のアップグレード

古い OMIMSSC アプライアンスをバックアップしてあることを確認してください。詳細については、「OMIMSSC アプライアンスのバックアップ」を参照してください。

1. OMIMSSC 管理ポータルで、**インストールツールのダウンロード** をクリックして、インストールツールを任意の場所に保存します。
2. OMIMSSC インストールツールを実行します。
3. アップグレードを求めるメッセージで、**はい** をクリックします。
4. OMIMSSC の ようこそ ページで、**次へ** をクリックします。
5. **ライセンス契約** ページで、**ライセンス契約の条件に同意します** を選択し、**次へ** をクリックします。
6. **プログラムインストールの準備完了** ページで、**インストール** をクリックします。
7. **InstallShield ウィザードの完了** ページで、**終了** をクリックし、インストールを完了します。

SCVMM 用 OMIMSSC コンソール拡張機能のアップグレード

古い OMIMSSC アプライアンスをバックアップしてあることを確認してください。詳細については、「OMIMSSC アプライアンスのバックアップ」を参照してください。

1. OMIMSSC 管理ポータルで、**インストールツールのダウンロード** をクリックして、インストールツールを任意の場所に保存します。
2. OMIMSSC インストールツールを実行します。
3. アップグレードを求めるメッセージで、**はい** をクリックします。
4. OMIMSSC の ようこそ ページで、**次へ** をクリックします。
5. **ライセンス契約** ページで、**ライセンス契約の条件に同意します** を選択し、**次へ** をクリックします。
6. **プログラムインストールの準備完了** ページで、**インストール** をクリックします。
7. **InstallShield ウィザードの完了** ページで、**終了** をクリックし、インストールを完了します。
8. SCVMM 用 OMIMSSC コンソール拡張機能を削除して、再度インポートします。コンソールの削除の詳細については、「SCVMM 用 OMIMSSC コンソール拡張機能の削除」を参照してください。

11

OMIMSSC アプライアンスの再起動

OMIMSSC アプライアンスを再起動するには、次の手順を実行します。

1. OMIMSSC アプライアンス VM を起動して、ログインします。
2. **この仮想アプライアンスを再起動** に移動して、**Enter** キーを押します。
3. 確定するには、**はい** をクリックします。
   OMIMSSC アプライアンスと必要なすべてのサービスが再起動されます。
4. VM の再起動後、OMIMSSC アプライアンスにログインします。

12

OMIMSSC アプライアンスからのログアウト

1. OMIMSSC アプライアンス VM を起動して、ログインします。
2. **ログアウト**に移動して、**Enter** キーを押します。

13

プロファイルの管理

プロファイルには、OMIMSSC での操作を実行するために必要なすべてのデータが含まれています。

トピック：

- 資格情報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ついて（SCVMM ユーザー用）

資格情報プロファイルについて

資格情報プロファイルは、ユーザーの役割ベースの機能を認証することにより、ユーザー資格情報の使用と管理を簡素化します。各資格情報プロファイルには、単一ユーザーアカウントのユーザー名とパスワードが含まれています。

OMIMSSC は、資格情報プロファイルを使用して管理下システムの iDRAC に接続します。また、資格情報プロファイルは、FTP サイトや Windows 共有で使用可能なリソースへのアクセスに使用したり、iDRAC のさまざまな機能を操作する際に使用することができます。

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

- デバイス資格情報プロファイル - iDRAC または CMC へのログインに使用されます。また、サーバの検出、同期問題の解決、およびオペレーティングシステムの導入のために、このプロファイルを使用できます。このプロファイルは、コンソールに固有です。このプロファイルは、プロファイルが作成されたコンソールでのみ使用および管理できます。
- Windows 資格情報プロファイル - Windows オペレーティングシステムの共有フォルダにアクセスするために使用されます。
- FTP 資格情報プロファイル - 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 - アップデート用の FTP サイトにアクセスするためのプロキシ資格情報を提供するため使用されます。

  メモ: デバイスプロファイル以外のすべてのプロファイルは共有リソースです。これらのプロファイルは、登録されている任意のコンソールから使用および管理できます。

事前定義された資格情報プロファイル

システムデフォルト FTP アカウントは、OMIMSSC で使用可能な事前定義された資格情報プロファイルです。事前定義された資格情報プロファイルのタイプは FTP で、**ユーザー名** と **パスワード** は **匿名** です。このプロファイルを使用すると `ftp.dell.com` にアクセスできます。

認定資格プロフィールの作成

認定資格プロフィールを作成する場合は、次の点に注意してください。

- 自動検出中に iDRAC に対してデフォルトの認定資格プロフィールを使用できない場合は、デフォルトの iDRAC 資格情報が使用されます。デフォルト iDRAC のユーザー名は `root` で、パスワードは `calvin` です。
- モジュラー型システムに関する情報を取得するには、デフォルトの CMC プロファイルを使用してモジュラー型サーバーにアクセスします。デフォルト CMC プロファイルのユーザー名は `root` で、パスワードは `calvin` です。
- （SCVMM ユーザーの場合のみ）デバイス タイプの認定資格プロフィールが作成されると、サーバー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。
- SCVMM 内で **RunAsAccount** を編集または削除しないでください。

1. OMIMSSC で、次のいずれかの手順を実行して [**認定資格プロフィール**] を作成します。
   - OMIMSSC ダッシュボードで、[**認定資格プロフィールの作成**] をクリックします。
   - ナビゲーション ペインで、**[プロファイル]** > **[認定資格プロフィール]** の順にクリックして、[**作成**] をクリックします。

2. [**資格情報タイプ**] で、使用する認定資格プロフィールのタイプを選択します。
3. プロファイル名および説明を指定します。

   メモ: [**デフォルト プロファイル**] オプションは、デバイス タイプの認定資格プロフィールにのみ適用できます。

4. **資格情報** で、ユーザー名とパスワードを指定します。
   - **デバイス認定資格プロフィール**を作成している場合は、[**デフォルト プロファイル**] オプションを選択し、iDRAC または CMC にログインするデフォルト プロファイルとしてこのプロファイルを選択します。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、**なし** を選択します。
   - **Windows 認定資格プロフィール**を作成している場合は、[**ドメイン**] にドメインの詳細を指定します。

     メモ: コンソールの登録用の認定資格プロフィールを作成しているときに、NETBIOS 名が Active Directory (AD) で設定されている場合は、その NETBIOS 名をドメインとして入力します。NETBIOS 名が AD で設定されていない場合は、ドメイン名にトップ レベル ドメイン (TLD) の詳細情報を入力します。

     たとえば、ドメイン名が `mydomain` で、TLD が `com` の場合、認定資格プロフィールに次のようにドメイン名を指定します : `mydomain.com`
   - **プロキシサーバの資格情報** を作成している場合、**プロキシサーバの URL** にプロキシサーバの URL を `http://hostname:port` または `http://IPaddress:port` の形式で指定します。
5. プロファイルを作成するには、**終了** をクリックします。

メモ: SCVMM でデバイス タイプの認定資格プロフィールを作成すると、対応する **RunAsAccount** が作成されます。この名前は、**Dell_** で始まります。登録済みユーザーが、作成されたデバイス認定資格プロフィールを使用するオペレーティング システムの導入などの操作に対して、対応する **RunAsAccount** へのアクセス権を持っていることを確認します。

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前に、次の点に注意してください。

- 作成後は、資格情報プロファイルのタイプを変更できません。ただし、他のフィールドは変更できます。
- 資格情報プロファイルが使用中の場合は変更できません。

メモ: 資格情報プロファイルのタイプを変更する手順は同じです。

1. 変更する資格情報プロファイルを選択し、**編集** をクリックして、プロファイルをアップデートします。
2. 変更を保存するには、**保存** をクリックします。

変更内容を表示するには、**資格情報プロファイル** ページを更新します。

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、それに対応する資格情報プロファイルが OMIMSSC で使用不可となります。
- サーバの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、検出されたサーバ情報を削除してから、資格情報プロファイルを削除します。
- 導入に使用されるデバイスタイプ資格情報プロファイルを削除するには、最初に、SCVMM 環境に導入されたサーバを削除し、その後に資格情報プロファイルを削除します。
- アップデートソースで使用されている資格情報プロファイルを削除することはできません。

メモ: 資格情報プロファイルのタイプを削除する手順は同じです。

削除するプロファイルを選択し、**削除** をクリックします。

変更内容を表示するには、**資格情報プロファイル** ページを更新します。

ハイパーバイザープロファイルについて（SCVMM ユーザー用）

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（ハイパーバイザーの導入には WinPE ISO が使用されます）、SCVMM から取得したホストグループ、およびインジェクションのための LC ドライバが含まれます。ハイパーバイザープロファイを作成および管理できるのは、SCVMM ユーザー向けの OMIMSSC コンソール拡張機能だけです。

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ハイパーバイザーを導入します。

- WinPE ISO イメージをアップデートし、イメージが保存されている共有フォルダにアクセスできるようにします。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が作成されます。SCVMM でのホストグループの作成については、Microsoft のマニュアルを参照してください。

1. OMIMSSC で、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、**ハイパーバイザープロファイルの作成** をクリックします。
   - 左側のナビゲーションペインで、**プロファイルとテンプレート** をクリックし、**ハイパーバイザープロファイル** をクリックして、**作成** をクリックします。

   ハイパーバイザープロファイルウィザード が表示されます。
2. **ようこそ** ページで、**次へ** をクリックします。
3. **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、**次へ** をクリックします。
4. **SCVMM 情報** ページで、
   a. **SCVMM ホストグループの宛先** については、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て、ホストをこのグループに追加します。
   b. **SCVMM ホストプロファイル/物理コンピュータプロファイル** から、サーバに適用する設定情報を含む SCVMM から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選択します。

      SCVMM で、**物理コンピュータプロファイル** で次のいずれかのディスクパーティション方法を選択します。
      - UEFI モードで起動する場合は、**GUID パーティションテーブル（GPT）** オプションを選択します。
      - BIOS モードで起動する場合は、**マスターボードレコード（MBR）** オプションを選択します。
5. **WinPE 起動イメージソース** で、次の詳細を入力し、**次へ** をクリックします。
   a. **ネットワーク WinPE ISO 名** には、アップデートされた WinPE ファイル名を持つ共有フォルダパスを指定します。WinPE ファイル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。
   b. **資格情報プロファイル** では、WinPE ファイルを持つ共有フォルダへのアクセス権を持つ資格情報を選択します。
   c. （オプション）Windows 資格情報プロファイルを作成するには、**新規作成** をクリックします。資格情報プロファイルの作成の詳細については、「資格情報プロファイルの作成」を参照してください。
6. （オプション）LC ドライバインジェクションを有効にするには、次の手順を実行します。

   メモ: NIC カードの最新のオペレーティングシステムドライバパックは最新のオペレーティングシステムドライバで利用できるため、**Dell Lifecycle Controller ドライバインジェクションを有効にする** チェックボックスを必ず選択してください。

   a. 適切なドライバが選択されるように、導入するオペレーティングシステムを選択します。
   b. **LC ドライバインジェクションを有効にする** を選択します。
   c. ハイパーバイザーのバージョンを **ハイパーバイザーのバージョン** で選択します。
7. **概要** で **終了** をクリックします。

変更内容を表示するには、**ハイパーバイザープロファイル** ページを更新します。

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 名を変更できます。ただし、ISO イメージは変更できません。

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. 詳細を入力し、**終了** をクリックします。

変更内容を表示するには、**ハイパーバイザープロファイル** ページを更新します。

ハイパーバイザープロファイルの削除

削除するハイパーバイザープロファイルを選択し、**削除** をクリックします。

変更内容を表示するには、**ハイパーバイザープロファイル** ページを更新します。

14

デバイスの検出および MSSC コンソールとサーバの同期

検出とは、サポートされているモジュラーシステム、および PowerEdge ベアメタルサーバ、ホストサーバ、またはノードを OMIMSSC に追加するプロセスです。

MSSC コンソールとの同期とは、登録された Microsoft コンソール（SCCM または SCVMM）から OMIMSSC にホストサーバを追加するプロセスです。したがって、どちらかのプロセスを使用すると、OMIMSSC にデバイスを追加できます。デバイスが検出された後にのみ、OMIMSSC でデバイスを管理できます。

トピック：

- デバイスの検出： OMIMSSC
- OMIMSSC コンソール拡張機能と登録された SCCM との同期
- 同期エラーの解決
- システムロックダウンモードの表示
- OMIMSSC からのサーバの削除

デバイスの検出： OMIMSSC

OMIMSSC で、MX7000 モジュラー型システム、ホスト、および未割り当てサーバーを検出します。検出されたデバイスに関する情報は、OMIMSSC アプライアンスに保存されます。

次の方法を使用して、iDRAC IP アドレスを使用して Dell EMC サーバを検出できます。

- 自動検出を使用したサーバーの検出
- 手動検出を使用したサーバーの検出

メモ: 検出されたデバイスは、OMIMSSC と連携するために必要な対応バージョンの LC ファームウェア、iDRAC、および BIOS が含まれている場合、ハードウェア互換性ありとマークされます。対応バージョンの詳細については、『*Microsoft System Center 向け OpenManage Integration リリース ノート*』を参照してください。

手動検出を使用してモジュラー型システムを検出する方法で、デバイスの IP アドレスを使用してモジュラー型システムを検出します。

SCCM 用の OMIMSSC コンソール拡張機能でのデバイス検出

SCCM 用の OMIMSSC コンソール拡張機能でデバイスを検出します。サーバーを検出した後、そのサーバーは OMIMSSC の事前定義されたグループ、ならびに SCCM の事前定義されたグループまたはコレクション（[**デバイス コレクション**] の下に作成された [**すべての Dell Lifecycle Controller サーバー コレクション**] および [**Dell サーバーのインポート 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 SCCM に事前定義されたグループまたはコレクションが存在しない場合は、事前定義されたコレクションが作成され、検出されたサーバがそれぞれのグループに追加されます。

SCVMM 用の OMIMSSC コンソール拡張機能でのデバイス検出

SCVMM 用の OMIMSSC コンソール拡張機能で、モジュラー型システム、Hyper-V ホスト、および未割り当てサーバーを検出します。検出した後、デバイスは事前定義された各アップデートグループに追加されます。

管理対象システムのシステム要件

管理対象システムは、OMIMSSC を使用して管理されるデバイスです。OMIMSSC のコンソール拡張機能を使用してサーバーを検出するためのシステム要件は、次のとおりです。

- OMIMSSC の SCCM 用コンソール拡張機能は、第 12 世代以降のサーバーでモジュラー型、モノリス型、およびタワー型のサーバー モデルをサポートします。
- OMIMSSC の SCVMM 用コンソール拡張機能は、第 12 世代以降のサーバーでモジュラー型およびモノリス型のサーバー モデルをサポートします。
- ソース設定と宛先設定では、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。
- Collect System Inventory on Restart (CSIOR) を有効にします。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

サーバを自動的に検出するには、サーバをネットワークに接続してサーバの電源をオンにします。OMIMSSC は、iDRAC のリモート有効化機能を使用して未割り当てのサーバを自動的に検出します。OMIMSSC はプロビジョニングサーバとして機能し、iDRAC リファレンスを使用してサーバを自動検出します。

1. OMIMSSC では、iDRAC 資格情報を提供してデバイスタイプの資格情報プロファイルを作成し、それをサーバのデフォルトとして設定します。資格情報プロファイル作成するの詳細については、「資格情報プロファイルの作成」を参照してください。
2. 管理対象デバイスの iDRAC 設定で、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 iDRAC にログインするために、オペレータ権限を持つゲストユーザーアカウントを用意することをお勧めします。

3. 管理対象デバイスの iDRAC 設定で、自動検出機能を有効にします。詳細については、iDRAC のマニュアルを参照してください。
4. 管理対象デバイスの iDRAC 設定で、**プロビジョニングサーバの IP** に OMIMSSC アプライアンス IP を指定し、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するには、次の手順に従います。サーバを検出するには、サーバの iDRAC IP アドレスとデバイスタイプ資格情報を入力します。IP 範囲を使用してサーバを検出する場合は、サブネット内の IP (IPv4) 範囲を指定してサーバの範囲の開始と終了、およびデバイスタイプ資格情報を含めます。

デフォルトの認定資格プロフィールが使用可能であることを確認します。

1. OMIMSSC コンソールで、次のいずれかの手順を実行します。
   - ダッシュボードで、**サーバを検出** をクリックします。
   - ナビゲーション ペインで、**設定と導入** をクリックし、**サーバビュー** をクリックして、**検出** をクリックします。
2. **検出** ページで、次の中から必要なオプションを選択します。
   - **IP アドレスを使用した検出** - IP アドレスを使用してサーバを検出します。
   - **IP 範囲を使用した検出** - IP 範囲内のすべてのサーバを検出します。
3. デバイス タイプ認定資格プロフィールを選択するか、[**新規作成**] をクリックしてデバイス タイプ認定資格プロフィールを作成します。

   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. **iDRAC IP アドレス** で、検出するサーバの IP アドレスを入力します。
5. **IP アドレスまたは IP アドレスの範囲を使用した検出** で、次のいずれかを実行します。
   - **IP アドレスの開始範囲** と **IP アドレスの終了範囲** には、含める IP アドレス範囲を指定します。これは開始範囲と終了範囲です。

- IP アドレス範囲を除外する場合は、**除外範囲の有効化** を選択して、**IP アドレスの開始範囲** と **IP アドレスの終了範囲** で除外する範囲を指定します。

6. 固有のジョブ名、ジョブの説明を入力し、**終了** をクリックします。

   このジョブを追跡するには、デフォルトで **ジョブリストへ移動** オプションが選択されています。

   ジョブとログセンター ページが表示されます。検出ジョブを展開して、**実行中** タブでジョブの進行状況を表示します。

サーバが検出されると、そのサーバは **設定と導入** セクションの **サーバビュー** ページにある **ホスト** タブまたは **未割り当て** タブに追加されます。

- オペレーティングシステムが導入済みのサーバを検出し、そのサーバが SCCM または SCVMM コンソールにすでに存在している場合、そのサーバは **ホスト** タブにホストサーバとして表示されます。
- SCCM または SCVMM にリストされていない PowerEdge サーバーを検出した場合、そのサーバーはすべての OMIMSSC コンソール拡張機能の [**未割り当て**] タブに未割り当てサーバーとして表示されます (複数の Microsoft コンソールが単一の OMIMSSC アプライアンスに登録されている場合) 。

サーバーを検出し、そのサーバーに OMIMSSC と連携するための対応バージョンの LC ファームウェア、iDRAC、および BIOS が含まれている場合、そのサーバーはハードウェア互換性ありとマークされます。サーバコンポーネントのファームウェアバージョンを表示するには、サーバ行の **ハードウェア互換性** 列にマウスを合わせます。対応バージョンの詳細については、『*Microsoft System Center 向け OpenManage Integration リリース ノート*』を参照してください。

ライセンスは、検出されたサーバごとに使用されます。**ライセンスセンター** ページの **ライセンスされたノード** は、サーバが検出されると減少します。

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ーを操作するには、それらのサーバーを再検出してください。

メモ: OMIMSSC に委任管理者としてログインすると、ログインしたユーザー固有のものではない、すべてのホスト サーバーおよび未割り当てサーバーを表示できます。したがって、このようなサーバでは操作を実行できません。このようなサーバで操作を実行する前に、必要な権限があることを確認してください。

手動検出を使用した MX7000 の検出

IP アドレスまたは IP 範囲を使用して PowerEdge MX7000 モジュラーシステムを手動で検出するには、モジュラーシステムの IP アドレスとデバイスタイプの認証情報を入力します。IP 範囲を使用してモジュラーシステムを検出する場合は、サブネット内の IP (IPv4) 範囲を指定してモジュラーシステムの範囲の開始と終了、およびデバイスタイプの認証情報を含めます。

検出するモジュラーシステムのデフォルトの資格情報プロファイルが使用可能であることを確認します。

モジュラーシステムを検出するには、次の手順を実行します。

1. OMIMSSC で、**設定と導入** をクリックし、**モジュラーシステムビュー** をクリックして、**検出** をクリックします。
2. **検出** ページで、次の中から必要なオプションを選択します。
   - **IP アドレスを使用した検出** - IP アドレスを使用してモジュラーシステムを検出します。
   - **IP 範囲を使用した検出** - IP 範囲内のすべてのモジュラーシステムを検出します。
3. デバイスタイプ資格情報プロファイルを選択するか、**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. **IP アドレス** で、検出するモジュラーシステムの IP アドレスを指定します。
5. **IP アドレスまたは IP アドレスの範囲を使用した検出** で、次のいずれかを実行します。
   - **IP アドレスの開始範囲** と **IP アドレスの終了範囲** には、含める IP アドレス範囲を指定します。これは開始範囲と終了範囲です。
   - IP アドレス範囲を除外する場合は、**除外範囲の有効化** を選択して、**IP アドレスの開始範囲** と **IP アドレスの終了範囲** で除外する範囲を指定します。
6. **モジュラーシステム検出メソッド** で、次のいずれかを選択します。
   - **簡易検出** - モジュラーシステムおよびモジュラーシステム内のサーバ数を検出します。
   - **詳細検出** - 入出力モジュール (IOM) やストレージデバイスなど、モジュラーシステム内に存在するモジュラーシステムおよびデバイスを検出します。

     メモ: MX7000 とそのコンポーネントを詳細に検出するには、PowerEdge MX7000 とそのすべてのコンポーネントで IPv4 アドレスが有効になっていることを確認します。
7. 固有のジョブ名を入力し、**終了** をクリックします。

このジョブを追跡するには、デフォルトで **ジョブリストへ移動** オプションが選択されています。

実行 タブでジョブの進行状況を表示するには、**ジョブとログセンター** で検出ジョブを展開します。

OMIMSSC コンソール拡張機能と登録された SCCM との同期

すべてのサーバ (ホストおよび未割り当て) を登録された SCCM から OMIMSSC と同期できます。また、同期後に、サーバに関する最新のファームウェアインベントリ情報を取得します。

OMIMSSC と登録されている SCCM コンソールを同期する前に、次の要件が満たされていることを確認します。

- サーバのデフォルト iDRAC 資格情報プロファイルの詳細を取得します。
- OMIMSSC を SCCM と同期させる前に、**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、割り当てられていないサーバが SCCM で検出された場合、そのサーバは **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 デフォルトコレクション** に追加するには、**OOB** ページでサーバの iDRAC IP アドレスを追加します。
- SCCM にデバイスの重複エントリがないことを確認します。

OMIMSSC と SCCM を同期した後、デバイスが SCCM に存在しない場合は、**デバイスコレクション** の下に **すべての Dell Lifecycle Controller サーバ** コレクションと **Dell サーバのインポート** コレクションが作成され、それぞれのグループにサーバが追加されます。

OMIMSSC コンソール拡張機能と登録された SCVMM との同期

SCVMM コンソールから、すべての Hyper-V ホスト、Hyper-V ホストクラスタ、モジュラー Hyper-V ホスト、未割り当てサーバを、SCVMM 用の OMIMSSC コンソール拡張機能と同期できます。また、同期後に、サーバに関する最新のファームウェアインベントリ情報を取得します。

OMIMSSC を SCVMM と同期する前に、次の点に注意してください。

- サーバのデフォルト iDRAC 資格情報プロファイルの詳細を取得します。
- ホストサーバのベースボード管理コントローラ (BMC) が iDRAC IP アドレスで設定されていない場合、ホストサーバを OMIMSSC と同期できません。そのため、SCVMM で BMC を設定 (詳細については、`technet.microsoft.com` の MSDN の記事を参照) してから、OMIMSSC を SCVMM と同期します。
- SCVMM は環境内で多数のホストをサポートするため、同期の実行には長い時間がかかります。

登録された Microsoft コンソールとの同期

Microsoft コンソールで管理されているサーバを OMIMSSC に追加するには、次の手順を実行します。

OMIMSSC で、[**設定と導入**] をクリックし、[**サーバー ビュー**] をクリックして、[**OMIMSSC** との同期] をクリックし、登録した 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ともにリストされます。

メモ: 無効な資格情報、iDRAC IP アドレス、接続、またはその他の問題が原因で同期されていないすべてのサーバについては、先に問題を解決してから、同期してください。

メモ: 再同期中に、登録された MSSC 環境から削除されたホストサーバは、OMIMSSC コンソール拡張機能の **未割り当てサーバ** タブに移動されます。サーバが退避された場合は、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。

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

1. OMIMSSC で、**設定と導入** をクリックし、**サーバビュー** をクリックして、**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 **新規作成** をクリックします。
3. ジョブ名を入力し、必要に応じて **ジョブリストに移動** オプションを選択すると、ジョブが送信されると自動的にジョブのステータスが表示されます。

4. **終了** をクリックしてジョブを送信します。

システムロックダウンモードの表示

システムロックダウンモード設定は、第 14 世代以降のサーバの iDRAC で使用できます。この設定をオンにするとファームウェアアップデートなどのシステム構成がロックされます。システムロックダウンモードが有効になると、ユーザーは構成設定を変更できません。この設定は、システムが誤って変更されないようにするためのものです。管理対象サーバでいずれかの操作を実行するには、iDRAC コンソールで設定を無効にします。OMIMSSC コンソールでは、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 アドレスより前にロックイメージで表されます。

- その設定がシステムで有効になっている場合、ロックイメージはサーバの iDRAC IP とともに表示されます。
- その設定がシステムで無効になっている場合、ロックされないイメージがサーバの iDRAC IP とともに表示されます。

メモ: OMIMSSC コンソール拡張機能を起動する前に、管理対象サーバで iDRAC システムロックダウンモードの設定を確認します。

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。

OMIMSSC からのサーバの削除

サーバを削除するには、次の手順を実行します。

サーバを削除する前に、次の点を考慮してください。

- サーバを削除すると、使用済みライセンスは放棄されます。
- 次の基準に基づいて、OMIMSSC にリストされているサーバを削除できます。
  - **未割り当てサーバ** タブにリストされている未割り当てのサーバ。
  - 登録された SCCM または SCVMM でプロビジョニングされ、OMIMSSC の **ホスト** タブに存在するホストサーバを削除する場合は、SCCM または SCVMM でサーバを削除してから、OMIMSSC からサーバを削除します。

1. OMIMSSC コンソールで **設定と導入** をクリックし、**サーバビュー** をクリックします。
   - 未割り当てのサーバを削除するには、**未割り当てサーバ** タブでサーバを選択し、**削除** をクリックします。
   - ホストサーバを削除するには、**ホストサーバ** タブでサーバを選択し、**削除** をクリックします。
2. 確認 ダイアログボックスで、**はい** をクリックします。

OMIMSSC からのモジュラーシステムの削除

モジュラーシステムを削除するには、次の手順を実行します。

1. OMIMSSC コンソールで、**設定と導入** をクリックし、次に **モジュラーシステムビュー** をクリックします。
2. モジュラーシステムを選択して、**削除** をクリックします。

15

OMIMSSC のビュー

設定と導入 ページの OMIMSSC で検出されたすべてのデバイスと、そのハードウェアおよびファームウェアのインベントリ情報を表示します。また、**ジョブとログセンター** ページに、すべてのジョブとそのステータスも表示します。

