Dell EMC OpenManage Integration with Microsoft Windows Admin Center バージョン 1.1.1

ユーザーズ ガイド

February 2021
Rev. A01

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

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

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

目次

1

OpenManage Integration with Microsoft Windows Admin Center の概要

IT 管理者は、Dell EMC OpenManage Integration with Microsoft Windows Admin Center（OMIMSWAC）を使用して、ホストとしての PowerEdge サーバー、PowerEdge サーバーで作成された Microsoft フェールオーバー クラスター、Microsoft Azure Stack HCI 向け Dell EMC ソリューション（Storage Space Direct Ready Nodes または AX ノード）を使用して作成されたハイパーコンバージド インフラストラクチャ（HCI）を管理できます。OMIMSWAC は、PowerEdge サーバーやクラスターのライフサイクル全体を通してリモートに管理することにより、IT 管理者の作業をシンプルにします。OMIMSWAC の機能と利点の詳細については、Dell.com/OpenManageManuals にあるマニュアルを参照してください。

OMIMSWAC の主な機能

- OMIMSWAC は、以下のものを効率的に管理するためのシンプルなソリューションを IT 管理者に提供します。
  - サポートされている Windows オペレーティング システムで実行されている Dell EMC PowerEdge サーバー。
  - Dell EMC の AX ノードまたは Storage Spaces Direct Ready Node をベースとした Azure Stack HCI クラスター。
  - Dell EMC PowerEdge サーバーを使用して作成された Microsoft フェールオーバー クラスター。
- サポートされているすべての Dell EMC プラットフォームのコンポーネント レベルの情報など、ノードの全体的な正常性、ハードウェア インベントリー、および iDRAC インベントリーを表示します。
- Dell EMC による検証済みアップデート カタログのアップデート コンプライアンス レポートの生成と、新しいカタログ バージョンの通知の受信。
- インターネットに接続されている場合、OMIMSWAC での異なるベースラインのサポート：
  - PowerEdge サーバーおよび PowerEdge サーバーを含むクラスター用の Dell EMC エンタープライズ カタログ。
  - Microsoft Azure Stack HCI 向け Dell EMC ソリューション用の Dell EMC Azure Stack HCI ソリューション カタログ。
  - PowerEdge MX モジュラー用の Dell EMC MX ソリューション カタログ。
- Dell EMC Repository Manager（DRM）を使用して作成されたローカル ベースラインのサポート。
- ベースラインに応じた PowerEdge サーバーのアップデート（BIOS、ドライバー、ファームウェア、システム管理アプリケーション）。
- PowerEdge サーバー ベースのフェールオーバー クラスター用の検証済みベースライン（BIOS、ドライバー、ファームウェア、システム管理アプリケーション）および Microsoft Azure Stack HCI 向け Dell EMC ソリューションに対するクラスター対応アップデート。
- PowerEdge サーバーの iDRAC 情報を表示します。帯域外管理の場合は、Windows Admin Center から iDRAC コンソールを直接起動できます。
- 英語、フランス語、ドイツ語、スペイン語、簡体字中国語、日本語の言語でローカライズされた OMIMSWAC 拡張機能とマニュアルが利用可能。

トピック：

変更履歴

日付	文書のリビジョン	変更の説明
2020 年 8 月	A00	OMIMSWAC 1.1.1 のイニシャル リリース
2021 年 1 月	A01	• Windows Admin Center 2009 GA のサポートを追加。

日付	文書のリビジョン	変更の説明
		• Windows Server Core OS を実行しているターゲット ノードはサポートされません。

本リリースの新機能

リリース 1.1.1

- Microsoft Windows Admin Center バージョン 2007 GA および 2009 GA のサポート。
- iDRAC ファームウェア 4.00.129.00 以降がインストールされた PowerEdge XE2420 Edge サーバーのサポート。
- 修正と機能拡張：
  - 管理者権限のないゲートウェイ ユーザー資格情報を使用して WAC にログインした後、Windows Admin Center（WAC）コンソールから OMIMSWAC にアクセスできるようになりました。

    以前のリリースでは、管理者権限のないゲートウェイ ユーザー資格情報を使用して WAC にログインした場合、WAC コンソールから OMIMSWAC にアクセスしようとすると拒否されました。
  - OMIMSWAC で、シングル サインオンを使用して接続したクラスターのインベントリー情報を取得できるようになりました。

    以前のリリースでは、シングル サインオン認証を使用してクラスターに接続すると、インベントリー情報の取得に失敗し、WAC は応答しなくなりました。
  - 特定の特殊文字を含むパスワードを使用して接続したターゲット ノードまたはクラスターのコンプライアンス レポートを生成できるようになりました。

    以前のリリースでは、二重引用符（"）、グレイブ アクセント（'）、セミコロン（;）などの特殊文字を含むパスワードを使用してサーバーまたはクラスターを接続した場合、コンプライアンスの生成に失敗していました。
- `CauClusterRole` パラメーターのリセット。クラスター対応アップデート（CAU）の操作が完了した後に、指定したクラスターの自己更新機能を有効にします。

リリース 1.1.0

- 次の Dell EMC オンライン カタログのサポートが追加されました。
  - PowerEdge サーバーおよび PowerEdge サーバーを含むクラスター用の Dell EMC エンタープライズ カタログ。
  - Microsoft Azure Stack HCI 向け Dell EMC ソリューション用の Dell EMC Azure Stack HCI ソリューション カタログ。
  - PowerEdge MX モジュラー用の Dell EMC MX ソリューション カタログ。
- 