トピック：

- サーバビューの起動
- モジュラー型システム ビューの起動
- クラスタビューの起動
- iDRAC コンソールの起動
- メンテナンスセンターの起動
- ジョブとログセンターの起動

サーバビューの起動

[**サーバー ビュー**] ページには、OMIMSSC の [**未割り当てサーバー**] タブと [**ホスト**] タブにあるすべての未割り当てサーバーとホスト サーバーが一覧表示されます。

[**未割り当てサーバー**] タブで、iDRAC の IP アドレス、サービス タグ、モデル、生成、プロセッサー速度、サーバーのメモリー、割り当てられた Operational Template (運用テンプレート) のテンプレート コンプライアンス ステータス、モジュラー型システムのサービス タグ (モジュラー型サーバーの場合)、ハードウェア互換性情報を表示します。**ハードウェア互換性** 列にカーソルを合わせると、デバイスの BIOS、iDRAC、LC、およびドライバパックのバージョンが表示されます。ハードウェアの互換性の詳細については、「ファームウェアのアップデートについて」を参照してください。

[**ホスト**] タブで、ホスト名、iDRAC Ip アドレス、サービス タグ、モデル、生成、プロセッサー速度、サーバーのメモリー、モジュラー型システムのサービス タグ (モジュラー型サーバーの場合)、サーバーがクラスターの一部である場合、完全修飾ドメイン名 (FQDN)、割り当てられた Operational Template (運用テンプレート) のコンプライアンス ステータス、ハードウェア互換性情報を表示します。**ハードウェア互換性** 列にカーソルを合わせると、デバイスの BIOS、iDRAC、LC、およびドライバパックのバージョンが表示されます。ハードウェアの互換性の詳細については、「ファームウェアのアップデートについて」を参照してください。

サーバビュー ページでは、次のタスクを実行できます。

- サーバーの検出
- ページを更新して、更新された情報を表示します。
- OMIMSSC からサーバーを削除します。
- 登録済みの Microsoft コンソールと同期します。
- 同期化エラーの解決。
- Operational Template (運用テンプレート) を割り当て、Operational Template (運用テンプレート) コンプライアンスを実行します。
- 運用テンプレートの導入
- サーバーが所属するクラスター グループとモジュラー型システムにサーバーを関連付けます。
- iDRAC コンソールの起動

サーバーを表示するには、次の手順を実行します。

1. OMIMSSC コンソール拡張機能で、[**設定と導入**] をクリックし、[**サーバー ビュー**] をクリックします。
2. ベアメタルサーバを表示するには、**未割り当てサーバ** タブをクリックします。
3. ホストサーバを表示するには、**ホスト** タブをクリックします。
   a. SCCM または SCVMM でグループ化されたホストグループをネストされた形式で表示するには、**コンソールホストの選択** ドロップダウンメニューをクリックします。

コンソールホストの選択 ドロップダウンメニューには、SCCM に存在するすべてのホストグループと内部グループ名が一覧表示されます。内部グループ名を選択すると、SCCM および OMIMSSC で検出および管理されるすべてのホストが表示されます。

サーバを検出したら、次の点を考慮します。

- サーバが検出されると、**運用テンプレート** の列に **未割り当て** と表示されます。ファームウェアをアップデートし、これらのサーバにオペレーティングシステムを導入するには、Operational Template (運用テンプレート) を割り当てて導入します。詳細は、「Operational Template (運用テンプレート) の管理」を参照してください。
- 検出されたサーバーは、OMIMSSC で事前定義されたグループに追加されます。機能要件に基づいて、カスタムアップデートグループを作成できます。詳細については、「アップデートグループについて」を参照してください。
- OMIMSSC に委任管理者としてログインすると、このユーザーに固有ではないすべてのホストおよび未割り当てサーバーを表示できます。したがって、サーバで操作を実行する前に、必要な権限があることを確認してください。
- OMIMSSC に複数の Microsoft コンソールが登録されている場合、ホスト サーバーは、それらが管理されている Microsoft コンソールに固有のものになります。また、未割り当てサーバはすべてのコンソールに共通です。

モジュラー型システム ビューの起動

[**モジュラー型システム ビュー**] ページには、OMIMSSC で検出されたすべてのモジュラー型システムが一覧表示されます。

CMC Ip アドレス、サービス タグ、モデル、ファームウェア バージョン、割り当てられた Operational Template (運用テンプレート) に対するモジュラー型システムのテンプレート コンプライアンス ステータス、サーバー数、入力/出力 (I/O) モジュール、およびそのモジュラー型システムに存在するストレージ デバイスを表示します。Operational Template (運用テンプレート) を導入して、ハードウェアを構成し、モジュラー型システム ファームウェアをアップデートします。

[**モジュラー型システム ビュー**] ページでは、次のタスクを実行できます。

- 手動検出を使用したモジュラー型システムの検出
- モジュラー型システムの削除
- 最新のインベントリ情報を表示するには、ページを更新します。
- モジュラー型システムの Operational Template (運用テンプレート) の割り当て
- モジュラー型システムの Operational Template (運用テンプレート) の導入
- I/O モジュールの表示
- I/O モジュールの起動

OMIMSSC で検出されたモジュラー型システムを表示するには、次の手順を実行します。

1. OMIMSSC で、[**設定と導入**] をクリックし、次に [**モジュラー型システム ビュー**] をクリックします。
   すべてのモジュラー型システムで検出されたモデル名が表示されます。
2. 特定のモジュラー型システムを表示するには、[**モジュラー型システム ビュー**] でモデル名をクリックします。
   該当モデルのすべてのモジュラー型システムが、サービス タグとともに表示されます。
3. 該当のモジュラー型システムに存在するすべてのデバイスを表示するには、サービス タグをクリックします。
   すべてのサーバ、入力出力モジュール、およびストレージデバイスとその詳細が表示されます。

   メモ: モジュラー型システムの詳細検出をした後にのみ、モジュラー型システム内のすべてのデバイスとその情報が表示されます。

   - デフォルトでは、**サーバ** タブが表示されます。
     このモジュラー型システムで検出されたすべてのサーバーが表示されます。
   - モジュラー型システムに存在するすべての入力出力モジュールを表示するには、[**I/O モジュール**] タブをクリックします。
   - モジュラー型システムに存在するすべてのストレージ デバイスを表示するには、[**ストレージ デバイス**] タブをクリックします。

モジュラー型システムを検出したら、次の点を考慮してください。

- [**運用テンプレート**] 列は、モジュラー型システムが検出されると、[**未割り当て**] として表示されます。これらのモジュラー型システムでファームウェアをアップデートしてオペレーティング システムを導入するには、Operational Template (運用テンプレート) を割り当てて導入します。詳細は、「Operational Template (運用テンプレート) の管理」を参照してください。
- 簡易検出後に、モジュラー型システム内に存在する入力/出力、ストレージ デバイス、およびサーバーの数を表示します。詳細検出を実行して、モジュラー型システムのコンポーネントの詳細を表示します。

OpenManage Enterprise Modular コンソールの起動

OpenManage Enterprise Modular コンソールを起動するには、次の手順に従います。

1. OMIMSSC で **設定と導入** を展開し、**モジュラーシステム** をクリックします。
2. モジュラーシステムの **デバイス IP** をクリックします。

入力 / 出力モジュール

すべてのネットワーク入力 / 出力モジュールとそれらの IP アドレス、サービスタグ、入力 / 出力タイプ、モデル、ファームウェアバージョン、スロット情報が表示されます。

I/O モジュールの起動コンソールを 入力 / 出力モジュール ページから起動します。

入力 / 出力モジュールに関する情報を表示するには、次の手順を実行します。

1. OMIMSSC で、**設定と導入** をクリックし、次に **モジュラーシステムビュー** をクリックします。**モジュラーシステムビュー** を展開し、サービスタグをクリックします。

   該当モデルのすべてのサービスタグが表示されます。
2. 入力 / 出力モジュールを表示するには、**I/O モジュール** タブをクリックします。

入出力モジュールコンソールの起動

入力出力モジュール コンソールを起動するには、次の手順に従います。

1. OMIMSSC で、[**設定と導入**] を展開し、[**モジュラー型システム ビュー**] をクリックします。モデルを個々のデバイスレベルに展開します。

   そのモデルの下にあるすべてのデバイスが表示されます。
2. **I/O モジュール** タブをクリックします。
3. デバイスの **IP アドレス** をクリックします。

クラスタビューの起動

[**クラスター ビュー**] ページには、OMIMSSC で検出されたすべてのクラスターが一覧表示されます。クラスタの FQDN (完全修飾名) 、サービスタグ、そのクラスタに存在するサーバの数を表示します。また、クラスター用の論理スイッチを作成し、事前定義済みの Operational Template (運用テンプレート) を使用して Storage Spaces Direct クラスターを作成します。

クラスタビュー ページでは、次のタスクを実行できます。

- 論理スイッチの作成 (SCVMM 2016 および 2019 ユーザーのみ)
- Storage Spaces Direct クラスターの作成 (SCVMM 2016 および 2019 ユーザーのみ)
- iDRAC コンソールの起動
- 検出された最新のクラスターを表示するには、ページを更新します。

OMIMSSC で検出されたクラスター グループを表示するには、次の手順を実行します。

1. OMIMSSC で、[**設定と導入**] をクリックし、[**クラスター ビュー**] をクリックします。
   さまざまなタイプのクラスタがすべてグループ化され、一覧表示されます。
2. 特定のタイプのクラスタに関する情報を表示するには、クラスタタイプを展開します。
   このタイプのすべてのクラスタが左側のペインに表示されます。
3. クラスタ内のサーバを表示するには、クラスタ名をクリックします。

iDRAC コンソールの起動

iDRAC コンソールを起動するには、次の手順に従います。

OMIMSSC で、[**設定と導入**] を展開し、以下のいずれかを選択します。

- **サーバビュー** をクリックします。サーバ (ホストまたは未割り当てサーバの場合) に基づいて、**未割り当てサーバ** または **ホスト** タブをクリックし、サーバの **iDRAC IP** アドレスをクリックします。

  デフォルトでは **未割り当てサーバ** タブが表示されます。

ホスト タブを表示するには、**ホスト** をクリックします。

- **クラスタビュー** をクリックします。クラスタタイプを展開し、クラスタグループをサーバレベルに展開します。

  サーバ タブが表示されます。

メンテナンスセンターの起動

メンテナンスセンター ページには、グループ内で検出されたすべてのデバイスと、OMIMSSC でデバイスを保守するために必要なリソースが一覧表示されます。[**メンテナンス センター**] ページで S2D クラスター グループを表示するには、[**アップデート グループ**] ドロップダウン メニューから [**すべてのアップデート グループ**] を選択していることを確認します。デバイスのファームウェア インベントリーを表示し、推奨に従ってファームウェアを最新の状態に維持することでデバイスを管理し、サーバーがクラッシュした場合はそれを以前の状態に戻し、置換されたコンポーネントを以前のコンポーネントと同じ設定にし、問題をトラブルシューティングするためにサーバー ログをエクスポートします。**アップデート設定** ページでは、すべてのアップデートソース、デフォルトのアップデートソースからの最新アップデートのポーリングと通知、同様の管理を必要とするデバイスのアップデートグループ、およびサーバ構成に必要なすべての保護ボールトを表示します。

メモ: デフォルトでは、OMIMSSC とともに、事前定義された FTP、HTTP、および HTTPS アップデート ソースに対する以前のバージョンの比較レポートを表示するカタログ ファイルがパッケージ化されています。したがって、最新のカタログをダウンロードして、最新の比較レポートを表示してください。最新のカタログをダウンロードするには、FTP、HTTP、および HTTPS アップデート ソースを編集して保存します。

メモ: 選択したアップデート ソース カタログにアップデートが存在しない場合、デバイスの特定コンポーネントのベースライン バージョンは使用不可とマークされます。

メンテナンスセンター ページでは、次のタスクを実行できます。

- アップデート ソースの作成
- ポーリング頻度の設定
- 事前定義されたアップデートグループを選択するか、カスタムアップデートグループを作成します。
- ファームウェアインベントリの表示と更新
- アップデートの実行メソッドを使用したファームウェアバージョンのアップグレードとダウングレード
- 保護ボールトの作成
- サーバプロファイルのエクスポート
- サーバプロファイルのインポート
- インベントリのエクスポート

メンテナンスセンター ページを表示するには、次の手順を実行します。

OMIMSSC で、[**メンテナンス センター**] をクリックします。
メンテナンスセンター ページが表示されます。

ジョブとログセンターの起動

OMIMSSC で開始されたジョブに関する情報、およびジョブの進行状況とそのサブタスクのステータスが表示されます。また、特定のジョブカテゴリのジョブをフィルタリングして表示することもできます。

OMIMSSC 管理ポータルおよび OMIMSSC コンソール拡張機能で、OMIMSSC から開始されたジョブを表示できます。

- OMIMSSC 管理ポータル—すべての OMIMSSC コンソールおよびユーザーから開始されたジョブが表示されます。
- OMIMSSC コンソール—ユーザーおよびコンソールに固有のジョブが表示されます。

ジョブ名は、システムによって生成されるか、ユーザーによって提供されます。サブタスクの名前は、管理対象システムの IP アドレスまたはホスト名の後に付けられます。サブタスクを展開して、そのジョブのアクティビティログが表示されます。ジョブは次の 4 つのグループに分類されます。

- **実行中**—現在実行中のすべてのジョブ、または進行中の状態が表示されます。
- **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**—将来の日時にスケジュールされているすべてのジョブが表示されます。また、これらのスケジュール済みジョブを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が表示されます。すべてのジョブは、ユーザー名と開始されたコンソール FQDN で表示されます。
  - **アプライアンスログメッセージ**—OMIMSSC アプライアンスの再起動など、すべての OMIMSSC アプライアンス固有のログメッセージが表示されます。このカテゴリのメッセージは、OMIMSSC 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** タブに表示されているさまざまなジョブカテゴリに共通のログメッセージが表示されます。これらのログは、コンソールとユーザーに固有です。

  たとえば、サーバの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、タブにはそのジョブの Server Update Utility (SUU) リポジトリの作成に関連するログメッセージが表示されます。

OMIMSSC で定義されるジョブのさまざまな状態は次のとおりです。

- **キャンセル**—ジョブは手動で、または OMIMSSC アプライアンスの再始動後に取り消されました。
- **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**—ジョブは将来の日時にスケジュールされています。

  メモ: 複数のジョブが同じデバイスに同時に送信された場合、ジョブは失敗します。そのため、同じデバイスのジョブを異なる時間にスケジュールするようにしてください。
- **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。
- **繰り返しスケジュール**—ジョブは定期的にスケジュールされています。

1. OMIMSSC で、**ジョブとログセンター** をクリックします。
2. **スケジュール済み**、**履歴**、**一般** など、ジョブの特定のカテゴリを表示するには、必要なタブをクリックします。

   ジョブに含まれているすべてのデバイスを表示するには、ジョブを展開します。さらに展開すると、ジョブのログメッセージが表示されます。

   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) さまざまなグループのジョブとジョブのステータスを **ステータス** 列に表示するには、フィルタを適用します。

16

Operational Template（運用テンプレート）

Operational Template（運用テンプレート）には、Microsoft 環境内の PowerEdge サーバーおよびモジュラー型システムの完全なデバイス構成が含まれ、オペレーティング システムの導入とファームウェアのアップデートに使用されます。

Operational Template（運用テンプレート）は、参照サーバー（ゴールデン サーバー）のハードウェアとファームウェアを他の多くのサーバーに複製し、同時にオペレーティング システムをプロビジョニングします。これには、参照サーバーの現在の値で設定された属性を持つファームウェア、ハードウェア、オペレーティング システム コンポーネントが含まれます。これらの値は、このテンプレートをデバイスに適用する前に変更できます。また、割り当てられた Operational Template（運用テンプレート）に対するコンプライアンスステータスを確認し、コンプライアンスレポートをサマリページに表示することもできます。

参照サーバーで使用可能なこれらのコンポーネントのみが取得され、Operational Template（運用テンプレート）コンポーネントとして動的に表示されます。たとえば、サーバーに FC コンポーネントがない場合は、Operational Template（運用テンプレート）に同じコンポーネントは表示されません。

参照サーバーおよび参照モジュラー型システムの詳細については、「参照サーバーの構成について」および「参照モジュラー型システムの構成について」を参照してください。

次の表に、Operational Template（運用テンプレート）に記載されているコンポーネントと、各コンポーネントの機能の表示と導入を示します。

表 7. Operational Template（運用テンプレート）の機能

コンポーネント	設定の導入	ファームウェアアップデート	設定の表示	運用テンプレートのコンプライアンスステータス
BIOS	はい	はい	はい	はい
iDRAC	はい	はい	はい	はい
NIC/CNA	はい	はい	はい	はい
RAID	はい	はい	はい	はい
FC	はい	はい	はい	はい
Windows	はい	—	いいえ	—
RHEL	はい	—	いいえ	—
ESXI	はい	—	いいえ	—
管理モジュール	はい	はい	はい	はい

トピック：

- 事前定義された Operational Template（運用テンプレート）
- 参照サーバの構成について
- 参照サーバからの Operational Template（運用テンプレート）の作成
- 参照モジュラー型システムからの Operational Template（運用テンプレート）の作成
- Operational Template（運用テンプレート）の表示
- Operational Template（運用テンプレート）の変更
- 複数サーバーでの運用テンプレートを使用したシステム固有値（プール値）の設定
- Operational Template（運用テンプレート）の削除
- Operational Template（運用テンプレート）の割り当てとサーバの Operational Template（運用テンプレート）コンプライアンスの実行
- サーバへの Operational Template（運用テンプレート）の導入
- モジュラー型システムの Operational Template（運用テンプレート）の割り当て
- モジュラー型システムへの Operational Template（運用テンプレート）の導入
- Operational Template（運用テンプレート）の割り当て解除

- 参照モジュラー型システムの構成について

事前定義された Operational Template（運用テンプレート）

事前定義されたテンプレートには、Storage Spaces Direct クラスターまたは Windows Server Software-Defined（WSSD）を作成するために必要なすべての設定が含まれています。 OMIMSSC R740XD、R740XD2、および R640 Storage Spaces Direct Ready Node モデルでのクラスターの作成とその固有のネットワーク アダプターがサポートされています。

表 8. 事前定義された Operational Template（運用テンプレート）のリスト

Operational Template（運用テンプレート）の名前	説明
R740XD_Mellanox_S2D_Template	このテンプレートは、Mellanox カードを搭載した R740XD Storage Spaces Direct Ready Node モデルに使用します。
R740XD2_Mellanox_S2D_Template	このテンプレートは、Mellanox カードを搭載した R740XD2 Storage Spaces Direct Ready Node モデルに使用します。
R740XD_QLogic_S2D_Template	このテンプレートは、QLogic カードを搭載した R740XD Storage Spaces Direct Ready Node モデルに使用します。
R740XD2_QLogic_S2D_Template	このテンプレートは、QLogic カードを搭載した R740XD2 Storage Spaces Direct Ready Node モデルに使用します。
R640_Mellanox_S2D_Template	このテンプレートは、Mellanox カードを搭載した R640 Storage Spaces Direct Ready Node モデルに使用します。
R640_QLogic_S2D_Template	このテンプレートは、QLogic カードを搭載した R640 Storage Spaces Direct Ready Node モデルに使用します。

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

- 事前定義されたテンプレートは、SCVMM 2016 および 2019 を実行している管理対象システムでのみ使用できます。
- 事前定義された Storage Spaces Direct テンプレートには、スロット 1 に NIC カードが表示されます。ただし、Operational Template（運用テンプレート）の導入中は、正しいスロットに NIC 設定が適用されます。また、デバイスに複数の NIC カードがある場合は、すべての NIC カードが、Operational Template（運用テンプレート）の指定と同様に設定されます。

参照サーバの構成について

ブートシーケンス、BIOS、RAID 設定、ハードウェア構成、ファームウェアアップデート属性、および組織に最適なオペレーティングシステムパラメータが選択されたサーバ設定を、参照サーバ設定と呼びます。

参照サーバを検出し、Operational Template（運用テンプレート）で参照サーバの設定をキャプチャして、同じハードウェア構成を持つ異なるサーバ間で複製します。

参照サーバからの 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、次のタスクが完了していることを確認します。

- **検出** 機能を使用して、参照サーバを検出します。サーバの検出の詳細については、「手動検出を使用したサーバの検出」を参照してください。
- SCCM ユーザーの場合：
  - 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場合は、デバイス タイプの認定資格プロフィールを用意します。詳細については、「認定資格プロフィールの作成」を参照してください。
- SCVMM ユーザーの場合：
  - 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の詳細については、「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。

- Windows 導入の場合は、デバイス タイプの認定資格プロフィールを用意します。詳細については、「認定資格プロフィールの作成」を参照してください。

- デフォルトのアップデートソースを使用していない場合は、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。

参照サーバの設定をキャプチャすると、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か、必要に応じてアップデートソース、ハードウェア構成、および Windows コンポーネントの属性を編集します。これでテンプレートを保存し、PowerEdge の同種サーバで使用できるようになります。

1. OMIMSSC で、次のいずれかの操作を実行して Operational Template (運用テンプレート) を開きます。
   - OMIMSSC ダッシュボードで、[**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、**プロファイル** > **運用テンプレート** を順にクリックして、**作成** をクリックします。

   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。
3. デバイスのタイプを選択し、参照デバイスの IP アドレスを入力して、**次へ** をクリックします。

   メモ: iDRAC 2.0 以降の参照サーバの構成をキャプチャできます。

4. **デバイスコンポーネント** で、コンポーネントをクリックすると、使用可能な属性とその値が表示されます。

   コンポーネントは次のとおりです。
   - ファームウェアアップデート
   - RAID、NIC、および BIOS などのハードウェアコンポーネント。

     メモ: iDRAC Embedded 1 コンポーネントでは、**ユーザー管理者権限** 属性の権限と値は次のとおりです。

     表 9. 権限値テーブル

値	権限
1	ログイン
2	設定
4	ユーザーの設定
8	ログ
16	システム制御
32	仮想コンソールへのアクセス
64	仮想メディアへのアクセス
128	システム操作
256	デバッグ
499	オペレータ権限

   - オペレーティングシステム—Windows、ESXi、または RHEL のいずれかを選択します。
5. 水平スクロール バーを使用してコンポーネントを探します。コンポーネントを選択し、グループを展開して、その属性値を編集します。垂直スクロール バーを使用して、コンポーネントのグループと属性を編集します。
6. Operational Template (運用テンプレート) が適用されると、選択したコンポーネントの設定が管理対象デバイスに適用されるため、各コンポーネントに対してチェックボックスをオンにします。ただし、参照デバイスのすべての設定がキャプチャされ、テンプレートに保存されます。

   メモ: チェックボックスで各コンポーネントに対して行った選択に関係なく、すべての設定がテンプレートに取り込まれます。

   オペレーティングシステム コンポーネントで、要件に応じて次のいずれかのオプションの手順を実行します。
   - SCCM での Windows オペレーティング システムの導入については、「SCCM 用の OMIMSSC コンソール拡張機能用の Windows コンポーネント」を参照してください。
   - SCVMM での Windows オペレーティング システムの導入については、「SCVMM 用の OMIMSSC コンソール拡張機能用の Windows コンポーネント」を参照してください。
   - OMIMSSC

- Windows 以外のオペレーティング システムの導入については、「OMIMSSC コンソール拡張機能用の Windows 以外のコンポーネント」を参照してください。

7. プロファイルを保存するには、**終了** をクリックします。

SCCM 用の OMIMSSC コンソール拡張機能の Windows OS コンポーネント

サーバの Operational Template (運用テンプレート) を作成または編集しながら、Windows コンポーネントに対し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: ドロップダウンメニューには、コレクションに導入されているタスクシーケンスだけが表示されます。

   タスクシーケンスについての詳細は、「タスクシーケンス」を参照してください。

2. **導入方法** について、以下のいずれかのオプションを選択します。
   - **ネットワーク ISO で起動**—指定された ISO を再起動します。
   - **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。
   - **vFlash で再起動**—vFlash で再起動します。ISO が vFlash にあることを確認します。

     メモ: vFlash で再起動 オプションを使用するには、vFlash 上で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) ネットワーク共有にあるイメージを使用するには、**フォールバックとしてネットワーク ISO を使用** オプションを選択します。
4. LC ブートメディアイメージファイルを入力します。
5. オペレーティングシステムに必要なドライバを選択します。

SCVMM 用の OMIMSSC コンソール拡張機能の Windows コンポーネント

サーバの Operational Template (運用テンプレート) を作成または編集しながら、Windows コンポーネントに対して次の手順を実行します。

[**ハイパーバイザー プロファイル**]、[**認定資格プロフィール**]、および [**サーバー IP 取得先**] を選択します。

メモ: ホスト名、および **サーバ管理 NIC** は常にプール値です。サーバー管理 NIC の場合は、オペレーティング システムが SCVMM と通信するために使用するネットワーク ポートの MAC アドレスを指定します。

サーバ IP 取得先 を **静的** として選択し、SCVMM で論理ネットワークを構成したことを確認すると、次のフィールドがプール値になります。

- **コンソール論理ネットワーク**
- **IP サブネット**
- **固定 IP アドレス**

OMIMSSC コンソール拡張機能の Windows 以外のコンポーネント

サーバの Operational Template (運用テンプレート) を作成または編集しながら、Windows 以外のコンポーネントに対して次の手順を実行します。

Windows 以外のオペレーティングシステム、オペレーティングシステムのバージョン、共有フォルダのタイプ、ISO ファイル名、ISO ファイルの場所、オペレーティングシステムのルートアカウントのパスワードを選択します。

(オプション) CIFS 共有にアクセスするための Windows タイプの認定資格プロフィールを選択します。

ホスト名はプール値であり、DHCP オプションを無効にすると、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**
- **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 以外のオペレーティングシステムの導入では、ネットワークファイルシステム（NFS）および Common Internet File System（CIFS）共有タイプがサポートされます。

参照モジュラー型システムからの 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、次のタスクが完了していることを確認します。

- **検出**機能を使用して、モジュラー型システムを検出します。モジュラー型システムの検出の詳細については、「手動検出を使用したモジュラー型システムの検出」を参照してください。
- デフォルトのアップデートソースを使用していない場合は、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。

参照モジュラー型システムの設定をキャプチャすることで、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か、必要に応じてアップデートソースとハードウェア構成の属性を編集できます。これで、テンプレートを保存し、それを使用して同じモデルの他のモジュラー型システムを設定することができます。

メモ: 他の MX7000 デバイスで Active Directory（AD）ユーザーを設定する場合は、すべての AD ユーザーが設定されている MX7000 モジュラー型システムから Operational Template（運用テンプレート）を作成する必要があります。

メモ: ユーザーアカウントのパスワードは、セキュリティ上の理由から、参照モジュラー型システムから運用テンプレートにキャプチャされません。Operational Template（運用テンプレート）を編集して新しいユーザーアカウントとパスワードを追加してから、管理下のモジュラー型システムに Operational Template（運用テンプレート）を適用します。それ以外の場合は、ユーザーアカウントに変更を加えずに Operational Template（運用テンプレート）を適用でき、参照モジュラー型システムで使用されているものと同じパスワードが管理下のモジュラー型システムに適用されます。

1. OMIMSSC で、次のいずれかの操作を実行して Operational Template（運用テンプレート）を開きます。
   - OMIMSSC ダッシュボードで、[**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、**プロファイル** > **運用テンプレート** を順にクリックして、**作成** をクリックします。

   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。
3. **デバイスコンポーネント** で、コンポーネントをクリックすると、使用可能な属性とその値が表示されます。

   コンポーネントは次のとおりです。
   - ファームウェアアップデート
   - 内蔵の管理モジュール

     メモ: **Web サーバー**属性が有効であることを確認します。このコンポーネントが有効でない場合、Operational Template（運用テンプレート）の導入後、OMIMSSC から MX7000 モジュラー型システムにアクセスできなくなります。

     メモ: **SNMP 設定**および **Syslog 設定**の場合、各属性で使用可能な 4 つの設定すべてを選択して、管理対象デバイスに適用します。
4. 水平スクロールバーを使用してコンポーネントを探します。コンポーネントを選択し、グループを展開して、その属性値を編集します。垂直スクロールバーを使用して、コンポーネントのグループと属性を編集します。
5. Operational Template（運用テンプレート）が適用されると、選択したコンポーネントの設定が管理対象デバイスに適用されるため、各コンポーネントに対してチェックボックスをオンにします。ただし、参照デバイスのすべての設定がキャプチャされ、テンプレートに保存されます。
6. プロファイルを保存するには、**終了** をクリックします。

Operational Template（運用テンプレート）の表示

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

OMIMSSC コンソールで、[**プロファイルとテンプレート**] をクリックし、[**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）の変更

運用テンプレートのアップデートソース、ハードウェア構成、オペレーティングシステムを変更できます。

Operational Template（運用テンプレート）を変更する前に、次の点に注意してください。

- いくつかの属性の値は、他の属性の値に依存します。属性の値を手動で変更する場合は、相互に依存する属性も変更してください。これらの相互に依存する値が適切に変更されていない場合、ハードウェア構成の適用が失敗する可能性があります。
- Operational Template（運用テンプレート）を作成すると、システム固有の属性を含む可能性がある指定された参照サーバーからすべてのハードウェア構成が取得されます。たとえば、固定 IPv4 アドレス、資産タグなどです。システム固有の属性を設定するには、「Operational Template（運用テンプレート）」を参照してください
- Operational Template（運用テンプレート）の属性には、参照サーバーの現在の値が割り当てられます。Operational Template（運用テンプレート）には、属性に適用可能な他の値も表示されます。
- 定義済みの Operational Template（運用テンプレート）とカスタムで作成された Operational Template（運用テンプレート）を変更するには、次の手順を実行します。

メモ:（SCVMM ユーザーおよびサーバーの場合のみ）すべての必須属性（運用テンプレートで取得される必須属性は、S2D クラスター用に Dell EMC が推奨する属性です）、つまり Storage Spaces Direct に必要な属性は、事前定義された Storage Spaces Direct テンプレートの読み取り専用属性です。ただし、テンプレートの名前、オペレーティング システム コンポーネント、必須ではないハードウェア構成属性は編集できます

1. 編集するテンプレートを選択し、**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. （オプション）テンプレートの名前と説明を編集して、**次へ** をクリックします。
3. **デバイスコンポーネント** で使用可能な属性とその値を表示するには、コンポーネントをクリックします。
4. 使用可能な属性の値を変更します。

   メモ: Operational Template（運用テンプレート）が適用されるとき、選択したコンポーネントの設定だけが管理対象システムに適用されるため、適用する各コンポーネントのチェックボックスをオンにします。

   メモ: Operational Template（運用テンプレート）を編集する場合、Advanced Host Controller Interface（AHCI）コンポーネントのほとんどの読み取り専用の属性は編集可能として表示されません。ただし、これらの読み取り専用属性が設定されて Operational Template（運用テンプレート）が展開されている場合、デバイスには変更が加えられません。

   - MX7000 モジュラー型システムの場合：
     - 設定は、グループのすべての属性が選択されている場合にのみ適用されます。したがって、グループ内の属性の 1 つを変更する場合でも、グループ内のすべての属性を選択してください。
     - Operational Template（運用テンプレート）を使用して新しいユーザーを追加するには、Operational Template（運用テンプレート）をキャプチャしたときにエクスポートされた既存ユーザーのすべての属性を選択し、最近追加したユーザーグループを選択して、Operational Template（運用テンプレート）を保存します。
     - タイムゾーンの値を指定する方法については、付録を参照してください。
5. オペレーティングシステムコンポーネントに対して、要件に応じて次のいずれかのタスクを実行します。
   - SCCM での Windows オペレーティング システムの導入については、「SCCM 用の OMIMSSC コンソール拡張機能用の Windows コンポーネント」を参照してください。
   - SCVMM での Windows オペレーティング システムの導入については、「SCVMM 用の OMIMSSC コンソール拡張機能用の Windows コンポーネント」を参照してください。
   - OMIMSSC
   - Windows 以外のオペレーティング システムの導入については、「OMIMSSC コンソール拡張機能用の Windows 以外のコンポーネント」を参照してください。
6. プロファイルを保存するには、**終了** をクリックします。

複数サーバーでの運用テンプレートを使用したシステム固有値（プール値）の設定

OMIMSSC は、デバイスの設定をそのまま取得します。システム固有の属性、たとえば、iDRAC の静的 IPv4 アドレスは、運用テンプレートにプール値として表示されます。依存属性であるプール値属性はデフォルトでは選択されず、他の属性はデフォルトで選択されます。

1. 編集するテンプレートを選択し、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. （オプション）テンプレートの名前と説明を編集して、**次へ** をクリックします。
3. **デバイスコンポーネント** で使用可能な属性とその値を表示するには、コンポーネントをクリックします。
4. [**属性グループ**] を展開します。属性の値がプール値の場合、属性はシステム固有の属性とされます。
5. これらのシステム固有属性への入力は、運用テンプレートの導入時に [**プール属性のエクスポート**] を使用して.CSV ファイルを介して複数のサーバーに対して行うことができます。「サーバーへの運用テンプレートの導入」を参照してください。
6. これらのシステム固有属性を適用しない場合は、これらの属性（手順 3 で説明）を指定し、運用テンプレートの編集中に選択を解除します。

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、次のことを確認します。

- 選択した Operational Template（運用テンプレート）が、どのサーバーまたはモジュラー型システムにも関連付けられていないこと。デバイス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）に関連付けられているジョブが実行中でないこと。
- 事前定義されたテンプレートは削除できないため、事前定義された Operational Template（運用テンプレート）が選択されていないこと。
- Operational Template（運用テンプレート）を削除する手順が同じであること。

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

Operational Template（運用テンプレート）の割り当てとサーバの 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でのみ、その Operational Template（運用テンプレート）の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、サーバの設定を 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）のステータスが表示されます。

Operational Template（運用テンプレート）を割り当てるには、次の手順を実行します。

1. OMIMSSC で、[**設定と導入**] をクリックし、[**サーバー ビュー**] をクリックします。必要なサーバを選択して、**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。

   [**Operational Template（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から、**割り当て** をクリックします。

   Operational Template（運用テンプレート）ドロップダウンリストには、前のステップで選択したデバイスと同じタイプのテンプレートが表示されます。

   デバイスがテンプレートに準拠している場合は、チェックマークが付いた **緑色** のボックスが表示されます。

   Operational Template（運用テンプレート）がデバイスに正常に適用されていない場合、または Operational Template（運用テンプレート）のハードウェアコンポーネントが選択されていない場合は、**情報** シンボルボックスが表示されます。

デバイスがテンプレートに準拠していない場合は、**警告** シンボルボックスが表示されます。割り当てられた Operational Template（運用テンプレート）にデバイスが準拠していない場合に限り、テンプレート名のリンクをクリックすることでサマリーレポートを表示できます。［**Operational Template（運用テンプレート）コンプライアンス サマリー レポート**］ページには、テンプレートとデバイスの相違点のサマリー レポートが表示されます。

詳細レポートを表示するには、次の手順を実行します。

a. **詳細なコンプライアンスの表示** をクリックします。ここでは、割り当てられたテンプレートとは異なる属性値を持つコンポーネントが表示されます。Operational Template（運用テンプレート）コンプライアンスのさまざまな状態が色別で表示されます。
   - 黄色の警告シンボル—準拠していません。デバイスの設定がテンプレートの値と一致しないことを表します。
   - 赤色のボックス—コンポーネントがデバイスに存在しないことを示します。

サーバへの Operational Template（運用テンプレート）の導入

管理対象サーバにオペレーティングシステムを導入するには、導入に使用される管理システムとオペレーティングシステムイメージに KB 記事 4093492 以降がインストールされていることを確認します。

サーバに割り当てられた Operational Template（運用テンプレート）を導入することにより、Windows および Windows 以外のオペレーティングシステム（ESXi および RHEL）を導入できます。

メモ: 第 12 世代のサーバーに Windows 2016 または Windows 2019 オペレーティング システムを導入した後、デバイス マネージャー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ーをダウンロードしてインストールします。

メモ: サーバーでロックダウン モードが有効になっている場合、サーバーへの運用テンプレートの導入はブロックされます。

メモ: Windows を UEFI ベースのデバイスに導入する場合は、GUID パーティション テーブル（GPT）ファイル システムを使用して、Windows パーティションを含むハード ドライブをフォーマットします。詳細については、Microsoft マニュアルの「UEFIGPT ベースのハード ドライブ パーティション」セクションを参照してください。

1. OMIMSSC で、［**設定と導入**］をクリックし、［**サーバー ビュー**］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、**Operational Template（運用テンプレート）の導入** をクリックします。
   Operational Template（運用テンプレート）の導入 ページが表示されます。

   メモ: タスク シーケンス メディアの起動中に、*Press any key to boot to CD \ DVD .....* プロンプトが表示された場合。プロンプトを削除してタスク シーケンス メディアを自動的に起動する方法については、Microsoft マニュアルの「EFI ベースのコンピューターへの Windows のインストール」セクションを参照してください。

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ているすべての属性を .CSV ファイルにエクスポートするには、**プール属性のエクスポート** をクリックします。エクスポートしない場合は、ステップ 4 に進みます。
   プールの値をエクスポートする前に、OMIMSSC コンソール拡張機能がインストールされている OMIMSSC 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。

3. 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ているすべての属性の値を .CSV ファイルに入力し、ファイルを保存します。**属性値プール** で、ファイルを選択してインポートします。
   .CSV ファイルの形式は次のとおりです： `attribute-value-pool.csv`

   メモ: iDRAC IP または iDRAC の認証情報が変更された後でジョブが OMIMSSC によって追跡されず、iDRAC でジョブが成功しても失敗とマークされる可能性があるため、すべて適切な属性を持つ.CSV ファイルを選択し、iDRAC IP または iDRAC の認証情報がテンプレートによって変更されないことを確認します。

4. 一意のジョブ名、ジョブの説明を入力し、**導入** をクリックします。
   このジョブを追跡するには、デフォルトで **ジョブリストへ移動** オプションが選択されています。

モジュラー型システムの Operational Template（運用テンプレート）の割り当て

Operational Template（運用テンプレート）をモジュラー型システムに割り当て、Operational Template（運用テンプレート）コンプライアンスを実行します。この操作では、選択したテンプレートをモジュラー型システムに割り当てることで、モジュラー型システムと Operational Template（運用テンプレート）の設定を比較します。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、完了時にコンプライアンスステータスが表示されます。

モジュラー型システムの Operational Template（運用テンプレート）を割り当てるには、次の手順を実行します。

1. OMIMSSC で、[**設定と導入**] をクリックし、[**モジュラー型システム ビュー**] をクリックします。必要なモジュラー型システムを選択し、[**運用テンプレートの割り当て**] をクリックします。

   [**Operational Template（運用テンプレート）の割り当て**] 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から、**割り当て** をクリックします。

   デバイスがテンプレートに準拠している場合は、チェックマークが付いた **緑色** のボックスが表示されます。

   Operational Template（運用テンプレート）がデバイスに正常に適用されていない場合、または Operational Template（運用テンプレート）のハードウェアコンポーネントが選択されていない場合は、**情報** シンボルボックスが表示されます。

   メモ: Operational Template（運用テンプレート）のコンプライアンスステータスでは、ユーザー属性に加えられた変更はすべて除外されます。

   デバイスがテンプレートに準拠していない場合は、**警告** シンボルボックスが表示されます。割り当てられた Operational Template（運用テンプレート）にデバイスが準拠していない場合に限り、テンプレート名のリンクをクリックすることでサマリーレポートを表示できます。[**Operational Template（運用テンプレート）コンプライアンス サマリー レポート**] ページには、テンプレートとデバイスの相違点のサマリー レポートが表示されます。

   詳細レポートを表示するには、次の手順を実行します。
   a. **詳細なコンプライアンスの表示** をクリックします。ここでは、割り当てられたテンプレートとは異なる属性値を持つコンポーネントが表示されます。Operational Template（運用テンプレート）コンプライアンスのさまざまな状態が色別で表示されます。
      - 黄色の警告シンボル—準拠していません。デバイスの設定がテンプレートの値と一致しないことを表します。
      - 赤色のボックス—コンポーネントがデバイスに存在しないことを示します。

モジュラー型システムへの Operational Template（運用テンプレート）の導入

割り当てられた Operational Template（運用テンプレート）を導入することで、モジュラー型システムコンポーネントを設定し、モジュラー型システム ファームウェア バージョンをアップデートできます。

メモ: マルチシャーシ管理（MCM）では、リードシャーシが **メンバーシャーシへの伝播** を使用して設定されている場合に、OMIMSSC からリードシャーシとメンバーシャーシを設定およびアップデートすると、伝播によって行われた変更が上書きされます。

1. OMIMSSC で、[**設定と導入**] をクリックし、[**モジュラー型システム ビュー**] をクリックします。テンプレートを割り当てたモジュラー型システムを選択し、[**Operational Template（運用テンプレート）の導入**] をクリックします。**Operational Template（運用テンプレート）の導入** 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ているすべての属性を .CSV ファイルにエクスポートするには、**プール属性のエクスポート** をクリックします。エクスポートしない場合は、ステップ 4 に進みます。
3. 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ているすべての属性の値を .CSV ファイルに入力し、ファイルを保存します。**属性値プール** で、ファイルを選択してインポートします。

   .CSV ファイルの形式は次のとおりです： `attribute-value-pool.csv`

   メモ: CMC IP または CMC 資格情報が変更された後は、ジョブが OMIMSSC によって追跡されないため、選択した .CSV ファイルにすべて適切な属性があり、テンプレートによって CMC IP または CMC 資格情報が変更されていないことを確認します。

4. 一意のジョブ名、ジョブの説明を入力し、**導入** をクリックします。

   メモ: モジュラー型システムに対してサポートされているシステム固有のプール値属性はありません。したがって、エクスポートするプール値はありません。

   このジョブを追跡するには、デフォルトで **ジョブリストへ移動** オプションが選択されています。

Operational Template（運用テンプレート）の割り当て解除

1. OMIMSSC で、次のいずれかのタスクを実行します。
   - **設定と導入** をクリックし、**サーバビュー** をクリックします。
   - [**設定と導入**] をクリックし、[**モジュラー型システム ビュー**] をクリックします。

   必要なデバイスを選択して、**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。

   [**Operational Template（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 **割り当て解除** を選択し、**割り当て** をクリックします。
   選択したデバイスで Operational Template（運用テンプレート）の割り当てが解除されます。

参照モジュラー型システムの構成について

組織に最適な優先ネットワーク構成、ユーザー アカウント、セキュリティ、アラートを備えたモジュラー型システム構成は、参照モジュラー型システム構成または参照シャーシと呼ばれます。

参照モジュラー型システムを検出し、Operational Template（運用テンプレート）内の参照モジュラー型システムの設定を取得して、同じモデルの異なるモジュラー型システム間で複製します。

17

オペレーティングシステムの導入の準備

管理対象サーバに Windows オペレーティングシステムを導入する前に、WinPE イメージをアップデートし、タスクシーケンス、LC ブートメディアファイル、およびタスクシーケンスメディアのブータブル ISO ファイルを作成します。SCCM コンソールユーザーと SCVMM コンソールユーザーでは、手順が異なります。詳細については、以下の各セクション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場合は、「Windows 以外の OS 導入の準備」セクションに記載されているポイントに留意してください。

トピック：

- WinPE イメージについて
- SCCM コンソールでのオペレーティングシステム導入の準備
- Windows 以外のオペレーティングシステムの導入の準備

WinPE イメージについて

Windows プレインストール環境（WinPE）イメージは、オペレーティングシステムの導入に使用します。SCCM または SCVMM から使用できる WinPE イメージに最新のドライバが含まれていない可能性があるため、アップデートされた WinPE イメージを使用してオペレーティングシステムを導入します。必要なドライバをすべて含む WinPE イメージを作成するには、DTK を使用してイメージをアップデートします。該当する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ことを確認します。

メモ: `boot.wim` ファイルのファイル名は変更しないでください。

SCCM 用の WIM ファイルの提供

`\\shareip\sms_sitecode\OSD\boot\x64\boot.wim` から `boot.wim` ファイルをコピーして、OMIMSSC がアクセスできる共有フォルダーに貼り付けます。
例えば、共有パスの場所はこのようになります：`\\shareip\sharefolder\boot.wim`

SCVMM 用の WIM ファイルの提供

DTK から最新の起動に必要な Dell ドライバーを挿入するために提供される Boot.WimPE ベース イメージは、SCVMM に PXE サーバーをインストールすることによって生成されます。

1. サーバーに Windows Deployment Server（WDS）ロールをインストールして設定し、PXE サーバーを SCVMM に追加します。
   サーバーに WDS ロールを追加する方法、および SCVMM に PXE サーバーを追加する方法については、Microsoft マニュアルの「ベアメタル コンピューターからの Hyper-V ホストまたはクラスターのプロビジョニング」を参照してください。
2. `C:\RemoteInstall\DCMgr\Boot\Windows\Images` にある PXE サーバーから `boot.wim` ファイルをコピーし、OMIMSSC がアクセスできる共有フォルダーに貼り付けます。
   例えば、共有パスの場所はこのようになります：`\\shareip\sharefolder\boot.wim`

WDS および PXE サーバーは、WinPE ベースの boot.in イメージの生成にのみ必要であり、導入シナリオでは使用されません。

DTK ドライバの解凍

DTK ファイルには、オペレーティングシステムを導入するサーバに必要なファームウェアバージョンが含まれています。

To download DTK driver, launch **https://www.dell.com/support**/ -> Browse all products -> Servers -> PowerEdge -> Select the server type < C Series, Modular, Rack, or Tower> -> Select the server model -> Search for the keyword **DTK** and download the required version.

メモ: WinPE ISO イメージの作成に最新バージョンの DTK を使用している間に、**Dell EMC OpenManage Deployment Toolkit for Windows** ファイルを使用します。**Dell EMC OpenManage Deployment Toolkit for Windows** ファイルには、オペレーティングシステムを導入するシステムに必要なファームウェアバージョンが含まれています。ファイルの最新バージョンを使用し、WinPE アップデートに **Dell EMC OpenManage Deployment Toolkit Windows Driver Cabinet** ファイルを使用しないでください。

1. DTK 実行可能ファイルをダブルクリックします。
2. DTK ドライバを解凍するには、フォルダを選択します。
   たとえば、`C:\DTK501` などです。
3. 解凍した DTK フォルダを共有フォルダにコピーします。
   例： `\\Shareip\sharefolder\DTK\DTK501`

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

WinPE イメージのアップデート

各 WinPE アップデートジョブには、一意のジョブ名が割り当てられます。

1. OMIMSSC で、[**WinPE アップデート**] を選択します。
   WinPE アップデート ページが表示されます。
2. **イメージソース** の **カスタム WinPE イメージパス** で、WinPE イメージパスとイメージが存在するファイル名を入力します。
   たとえば、`\\Shareip\sharefolder\WIM\boot.wim` などです。
3. **DTK パス** の下で、**DTK ドライバパス** に、Dell EMC Deployment Toolkit ドライバの場所を入力します。
   例： `\\Shareip\sharefolder\DTK\DTK501`
4. [**出力ファイル**] の [**ISO または WIM ファイル名**] に、WinPE イメージが生成される共有ファイルのパスと共にファイルの名前を入力します。

   次のいずれかの出力ファイルタイプを入力します。
   - SCCM 用 WIM ファイル
   - SCVMM 用 ISO ファイル

   メモ: 共有フォルダーは、System Center マシンにある必要があります。

5. [**認定資格プロフィール**] の下の、[**認定資格プロフィール**] に、WinPE イメージが保存されている共有フォルダーへのアクセス権を持つ資格情報を入力します。
6. （オプション）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。
7. **アップデート** をクリックします。
   前のステップで指定したファイル名を持つ WinPE イメージは、`\\Shareip\sharefolder\WIM` に作成されます。

SCCM コンソールでのオペレーティングシステム導入の準備

SCCM コンソールで OMIMSSC を使用して検出された管理対象サーバにオペレーティングシステムを導入する前に、Dell EMC 固有またはカスタムのタスクシーケンス、LC ブートメディアファイル、およびタスクシーケンスメディアのブータブル ISO ファイルを作成します。

タスクシーケンス - SCCM

タスクシーケンスは、SCCM を使用して管理対象システムにオペレーティングシステムを導入するために使用される一連のコマンドです。

Operational Template（運用テンプレート）を作成する前に、次の前提条件を完了することをお勧めします。

- Configuration Manager で、システムが検出され、**[資産およびコンプライアンス]** > **[デバイス コレクション]** > **[すべての Dell Lifecycle Controller サーバー]** に表示されていることを確認してください。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タイプ

タスクシーケンスは、次の 2 とおりの方法で作成できます。

- OMIMSSC 展開テンプレートを使って 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ステップに進みます。

Dell 固有のタスクシーケンスの作成

SCCM の **OMIMSSC サーバ展開テンプレート** を使って Dell のタスクシーケンスを作成するには、次の手順に従ってください。

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. **タスクシーケンス** を右クリックしてから、**OMIMSSC サーバ展開** > **OMIMSSC サーバ展開テンプレートの作成** の順に選択します。
   OMIMSSC サーバ展開タスクシーケンスウィザード が表示されます。
4. **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. **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. **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、**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、**<今は選択しない>** を選択します。
9. **作成** をクリックします。
   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、**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 コンソールを起動します。
   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、**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 および 2019 でタスク シーケンスを編集中の場合、オブジェクト参照が見つからないというメッセージに、**セットアップ ウィンドウと ConfigMgr** パッケージのリストは表示されません。パッケージを追加してから、タスクシーケンスを保存します。

1. Configuration Manager コンソールを起動します。
   Configuration Manager 画面が表示されます。
2. 左ペインで、**[ソフトウェア ライブラリー]** > **[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 導入]** > **[Dell Lifecycle Controller からドライバーを適用]** の順にクリックします。
   Dell サーバー導入のカスタム アクションがロードされます。タスク シーケンスを変更できるようになります。

   メモ: タスク シーケンスを初めて編集するときは、[**Windows のセットアップと Configuration Manager のエラーメッセージ**] が表示されます。エラーを解決するには、Configuration Manager クライアント アップグレード パッケージを作成して選択します。パッケージの作成の詳細については、**technet.microsoft.com** の「Configuration Manager マニュアル」を参照してください。

   メモ: SCCM 2016 および 2019 でタスク シーケンスを編集する場合、オブジェクト参照が見つからないというメッセージに、セットアップ ウィンドウと ConfigMgr パッケージのリストは表示されません。したがって、パッケージを追加してから、タスクシーケンスを保存する必要があります。

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、**管理** > **サイトの構成** > **サイト** を選択します。
2. **<サイトサーバ名>** を右クリックし、**サイトコンポーネントの設定** を選択してから、**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. **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 **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. **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. Configuration Manager の **ソフトウェアライブラリ** で **タスクシーケンス** を右クリックし、**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。

   メモ: OMIMSSC は、タスクシーケンスメディアの作成に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** で、**ブータブルメディア** を選択し、**無人オペレーションシステム展開を許可** オプションを選択して、**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. **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 のみを使用して作成した起動イメージを使用します。

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. **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 **サマリー** 画面が表示されます。
9. **次へ** をクリックします。
進捗バーが表示されます。
10. 画像の作成が完了したら、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の準備

管理対象システムに Windows 以外のオペレーティングシステムを導入する場合は、次の点に注意してください。

- ISO ファイルは、Network File System バージョン（NFS）または Common Internet File System（CIFS）共有で、読み取り/書き込みアクセスが可能です。
- 管理対象システムで仮想ドライブが使用可能であることを確認します。
- ESXi オペレーティングシステムを導入した後、サーバは SCCM の **Managed Lifecycle Controller（ESXi）** コレクションに移動します。
- Windows 以外のオペレーティングシステムを導入した後、サーバは **デフォルトの Windows 以外のホストアップデートグループ** に移動します。
- ネットワークアダプタは、オペレーティングシステムを導入しているサーバー内のネットワークポートに接続することをお勧めします。

18

Operational Template（運用テンプレート）を使用したクラスタの作成

この章では、Storage Spaces Direct クラスターの作成について説明します。

トピック：

- Storage Spaces Direct クラスター用の論理スイッチの作成
- Storage Spaces Direct クラスターの作成

Storage Spaces Direct クラスター用の論理スイッチの作成

SCVMM の OMIMSSC から論理スイッチを作成します。

メモ: [**管理用の設定**] セクションに入力した IP アドレスは、Storage Spaces Direct の事前定義された Operational Template（運用テンプレート）のオペレーティング システム コンポーネントに入力された IP アドレスよりも優先されます。

1. OMIMSSC で、[**設定と導入**] を展開し、[**クラスター ビュー**] をクリックして、クラスターの [**論理スイッチの作成**] をクリックします。
2. 論理スイッチに名前を付けて、論理スイッチと関連付ける SCVMM 内のホストグループを選択します。
3. 次の詳細を入力し、**作成** をクリックします。
   a. **管理用の設定**で、**サブネット**、**開始 IP**、**終了 IP**、**DNS サーバ**、**DNS サフィックス**、および **ゲートウェイ** の詳細を指定します。

      メモ: サブネット情報は、Classless InterDomain Routing（CIDR）表記で指定します。

   b. **ストレージの設定**で、**VLAN**、**サブネット**、**開始 IP**、および **終了 IP** の詳細を指定します。
4. 一意のジョブ名、ジョブの説明を入力し、**作成** をクリックします。

   このジョブを追跡するには、デフォルトで **ジョブリストへ移動** オプションが選択されています。

論理スイッチが正常に作成されたことを確認するには、**クラスタの作成** ページに表示されるドロップダウンメニューで論理スイッチ名を確認します。

論理スイッチの詳細を表示するには、SCVMM で次の手順を実行します。

1. 論理スイッチ名を表示するには、**ファブリック** をクリックし、**ネットワーキング** で **論理スイッチ** をクリックします。
2. 論理スイッチのアップリンクポートプロファイル（UPP）を表示するには、**ファブリック** をクリックし、**ネットワーキング** で **論理スイッチ** をクリックします。
3. 論理スイッチのネットワークを表示するには、**ファブリック** をクリックし、**ネットワーキング** で **論理ネットワーク** をクリックします。

Storage Spaces Direct クラスターの作成

- クラスターの**論理スイッチの作成**機能を使用して、論理ネットワークを作成してください。
- SCVMM 2016 または 2019 を使用していることを確認します。
- Windows Server 2016 または 2019 Datacenter エディションを使用していることを確認します。
- 管理対象サーバーの構成が Storage Spaces Direct ソリューション ファームウェアおよびドライバーのバージョン要件と一致していることを確認します。詳細については、『*Dell EMC Storage Spaces Direct Ready Node PowerEdge R740XD、R740XD2、および PowerEdge R640 サポート マトリックス*』マニュアルを参照してください。

- Storage Spaces Direct のインフラストラクチャと管理の詳細については、『*R740xd、R740XD2、および R640 Storage Spaces Direct Ready Node を使用したスケーラブルなハイパーコンバージド インフラストラクチャ向けの Dell EMC Microsoft Storage Spaces Direct Ready Node 導入ガイド*』マニュアルを参照してください。

  メモ: Storage Spaces Direct (S2D) は、Windows Server Software-Defined (WSSD) や Azure Stack Hyper-converged Infrastructure (ASHCI) とも呼ばれます。

Storage Spaces Direct クラスターを作成する前に、次の点を考慮してください。

- 固定 IP アドレスのみを指定することで、OMIMSSC で Storage Spaces Direct クラスターを作成できます。
- 仮想ディスク サイズは、Storage Spaces Direct の定義済み運用テンプレートでゼロとして表示されます。ただし、Storage Spaces Direct の定義済み運用テンプレートを適用した後、仮想ドライブは、M.2 物理ストレージ メディアのフル サイズと同じサイズのみ作成されます。仮想ドライブの容量の詳細については、`dell.com/support` にある iDRAC のユーザーズ ガイドを参照してください。
- オペレーティング システムから iDRAC へのパススルー オプションが有効になっている場合は、IP アドレスが運用テンプレートで設定されていることを確認する必要があります。

Storage Spaces Direct クラスターを作成するには、次の手順を実行します。

1. OMIMSSC で、[**設定と導入**] をクリックし、[**クラスター ビュー**] をクリックします。
   クラスタビュー ページが表示されます。
2. クラスター名を指定し、Storage Spaces Direct クラスターを作成するための定義済み Operational Template (運用テンプレート) を選択します。
   - 特定のサーバモデルおよび NIC カードにのみ属する未割り当てのサーバは、**Operational Template (運用テンプレート)** ドロップダウンメニューから選択した Operational Template (運用テンプレート) に基づいて表示されます。
3. サーバをクラスタに追加するには、チェックボックスを使用してサーバを選択します。
4. システム固有のプール値を追加するには、**属性値プールのエクスポート** をクリックします。
   システム固有のプール値を指定できるように、ファイルを編集して保存します。詳細については、「プール値 CSV ファイルへの入力」を参照してください。
5. (オプション) システム固有の値を設定する必要がある場合は、**属性値プール** で **参照** をクリックし、編集した .csv ファイルを選択します。
6. 固有のジョブ名を入力し、**作成** をクリックします。
   このジョブを追跡するには、デフォルトで **ジョブリストへ移動** オプションが選択されています。

   メモ: オペレーティング システムの導入が進行中の場合、SCVMM でクローンされているホスト プロファイル/物理コンピューター プロファイル (サーバー GUID が付加された名前) が表示されます。これらのプロファイルは個々のサーバー OSD で使用されます。

クラスタが正常に作成されたかどうかを確認するには、次の手順を実行します。

1. クラスタジョブ作成の成功ステータスを確認します。
2. **クラスタビュー** ページでクラスタを表示します。
3. SCVMM でクラスタを表示します。

詳細については、ベアメタル PC からの Hyper-V ホストまたはクラスターのプロビジョニングに関する Microsoft マニュアルの「前提条件」セクションの「物理コンピューターのプロファイルの作成」セクションを参照してください。

メモ: 2 ノード クラスターに対してはクラスター監視を設定することをお勧めします。クラスター監視の設定は、ノードまたはネットワークの通信に失敗した場合に、クラスターまたは Storage Quorum を維持するのに役立ちます。詳細については、『Storage Spaces Direct 導入ガイド』を参照してください。

19

OMIMSSC のファームウェアアップデート

Dell EMC デバイスを最新の状態に維持するために、OMIMSSC を使用して、セキュリティ、問題の修正、拡張機能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します。Dell EMC アップデートリポジトリを使用してデバイスのファームウェアをアップデートします。

ファームウェアのアップデートは、ハードウェア互換性のあるデバイスでのみサポートされています。管理対象デバイスの OMIMSSC で使用可能な機能を使用するために、管理対象デバイスには iDRAC、Lifecycle Controller（LC）、および BIOS の必要最小限のファームウェアバージョンが必要です。必要なファームウェアバージョンを持つデバイスには、ハードウェア互換性があります。

トピック：

- アップデートグループについて
- アップデートソースとは
- Dell EMC Repository Manager（DRM）との統合
- ポーリング頻度の設定
- デバイスインベントリの表示と更新
- フィルタの適用
- アップデートの実行メソッドを使用したファームウェアバージョンのアップグレードとダウングレード

アップデートグループについて

アップデートグループは、同様のアップデート管理を必要とするデバイスのグループです。OMIMSSC でサポートされているアップデートグループには、次の 2 種類があります。

- 事前定義されたアップデートグループ—手動で作成、変更、または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—これらのグループ内のデバイスの変更および削除を作成できます。

メモ: SCVMM に存在するすべてのサーバグループは、OMIMSSC に一覧表示されます。ただし、OMIMSSC のサーバのリストはユーザー固有ではありません。そのため、これらのデバイスで操作を実行するためのアクセス権があることを確認してください。

事前定義されたアップデートグループ

デバイスを検出すると、検出されたデバイスが次の定義済みグループのいずれかに追加されます。

- **デフォルトのホストグループ**—このグループは、Windows オペレーティングシステムに導入されているか、登録済みの Microsoft コンソールと同期されているサーバで構成されます。
- **デフォルトの未割り当てグループ**—このグループは、未割り当てまたはベアメタルのサーバで構成されます。
- **デフォルトの Windows 以外のホストグループ**—このグループは、Windows 以外のオペレーティングシステムで導入されたサーバで構成されます。
- **シャーシアップデートグループ**—このグループは、モジュラーサーバとシャーシまたはモジュラーシステムで構成されます。第 12 世代のサーバとそのシャーシ情報が検出されます。デフォルトでは、グループは `Chassis-Service-tag-of-Chassis-Group` という名前形式で作成されます。たとえば、`Chassis-GJDC4BS-Group` のように作成されます。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、サーバは CMC 情報ととも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ない場合でも、シャーシ内のすべてのモジュラーサーバがクラスタアップデートグループにあるため、シャーシアップデートグループは引き続き存在しますが、CMC 情報だけが表示されます。
- **クラスタアップデートグループ**—このグループは、**Windows サーバフェールオーバークラスタ** で構成されます。第 12 世代以降のモジュラーサーバがクラスタの一部である場合、CMC 情報も **メンテナンスセンター** ページのインベントリに追加されます。

カスタムアップデートグループ

検出されたデバイスを、類似した管理が必要なグループに追加して、タイプが **汎用アップデートグループ** のカスタムアップデートグループを作成します。ただし、カスタムアップデートグループにデバイスを追加できるのは、**デフォルトの未割り当てアップデートグループ** および **デフォルトのホストアップデートグループ** からだけです。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デバイスを検索します。カスタムアップデートグループにデバイスを追加すると、そのデバイスは事前定義されたアップデートグループから削除され、カスタムアップデートグループでだけ使用可能になります。

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、**メンテナンスセンター** をクリックし、次に **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、**作成** をクリックします。
   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、説明を入力し、作成するアップデートグループのタイプを選択します。
   カスタムアップデートグループには、次のアップデートグループタイプのサーバのみを含めることができます。
   - 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サーバを組み合わせることもできます。
4. アップデートグループにサーバを追加するには、サーバのサービスタグを使用してサーバを検索し、**アップデートグループに含まれるサーバ** テーブルにサーバを追加するには、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には、**保存** をクリックします。
   メモ： カスタム アップデート グループはシステム センターごとであり、同じシステム センターの他のユーザーに表示されます。

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場合は、次の点に注意してください。

- アップデートグループは、作成後にタイプを変更することはできません。
- カスタム アップデート グループのサーバーを別のカスタム アップデート グループに移動するには、次の手順を実行します。
  1. 既存のカスタム アップデート グループからサーバーを削除します。これで、サーバーは事前定義されたアップデート グループに自動的に追加されます。
  2. カスタム グループを編集してサーバーを追加し、サービス タグを使用してサーバーを検索します。

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**] をクリックして、アップデート グループを選択し、[**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。したがって、カスタムアップデートグループに関連付けられているスケジュール済みジョブを削除してから、サーバグループを削除してください。
- アップデートグループは、そのアップデートグループにサーバが存在する場合でも削除できます。ただし、このようなアップデートグループを削除すると、サーバはそれぞれの事前定義されたアップデートグループに移動されます。

- カスタムアップデートグループに存在するデバイスを MSSC から削除した後で、登録済みの MSSC と OMIMSSC を同期すると、該当デバイスは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。

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** をクリックしてアップデートグループを選択し、**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。

アップデートソースとは

アップデートソースには、Dell EMC アップデート（BIOS、およびドライバパック（管理コンポーネント、ネットワークカード、など））が含まれているカタログファイルへのリファレンスがあり、Dell Update Packages（DUP）と呼ばれる自己完結型実行可能ファイルを提供します。

アップデートソースまたはリポジトリを作成し、比較レポートを生成するためのデフォルトのアップデートソースとして設定し、リポジトリで新しいカタログファイルが使用可能になったときにアラートを受信するようにできます。

OMIMSSC を使用すると、オンラインまたはオフラインのアップデートソースを使用して、デバイスのファームウェアを最新の状態に保つことができます。

オンラインアップデートソースは、Dell EMC が管理するリポジトリです。

オフラインアップデートソースはローカルリポジトリであり、インターネット接続がない場合に使用されます。

カスタムリポジトリを作成して、OMIMSSC アプライアンスのローカルイントラネットにネットワーク共有を配置することをお勧めします。これにより、インターネット帯域幅が節約され、安全な内部リポジトリも提供されます。

次のいずれかのアップデートソースを使用して、ファームウェアをアップデートします。

- **DRM リポジトリ** - オフラインリポジトリです。検出されたデバイスのインベントリ情報を OMIMSSC アプライアンスからエクスポートして、DRM でリポジトリを準備します。DRM との統合と DRM によるアップデートソースの作成の詳細については、「DRM との統合」を参照してください。DRM でリポジトリを作成した後、OMIMSSC で、DRM で作成されたアップデートソース、関連するデバイスを選択し、デバイスでアップデートを開始します。DRM の詳細については、`dell.com\support` にある *Dell Repository Manager* のマニュアルを参照してください。
- **FTP、HTTP、または HTTPS** - オンラインまたはオフラインのリポジトリーです。FTP、HTTP、または HTTPS サイトで提供される最新アップデートに関しては、デバイスの特定のコンポーネントをアップデートします。Dell EMC では、2 か月ごとにリポジトリーを準備し、PDK カタログを通じて次のアップデートを発行しています。
  - サーバー BIOS とファームウェア
  - Dell EMC 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）

  メモ: オンラインアップデートソースを選択すると、Operational Template（運用テンプレート）の展開中に、最新のファームウェアバージョンがダウンロードされ、管理対象デバイスに適用されます。したがって、ファームウェアバージョンは、参照と導入されたデバイスで異なる場合があります。
- **参照ファームウェアインベントリと比較** - DRM を使用してオフラインリポジトリに変換できます。選択したデバイス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。参照インベントリファイルには、同じタイプまたはモデルのデバイスのインベントリ情報を含めることも、さまざまなタイプやモデルの複数のデバイスを含めることもできます。OMIMSSC に存在するデバイスのインベントリ情報を、保存されている参照インベントリファイルと比較できます。エクスポートされたファイルを DRM に渡してリポジトリを作成する方法については、`dell.com\support` にある *Dell Repository Manager* のマニュアルを参照してください。

事前定義されたデフォルトのアップデートソース

OMIMSSC には、新規インストールまたはアップグレード後に使用できる 3 つの事前定義されたアップデート ソースが含まれています。**Dell Online FTP カタログ** は FTP タイプの事前定義されたアップデート ソース、**Dell Online HTTP カタログ** は HTTP タイプの事前定義されたアップデート ソース、**Dell Online HTTPS カタログ** は HTTPS タイプの事前定義されたアップデート ソース（デフォルト）です。ただし、別のアップデートソースを作成して、それをデフォルトのアップデートソースとしてマークすることもできます。

メモ: プロキシサーバを使用している場合は、リポジトリにアクセスするために、アップデートソースを編集してプロキシの詳細を追加し、変更を保存します。

Storage Spaces Direct クラスタ用の事前定義されたデフォルトのアップデートソース

OMIMSSC では、特定の事前定義されたアップデートソースによる Storage Spaces Direct クラスタのアップデートがサポートされています。これらのアップデートソースは、Storage Spaces Direct クラスタのコンポーネントの最新の推奨ファームウェアバージョンを含むカタログファイルを参照しています。これらは、**メンテナンスセンター** ページにのみ表示されます。

Dell Online FTP S2D カタログ は、FTP タイプの事前定義されたアップデートソースで、**Dell Online FTP カタログ** に含まれています。

Dell Online HTTP S2D カタログ は、HTTP タイプの事前定義されたアップデートソースで、**Dell Online HTTP カタログ** に含まれています。

Dell Online HTTPS S2D カタログは、HTTPS タイプの事前定義されたデフォルトのアップデート ソースで、**Dell Online HTTPS カタログ**に含まれています。

メモ: Storage Spaces Direct (S2D) は、Windows Server Software-Defined (WSSD) や Azure Stack Hyper-converged Infrastructure (ASHCI) とも呼ばれます。

モジュラーシステム用の事前定義されたデフォルトのアップデートソース

OMIMSSC では、特定の事前定義されたアップデートソースによるモジュラーシステムのアップデートがサポートされています。これらのアップデートソースは、モジュラーシステムのコンポーネントの最新の推奨ファームウェアバージョンを含むカタログファイルを参照しています。これらは、**メンテナンスセンター** ページにのみ表示されます。

Dell Online FTP MX7000 カタログ は、FTP タイプの事前定義されたアップデートソースで、**Dell Online FTP カタログ** に含まれています。

Dell Online HTTP MX7000 カタログ は、HTTP タイプの事前定義されたアップデートソースで、**Dell Online HTTP カタログ** に含まれています。

Dell Online HTTPS MX7000 カタログは、HTTPS タイプの事前定義されたデフォルトのアップデート ソースで、**Dell Online HTTPS カタログ**に含まれています。

テスト接続を使用したデータの検証

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するために、**テスト接続**を使用します。接続が成功した場合のみ、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.gz` ファイルをダウンロードし、ファイルを解凍します。
3. `catalog.xml` ファイルを開き、**baseLocation** をお使いのローカル FTP URL に変更して、そのファイルを `.gz` 拡張子で圧縮します。
   たとえば、**baseLocation** を `ftp.dell.com` から `ftp.yourdomain.com` に変更します。
4. カタログファイルと DUP ファイルを `ftp.dell.com` と同じ構造でローカル FTP フォルダ内に配置します。

ローカル HTTP のセットアップ

ローカル HTTP をセットアップするには、次の手順を実行します。

1. ローカル HTTP に `downloads.dell.com` と全く同一のフォルダ構造を作成します。
2. `http://downloads.dell.com/catalog/catalog.xml.gz` のオンライン HTTP から `catalog.gz` ファイルをダウンロードし、ファイルを解凍します。

3. catalog.xml ファイルを解凍し、**baseLocation** をお使いのローカル HTTP URL に変更して、そのファイルを .gz 拡張子で圧縮します。
   たとえば、**baseLocation** を downloads.dell.com から hostname.com などのホスト名または IP アドレスに変更します。
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。

ローカル HTTPS のセットアップ

ローカル HTTPS 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 HTTPS に、downloads.dell.com とまったく同一のフォルダー構造を作成します。
2. https://downloads.dell.com/catalog/catalog.xml.gz のオンライン HTTPS から catalog.gz ファイルをダウンロードして、ファイルを解凍します。
3. catalog.xml ファイルを解凍し、**baseLocation** をローカル HTTPS の URL に変更して、そのファイルを.gz 拡張子で圧縮します。
   たとえば、**baseLocation** を downloads.dell.com から hostname.com などのホスト名または IP アドレスに変更します。
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 HTTPS フォルダー内に配置します。

アップデートソースの表示

1. **OMIMSSC** で、**メンテナンスセンター** をクリックします。
2. **メンテナンスセンター** で **メンテナンス設定** をクリックし、次に **アップデートソース** をクリックします。
   説明、ソースタイプ、場所、資格情報プロファイル名とともに作成されたすべてのアップデートソースが表示されます。

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可能であることを確認してください。
- DRM アップデートソースを作成する場合は、管理者の役割を持つ DRM をインストールおよび設定してください。

1. OMIMSSC コンソールで、**メンテナンスセンター** をクリックしてから、**メンテナンス設定** をクリックします。
2. **アップデートソース** ページで、**新規作成** をクリックし、アップデートソース名と説明を入力します。
3. **ソースタイプ** ドロップダウンメニューから、次のいずれかのタイプのアップデートソースを選択します。
   - 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場合に選択します。
     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 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場合に選択します。
     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。
   - HTTPS ソース：オンライン HTTPS アップデート ソースを作成する場合に選択します。
     メモ: HTTPS タイプのアップデート ソースを作成している場合は、カタログの完全なパスを入力し、加えてカタログ名とアップデート ソースにアクセスするためのプロキシー資格情報も入力します。

     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場合に選択します。DRM をインストールしたことを確認します。
     メモ: DRM ソースを作成する場合は、Windows の資格情報を入力し、Windows の共有場所にアクセスできることを確認します。場所 フィールドで、ファイル名を含むカタログファイルの完全なパスを指定します。
   - 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場合に選択します。
     メモ: **インベントリ出力ファイル** をアップデートソースとして使用すると、比較レポートを表示できます。参照サーバのインベントリ情報は、OMIMSSC で検出された他のすべてのサーバと比較されます。
4. [**場所**] に、FTP、HTTP、または HTTPS ソースのアップデート ソースの URL と、DRM の Windows の共有場所を指定します。

メモ: ローカル FTP サイトは、オンライン FTP を複製する必要があります。

メモ: ローカル HTTP サイトは、オンライン HTTP を複製する必要があります。

メモ: FTP ソースの URL に HTTP または HTTPS を指定すること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、**資格情報** で必要な資格情報プロファイルを選択します。
6. **プロキシ資格情報** で、FTP または HTTP ソースにアクセスするためにプロキシが必要な場合は、適切なプロキシ資格情報を選択します。
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、**これをデフォルトのソースにする** を選択します。
8. 前述の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ことを確認するには、**テスト接続** をクリックし、**保存** をクリックします。

   メモ: アップデートソースは、テスト接続が成功し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を変更する前に、次の点に注意してください。

- **Dell Online FTPS2D カタログ**、**Dell Online HTTPS2D カタログ**、または **Dell Online HTTPS S2D カタログ**のアップデート ソースを編集するには、それぞれの事前定義されたアップデート ソースを編集して、変更を保存します。このアップデートは、**Dell Online FTP S2D カタログ**、**Dell Online HTTP S2D カタログ**、または **Dell Online HTTPS S2D カタログ**のアップデート ソースに反映されます。
- アップデートソースの作成後、そのアップデートソースのタイプと場所を変更することはできません。
- アップデートソースは、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で使用されている場合でも、導入テンプレートで使用されている場合でも変更できます。使用中のアップデートソースを変更しているときに、警告メッセージが表示されます。**確認** をクリックして変更に移動します。
- アップデートソースでカタログファイルがアップデートされても、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アップデートされません。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削除してから再作成します。

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

アップデートソースの削除

アップデートソースを削除する前に、次の点に注意してください。

- 事前定義されたアップデートソースは削除できません。
- 進行中またはスケジュール済みのジョブで使用されているアップデートソースは削除できません。
- デフォルトのアップデートソースであるアップデートソースは削除できません。

削除するアップデートソースを選択し、**削除** をクリックします。

Dell EMC Repository Manager（DRM）との統合

OMIMSSC は DRM と統合され、OMIMSSC 内にカスタムのアップデート ソースが作成されます。この統合は DRM バージョン 2.2 以降で利用可能です。OMIMSSC アプライアンスから検出されたデバイス情報を DRM に提供し、使用可能なインベントリー情報を使用して、DRM でカスタム リポジトリーを作成し、それを OMIMSSC 内でアップデート ソースとして設定することで、ファームウェアのアップデートを実行し、管理対象デバイスでクラスターを作成できます。DRM でリポジトリーを作成する方法の詳細については、`Dell.com/support/home` にある *Dell EMC Repository Manager* のマニュアルを参照してください。

DRM との統合： OMIMSSC

このセクションでは、統合を使用してリポジトリーを作成するプロセスについて説明します。

メモ: 必要なアップデートを準備するために、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 EMC アドバイザリなどの要因を考慮してください。

メモ: 検出されたデバイスに関する最新のインベントリー情報を表示するには、OMIMSSC をアップグレードした後で、DRM を OMIMSSC アプライアンスに再統合します。

1. ホームページで、[**新規リポジトリーを追加**] をクリックします。[**新規リポジトリーを追加**] ウィンドウが表示されます。
2. [**統合**] タブを選択し、[**リポジトリー名**] と [**説明**] を入力します。
3. [**カスタム**] を選択し、[**システムの選択**] をクリックして特定のシステムを選択します。
4. [**統合タイプ**] ドロップダウン メニューから、統合する製品を選択します。選択した製品に基づいて、次のオプションが表示されます。使用可能なオプションは次のとおりです。
   a. Dell OpenManage Integration for Microsoft System Center — ホスト名または IP、ユーザー名、パスワード、プロキシ サーバーを入力します。

      メモ: パスワードに、<, >, ',", & などの特殊文字が含まれていないことを確認します。

   b. Dell コンソール統合 — URL https://<IP>/genericconsolerepository で、ユーザー名、パスワード、プロキシ サーバーの管理者情報を入力します。

   メモ: Dell コンソール統合は、OpenManage Integration for System Center Virtual Machine Manager (SCVMM) などの Web サービスを組み込んだコンソールに適用されます。
5. 必要なオプションを選択したら、[**接続**] をクリックします。使用可能なシステムとモデルが [**統合タイプ**] セクションに表示されます。
6. [**追加**] をクリックして、リポジトリーを作成します。リポジトリーは、ホームページで利用可能なリポジトリー ダッシュボードに表示されます。

   注 : バンドル タイプまたは DUP フォーマットを選択する際、Dell PowerEdge MX7000 シャーシが OMIMSSC のインベントリーの一部である場合は、Windows 64 ビットおよびオペレーティング システム非依存を選択するようにしてください。

DRM を OMIMSSC と統合した後は、『*Ready Node のライフサイクル管理および監視のための Dell EMC Microsoft Storage Space Direct Ready Node 操作ガイド*』の「*Dell Repository Manager を使用した Storage Spaces Direct 対応ノードのファームウェア カタログの取得*」セクションを参照してください。参照先 : dell.com/support

ポーリング頻度の設定

ポーリングと通知を設定して、アップデートソースで使用可能な新しいカタログファイルがある場合にアラートを受信します (デフォルトとして選択済み)。OMIMSSC アプライアンスは、アップデートソースのローカルキャッシュを保存します。アップデートソースで新しいカタログファイルが使用可能になると、通知ベルの色がオレンジ色に変化します。OMIMSSC アプライアンスでローカルにキャッシュされた使用可能なカタログに置き換えるには、ベルアイコンをクリックします。古いカタログファイルを最新のカタログファイルに置き換えると、ベルの色が緑に変化します。

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、[**メンテナンス センター**] をクリックし、[**ポーリングと通知**] をクリックします。
2. ポーリングの発生頻度を選択します。
   - **行わない** - このオプションはデフォルトで選択されています。アップデートを受信しない場合に選択します。
   - **週に 1 回** - 週に 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受信する場合に選択します。
   - **2 週間に 1 回** - 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受信する場合に選択します。
   - **月に 1 回** - 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受信する場合に選択します。

デバイスインベントリの表示と更新

メンテナンスセンター ページで、アップデートソースに対するデバイスの比較レポートを表示します。アップデートソースを選択すると、既存のファームウェアと、選択したアップデートソースにあるファームウェアを比較するレポートが表示されます。アップデートソースを変更すると、レポートが動的に生成されます。サーバインベントリがアップデートソースと比較され、解決策が一覧表示されます。このアクティビティには、存在するデバイスとデバイスコンポーネントの数に基づいて、かなりの

時間がかかります。このプロセス中は、他のタスクを実行できません。インベントリを更新すると、デバイス内の 1 つのコンポーネントを選択した場合でも、デバイスのインベントリ全体が更新されます。

場合によっては、デバイスのインベントリがアップデートされても、ページに最新のインベントリが表示されないことがあります。したがって、更新オプションを使用すると、検出されたデバイスの最新のインベントリ情報を表示できます。

メモ: 最新バージョンの OMIMSSC にアップグレードした後、`ftp.dell.com` または `downloads.dell.com` への接続に失敗した場合は、デフォルトの Dell Online FTP、Dell HTTP、または Dell HTTPS アップデート ソースでカタログ ファイルをダウンロードすることはできません。したがって、比較レポートは使用できません。デフォルトのアップデート ソースの比較レポートを表示するには、デフォルトの Dell Online FTP、Dell HTTP、または Dell HTTPS アップデート ソースを編集し（必要に応じてプロキシー認証情報を入力）、[**アップデート ソースを選択**] ドロップダウン メニューから同じものを選択します。アップデートソースの編集についての詳細は、「アップデートソースの変更」を参照してください。

メモ: 製品が提供されると、カタログ ファイルのローカル コピーが OMIMSSC に存在します。したがって、最新の比較レポートは使用できません。最新の比較レポートを表示するには、カタログファイルをアップデートします。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して保存するか、アップデートソースを削除してから再作成します。

メモ: SCCM では、インベントリ情報をアップデートした後でも、**ドライバパックのバージョン** やオペレーティングシステムで **使用可能なドライバ** などのサーバの詳細は、**Dell アウトオブバンドコントローラ**（OOB）のプロパティページでアップデートされません。OOB プロパティをアップデートするには、OMIMSSC を登録済み SCCM と同期します。

メモ: OMIMSSC をアップグレードしても、以前のバージョンで検出されたサーバーに関する情報は表示されません。最新のサーバ情報と正しい比較レポートについては、サーバを再検出してください。

検出されたデバイスのファームウェアインベントリを更新および表示するには、次の手順を実行します。

1. **OMIMSSC** で、[**メンテナンス センター**] をクリックします。
   [**メンテナンス センター**] ページには、選択したアップデート ソースに対して OMIMSSC で検出されたすべてのデバイスの比較レポートが表示されます。
2. （オプション）特定のデバイスグループの比較レポートだけを表示するには、必要なデバイスだけを選択します。
3. （オプション）別のアップデートソースの比較レポートを表示するには、**アップデートソースの選択** ドロップダウンリストからアップデートソースを選択して、アップデートソースを変更します。
4. 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 Dell EMC が推奨するアップデートアクションなどのデバイスコンポーネントのファームウェア情報を表示するには、**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。また、デバイスの推奨されるアップデートの数も表示します。利用可能なアップデートアイコンにカーソルを合わせると、重要なアップデートの数、推奨されるアップデートの数など、アップデートの対応する詳細が表示されます。

   利用可能なアップデートアイコンの色は、アップデートの全体的な重要度に基づいています。重要なアップデートカテゴリは次のとおりです。
   - サーバまたはサーバグループに 1 つの重要なアップデートがあっても、色は赤色です。
   - 重要なアップデートがない場合、色は黄色になります。
   - ファームウェアのバージョンが最新の場合、色は緑色になります。

   比較レポートに入力した後は、次のアップデートアクションが提案されます。
   - ダウングレード—以前のバージョンを使用でき、既存の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。
   - 対処不要—既存のファームウェアは、アップデートソースのファームウェアと同じです。
   - 利用可能なアップデートはありません—このコンポーネントのアップデートは利用できません。

     メモ: MX7000 モジュラー型システム用の電源供給ユニット（PSU）コンポーネントおよびオンライン カタログのサーバーに利用可能なアップデートはありません。MX7000 モジュラー型システムの PSU コンポーネントをアップデートする場合は、「*Dell EMC PowerEdge Mx7000 デバイスの電源供給ユニット コンポーネントのアップデート*」を参照してください。サーバの PSU コンポーネントをアップデートする場合は、Dell EMC サポートにお問い合わせください。
   - アップグレード - オプション—アップデートはオプションで、新しい機能または特定の設定のアップグレードで構成されます。
   - アップグレード - 重要—アップデートは重要であり、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ます。
   - アップグレード - 推奨—アップデートは、問題の修正、またはコンポーネントの機能拡張です。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。

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。

使用可能なサーバコンポーネントに基づいて比較レポートをフィルタリングします。OMIMSSC では、次の 3 つのカテゴリのフィルタがサポートされます。

- **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。
- **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。
- **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、**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。

フィルタの削除

フィルタを削除するには、次の手順を実行します。

OMIMSSC で、**メンテナンスセンター** をクリックし、**フィルタのクリア** をクリックするか、選択されているチェックボックスをクリアします。

アップデートの実行メソッドを使用したファームウェアバージョンのアップグレードとダウングレード

デバイスに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ことを確認します。

- アップデートソースが使用可能であること。

  メモ: Storage Spaces Direct アップデート ソースまたは MX7000 アップデート ソースを選択して、Storage Spaces Direct クラスターまたは MX7000 モジュラー型システムにファームウェア アップデートを適用する場合、これらのアップデート ソースには、Storage Spaces Direct クラスターおよびモジュラー型システム用のコンポーネントの推奨ファームウェア バージョンを含むカタログへの参照が修正されて表示されます。
- iDRAC または管理モジュール (MM) のジョブキューが、管理対象デバイスにアップデートを適用する前にクリアされていること。

OMIMSSC とハードウェア互換性のある選択したデバイス グループに、アップデートを適用します。アップデートはすぐに適用することも、スケジュールすることもできます。ファームウェアアップデート用に作成されたジョブは、**ジョブとログセンター** ページに一覧表示されます。

ファームウェアをアップグレードまたはダウングレードする前に、次の点に注意してください。

- このタスクを開始すると、存在するデバイスとデバイスコンポーネントの数によっては、かなりの時間がかかります。
- デバイスの単一コンポーネント、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。
- デバイスに適用可能なアップグレードまたはダウングレードがない場合は、そのデバイスでファームウェアアップデートを実行しても、デバイスに対するアクションは発生しません。
- シャーシのアップデートについては、『*Dell PowerEdge M1000e Chassis Management Controller ファームウェア ユーザーズ ガイド*』の「*CMC ファームウェアのアップデート*」セクションを参照してください。
  - VRTX のシャーシ ファームウェアをアップデートする方法については、『*Dell PowerEdge VRTX 用 Dell Chassis Management Controller ユーザーズ ガイド*』の「*ファームウェアのアップデート*」セクションを参照してください。
  - FX2 のシャーシ ファームウェアをアップデートする方法については、『*Dell PowerEdge FX2 用 Dell Chassis Management Controller ユーザーズ ガイド*』の「*ファームウェアのアップデート*」セクションを参照してください。

1. OMIMSSC で、[**メンテナンス センター**] をクリックし、サーバーまたはモジュラー型システム グループとアップデートソースを選択してから、[**アップデートの実行**] をクリックします。
2. **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. ファームウェアバージョンのダウングレードを有効にするには、**ダウングレードを許可** チェックボックスをオンにします。

   このオプションが選択されていない場合、ファームウェアのダウングレードを必要とするコンポーネントに対するアクションは実行されません。

4. **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。
   - **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。
5. 次のいずれかの方法を選択して、**終了** をクリックします。
   - **エージェントフリーのステージングアップデート** - 適用時にシステムの再起動を必要としないアップデートはただちに適用され、システムの再起動が必要なアップデートはシステムの再起動時に適用されます。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。デバイスの操作が 1 つでも失敗すると、アップデートジョブ全体が失敗します。
   - **エージェントフリーのアップデート** - アップデートが適用されシステムがただちに再起動します。

     メモ: OMIMSSC では、MX7000 モジュラー型システムの場合、[**エージェント フリーのアップデート**] のみがサポートされています。

メモ: **クラスタ対応アップデート (CAU)** - クラスタアップデートグループ上で Windows CAU 機能を使用してアップデート処理を自動化することで、サーバの可用性を維持します。アップデートは、SCVMM サーバがインストールされている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に渡されます。アップデートプロセスは自動化されて、サーバの可用性が維持されます。アップデートジョブは、**アップデート方法** ドロップダウンメニューからの選択に関係なく Microsoft クラスタ対応アップデート (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 は iDRAC と対話してジョブのステータスを確認し、OMIMSSC 管理ポータルの [**ジョブとログ**] ページに表示します。長時間 iDRAC からジョブのステータスに関する応答がない場合、ジョブのステータスは失敗とマークされます。

CAU を使用したアップデート

サーバ (クラスタの一部) のアップデートは、SCVMM サーバがインストールされている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通じて行われます。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。Cluster Aware Update (CAU) を使用すると、中断やサーバのダウンタイムを最小限に抑えて、ワークロードの継続的な可用性を実現できます。したがって、クラスタグループによって提供されるサービスには影響がありません。CAU の詳細については、`technet.microsoft.com` の「Cluster-Aware アップデートの概要」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、次のことを確認します。

- 登録されたユーザーが、CAU 機能を使用してクラスタをアップデートするための管理者権限を持っていることを確認します。
- 選択した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。
- クラスタのアップデート準備状況を確認し、CAU メソッドを適用するクラスタ準備状況レポートに重大なエラーや警告がないことを確認します。クラスタアップデート準備を確認します。CAU に関する詳細については、`technet.microsoft.com` にある「クラスタ対応アップデートの要件とベストプラクティス」のセクションを参照してください。
- CAU 機能をサポートするには、Windows Server 2012、Windows Server 2012 R2、Windows 2016、または Windows 2019 オペレーティング システムが、すべてのフェールオーバー クラスター ノードにインストールされているようにしてください。
- 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有効にするファイアウォールルールを有効にします。
- クラスター グループに、ノードが 2 つ以上あることを確認します。

メモ:

- アップデートの適用については、「アップデートの実行メソッドを使用したファームウェアバージョンのアップグレードとダウングレード」を参照してください。
- Dell EMC Repository Manager のファームウェアおよびドライバーのアップデートをダウンロードする方法については、`dell.com\support` の *Dell EMC Solutions for Microsoft Azure Stack HCI ページの [ファームウェアおよびドライバーのアップデート カタログ]* に移動し、カタログ ファイルをダウンロードしてください。

20

OMIMSSC でのデバイスの管理

サーバおよびモジュラーシステムコンポーネントのファームウェアをアップグレードするジョブをスケジュールすることで、サーバおよびモジュラーシステムを最新の状態に維持します。サーバの以前の設定をエクスポートしたり、交換したコンポーネントに古いコンポーネントの設定を適用したり、トラブルシューティングのために LC ログをエクスポートしたりして、サーバを以前の状態に回復してサーバを管理します。

トピック：

- サーバのリカバリ
- 交換したコンポーネントに対するファームウェアおよび構成設定の適用
- サーバの LC ログの収集
- インベントリのエクスポート
- スケジュール済みジョブのキャンセル

サーバのリカバリ

サーバの構成をプロファイルにエクスポートし、そのプロファイルを同じサーバにインポートすることで以前の状態に戻し、サーバの構成を保護ボールトに保存します。

保護ボールト

保護ボールトは、サーバプロファイルを保存できる安全な場所です。サーバまたはサーバのグループからサーバプロファイルをエクスポートし、それを同じサーバまたはサーバのグループにインポートします。このサーバプロファイルは、外部ボールトを作成してネットワーク上の共有の場所に保存するか、内部ボールトを作成して vFlash Secure Digital (SD) カード上に保存できます。サーバまたはサーバのグループは、1 つの保護ボールトにのみ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多数のサーバまたはサーバのグループに関連付けることはできます。サーバプロファイルは 1 つの保護ボールトにのみ保存できます。ただし、1 つの保護ボールトに保存できるサーバプロファイルの数に制限はありません。

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、**[メンテナンス センター]** > **[メンテナンス設定]** > **[保護ヴォールト]** の順にクリックします。
2. ヴォールトを変更するには、ヴォールトを選択し、[**編集**] をクリックします。

   メモ: サーバー プロファイルのエクスポートまたはインポート ジョブの進行中に保護ヴォールトが変更された場合、編集された情報には、ジョブ内の保留中のサブ タスクが考慮されます。

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、これらのコンポーネントの設定など、さまざまなコンポーネントにインストールされているファームウェアイメージを含むサーバプロファイルをエクスポートします。OMIMSSC アプライアンスは、すべての設定を含む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保護ボールトを選択してください。サーバまたはサーバグループの設定プロファイルをすぐにエクスポートすることも、後で使用するように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をエクスポートする頻度について、関連する繰り返しオプションを選択することもできます。

BIOS 設定 で **エラー時の F1/F2 プロンプト** オプションを無効にします。

サーバプロファイルをエクスポートする前に、次の点を考慮してください。

- インスタンスでは、1 つのサーバグループに対して 1 つのエクスポート設定ジョブのみをスケジュールできます。
- 設定プロファイルがエクスポートされるサーバまたはサーバグループに対して、他のアクティビティを実行することはできません。
- iDRAC で **自動バックアップ** ジョブが同じ時間にスケジュールされていないことを確認します。
- フィルタが適用されている場合、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、適用されているすべてのフィルタをクリアします。
- サーバプロファイルをエクスポートするには、iDRAC Enterprise ライセンスがあることを確認します。
- 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ていないことを確認します。他の操作のためにサーバ IP 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ジョブのエクスポートをスケジュールします。

1. OMIMSSC で、[**メンテナンス センター**] をクリックします。プロファイルをエクスポートするサーバーを選択し、[**デバイス プロファイル**] ドロップダウン メニューから [**エクスポート**] をクリックします。
   サーバプロファイルのエクスポート ページが表示されます。
2. **サーバプロファイルのエクスポート** ページで、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。

   サーバプロファイルのエクスポート で、次のいずれかを選択します。
   - **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。
   - 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提供します。
     - **行わない**—スケジュールされた時間中に一度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。
     - **1 週間に 1 回**—1 週間に 1 回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。
     - **2 週間に 1 回**—2 週間に 1 回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。
     - **4 週間に 1 回**—4 週間に 1 回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

同じサーバまたはサーバのグループに対して以前にエクスポートされたサーバプロファイルを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ている状態に復元する場合に便利です。

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：そのサーバに対してエクスポートされた最新のサーバプロファイルを自動的にインポートできます。この操作では、サーバごとに個別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：個別に選択された各サーバのサーバプロファイルをインポートできます。たとえば、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、インポートされ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：

- サーバプロファイルは、そのサーバのエクスポートされたサーバプロファイルのリストからのみインポートできます。異なるサーバまたはサーバグループに同じサーバプロファイルをインポートすることはできません。別のサーバ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、その特定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、それを実行する、サーバプロファイルを持たないそれらの特定のサーバに対してサーバプロファイルのインポートジョブは失敗します。障害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をエクスポートした後で、サーバからコンポーネントが削除され、プロファイルのインポートジョブが開始されると、不足しているコンポーネント情報がスキップされる以外は、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表示されません。不足しているコンポーネントの詳細については、iDRAC の「**ライフサイクルログ**」を参照してください。
- フィルタを適用した後は、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、適用されているすべてのフィルタをクリアします。
- 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 [**メンテナンス センター**] で、プロファイルをインポートするサーバーを選択し、[**デバイス プロファイル**] ドロップダウン メニューから [**インポート**] をクリックします。
   サーバープロファイルのインポート ページが表示されます。
2. 詳細を入力し、必要な **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: サーバプロファイルは、既存の RAID 設定とともにエクスポートされます。ただし、サーバまたはサーバグループの RAID 設定を含む、または除外するサーバプロファイルをインポートできます。**データの保存** はデフォルトで選択されており、サーバ内の既存の 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、このチェックボックスをオフにします。

3. サーバプロファイルをインポートするには、**終了** をクリックします。

交換したコンポーネントに対するファームウェアおよび構成設定の適用

部品交換の自動アップデート機能によって、交換したサーバコンポーネントは必要なファームウェアバージョンか以前のコンポーネントの設定、またはその両方にアップデートされます。コンポーネントを交換した後でサーバを再起動すると、アップデートが自動的に実行されます。

部品交換用の構成を設定するには、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、サーバーまたはサーバーのグループを選択してから、[**部品交換**] をクリックします。

   メモ: **部品交換** にポインタを合わせると、オプション名が **部品交換設定** に展開されます。

   部品交換設定 ウィンドウが表示されます。
2. **CSIOR**、**部品ファームウェアアップデート**、**部品設定のアップデート** を次のいずれかのオプションに設定し、**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。
     - **有効** - サーバ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。
     - **無効** - サーバ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。
     - **サーバの値を変更しない** - 既存のサーバ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。
     - **無効** - 部品ファームウェアアップデートの機能は無効にされ、交換したコンポーネントに同じ設定が適用されます。
     - **バージョンのアップグレードのみを許可** - 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のバージョンが交換したコンポーネントに適用されます。

- **交換部品のファームウェアを一致させる** - 新しいコンポーネント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。
- **サーバの値を変更しない** - コンポーネントの既存の設定が保持されます。

- 部品設定のアップデート - 選択に基づいて、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。
  - **無効** - 部品設定のアップデートの機能は無効にされ、古いコンポーネントの保存された設定は交換したコンポーネントに適用されません。
  - **常に適用** - 部品設定のアップデートの機能が有効にされ、古いコンポーネントの保存された設定は交換したコンポーネントに適用されます。
  - **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された設定は、ファームウェアバージョンが一致している場合にのみ、交換したコンポーネントに適用されます。
  - **サーバの値を変更しない** - 既存の設定が保持されます。

サーバの LC ログの収集

LC ログは、管理対象サーバ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は、推奨処置に関する詳細情報およびトラブルシューティングの際に役立つテクニカル情報を提供するため、サーバ管理者には有益です。

LC ログからさまざまなタイプの情報を入手できます。たとえば、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、アップデートまたは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、アクティビティ開始時の詳細なタイムスタンプ、アクティビティの重大度などがあります。

エクスポートされた LC ログファイルはフォルダに保存され、そのフォルダにはサーバのサービスタグを使用して名前が付けられます。LC ログは、`<YYYYMMDDHHMMSSSSS>.<file format>`の形式で保存されます。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。

LC ログを収集するための 2 つのオプションがあります：

- LC 完了ログ - アクティブ LC ログファイルとアーカイブされた LC ログファイルをエクスポートします。サイズが大きいため、`.gz` 形式に圧縮されて、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。
- アクティブ LC ログ - 最近の LC ログファイルをただちにエクスポートするか、ジョブをスケジュールして定期的にログファイルをエクスポートします。これらのログ ファイルを表示、検索、および OMIMSSC アプライアンスにエクスポートします。さらに、ログファイルのバックアップをネットワーク共有に保存することもできます。

LC ログを収集するには、次の手順を実行します。

1. OMIMSSC で、[**メンテナンス センター**] をクリックします。サーバーまたはサーバーのグループを選択し、[**LC ログ**] ドロップダウン メニューをクリックして、[**LC ログの収集**] をクリックします。
2. **LC ログの収集** で次のいずれを選択し、**終了** をクリックします。
   - **LC 完了ログのエクスポート (.gz)** - Windows の資格情報を提供することにより、LC 完了ログが CIFS ネットワーク共有にエクスポートされます。
   - **アクティブ ログのエクスポート (今すぐ実行)** - 選択すると、アクティブ ログがすぐに OMIMSSC アプライアンスにエクスポートされます。
     - （オプション）**LC ログをネットワーク共有にバックアップ** チェックボックスを選択すると、Windows の資格情報を提供することにより、LC ログのバックアップが CIFS ネットワーク共有上に保存されます。
   - **LC ログ収集のスケジュール** - アクティブログが定期的にエクスポートされます。

     LC ログ収集のスケジュール で、ログファイルをエクスポートする日時を選択します。

     ファイルをエクスポートする頻度に応じて、ラジオボタンを選択します。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：

     - **行わない** - このオプションはデフォルトで選択されています。スケジュールされた時間に一度だけ LC ログをエクスポートする場合に選択します。
     - **日次** - 毎日スケジュールされた時間に LC ログをエクスポートする場合に選択します。
     - **週に 1 回** - 週に 1 回スケジュールされた時間に LC ログをエクスポートする場合に選択します。
     - **4 週間に 1 回**- 4 週間に 1 回スケジュールされた時間に LC ログをエクスポートする場合に選択します。
     - （オプション）**LC ログをネットワーク共有にバックアップ** チェックボックスを選択すると、Windows の資格情報を提供することにより、LC ログのバックアップが CIFS ネットワーク共有上に保存されます。

     メモ: エクスポートされるファイルのサイズが大きいため、十分なストレージ容量を持つ共有フォルダを指定してください。

   このジョブを追跡するには、デフォルトで **ジョブリストへ移動** オプションが選択されています。

LC ログの表示

すべてのアクティブな LC ログの表示、詳細な説明の検索、および CSV 形式でのログのダウンロードができます。

『*System Center Configuration Manager および System Center Virtual Machine Manager 用 Dell EMC OpenManage Integration for Microsoft System Center バージョン 7.2.1 ユーザー ガイド*』の「*ブラウザー設定*」セクションで説明されているように、OMIMSSC アプライアンスを [**ローカル イントラネット サイト**] リストに追加します。

1. OMIMSSC で、[**メンテナンス センター**] をクリックします。サーバーまたはサーバーのグループを選択し、[**LC ログ**] ドロップダウン メニューをクリックして、[**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 ログファイルのすべてのログエントリが表示されます。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ための 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文を入力すると、その説明文を持つインスタンスが含まれるすべての LC ファイルが表示されます。

   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 ログメッセージで表示される時間は、iDRAC のタイムゾーンに従います。

ファイルの説明

このページを使用して、推奨されるアクションに関する詳細情報や、特定のサーバのトラッキングやアラートの目的に役立つさまざまな技術情報を表示します。

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できます。
- アクティビティに関してユーザーから提供され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、検索結果のみが CSV ファイルにエクスポートされます。

メモ: メッセージが長い場合、メッセージは 80 文字に切り捨てられます。

メモ: **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

選択したサーバまたはサーバのグループのインベントリを XML または CSV 形式のファイルにエクスポートします。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できます。このインベントリ情報を使用して、アップデートソースに参照インベントリファイルを作成します。

『*System Center Configuration Manager および System Center Virtual Machine Manager 用 Dell EMC OpenManage Integration for Microsoft System Center バージョン 7.2.1 ユーザーズ ガイド*』の「*ブラウザー設定*」セクションで説明されているように、ブラウザーが設定されていることを確認します。

メモ: 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できます。

メモ: サーバのコンポーネント情報のみを選択してエクスポートしても、サーバ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、[**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。

   ファイルは、選択に基づいて CSV または XML 形式でエクスポートされます。このファイルは、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のファームウェアバージョン、そのコンポーネントに対するアップデートアクションなどの詳細で構成されます。

スケジュール済みジョブのキャンセル

ジョブが **スケジュール済み** 状態であることを確認します。

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、**メンテナンスセンター** をクリックし、**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、**ジョブとログセンター** をクリックし、**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、**キャンセル** をクリックし、確定するには **はい** をクリックします。

21

デバイスのプロビジョニングに使用：OMIMSSC

この章では、OMIMSSC を使用して、オペレーティング システムの検出と導入、クラスターの作成、および Dell EMC デバイスの保守を行うための高度な詳細について説明します。

トピック：

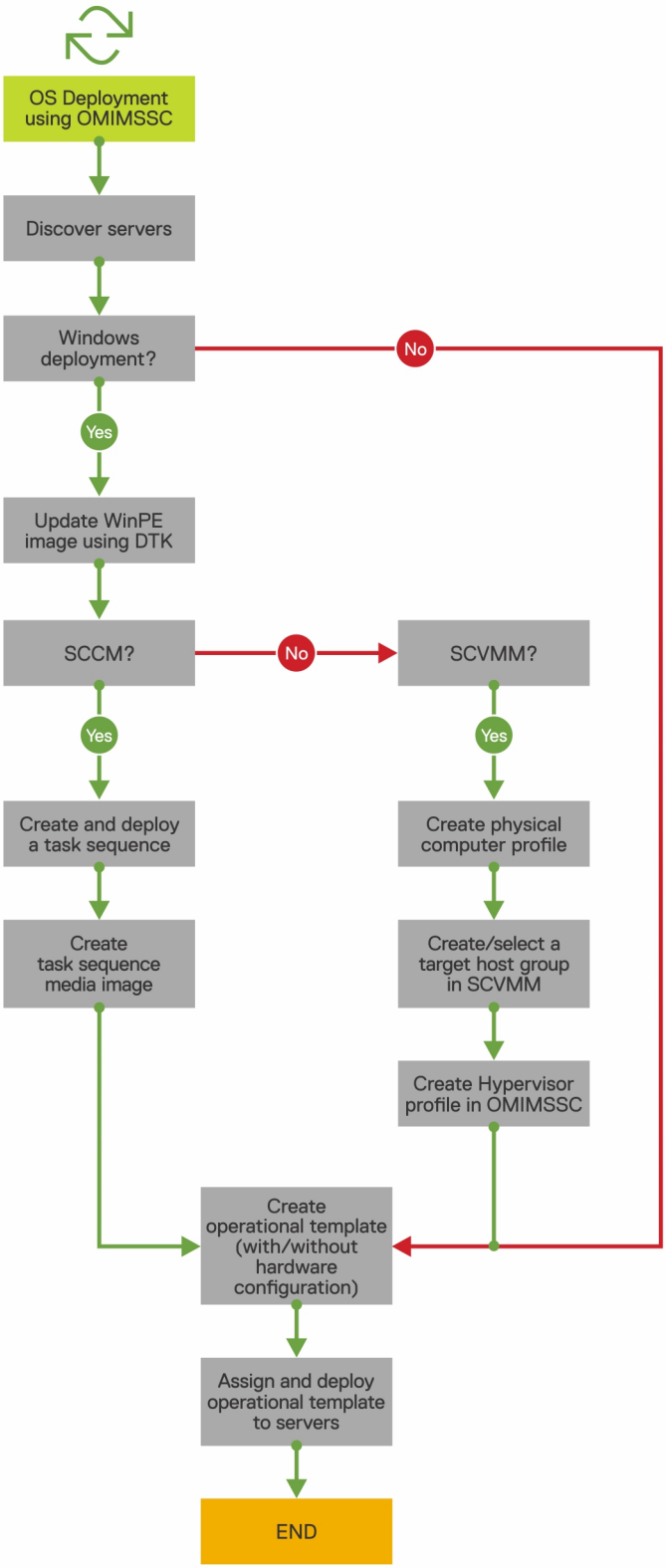
- 導入シナリオのワークフロー
- 事前定義された Operational Template（運用テンプレート）を使用した Storage Spaces Direct クラスターの作成
- デバイスをメンテナンスするためのワークフロー

導入シナリオのワークフロー

Operational Template（運用テンプレート）を使用した SCCM または SCVMM 環境への Windows および Windows 以外のオペレーティング システムの導入を、OMIMSSC を使用して行います。

メモ: オペレーティング システムを導入する前に、デバイス ファームウェアのバージョンを `ftp.dell.com` または `downloads.dell.com` にある最新バージョンにアップグレードしてください。

次の図に、OMIMSSC でのオペレーティング システムの導入事例を示します。



SCCM 用の OMIMSSC コンソール拡張機能を使用した Windows OS の導入

OMIMSSC を使用して SCCM コンソールから Windows OS を導入するには、次の手順に従います。

メモ: ホストサーバに OS を導入する前に、SCCM で **サーバ** のクライアントステータスが **なし** であることを確認します。

1. 最新の Dell EMC Deployment Toolkit (DTK) をダウンロードし、Windows プレインストール環境 (WinPE) のブート WIM 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 .WIN イメージを SCCM コンソールにインポートし、SCCM にブート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 を使用して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。

   メモ: タスクシーケンスメディアの作成時に無人 OS 導入を有効にするには、**メディアのタイプを選択** して、**無人オペレーティングシステム導入を許可** チェックボックスをオンにします。

5. **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. 検出されたサーバの詳細をすべてキャプチャして、Operational Template (運用テンプレート) を作成します。詳細については、「参照サーバからの運用テンプレートの作成」を参照してください。
7. 管理対象デバイスに Operational Template (運用テンプレート) を割り当て、テンプレートのコンプライアンスを確認します。詳細については、「運用テンプレートの割り当ておよび運用テンプレートのコンプライアンスの実行」を参照してください。
8. 運用テンプレート を展開して、デバイステンプレートを準拠させます。詳細については、「運用テンプレートの導入」を参照してください。
9. **ジョブとログセンター** ページで、オペレーティングシステムの導入のジョブステータスを表示します。詳細については、「ジョブとログセンターの起動」を参照してください。

SCVMM 用の OMIMSSC コンソール拡張機能を使用したハイパーバイザーの導入

ハイパーバイザー導入のためのさまざまなシナリオは、次のとおりです。

表 10. ハイパーバイザー導入のシナリオ

状態	アクション
工場出荷時の最新の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) ドライバインジェクションを有効にします。
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) を作成する際に、変更を必要としないすべてのコンポーネントのチェックボックスをオフにします。

OMIMSSC を使用して SCVMM コンソールからハイパーバイザーを導入するには、次の手順を実行します。

1. 最新の Dell EMC Deployment ToolKit (DTK) をダウンロードして、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と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。
3. SCVMM 用 OMIMSSC コンソール拡張機能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。
4. 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。
5. 検出されたサーバの詳細をすべてキャプチャして、運用テンプレートを作成します。詳細については、「参照サーバからの運用テンプレートの作成」を参照してください。
6. 管理対象デバイスに運用テンプレートを割り当て、テンプレートのコンプライアンスを確認します。詳細については、「運用テンプレートの割り当ておよび運用テンプレートのコンプライアンスの実行」を参照してください。
7. 運用テンプレート を展開して、デバイステンプレートを準拠させます。詳細については、「運用テンプレートの導入」を参照してください。
8. ジョブとログセンター ページで、オペレーティングシステムの導入のジョブステータスを表示します。詳細については、「ジョブとログセンターの起動」を参照してください。

Windows OS の再展開に使用： OMIMSSC

SCCM 用の OMIMSSC コンソール拡張機能または SCVMM 上の OMIMSSC コンソール拡張機能を使用してサーバーに Windows OS を再展開するには、次の手順を実行します。

1. Microsoft コンソールからサーバを削除します。詳細については、Windows のマニュアルを参照してください。
2. サーバーを再検出するか、登録されている Microsoft コンソールと OMIMSSC を同期します。サーバーは、OMIMSSC で未割り当てのサーバーとして追加されます。検出の詳細については、「手動検出を使用したサーバの検出」を参照してください。同期の詳細については、「登録済みの Microsoft コンソールとの同期」を参照してください。
3. 検出されたサーバの詳細をすべてキャプチャして、Operational Template（運用テンプレート）を作成します。詳細については、「参照サーバからの運用テンプレートの作成」を参照してください。
4. 管理対象デバイスに Operational Template（運用テンプレート）を割り当て、テンプレートのコンプライアンスを確認します。詳細については、「運用テンプレートの割り当ておよび運用テンプレートのコンプライアンスの実行」を参照してください。
5. 運用テンプレート を展開して、デバイステンプレートを準拠させます。詳細については、「運用テンプレートの導入」を参照してください。
6. **ジョブとログセンター** ページで、オペレーティングシステムの導入のジョブステータスを表示します。詳細については、「ジョブとログセンターの起動」を参照してください。

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

OMIMSSC を使用して Windows 以外の OS を導入するには、次の手順を実行します。

メモ: OMIMSSC 経由で Windows 以外の OS を導入する手順は、Microsoft コンソールでは共通です。

1. **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。
2. 検出されたサーバの詳細をすべてキャプチャして、Operational Template（運用テンプレート）を作成します。詳細については、「参照サーバからの運用テンプレートの作成」を参照してください。
3. 管理対象デバイスに Operational Template（運用テンプレート）を割り当て、テンプレートのコンプライアンスを確認します。詳細については、「運用テンプレートの割り当ておよび運用テンプレートのコンプライアンスの実行」を参照してください。
4. 運用テンプレート を展開して、デバイステンプレートを準拠させます。詳細については、「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て SCCM の **Managed Lifecycle Controller Lifecycle Controller（ESXi）** コレクションには移動されません。

事前定義された Operational Template（運用テンプレート）を使用した Storage Spaces Direct クラスターの作成

OMIMSSC を使用してクラスターを作成するには、次の手順を実行します。

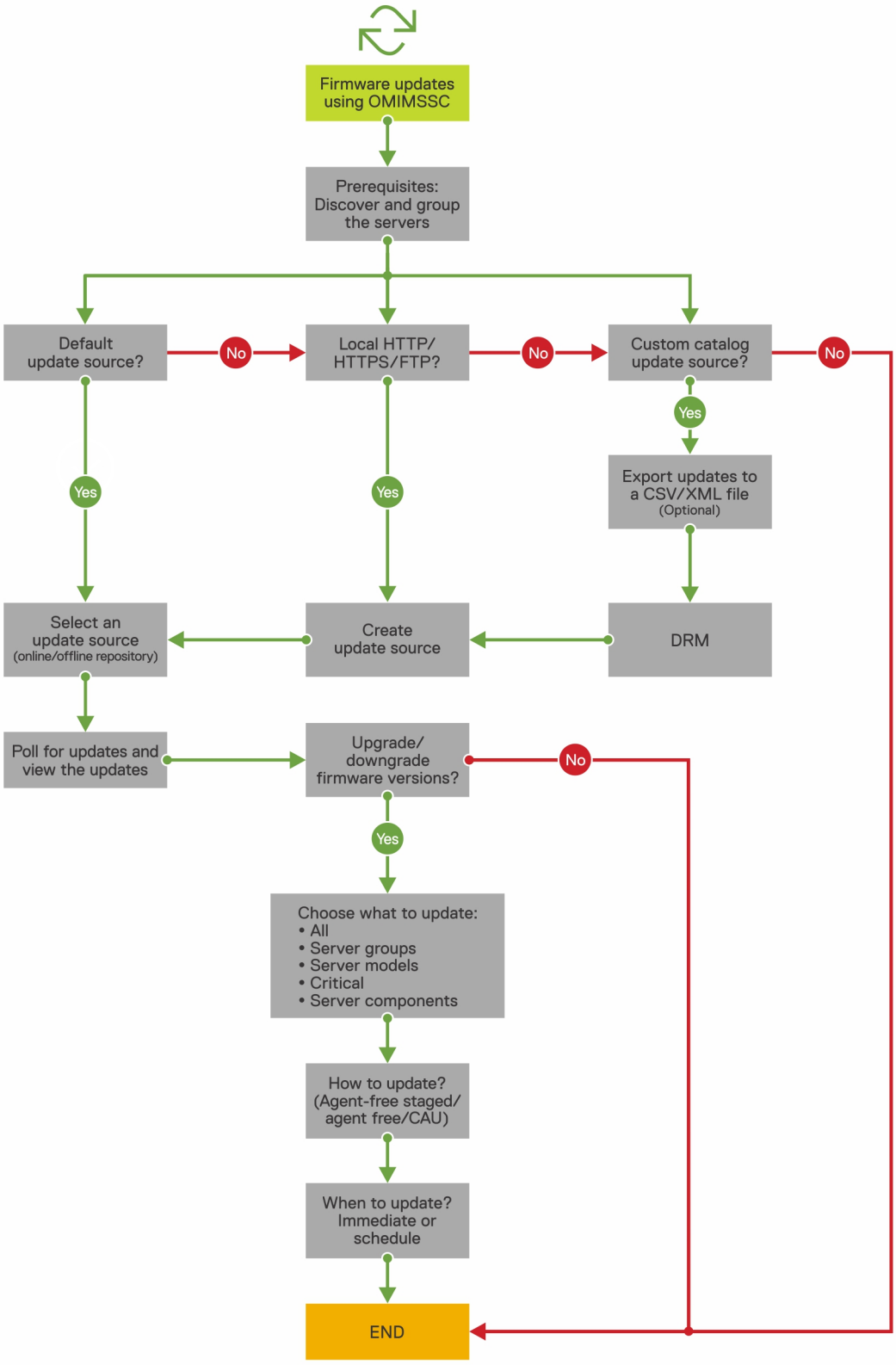
1. **検出** ページを使用して、参照サーバを検出します。詳細については、「手動検出を使用したサーバの検出」を参照してください。
2. 事前定義された Operational Template（運用テンプレート）を編集します。詳細については、「Operational Template（運用テンプレート）の変更」を参照してください。
3. 論理スイッチを作成します。詳細については、「論理スイッチの作成」を参照してください。
4. Storage Spaces Direct クラスターを作成します。詳細については、「Storage Spaces Direct クラスターの作成」を参照してください。

デバイスをメンテナンスするためのワークフロー

OMIMSSC で検出されたデバイスをメンテナンスします。

サーバおよび MX7000 デバイスのファームウェアのアップデート

次の図に、ファームウェアアップデートのワークフローを示します。



次のアップデートソースを使用して、選択したデバイスをアップデートできます。

- オンライン FTP またはローカル FTP ソース
- オンライン HTTP またはローカル HTTP ソース
- オンライン HTTPS またはローカル HTTPS ソース
- ローカル Dell Repository Manager（DRM）ソース

1. デフォルトのアップデートソースを作成または選択します。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。

メモ: ポーリングと通知の機能を使用して、最新のカタログでアップデートソースをアップデートしてください。ポーリングと通知の詳細については、「ポーリングと通知」を参照してください。

Storage Spaces Direct クラスターをアップデートする場合は、Storage Spaces Direct クラスター固有の事前定義されたアップデート ソースを選択します。これらのアップデートソースは、**メンテナンスセンター** ページにのみ表示されます。

Mx7000 デバイスをアップデートする場合は、モジュラー型システムに固有の事前定義されたアップデート ソースを選択します。これらのアップデートソースは、**メンテナンスセンター** ページにのみ表示されます。

2. デフォルトのアップデートグループを作成または選択します。アップデートソースの詳細については、「アップデートグループ」を参照してください。
3. デバイスを検出するか、登録されている Microsoft コンソールと同期し、デバイスインベントリが最新であることを確認します。検出と同期の詳細については、「デバイスの検出と同期」を参照してください。サーバインベントリの詳細については、「サーバビューの起動」を参照してください。
4. 次のいずれかのオプションを使用して、デバイスをアップデートします。
   - 必要なデバイスを選択して、**アップデートの実行** をクリックします。詳細については、「アップデートの実行を使用したファームウェアバージョンのアップグレードまたはダウングレード」を参照してください。

     メモ: デバイスコンポーネントのファームウェアをダウングレードするには、**ダウングレードを許可** チェックボックスをオンにします。このオプションが選択されていない場合、ファームウェアのダウングレードを必要とするコンポーネントに対するアクションは実行されません。
   - Operational Template (運用テンプレート) でファームウェアアップデートのコンポーネントを選択し、このテンプレートを展開します。Operational Template (運用テンプレート) の詳細については、「Operational Template (運用テンプレート) 」を参照してください。

交換したコンポーネントの設定

交換したコンポーネントのファームウェアのバージョンまたは設定を古いコンポーネントと一致させるには、「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

特定のインスタンスでサーバプロファイルをエクスポートし、そのプロファイルをインポートしてサーバを復元します。

1. 保護ボールトを作成します。保護ボールトの作成についての詳細は、「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。サーバプロファイルのエクスポートについての詳細は、「サーバプロファイルのエクスポート」を参照してください。
3. サーバプロファイルを、エクスポート元と同じサーバにインポートします。サーバプロファイルのインポートについての詳細は、「サーバプロファイルのインポート」を参照してください。

   メモ: RAID 設定を含むサーバプロファイルは、RAID 設定がプロファイルにエクスポートされている場合にのみインポートできます。

22

設定と導入

検出

1. OMIMSSC コンソールで、次のいずれかの手順を実行します。
   - ダッシュボードで、**サーバを検出** をクリックします。
   - ナビゲーション ペインで、**設定と導入** をクリックし、**サーバビュー** をクリックして、**検出** をクリックします。
2. **検出** をクリックします。

変更内容を表示するには、[**認定資格プロフィール**] ページを更新します。

トピック：

- 使用例
- 運用テンプレートの作成
- インストーラフォルダ
- 運用テンプレートの割り当て
- 運用テンプレートの導入
- SCCM 用の OMIMSSC コンソール拡張機能用の Windows OS コンポーネント
- SCVMM 用の OMIMSSC コンソール拡張機能用の Windows コンポーネント
- SCCM/SCVMM 用の OMIMSSC コンソール拡張機能用の Windows 以外のコンポーネント
- 登録した MSSC での検出
- サーバープロファイルのインポート
- サーバープロファイルのエクスポート
- LC ログの表示
- LC ログの収集
- 部品交換
- ポーリングと通知
- iDRAC の起動
- 入力出力モジュールの起動
- 同期化エラーの解決
- OMIMSSC と登録済み Microsoft コンソールの同期
- Azure Stack HCI クラスターの導入

使用例

1. **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。
2. 検出されたサーバの詳細をすべてキャプチャして、Operational Template (運用テンプレート) を作成します。詳細については、「参照サーバからの運用テンプレートの作成」を参照してください。
3. 管理対象デバイスに Operational Template (運用テンプレート) を割り当て、テンプレートのコンプライアンスを確認します。詳細については、「運用テンプレートの割り当ておよび運用テンプレートのコンプライアンスの実行」を参照してください。
4. Operational Template (運用テンプレート) を展開して、デバイステンプレートを準拠させます。詳細については、「運用テンプレートの導入」を参照してください。
5. **ジョブとログセンター** ページで、オペレーティングシステムの導入のジョブステータスを表示します。詳細については、「ジョブとログセンターの起動」を参照してください。

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、次のタスクが完了していることを確認します。

- **検出** 機能を使用して、参照サーバを検出します。サーバの検出の詳細については、「手動検出を使用したサーバの検出」を参照してください。
- **検出**機能を使用して、モジュラー型システムを検出します。モジュラー型システムの検出の詳細については、「手動検出を使用したモジュラー型システムの検出」を参照してください。
- デフォルトのアップデートソースを使用していない場合は、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。
- SCCM ユーザーの場合：
  - 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場合は、デバイス タイプの認定資格プロフィールを用意します。詳細については、「認定資格プロフィールの作成」を参照してください。
- SCVMM ユーザーの場合：
  - 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の詳細については、「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。
  - Windows 導入の場合は、デバイス タイプの認定資格プロフィールを用意します。詳細については、「認定資格プロフィールの作成」を参照してください。

1. OMIMSSC で、次のいずれかの操作を実行して Operational Template (運用テンプレート) を開きます。
   - OMIMSSC ダッシュボードで、[**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、**プロファイル** > **運用テンプレート** を順にクリックして、**作成** をクリックします。

   運用テンプレート ウィザードが表示されます。
2. **作成** をクリックします。
   運用テンプレート ウィザードが表示されます。
3. テンプレートの名前と説明を入力します。
4. デバイスのタイプを選択し、参照デバイスの IP アドレスを入力して、**次へ** をクリックします。

   メモ: iDRAC 2.0 以降の参照サーバの構成をキャプチャできます。

5. **デバイスコンポーネント** で、コンポーネントをクリックすると、使用可能な属性とその値が表示されます。
   コンポーネントは次のとおりです。
   - ファームウェアアップデート
   - RAID、NIC、および BIOS などのハードウェアコンポーネント。

     メモ: iDRAC Embedded 1 コンポーネントでは、**ユーザー管理者権限** 属性の権限と値は次のとおりです。

     表 11. 権限値テーブル

値	権限
1	ログイン
2	設定
4	ユーザーの設定
8	ログ
16	システム制御
32	仮想コンソールへのアクセス
64	仮想メディアへのアクセス
128	システム操作
256	デバッグ
499	オペレータ権限

   - オペレーティングシステム—Windows、ESXi、または RHEL のいずれかを選択します。
6. 水平スクロールバーを使用してコンポーネントを探します。コンポーネントを選択し、グループを展開して、その属性値を編集します。垂直スクロールバーを使用して、コンポーネントのグループと属性を編集します。
7. Operational Template (運用テンプレート) が適用されると、選択したコンポーネントの設定が管理対象デバイスに適用されるため、各コンポーネントに対してチェックボックスをオンにします。ただし、参照デバイスのすべての設定がキャプチャされ、テンプレートに保存されます。

メモ: チェックボックスで各コンポーネントに対して行った選択に関係なく、すべての設定がテンプレートに取り込まれます。

オペレーティングシステム コンポーネントで、要件に応じて次のいずれかのオプションの手順を実行します。

- SCCM での Windows オペレーティング システムの導入については、「SCCM 用の OMIMSSC コンソール拡張機能用の Windows コンポーネント」を参照してください。
- SCVMM での Windows オペレーティング システムの導入については、「SCVMM 用の OMIMSSC コンソール拡張機能用の Windows コンポーネント」を参照してください。
- OMIMSSC
- Windows 以外のオペレーティング システムの導入については、「OMIMSSC コンソール拡張機能用の Windows 以外のコンポーネント」を参照してください。

8. プロファイルを保存するには、**終了** をクリックします。

インストーラフォルダ

コンソール拡張機能をインストールすると、次のフォルダが作成されます。

- ログ—このフォルダは、コンソール関連のログ情報で構成されます。

メモ: ドメイン管理者アカウントとローカル管理者アカウントの資格情報が異なる場合は、SCCM または SCVMM へのログインにドメイン管理者アカウントを使用しないでください。代わりに、別のドメインユーザーアカウントを使用して SCCM または SCVMM にログインします。

運用テンプレートの割り当て

1. OMIMSSC で、[**設定と導入**] をクリックし、[**サーバー ビュー**] をクリックします。必要なサーバを選択して、**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。

   [**Operational Template (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. 必要なサーバを選択して、**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。
3. OMIMSSC で、[**設定と導入**] をクリックし、[**モジュラー型システム ビュー**] をクリックします。必要なモジュラー型システムを選択し、[**運用テンプレートの割り当て**] をクリックします。

   [**Operational Template (運用テンプレート) の割り当て**] ページが表示されます。
4. 必要なモジュラー型システムを選択し、[**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。

   [**Operational Template (運用テンプレート) の割り当て**] ページが表示されます。
5. **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から、**割り当て** をクリックします。

   Operational Template (運用テンプレート) ドロップダウンリストには、前のステップで選択したデバイスと同じタイプのテンプレートが表示されます。

   デバイスがテンプレートに準拠している場合は、チェックマークが付いた **緑色** のボックスが表示されます。

   Operational Template (運用テンプレート) がデバイスに正常に適用されていない場合、または Operational Template (運用テンプレート) のハードウェアコンポーネントが選択されていない場合は、**情報** シンボルボックスが表示されます。

   デバイスがテンプレートに準拠していない場合は、**警告** シンボルボックスが表示されます。割り当てられた Operational Template (運用テンプレート) にデバイスが準拠していない場合に限り、テンプレート名のリンクをクリックすることでサマリーレポートを表示できます。[**Operational Template (運用テンプレート) コンプライアンス サマリー レポート**] ページには、テンプレートとデバイスの相違点のサマリー レポートが表示されます。

   詳細レポートを表示するには、次の手順を実行します。

   a. **詳細なコンプライアンスの表示** をクリックします。ここでは、割り当てられたテンプレートとは異なる属性値を持つコンポーネントが表示されます。Operational Template (運用テンプレート) コンプライアンスのさまざまな状態が色別で表示されます。
      - 黄色の警告シンボル—準拠していません。デバイスの設定がテンプレートの値と一致しないことを表します。
      - 赤色のボックス—コンポーネントがデバイスに存在しないことを示します。

運用テンプレートの導入

メモ: Operational Template（運用テンプレート）の導入後に、資格情報を変更する属性を有効にしてデバイスにログインしないようにしてください。

1. OMIMSSC で、[**設定と導入**] をクリックし、[**サーバー ビュー**] をクリックします。テンプレートを適用したサーバを選択し、**Operational Template（運用テンプレート）の導入** をクリックします。
   Operational Template（運用テンプレート）の導入 ページが表示されます。
2. OMIMSSC で、[**設定と導入**] をクリックし、[**モジュラー型システム ビュー**] をクリックします。テンプレートを割り当てたモジュラー型システムを選択し、[**Operational Template（運用テンプレート）の導入**] をクリックします。
   Operational Template（運用テンプレート）の導入 ページが表示されます。
3. （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ているすべての属性を .CSV ファイルにエクスポートするには、**プール属性のエクスポート** をクリックします。エクスポートしない場合は、ステップ 4 に進みます。

   メモ: プールの値をエクスポートする前に、OMIMSSC コンソール拡張機能がインストールされている OMIMSSC アプライアンスの 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 ブラウザーで IP アドレスを追加する方法の詳細については、『*System Center Configuration Manager および System Center Virtual Machine Manager 用 Dell EMC OpenManage Integration for Microsoft System Center バージョン 7.2.1 ユーザー ガイド*』の「*ブラウザー設定*」セクションを参照してください。

4. 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ているすべての属性の値を .CSV ファイルに入力し、ファイルを保存します。**属性値プール** で、ファイルを選択してインポートします。

   .CSV ファイルの形式は次のとおりです： `attribute-value-pool.csv`

   メモ: iDRAC IP または iDRAC の認証情報が変更された後でジョブが OMIMSSC によって追跡されず、iDRAC でジョブが成功しても失敗とマークされる可能性があるため、すべて適切な属性を持つ.CSV ファイルを選択し、iDRAC IP または iDRAC の認証情報がテンプレートによって変更されないことを確認します。

5. 一意のジョブ名、ジョブの説明を入力し、**導入** をクリックします。

   このジョブを追跡するには、デフォルトで **ジョブリストへ移動** オプションが選択されています。

SCCM 用の OMIMSSC コンソール拡張機能用の Windows OS コンポーネント

1. タスクシーケンスと導入方法を選択します。

   メモ: ドロップダウンメニューには、コレクションに導入されているタスクシーケンスだけが表示されます。

   タスクシーケンスについての詳細は、「タスクシーケンス」を参照してください。

2. **導入方法** について、以下のいずれかのオプションを選択します。
   - **ネットワーク ISO で起動**—指定された ISO を再起動します。
   - **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。
   - **vFlash で再起動**—vFlash で再起動します。ISO が vFlash にあることを確認します。

     メモ: vFlash で再起動 オプションを使用するには、vFlash 上で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）ネットワーク共有にあるイメージを使用するには、**フォールバックとしてネットワーク ISO を使用** オプションを選択します。
4. LC ブートメディアイメージファイルを入力します。
5. オペレーティングシステムに必要なドライバを選択します。

SCVMM 用の OMIMSSC コンソール拡張機能用の Windows コンポーネント

[**ハイパーバイザー プロファイル**]、[**認定資格プロフィール**]、および [**サーバー IP 取得先**] を選択します。

メモ: ホスト名、および **サーバ管理 NIC** は常にプール値です。サーバー管理 NIC の場合は、オペレーティング システムが SCVMM と通信するために使用するネットワーク ポートの MAC アドレスを指定します。

サーバ IP 取得先 を **静的** として選択し、SCVMM で論理ネットワークを構成したことを確認すると、次のフィールドがプール値になります。

- **コンソール論理ネットワーク**
- **IP サブネット**
- **固定 IP アドレス**

SCCM/SCVMM 用の OMIMSSC コンソール拡張機能用の Windows 以外のコンポーネント

Windows 以外のオペレーティングシステム、オペレーティングシステムのバージョン、共有フォルダのタイプ、ISO ファイル名、ISO ファイルの場所、オペレーティングシステムのルートアカウントのパスワードを選択します。

(オプション) CIFS 共有にアクセスするための Windows タイプの認定資格プロフィールを選択します。

ホスト名はプール値であり、DHCP オプションを無効にすると、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**
- **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 以外のオペレーティングシステムの導入では、ネットワークファイルシステム (NFS) および Common Internet File System (CIFS) 共有タイプがサポートされます。

登録した MSSC での検出

検出後、サーバーは [**ホスト**] タブまたは [**未割り当て**] タブに追加されます。また、OMIMSSC と連携するために必要な最低限のバージョンの LC ファームウェア、iDRAC、および BIOS が搭載されている場合、そのホスト サーバーは準拠になります。

- オペレーティング システムがインストールされている PowerEdge サーバーを検出し、SCCM または SCVMM コンソールにすでに存在している場合、そのサーバーは、検出ジョブが開始されている OMIMSSC コンソールの [**ホスト**] タブの下にホスト サーバーとして表示されます。
  - ホストがモジュラー型サーバーの場合、サーバーを含むモジュラー型システムのサービス タグも表示されます。
  - 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。
- SCCM または SCVMM にリストされていない PowerEdge サーバーを検出すると、そのサーバーは登録されているすべての OMIMSSC コンソールの [**未割り当て**] タブに未割り当てサーバーとして表示されます。
- ライセンスは、サーバの検出後に使用されます。**ライセンスされたノード** 数は、ライセンスが検出されると減少します。

サーバープロファイルのインポート

1. OMIMSSC の [**メンテナンス センター**] で、プロファイルをインポートするサーバーを選択し、[**デバイス プロファイル**] ドロップダウン メニューから [**インポート**] をクリックします。
   サーバープロファイルのインポート ページが表示されます。
2. プロファイルをインポートするサーバーを選択し、[**デバイス プロファイル**] ドロップダウン メニューから [**インポート**] をクリックします。
   サーバープロファイルのインポート ページが表示されます。

サーバープロファイルのエクスポート

1. OMIMSSC で、[**メンテナンス センター**] をクリックします。プロファイルをエクスポートするサーバーを選択し、[**デバイス プロファイル**] ドロップダウン メニューから [**エクスポート**] をクリックします。
   サーバプロファイルのエクスポート ページが表示されます。
2. プロファイルをエクスポートするサーバーを選択し、[**デバイス プロファイル**] ドロップダウン メニューから [**エクスポート**] をクリックします。
   サーバプロファイルのエクスポート ページが表示されます。

LC ログの表示

1. OMIMSSC で、[**メンテナンス センター**] をクリックします。サーバーまたはサーバーのグループを選択し、[**LC ログ**] ドロップダウン メニューをクリックして、[**LC ログの表示**] をクリックします。
2. ログを表示するサーバーを選択し、[**LC ログ**] ドロップダウン メニューをクリックしてから、[**LC ログの表示**] をクリックします。

LC ログの収集

1. OMIMSSC で、[**メンテナンス センター**] をクリックします。サーバーまたはサーバーのグループを選択し、[**LC ログ**] ドロップダウン メニューをクリックして、[**LC ログの収集**] をクリックします。
2. ログをエクスポートするサーバーを選択し、[**LC ログ**] ドロップダウン メニューをクリックしてから、[**LC ログの表示**] をクリックします。

部品交換

1. OMIMSSC で、[**メンテナンス センター**] をクリックし、サーバーまたはサーバーのグループを選択してから、[**部品交換**] をクリックします。

   メモ: 部品交換 にポインタを合わせると、オプション名が **部品交換設定** に展開されます。

   部品交換設定 ウィンドウが表示されます。
2. 構成するコンポーネントを持つサーバを選択し、**部品交換** をクリックします。

   メモ: 部品交換 にポインタを合わせると、オプション名が **部品交換設定** に展開されます。

   部品交換設定 ウィンドウが表示されます。

ポーリングと通知

1. OMIMSSC で、[**メンテナンス センター**] をクリックし、[**ポーリングと通知**] をクリックします。
2. **ポーリングと通知** をクリックします。

iDRAC の起動

1. OMIMSSC で、[**設定と導入**] を展開し、以下のいずれかを選択します。
   - **サーバビュー** をクリックします。サーバ (ホストまたは未割り当てサーバの場合) に基づいて、**未割り当てサーバ** または **ホスト** タブをクリックし、サーバの **iDRAC IP** アドレスをクリックします。

     デフォルトでは **未割り当てサーバ** タブが表示されます。

     ホスト タブを表示するには、**ホスト** をクリックします。
   - **クラスタビュー** をクリックします。クラスタタイプを展開し、クラスタグループをサーバレベルに展開します。

サーバ タブが表示されます。

2. iDRAC コンソールを起動するには、**IP アドレス** をクリックします。
3. iDRAC コンソールを起動するには、**IP アドレス** をクリックします。

入力出力モジュールの起動

入力出力モジュール コンソールを起動するには、次の手順に従います。

1. OMIMSSC で、[**設定と導入**] を展開し、[**モジュラー型システム ビュー**] をクリックします。モデルを個々のデバイス レベルに展開します。

   そのモデルの下にあるすべてのデバイスが表示されます。
2. **I/O モジュール** タブをクリックします。
3. デバイスの **IP アドレス** をクリックします。

同期化エラーの解決

1. OMIMSSC で、[**設定と導入**] をクリックし、[**サーバー ビュー**] をクリックしてから、[**同期エラーの解決**] をクリックします。
2. **同期エラーの解決** をクリックします。

OMIMSSC と登録済み Microsoft コンソールの同期

1. OMIMSSC で、[**設定と導入**] をクリックし、[**サーバー ビュー**] をクリックして、[**OMIMSSC** との同期] をクリックし、登録した 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します。
2. 登録した MSSC に表示されているすべてのホストをアプライアンスと同期するには、**OMIMSSC と同期**] をクリックします。

   同期の実行タスクは長時間かかります。**ジョブおよびログ** ページでジョブステータスを表示します。

割り当ておよび導入

OMIMSSC で、[**設定と導入**] をクリックし、[**サーバー ビュー**] 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、**Operational Template (運用テンプレート) の導入** をクリックします。
Operational Template (運用テンプレート) の導入 ページが表示されます。

アップデートの実行

1. OMIMSSC で、[**メンテナンス センター**] をクリックし、サーバーまたはモジュラー型システム グループとアップデート ソースを選択してから、[**アップデートの実行**] をクリックします。
2. サーバーまたはモジュラー型システム グループとアップデート ソースを選択し、[**アップデートの実行**] をクリックします。
3. 一意のジョブ名、ジョブの説明を入力し、**作成** をクリックします。

   このジョブを追跡するには、デフォルトで **ジョブリストへ移動** オプションが選択されています。

Azure Stack HCI クラスターの導入

1. 必要な Windows とデバイス認定資格プロフィールを作成します。
2. WinPE イメージの作成
   a. SCVMM に WDS 機能をインストールしてから構成します。

b. [リソースの追加] を使用して SCVMM サーバーに PXE サーバーを追加し、同じサーバー名 (SCVMM ホスト名) PXE サーバーを指定します。
c. SCVMM サーバー内に共有フォルダーを作成し、Boot.wim を *C:\RemoteInstall\DCMgr\Boot\Windows\Images* から共有フォルダーにコピーします。
d. Dell EMC OpenManage deployment toolkit をダウンロードして、作成した共有フォルダーにこのファイルを展開します。たとえば、*\\Servername\sharefolder\DTK\DTK501* などです。
e. WinPE イメージを作成します。
f. WinPE イメージが SCVMM の共有フォルダーに配置されていることを確認します。

3. Windows Server 2016 および 2019 VM テンプレートを SCVMM ライブラリーに追加します。詳細については、Microsoft のマニュアルを参照してください。
   a. 次のプロパティを変更します。
   - オペレーティングシステム：Windows Server 2016 および 2019 Datacenter
   - 仮想化プラットフォーム：Microsoft Hyper-V

   メモ: OS の導入用の.iso ファイルを使用して Windows Server 2019 仮想ディスク (.vhdx) を作成するには、https://gallery.technet.microsoft.com/scriptcenter/Convert-WindowsImageps1-0fe23a8f を参照してください
4. SCVMM に物理コンピューター プロファイル (PCP) を作成します。[ハードウェア設定] > [ディスクとパーティション] で [**GUID パーティション テーブル**] としてパーティション構成を選択します。詳細については、ベアメタル PC からの Hyper-V ホストまたはクラスターのプロビジョニングに関する Microsoft マニュアルの「前提条件」セクションの「物理コンピューターのプロファイルの作成」セクションを参照してください。
5. Azure Stack HCI クラスターをホストするために、SCVMM にホスト グループを作成します。SCVMM でのホストグループの作成については、Microsoft のマニュアルを参照してください。
6. ハイパーバイザー プロファイルを作成します。
7. Dell EMC OpenManage 拡張機能でサーバーを検出します。
8. 事前定義された運用テンプレートを使用して構成します。
9. (オプション) コンプライアンスを確認します ([構成と導入] > [サーバー ビュー] > [サーバーの選択] および [運用テンプレートの割り当て])。
10. 論理スイッチの作成
11. Azure Stack HCI クラスターを導入します。
    クラスターの導入が正常に完了したことを確認するには、[**クラスター ビュー**] に移動して、クラスターがそれぞれのカテゴリでリストされているかどうかを確認します。

23

トラブルシューティングのシナリオ

トピック：

- 管理に必要なリソース： OMIMSSC
- SCCM 用 OMIMSSC コンソール拡張機能を使用するためのアクセス権の検証
- SCVMM 用 OMIMSSC コンソール拡張機能を使用するための PowerShell 許可の検証
- インストールおよびアップグレードのシナリオ： OMIMSSC
- OMIMSSC 管理ポータルのシナリオ
- 検出、同期、インベントリーのシナリオ： OMIMSSC
- 一般的なシナリオ： OMIMSSC
- ファームウェア アップデートのシナリオ： OMIMSSC
- OMIMSSC でのオペレーティングシステム導入シナリオ
- OMIMSSC でのサーバプロファイルのシナリオ
- OMIMSSC での LC ログシナリオ

管理に必要なリソース： OMIMSSC

このガイドでは、OMIMSSC で発生する問題について、必要な権限の確認および、その解決法について解説します。

OMIMSSC で発生する問題のトラブルシューティングでは、次のリソースが必要です。

- OMIMSSC アプライアンスにログインして、さまざまな操作を実行するのに必要な読み取り専用ユーザーのアカウントの詳細。

  OMIMSSC アプライアンス VM から読み取り専用ユーザーとしてログインする場合、ユーザー名は `readonly` と入力し、パスワードは OMIMSSC アプライアンス VM へのログインに使用したものと同じものを入力します。

- 次のような高レベルで包括的なエラーの詳細が記入されたログファイル：
  - アクティビティー ログ - OMIMSSC で開始されたジョブに関するユーザー固有の情報と高レベルの情報、および OMIMSSC で実行されたジョブのステータスが含まれています。アクティビティー ログを表示させるには、OMIMSSC コンソール拡張機能の［**ジョブおよびログ**］ページに移動します。
  - コンプリート ログ - 管理者関連のログおよび、OMIMSSC のシナリオに固有な各種の詳細なログが含まれています。コンプリート ログを表示させるには、**OMIMSSC 管理ポータル**の［**ジョブおよびログ**］ページに移動し、［**設定**］、［**ログ**］の順に選択します。
  - LC ログ - サーバー レベルの情報および、OMIMSSC で実行された操作に関する詳細なエラー メッセージが含まれています。LC ログをダウンロードして表示させる方法については、『*System Center Virtual Machine Manager および System Center Configuration Manager 用 Dell EMC OpenManage Integration for Microsoft System Center ユーザーズ ガイド*』を参照してください。

    メモ: iDRAC または OpenManage Enterprise Module（OME-Modular）ページから個々のデバイスをトラブルシューティングするには、OMIMSSC を起動して、［**設定と導入**］ページをクリックし、それぞれのビューを起動してデバイスの IP URL をクリックします。

メモ: SCVMM サーバーの管理者のユーザーは、 SCVMM のサービスアカウントにしないでください。

メモ: SC2012 VMM SP1 から SC2012 VMM R2 にアップグレードしている場合は、Windows PowerShell 4.0 へのアップグレードが必要です。

SCCM 用 OMIMSSC コンソール拡張機能を使用するためのアクセス権の検証

OMIMSSC のインストール後、登録ユーザーに次の権限があることを確認します。

1. OMIMSSC がインストールされているシステムで、*<Configuration Manager Admin Console Install Dir>\XmlStorage \Extensions\DLCPlugin* フォルダーへの [**書き込み**] アクセス権を、PowerShell コマンドを使用して付与します。

   OMIMSSC コンポーネントをインストールする前に、サイト サーバーおよび SMS プロバイダー サーバーで次の前提条件を満たすようにします。

   a. PowerShell で、`PSRemoting` コマンドを実行します。

      `PSRemoting` コマンドが無効化されている場合は、次のコマンドを使用して `PSRemoting` コマンドを有効化します。

      i. コマンド `Enable-PSRemoting` を実行します。

      ii. 確認メッセージで、「`Y`」を入力します。

   b. PowerShell で、`Get-ExecutionPolicy` コマンドを実行します。

      ポリシーが `RemoteSigned` に設定されていない場合は、次のコマンドを使用して `RemoteSigned` に設定します。

      i. コマンド `Set-ExecutionPolicy RemoteSigned` を実行します。

      ii. 確認メッセージで、「`Y`」を入力します。

2. Windows Management Instrumentation (WMI) へのユーザーアクセスを設定します。詳細については、「WMI へのユーザーアクセスの設定」を参照してください。
3. 受信トレイフォルダに、ファイルを書き込むための共有およびフォルダ許可を付与します。

   DDR 受信トレイにファイルを書き込むための共有およびフォルダー許可を付与するには、次の手順を実行します。

   a. Configuration Manager コンソールの **管理** で、**SMS_<サイトコード>** 共有に書き込みを行うためのユーザー許可を付与します。

   b. **エクスプローラー**を使用して、共有場所である **SMS_<サイトコード>**共有に移動し、次に `ddm.box` フォルダーに移動します。次のフォルダのドメインユーザーにフルコントロール権限を付与します。

      - **SMS_<サイトコード>**
      - 受信トレイ
      - `ddm.box`

WMI へのユーザーアクセスの設定

WMI へユーザーがリモートでアクセスできるように設定するには、次の手順を実行します。

メモ: システムのファイアウォールが WMI 接続をブロックしないことを確認します。

1. Distributed Component Object Model (DCOM) にリモートでアクセスするには、登録された SCCM ユーザーに権限を付与します。

   DCOM 用のユーザー許可を付与するには、次の手順を実行します。

   a. `dcomcnfg.exe` を起動します。

   b. **コンポーネントサービス** コンソールの左ペインで **コンピュータ** を展開し、**マイコンピュータ** を右クリックして **プロパティ** を選択します。

   c. **COM セキュリティ** で次の手順を実行します。

      - **アクセス許可** で **制限の編集** をクリックし、**リモートアクセス** を選択します。
      - **起動とアクティブ化のアクセス許可** で **制限の編集** をクリックし、**ローカルからの起動**、**リモートからの起動**、および **リモートからのアクティブ化** を選択します。

2. DCOM Config Windows Management and Instrumentation (WMI) コンポーネントにアクセスするには、登録ユーザーにユーザー権限を付与します。

   DCOM Config WMI 用のユーザー許可を付与するには、次の手順を実行します。

   a. `dcomcnfg.exe` を起動します。

   b. **[マイ コンピューター]** > **[DCOM Config]** の順に展開します。

   c. **Windows Management and Integration** を右クリックして、**プロパティ** を選択します。

   d. **セキュリティ** タブの **起動とアクティブ化のアクセス許可** で **編集** をクリックし、**リモートからの起動** および **リモートからのアクティブ化** の許可を選択します。

3. ネームスペース セキュリティを設定して、権限を付与します。

   ネームスペース セキュリティを設定し、アクセス許可を付与するには、次の手順を実行します。

   a. 次を起動します： `wmimgmt.msc`

   b. **WMI コントロール** ペインで、**WMI コントロール** を右クリックし、**プロパティ** を選択してから **セキュリティ** を選択します。

   c. `ROOT\SMS Namespace` に進みます。

d. **メソッドの実行**、**プロバイダーによる書き込み**、**アカウントの有効化**、**リモートの有効化の許可** を選択します。
e. `Root\cimv2\OMIMSSC` に進みます。
f. **メソッドの実行**、**プロバイダーによる書き込み**、**アカウントの有効化**、**リモートの有効化の許可** を選択します。
または、Configuration Manager ユーザーを **SMS_Admin** グループのメンバーにして、このグループの既存の許可に **リモートの有効化** を付与することもできます。

SCVMM 用 OMIMSSC コンソール拡張機能を使用するための PowerShell 許可の検証

PSRemoting ステータスが有効であり、**ExecutionPolicy** が **RemoteSigned** に設定されているかを確認します。ステータスが異なる場合は、PowerShell で次の手順を実行します。

a. PowerShell で、`PSRemoting` コマンドを実行します。
`PSRemoting` コマンドが無効化されている場合は、次のコマンドを使用して `PSRemoting` コマンドを有効化します。
i. コマンド `Enable-PSRemoting` を実行します。
ii. 確認メッセージで `Y` を入力します。
b. PowerShell で、`Get-ExecutionPolicy` コマンドを実行します。
ポリシーが `RemoteSigned` に設定されていない場合は、次のコマンドを使用して `RemoteSigned` に設定します。
i. コマンド `Set-ExecutionPolicy RemoteSigned` を実行します。
ii. 確認メッセージで `Y` を入力します。

インストールおよびアップグレードのシナリオ：OMIMSSC

ここでは、OMIMSSC のインストールおよびアップグレードに関するすべてのトラブルシューティング情報について説明します。

OMIMSSC アプライアンス VM 設定の確認

OMIMSSC アプライアンス VM が適切に設定されていることを検証するには、OMIMSSC アプライアンス VM を選択して右クリックして [**設定**] をクリックし、次のタスクを実行します。

1. OMIMSSC アプライアンスのメモリー割り当てが、『*System Center Configuration Manager および System Center Virtual Machine Manager 用 Dell EMC OpenManage Integration for Microsoft System Center バージョン 7.2.1 ユーザー ガイド*』の「*一般的な要件*」に記載されている要件に従っているかを確認します。足りない場合は、**スタートアップ RAM** にメモリを増設し、**適用** をクリックします。
2. プロセッサー数が、『*System Center Configuration Manager および System Center Virtual Machine Manager 用 Dell EMC OpenManage Integration for Microsoft System Center バージョン 7.2.1 ユーザー ガイド*』の「*一般的な要件*」に記載されている要件に従っているかを確認します。要件を満たしていない場合は、**プロセッサ数** の **仮想プロセッサ数** にプロセッサ数を指定します。
3. IDE コントローラーの [**仮想ハード ディスク**] フィールドを確認します。これには、**[IDE コントローラー 0]** > **[ハード ドライブ]** で [**OMIMSSC—v7**] ファイルを参照している [**仮想ハード ディスク**] を確認します。なければ、[**参照**] をクリックして VHD ファイルが解凍された場所を開き、**OMIMSSC—v7** ファイルを選択して [**適用**] をクリックします。
4. **[ネットワーク アダプター]** > **[仮想スイッチ]** で物理 NIC カードに接続されていることを確認して、接続されていなければ NIC カードを設定してください。[**仮想スイッチ**] ドロップダウン メニューで適切な NIC カードを選択して、[**適用**] をクリックします。

選択した仮想ハード ディスクで OMIMSSC アプライアンス用に新しく作成した仮想マシンが、カーネル パニックの例外で起動に失敗した場合は、仮想マシン設定を編集して、問題の仮想マシン用の動的メモリー オプションを有効にします。仮想マシン用の動的メモリー オプションの有効化は、次の手順で行えます。

1. OMIMSSC アプライアンス VM を右クリックして、[**設定**]、[**メモリー**] の順にクリックします。
2. **動的メモリ** で、**ダイナミックメモリを有効にする** チェックボックスを選択して、詳細を指定します。

登録の失敗

テスト接続または登録に失敗した場合に、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、次の手順を実行します。

- OMIMSSC アプライアンス VM に読み取り専用ユーザーとしてログインし、OMIMSSC アプライアンスから登録された SCCM または SCVMM サーバ FQDN に対して ping を実行します。応答があった場合、しばらく待ってから登録を続行します。

  OMIMSSC アプライアンス VM を読み取り専用ユーザーとして起動する場合、ユーザー名は `readonly` と入力し、パスワードは OMIMSSC アプライアンス VM へのログインに使用したものと同じものを入力します。

- SCCM または SCVMM サーバが実行されていることを確認します。
- コンソールの登録に使用する Microsoft アカウントは、System Center の管理者または委任管理であり、同じく System Center サーバのローカル管理者である必要があります。
- SCVMM ユーザー専用：
  - SCVMM サーバが他の OMIMSSC アプライアンスに登録されていないことを確認します。同じ SCVMM サーバを OMIMSSC アプライアンスに登録する場合は、**OMIMSSC 登録プロファイル**のアプリケーションプロファイルを SCVMM サーバから削除します。
  - SCVMM のロールアップがアップデート済みの場合、レジストリ (`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager AdministratorConsole\Settings`) の SCVMM コンソールの Indigo TCP ポート番号にチェックを入れます。ポート番号は、SCVMM コンソールの登録に使用されたものと同じものにする必要があります。デフォルトでは 8100 です。

テスト接続の失敗

ユーザー名は同じだが、パスワードはドメインユーザーアカウントとローカルユーザーアカウントとで異なる場合、Microsoft コンソールと OMIMSSC アプライアンス間の接続テストに失敗します。

たとえば、ドメインユーザーアカウントは `domain\user1` で、そのパスワードは `pwd1` だとします。そしてローカルユーザーアカウントは `user1` で、そのパスワードは `Pwd2` だとします。上記のドメインユーザーアカウントで登録しようとすると、テスト接続に失敗します。

この問題を回避するには、ドメインユーザーとローカルユーザーのアカウントで異なるユーザー名を使用するか、あるいは OMIMSSC アプライアンスでの Microsoft コンソール登録時に単一のユーザーアカウントをローカルユーザーとして使用します。

SCVMM 用 OMIMSSC コンソール拡張機能の接続の失敗

SCVMM 環境で OMIMSSC コンソール拡張機能を登録およびインストールした後、OMIMSSC を起動しようとすると、「`Connection to server failed`」というエラーが表示されます。

この問題を回避するには、次の手順を実行します。

1. OMIMSSC を起動させる時に、SCVMM コンソールで OMIMSSC アプライアンス IP と FQDN をローカル イントラネットに追加します。
2. OMIMSSC アプライアンスの IP と FQDN を DNS の **前方参照ゾーン** および **逆引き参照ゾーン** に追加します。
3. より詳しく調べるには、`C:\ProgramData\VMMLogs\AdminConsole` ファイルにエラーメッセージがないか確認します。

SCVMM R2 のアップデート後のコンソール拡張機能へのアクセスエラー

SC2012 R2 VMM 用アップデートロールアップの適用後に、インストール済みの OMIMSSC コンソールを開こうとすると、SCVMM によってセキュリティ上の理由によるエラーが表示され、OMIMSSC にアクセスできません。

回避策として、次の手順を実行します。

1. デフォルトパスにあるフォルダ `C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\<username>` を削除します。
2. SCVMM を再起動させます。

3. コンソール拡張機能を削除してから、『*System Center Configuration Manager および System Center Virtual Machine Manager 用 Microsoft System Center 向け Dell EMC OpenManage Integration インストール ガイド*』の「*SCVMM 用 OMIMSSC コンソール拡張機能のインポート*」の項での説明に従って、コンソール拡張機能をインポートします。

OMIMSSC アプライアンスに IP アドレスが割り当てられていない

OMIMSSC アプライアンス VM の作成および起動後に、OMIMSSC アプライアンスの IP アドレスが未割り当てとなっているか表示されません。

この問題を回避するには、仮想スイッチが物理スイッチにマップされているかを確認し、正しく設定されている場合は OMIMSSC アプライアンスに接続します。

OMIMSSC コンソール拡張機能のインポート中に SCVMM がクラッシュ

OMIMSSC コンソール拡張機能をインポートすると、SC2016 VMM RTM ビルド 4.0.1662.0 Administrator コンソールがクラッシュすることがあります。

この問題を回避するには、`support.microsoft.com/kb/4094925` にある KB の記事 4094925 を参照して SCVMM をアップグレードしてから、OMIMSSC コンソール拡張機能をインポートします。

OMIMSSC コンソール拡張機能へのログインに失敗

Microsoft コンソールへのログインに使用された異なる資格情報によって OMIMSSC コンソール拡張機能にログインした後、ログインアクティビティが失敗し、次のエラーメッセージが表示されます。`Username or Password is incorrect`

この問題を回避するには、OMIMSSC コンソール拡張機能へのログインに使用された資格情報を用いて、Microsoft コンソールへのログインおよび起動をします。これは 1 回限りのアクティビティです。

アップデート中の SC2012 VMM SP1 のクラッシュ

SC2012 VMM SP1 へのアップグレード後に OMIMSSC コンソール拡張機能を SC2012 VMM UR5 以降にインポートすると、SCVMM コンソールがクラッシュする場合があります。

この問題に関する情報と解決法については、`support.microsoft.com/kb/2785682` の URL にあるナレッジベースの 5 番目の記事を参照してください。

この問題を回避するには、インストールされているアップデートロールアップのすべてのバージョンに対して、SCVMM をアップデートします。

OMIMSSC 管理ポータルのシナリオ

ここでは、OMIMSSC の管理ポータルに関するすべてのトラブルシューティング情報について説明します

Mozilla Firefox ブラウザから OMIMSSC 管理ポータルへのアクセス時のエラーメッセージ

Mozilla Firefox ブラウザを使用して OMIMSSC 管理ポータルにアクセスすると、次の警告メッセージが表示されます。`"Secure Connection Failed".`

これを回避するには、ブラウザの admin portal の前回のエントリから作成された証明書を削除します。Mozilla Firefox ブラウザから証明書を削除する方法については、`support.mozilla.org` を参照してください。

OMIMSSC 管理ポータルに Dell EMC ロゴが表示されない

Windows 2016 のデフォルト IE ブラウザで OMIMSSC 管理ポータルが起動される場合、管理ポータルでの Dell EMC ロゴの表示がされません。

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。
- ブラウザの閲覧履歴を削除してから、OMIMSSC 管理ポータルの URL をブラウザのお気に入りリストに追加します。

検出、同期、インベントリーのシナリオ：OMIMSSC

ここでは、OMIMSSC 使用時における、認証情報の問題、サーバーの検出、サーバーのグループ化、登録済み Microsoft コンソールと OMIMSSC の同期に関するすべてのトラブルシューティング情報について説明します。

サーバの検出の失敗

1 つの OMIMSSC アプライアンスに複数の Microsoft コンソールが登録されている場合、サーバ検出を試みて到達不可能な SCCM コンソールがあると、サーバ検出ジョブは失敗します。

この問題を回避するには、到達不能な SCCM コンソールの登録を解除するか、エラーを修正して SCCM コンソールが OMIMSSC アプライアンスからアクセス可能になるようにします。

検出されるサーバが すべての Dell Lifecycle Controller サーバ コレクションに追加されていない

SCCM コンソール拡張機能用の OMIMSSC で検出されるサーバが、**すべての Dell Lifecycle Controller サーバ** コレクションに追加されていないことがあります。

この問題を回避するには、**すべての Dell Lifecycle Controller サーバ** コレクションを削除してからサーバを検出します。SCCM 中にコレクションが自動的に作成され、このグループにサーバが追加されます。

正しくない資格情報によるサーバ検出の失敗

検出時に誤った資格情報を入力してしまった場合、iDRAC のバージョンに応じて次の解決策を使用できます。

- iDRAC バージョン 2.10.10.10 以降の第 12 世代の PowerEdge サーバーの検出時、誤った詳細が認定資格プロフィールで提供されている場合、そのサーバーの検出は次の動作により失敗します。
  - 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、正しい認定資格プロフィー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。
- サーバーが検出され、アプライアンスに追加された後にデフォルトの iDRAC 認定資格プロフィールが変更された場合、サーバー上ではアクティビティを実行できません。サーバーを利用するには、新しい認定資格プロフィールを使用してサーバーを再検出します。

サーバ検出後の不正な VRTX シャーシグループの作成

別のシャーシに存在していたモジュラーサーバを VRTX シャーシに追加し、それが OMIMSSC で検出された場合、そのモジュラーサーバで以前のシャーシサービスタグ情報が引き続き使用されます。そのため、最新のシャーシ情報ではなく古いシャーシ情報が保持された VRTX シャーシグループがアプライアンスに作成されます。

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。

ホスト サーバーは登録済み SCCM と同期できない

OMIMSSC コンソール拡張を登録済み SCCM と同期している間、サーバーは同期ジョブにサブ タスクとしてリストされないため、同期されません。

この問題を回避するには、SCCM コンソールを「管理者権限で実行」で起動し、サーバーの帯域外設定をアップデートします。次に、OMIMSSC コンソール拡張機能を登録済み SCCM と同期します。

詳細については、『*System Center Configuration Manager および System Center Virtual Machine Manager 用 OpenManage Integration for Microsoft System Center バージョン 7.2.1 ユーザーズ ガイド*』の「登録済み Microsoft コンソールとの同期」トピックを参照してください。

空のクラスタアップデートグループが自動検出または同期化中に削除されない

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

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

再検出されたサーバでのメンテナンス関連タスクの実行に失敗

OMIMSSC から特定のサーバまたはアップデートグループ内のすべてのサーバを削除して再検出した場合、これらのサーバで、ファームウェアの更新、LC ログのエクスポートとインポート、サーバプロファイルのエクスポートとインポートなど、その他の操作を実行することができません。

この問題を回避するには、削除されたサーバーまたはサーバー群を再検出した後に、[**サーバー ビュー**] にある [**運用テンプレートの導入**] 機能を使用してファームウェア アップデートを実行し、他のメンテナンス シナリオでは iDRAC を使用します。

一般的なシナリオ : OMIMSSC

ここで説明するトラブルシューティング情報は、OMIMSSC のどのワークフローにも依存しません。

CIFS 共有へのホスト名を使用したアクセスの失敗

モジュラーサーバによる CIFS 共有へのアクセスが、OMIMSSC でのどのジョブ実行用のホスト名を使用しても行えません。

この問題を回避するには、ホスト名ではなく CIFS 共有を持つサーバの IP アドレスを指定します。

コンソール拡張機能での ジョブおよびログ ページの表示の失敗

ジョブおよびログセンター ページが、OMIMSSC コンソール拡張機能に表示されません。

この問題を回避するには、コンソールを再登録してから、**ジョブおよびログ** ページを起動します。

管理下システムでのオペレーションの失敗

Transport Layer Security (TLS) のバージョンが原因となって、OMIMSSC のすべての機能が管理下システムで期待どおりに動作しません。

iDRAC ファームウェアバージョン 2.40.40.40 以降を使用している場合は、Transport Layer Security (TLS) バージョン 1.1 以降がデフォルトで有効に設定されています。コンソール拡張機能のインストール前にアップデートをインストールし、`Support.microsoft.com/en-us/kb/3140245` にある KB 記事を参照して TLS 1.1 以降を有効にします。TLS 1.1 以降のサポートを SCVMM サーバおよび SCVMM コンソールで有効にして、OMIMSSC が所定の作動をすることを確認することが推奨されます。iDRAC の詳細については、Dell.com/idracmanuals を参照してください。

OMIMSSC のオンラインヘルプの起動の失敗

Windows 2012 R2 オペレーティングシステムを使用している場合、コンテキスト依存のオンラインヘルプコンテンツが起動し、エラーメッセージが表示されます。

解決策としては、最新の KB 記事を参照してオペレーティングシステムを更新し、オンラインヘルプコンテンツを表示させます。

ファームウェア アップデートのシナリオ：OMIMSSC

ここでは、アップデートソース、アップデートグループ、リポジトリ、アップデート後のインベントリに関するすべてのトラブルシューティング情報について説明します。

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に失敗します。

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。

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

OMIMSSC をセットアップ、設定、アップグレード、または移行した後、デフォルトのアップデートソース **Dell Online カタログ**を用いた FTP サイトへのアクセスを試行すると、プロキシ資格情報を必要とする場合にアクセスに失敗することがあります。

この問題を回避して、アップデートソースとして **Dell Online カタログ**を用いた FTP サイトへのアクセスを行うには、アップデートソースを編集してプロキシ資格情報を追加します。

ローカルアップデートソースのテスト接続に失敗

ローカルアップデートソースの詳細を提供した後、必要なファイルにアクセスできないため、テスト接続が失敗することがあります。

この問題を回避するには、`catalog.gz` ファイルが次のフォルダ構造に存在することを確認します。

- ローカル HTTP アップデートソース用：`http:\\IP address\catalog\catalog.gz`
- ローカル FTP アップデートソース用：`ftp:\\IP address\catalog\catalog.gz`
- ローカル DRM アップデートソース用：`\\IP address\\catalog\<catalogfile>.gz`

DRM アップデートソースの作成に失敗

Windows 10 オペレーティン グシステム（OS）上で実行されている管理サーバーで DRM アップデート ソースの作成に失敗し、次のエラー メッセージが表示されることがあります：「`Failed to reach location of update source. Please try again with correct location and/or credentials.`」

次のエラー メッセージが表示された場合は、OMIMSSC 管理ポータルの **omimsscappliance_main** ログを参照してください：*`Unix command failed SmbException: com.dell.pg.tetris.business.samba.smbclient.SmbException: session setup failed: NT_STATUS_IO_TIMEOUTwhere EnableSMB1Protocol = false.`*

この問題を回避するには、*support.microsoft.com/en-us/help/4034314* にある KB 記事を参照してください。

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

アップデートソース作成中に指定された資格情報が正しくないか、OMIMSSC アプライアンスがアップデートソースにアクセスできないことが原因で、ファームウェアアップデート中にリポジトリを作成できない可能性があります。

この問題を回避するには、OMIMSSC アプライアンスのホスト先からアップデートソースにアクセス可能であることを確認し、アップデートソースの作成時に正しい資格情報を提供します。

OMIMSSC のアップグレードまたは移行後に比較レポートを表示できない

最新バージョンの OMIMSSC にアップグレードした後、`ftp.dell.com` または `downloads.dell.com` への接続に失敗した場合は、デフォルトの Dell Online FTP または Dell HTTP アップデートソースでカタログファイルをダウンロードできません。したがって、比較レポートは使用できません。

この問題を回避してデフォルトアップデートソースの比較レポートを表示させるには、デフォルトの Dell オンライン FTP、または Dell HTTP アップデートソースを編集し、プロキシ資格情報を作成してから、**アップデートソースの選択** ドロップダウンメニューからアップデートソースを選択します。アップデート ソースの編集の詳細については、『*System Center Configuration Manager および System Center Virtual Machine Manager 用 Microsoft System Center 向け Dell EMC OpenManage Integration ユーザーズ ガイド*』の「*アップデート ソースの変更*」の項を参照してください。

クラスタのファームウェアアップデートに失敗

OMIMSSC にクラスタのファームウェアのアップデートジョブが送信された後、何らかの理由によりクラスタがアップデートされず、**アクティビティログ**に次のエラーメッセージが表示されます。

```
Cluster Aware Update failed for cluster group <cluster group name>.
```

```
Failed to perform Cluster Aware Update for cluster group <cluster group name>.
```

メモ: Cluster Aware Update アクションは、Cluster Aware Update レポートが保存される: \\<SCVMM CIFS share>\OMIMSSC_UPDATE\reports フォルダーに記録されます。\\SCVMM CIFS share\OMIMSSC_UPDATE\reports\log フォルダーには、さらに各ノードの Dell EMC System Update (DSU) プラグイン ログが含まれます。拡張スクリプト ログは、C:\Window\Temp にあります。この場所には、S2D クラスター用の各クラスター ノードにある precau.log ファイルと postcau.log ファイルが含まれています。

クラスタのファームウェアアップデートに失敗する理由および、それらの回避策には、次のものがあります。

- 必要な DUP およびカタログファイルが、選択したローカルアップデートソースに存在しない場合。

  この問題を回避するには、すべての必要な DUP およびカタログファイルがリポジトリで使用できることを確認してから、クラスタのファームウェアをアップデートします。

- クラスタグループが応答しなくなる、あるいは進行中のジョブが原因となってファームウェアアップデートジョブが CAU でキャンセルされるなどの場合、DUP がダウンロードされ、クラスタグループに属す各サーバクラスタノードに配置されます。

  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、クラスタファームウェアをアップデートします。

- Lifecycle Controller (LC) が他の操作でビジーとなった場合、特定のクラスタノードでのファームウェアアップデートタスクは失敗します。アップデート失敗の原因が LC がビジー状態のためかを確認するには、`C:\dell\suu\invcolError.log` のパスにあるクラスタの各ノードで次のエラーメッセージを確認します。

  ```
  Inventory Failure: IPMI driver is disabled. Please enable or load the driver and then reboot the system.
  ```

  この問題を回避するには、サーバをシャットダウンし、電源ケーブルを取り外してから、サーバを再起動させます。再起動後、クラスタのファームウェアをアップデートします。

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

OMIMSSC 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、OMIMSSC メインログに次のエラーが表示されます。`JobQueue Exceeds the size limit. Delete unwanted JobID(s).`

この問題を回避するには、iDRAC 内の完了済み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。

DRM アップデートソースの使用時の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権が不十分な場合に DRM アップデートソースを使用すると、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、「`Local cache creation failure`」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、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、**詳細設定** をクリックします。
2. **継承を有効にする** をクリックして、**子オブジェクトのアクセス許可エントリすべてを、このオブジェクトからの継承可能なアクセス許可エントリで置き換える** オプションを選択し、**すべてのユーザー** 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。

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

ファームウェアアップデート中に、同一サーバの同じコンポーネントがアップデートされる現象が、該当する各サーバでのコンポーネント選択とは無関係に発生します。この現象は、iDRAC の Enterprise ライセンスを持つ第 12 および第 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。

- 最初に、同一サーバにある共通コンポーネント用のアップデートを適用してから、次に個々のサーバ上で特定コンポーネント用のアップデートを個別に適用します。
- 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。

ファームウェアアップデート後に最新のインベントリ情報が表示されない

第 11 世代 PowerEdge サーバのファームウェアバージョンの正常な更新後に、最新のインベントリ情報が表示されません。

OMIMSSC でのインベントリーの更新は、ファームウェア アップデート ジョブの完了直後に実行されるアクティビティーです。ファームウェアアップデートが完了した時点で PowerEdge サーバの CSIOR アクティビティが完了前であると、表示されるファームウェアインベントリ情報は従来のままになります。

この問題を回避するには、PowerEdge サーバーで CSIOR アクティビティーが完了していることを確認してから、OMIMSSC でファームウェア インベントリーを更新させます。また、エージェントフリーのステージングされたアップデートを適用した後は、サーバの再起動も行うようにしてください。インベントリー更新の詳細については、『*Configuration Manager および Virtual Machine Manager 用 OpenManage Integration for Microsoft System Center ユーザーズ ガイド*』の「*ファームウェア インベントリーの表示と更新*」の項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 ユーザーズ ガイド*』の最新バージョンにあるトラブルシューティングの項を参照してください。

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上で任意のジョブをスケジュールした後、そのサーバが Microsoft コンソールから削除され、登録された Microsoft コンソールと OMIMSSC を同期させると、そのサーバは、カスタムアップデートグループから削除され、事前定義されたアップデートグループにサーバが移動します。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。

この問題を回避するには、スケジュールされているジョブを **ジョブおよびログ** 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。

WinPE イメージのアップデートに失敗

WinPE イメージをアップデートしようとすると、アップデートジョブが失敗し、次のエラーメッセージが表示されることがあります。`Remote connection to console failed.`

この問題を回避するには、**DISM** コマンドを実行し、以前にマウントされていたすべてのイメージを Microsoft コンソールでクリーンアップして、WinPE イメージのアップデートを再試行します。

頻度設定の変更後にポーリングと通知ベルの色が変わる

OMIMSSC に管理サーバが検出されない状況下で、ポーリングと通知の頻度オプションを変更すると、カタログに変更がない場合でも、しばらくするとベルの色が黄色に変わります。

この問題を回避するには、管理対象サーバを検出してから、ポーリングと通知の頻度オプションを変更します。

OMIMSSC でのオペレーティングシステム導入シナリオ

ここでは、OMIMSSC での運用テンプレートを使用したオペレーティングシステムまたはハイパーバイザー (SCVMM 用) 導入に関連するトラブルシューティング情報について紹介します。

オペレーティングシステム導入の一般的なシナリオ

ここでは、オペレーティングシステム導入に関する一般的なすべてのトラブルシューティング情報について説明します。

運用テンプレートの導入の失敗

選択したサーバへの運用テンプレートの導入後、属性や属性値が選択された .CSV ファイルでの適正値に一致していないか、テンプレート設定に起因して iDRAC IP や iDRAC 資格情報が変更されています。iDRAC でのジョブは成功していても、無効な .CSV ファイルに起因して OMIMSSC での当該ジョブのステータスが不成功または失敗として表示されるか、ターゲットサーバでの iDRAC 変更が原因となってジョブ追跡が不可能になっています。

この問題を回避するには、選択した .CSV ファイルに適切な属性と属性値がすべて含まれていること、テンプレート設定によって iDRAC IP や資格情報が変更されていないことを確認します。

運用テンプレートの保存に失敗

運用テンプレートの作成時に、プール値を持つ依存関係がある属性のチェックボックスをオンにしてオフにすると、運用テンプレートを保存できず、次のエラーメッセージが表示されます。

```
Select atleast one attribte, under the selected components, before creating the
Operational Template.
```

この問題を回避するには、次のいずれかを実行します。

- いずれかのプール値を持つ依存関係がある属性、または同じ依存関係がある属性を選択して、運用テンプレートを保存します。
- 新規の運用テンプレートを作成します。

SCCM ユーザー用のオペレーティングシステム導入シナリオ

ここでは、SCCM コンソールでの OMIMSSC を使用したオペレーティングシステム導入に関連するトラブルシューティング情報について説明します。

導入オプションがタスクシーケンスに表示されない

SCCM 用 OMIMSSC コンソール拡張機能をアンインストールして再インストールした後に、**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。

この問題を回避するには、編集のためにタスクシーケンスを開き、**適用** オプションを再度有効にして、**OK** をクリックします。**導入** オプションが再度表示されます。

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、**編集** を選択します。
2. **Windows PE で再起動** を選択します。**説明** セクションで、任意の文字を入力して削除し、変更が保存されないようにします。
3. [**OK**] をクリックします。

   これで **適用** オプションが再度有効になります。

SCCM の Managed Lifecycle Controller Lifecycle Controller ESXi コレクションへのサーバの追加に失敗

オペレーティングシステム導入中に 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 中の Managed Dell Lifecycle Controller (ESXi) にサーバが移動されません。

この問題を回避するには、SCCM クライアントサーバをインストールしてから、同期化を実行して、Managed Lifecycle Controller Lifecycle Controller (ESXi) コレクションにサーバを追加します。

SCVMM ユーザー用のオペレーティングシステム導入シナリオ

ここでは、SCVMM コンソールでの OMIMSSC を使用したハイパーバイザー導入に関連するトラブルシューティング情報について説明します。

LC またはファイアウォール保護によるハイパーバイザー導入の失敗

ハイパーバイザー導入に失敗し、アクティビティログに次のエラーメッセージが表示されます。`Error New-SCVMHost failed with following error : An out of band operation (SMASH) for the BMC <IP ADDRESS> failed on IDRAC IP : <IP ADDRESS>.`

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

ハイパーバイザー導入に失敗し、アクティビティログに次のエラーメッセージが表示されます。

- **Error**: `Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""`

- **Information**: `Successfully deleted drivers from library share sttig.<MicrosoftConsoleName>.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` が出力した例外と、ライブラリ共有内のドライバファイルが原因で発生することがあります。再試行する前、または別のハイパーバイザー導入を実行する前に、これらのファイルをライブラリ共有から削除する必要があります。

ライブラリ共有からファイルを削除するには、次の手順を実行します。

1. SCVMM コンソールから、**ライブラリ** > **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。

その後、ハイパーバイザーが導入可能になります。

Active Directory へのサーバ追加中の 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 にサーバが追加されたら、OMIMSSC でサーバを再度検出します。

   サーバが **ホスト** タブの下に表示されます。

LC ドライバインジェクションの失敗

SC2012 VMM を使用して OS の導入と LC ドライバインジェクションを行う場合、OS は正常に導入されますが、LC ドライバインジェクションには失敗します。

この問題を解決するには、SCVMM の最新のロールアップを適用します。

SCVMM ユーザー用の S2D クラスタ作成シナリオ

ここでは、SCVMM コンソールでの OMIMSSC を使用した Storage Spaces Direct 作成に関連するトラブルシューティング情報について説明します。

S2D クラスタの正常性ステータスが不明

既存クラスタ中のノードに Storage Spaces Direct クラスタを作成すると、ストレージプールおよびディスク設定に既存クラスタの設定が含まれます。そのため、クラスタストレージプールが作成されないことや、クラスタストレージプールが作成された場合でも正常性ステータスが不明と表示されることがあります。

この問題を回避するには、既存クラスタの詳細情報を含むストレージプールおよびディスク設定をクリアしてから Storage Spaces Direct クラスタを作成します。ストレージプールのクリアの詳細については、Microsoft ドキュメントの「*Storage Spaces Direct の正常性と動作状態のトラブルシューティング*」の項を参照してください。

OMIMSSC でのサーバプロファイルのシナリオ

ここでは、OMIMSSC でのサーバプロファイルのエクスポートとインポートに関するすべてのトラブルシューティング情報について説明します。

サーバープロファイルのエクスポートの失敗

サーバ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、サーバプロファイルがエクスポートされず、次のエラーメッセージが表示されます。`The selectors for the resource are not valid.`

この問題を回避するには、iDRAC をリセットしてから、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。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。

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

OMIMSSC でサーバー プロファイルのインポート ジョブを送信した後、2 時間後にそのジョブがタイムアウトします。

この問題を回避するには、次の手順を実行します。

1. サーバを起動し、F2 を押して、**BIOS 設定** 画面に移動します。
2. **セットアップユーティリティ** をクリックし、**その他の設定** を選択します。
3. **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、サーバプロファイルを再度エクスポートし、同じサーバプロファイルを使用してそのサーバにインポートします。

OMIMSSC での LC ログシナリオ

ここでは、LC ログのエクスポートおよび表示に関するすべてのトラブルシューティング情報について説明します。

LC ログの .CSV 形式でのエクスポートの失敗

LC ログファイルを .CSV 形式でダウンロードしようとすると、ダウンロードに失敗します。

この問題を回避するには、ローカルのイントラネットサイトでブラウザに OMIMSSC アプライアンスの FQDN を追加します。ローカル イントラネットでの OMIMSSC アプライアンスの追加については、『*System Center Configuration Manager および System Center Virtual Machine Manager 用 Dell EMC OpenManage Integration for Microsoft System Center バージョン 7.2.1 ユーザーズ ガイド*』の「*LC ログの表示*」セクションを参照してください。

LC ログファイルのオープンに失敗

LC ログを収集した後、サーバの LC ログファイルの表示を試行すると、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。iDRAC のリセットに関する詳細については、`dell.com/support` にある iDRAC のマニュアルを参照してください。

テスト接続の失敗

ユーザー名は同じだが、パスワードはドメインユーザーアカウントとローカルユーザーアカウントとで異なる場合、Microsoft コンソールと OMIMSSC アプライアンス間の接続テストに失敗します。

たとえば、ドメインユーザーアカウントは `domain\user1` で、そのパスワードは `pwd1` だとします。そしてローカルユーザーアカウントは `user1` で、そのパスワードは `Pwd2` だとします。上記のドメインユーザーアカウントで登録しようとすると、テスト接続に失敗します。

この問題を回避するには、ドメインユーザーとローカルユーザーのアカウントで異なるユーザー名を使用するか、あるいは OMIMSSC アプライアンスでの Microsoft コンソール登録時に単一のユーザーアカウントをローカルユーザーとして使用します。

24

付録

次の表を参照して、MX7000 デバイスのタイムゾーン属性値を手動で指定します。

表 12. タイムゾーンの詳細

タイムゾーン ID	時差
TZ_ID_1	(GMT-12:00) 国際日付変更線西側
TZ_ID_2	(GMT+14:00) サモア
TZ_ID_3	(GMT-10:00) ハワイ
TZ_ID_4	(GMT-09:00) アラスカ
TZ_ID_5	(GMT-08:00) 太平洋標準時 (米国およびカナダ)
TZ_ID_6	(GMT-08:00) バハカリフォルニア
TZ_ID_7	(GMT-07:00) アリゾナ
TZ_ID_8	(GMT-07:00) チワワ、ラパス、マサトラン
TZ_ID_9	(GMT-07:00) 山岳部時間 (米国およびカナダ)
TZ_ID_10	(GMT-06:00) 中央アメリカ
TZ_ID_11	(GMT-06:00) 中部時間 (米国およびカナダ)
TZ_ID_12	(GMT-06:00) グアダラハラ、メキシコシティ、モンテレー
TZ_ID_13	(GMT-06:00) サスカチュワン
TZ_ID_14	(GMT-05:00) ボゴタ、リマ、キト
TZ_ID_15	(GMT-05:00) 東部時間 (米国およびカナダ)
TZ_ID_16	(GMT-05:00) インディアナ (東部)
TZ_ID_17	(GMT-04:30) カラカス
TZ_ID_18	(GMT-04:00) アスンシオン
TZ_ID_19	(GMT-04:00) 大西洋時間 (カナダ)
TZ_ID_20	(GMT-04:00) クイアバ
TZ_ID_21	(GMT-04:00) ジョージタウン、ラパス、マナウス、サンファン
TZ_ID_22	(GMT-04:00) サンチャゴ
TZ_ID_23	(GMT-03:30) ニューファンドランド
TZ_ID_24	(GMT-03:00) ブラジリア
TZ_ID_25	(GMT-03:00) ブエノスアイレス
TZ_ID_26	(GMT-03:00) カイエンヌ、フォルタレザ
TZ_ID_27	(GMT-03:00) グリーンランド
TZ_ID_28	(GMT-03:00) モンテビデオ
TZ_ID_29	(GMT-02:00) 中部大西洋
TZ_ID_30	(GMT-01:00) アゾレス諸島

表 12. タイムゾーンの詳細（続き）

タイムゾーン ID	時差
TZ_ID_31	（GMT-01:00）カーボベルデ諸島
TZ_ID_32	（GMT+00:00）カサブランカ
TZ_ID_33	（GMT+00:00）協定世界時
TZ_ID_34	（GMT+00:00）ダブリン、エジンバラ、リスボン、ロンドン
TZ_ID_35	（GMT+00:00）モンロビア、レイキャビク
TZ_ID_36	（GMT+01:00）アムステルダム、ベルリン、ベルン、ローマ、ストックホルム、ウィーン
TZ_ID_37	（GMT+01:00）ベオグラード、ブラチスラバ、ブダペスト、リュブリャナ、プラハ
TZ_ID_38	（GMT+01:00）ブリュッセル、コペンハーゲン、マドリッド、パリ
TZ_ID_39	（GMT+01:00）サラエボ、スコピエ、ワルシャワ、ザグレブ
TZ_ID_40	（GMT+01:00）西部中央アフリカ
TZ_ID_41	（GMT+02:00）ビントフック
TZ_ID_42	（GMT+02:00）アンマン
TZ_ID_43	（GMT+03:00）イスタンブール
TZ_ID_44	（GMT+02:00）ベイルート
TZ_ID_45	（GMT+02:00）カイロ
TZ_ID_46	（GMT+02:00）ダマスカス
TZ_ID_47	（GMT+02:00）ハラレ、プレトリア
TZ_ID_48	（GMT+02:00）ヘルシンキ、キエフ、リガ、ソフィア、タリン、ヴィリニュス
TZ_ID_49	（GMT+02:00）エルサレム
TZ_ID_50	（GMT+02:00）ミンスク
TZ_ID_51	（GMT+03:00）バグダッド
TZ_ID_52	（GMT+03:00）クウェート、リヤド
TZ_ID_53	（GMT+03:00）モスクワ、サンクトペテルブルグ、ボルゴグラード
TZ_ID_54	（GMT+03:00）ナイロビ
TZ_ID_55	（GMT+03:30）テヘラン
TZ_ID_56	（GMT+04:00）アブダビ、マスカット
TZ_ID_57	（GMT+04:00）バクー
TZ_ID_58	（GMT+04:00）ポートルイス
TZ_ID_59	（GMT+04:00）トビリシ
TZ_ID_60	（GMT+04:00）エレヴァン
TZ_ID_61	（GMT+04:30）カブール
TZ_ID_62	（GMT+05:00）エカチェリンブルグ
TZ_ID_63	（GMT+05:00）イスラマバード、カラチ
TZ_ID_64	（GMT+05:00）タシケント

表 12. タイムゾーンの詳細（続き）

タイムゾーン ID	時差
TZ_ID_65	（GMT+05:30）チェンナイ、コルカタ、ムンバイ、ニューデリー
TZ_ID_66	（GMT+05:30）スリジャヤワルダナプラコッテ
TZ_ID_67	（GMT+05:45）カトマンズ
TZ_ID_68	（GMT+06:00）アスタナ
TZ_ID_69	（GMT+06:00）ダッカ
TZ_ID_70	（GMT+06:00）ノボシビルスク
TZ_ID_71	（GMT+06:30）ヤンゴン（ラングーン）
TZ_ID_72	（GMT+07:00）バンコク、ハノイ、ジャカルタ
TZ_ID_73	（GMT+07:00）クラスノヤルスク
TZ_ID_74	（GMT+08:00）北京、重慶、香港、ウルムチ
TZ_ID_75	（GMT+08:00）イルクーツク
TZ_ID_76	（GMT+08:00）クアラルンプール、シンガポール
TZ_ID_77	（GMT+08:00）パース
TZ_ID_78	（GMT+08:00）台北
TZ_ID_79	（GMT+08:00）ウランバートル
TZ_ID_80	（GMT+08:30）ピョンヤン
TZ_ID_81	（GMT+09:00）大阪、札幌、東京
TZ_ID_82	（GMT+09:00）ソウル
TZ_ID_83	（GMT+09:00）ヤクーツク
TZ_ID_84	（GMT+09:30）アデレード
TZ_ID_85	（GMT+09:30）ダーウィン
TZ_ID_86	（GMT+10:00）ブリスベン
TZ_ID_87	（GMT+10:00）キャンベラ、メルボルン、シドニー
TZ_ID_88	（GMT+10:00）グアム、ポートモレスビー
TZ_ID_89	（GMT+10:00）ホバート
TZ_ID_90	（GMT+10:00）ウラジオストク
TZ_ID_91	（GMT+11:00）マガダン、ソロモン諸島、ニューカレドニア
TZ_ID_92	（GMT+12:00）オークランド、ウェリントン
TZ_ID_93	（GMT+12:00）フィジー
TZ_ID_94	（GMT+13:00）ヌクアロファ
TZ_ID_95	（GMT+14:00）キリティマティ
TZ_ID_96	（GMT+02:00）アテネ、ブカレスト

25

付録 2

プール値 CSV ファイルへの入力

表 13. プール値ファイル

serviceTag（自動入力）	FQDD（自動入力）	poolAttributeName	poolAtrributeValue
システム固有の属性がエクスポートされるデバイスのサービス タグ	システム固有の属性に関連付けられているコンポーネントの特定	設定されるシステム固有属性の特定	指定されたシステム固有属性の値の設定

表 14. 例

serviceTag（自動入力）	FQDD（自動入力）	poolAttributeName	poolAtrributeValue	属性の説明とその値の入力方法の詳細
xxxxxxx	WINDOWS	HOSTNAME	WIN19SRVDTA	説明：これは、導入/プロビジョニングされたサーバーに設定されるホスト名です。
xxxxxxx	WINDOWS	ServerMngNIC	<MAC アドレス >	説明：これは、System Center および OMMISSC アプライアンスと通信できるネットワーク ポートの MAC アドレスです。 方法：特定のポートに移動することによって iDRAC から MAC アドレスを取得します。
xxxxxxx	WINDOWS	LOGICALNETWORK	固定 IP を使用した OSD	説明：これは、SCVMM で作成されたネットワーク プロファイルです。固定 IP プール、サブネット、および MN に適用されるその他のネットワークの詳細を含みます 方法：SCVMM に論理ネットワーク プロファイルを作成し、作成したテンプレート名を入力します。詳細については、Microsoft マニュアルの「VMM ネットワーク ファブリックの計画」セクションを参照してください。
xxxxxxx	WINDOWS	IPSUBNET	100.100.28.0/22	説明：これは、前述の論理ネットワーク プロファイルに入力された固定 IP プールのサブネット マスクです。
xxxxxxx	WINDOWS	IPADDRESS	100.100.31.145	説明：これは、導入/プロビジョニングされた管理下ノードに適用される固定 IP です。

26

Dell EMC サポートサイトからのドキュメントへのアクセス

必要なドキュメントにアクセスするには、次のいずれかの方法で行います。

- 次のリンクを使用します。
  - Dell EMC エンタープライズ システム管理、Dell EMC リモート エンタープライズ システム管理、および Dell EMC 仮想化ソリューションのマニュアル — www.dell.com/esmmanuals
  - Dell EMC OpenManage マニュアル — www.dell.com/openmanagemanuals
  - iDRAC マニュアル — www.dell.com/idracmanuals
  - Dell EMC OpenManage Connections エンタープライズ システム管理マニュアル — www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Dell EMC 保守ツール マニュアル — https://www.dell.com/serviceabilitytools
- Dell EMC サポート サイトからアクセスします。
  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、次の中から必要なリンクをクリックします。
     - **統計**
     - **クライアントシステム管理**
     - **エンタープライズアプリケーション**
     - **エンタープライズシステム管理**
     - **メインフレーム**
     - **オペレーティングシステム**
     - **公共機関向けソリューション**
     - **保守ツール**
     - **サポート**
     - **ユーティリティ**
     - **仮想化ソリューション**
  4. マニュアルを表示するには、該当する製品をクリックして、該当するバージョンをクリックします。
- 検索エンジンを使用します。
  - 検索 ボックスに名前および文書のバージョンを入力します。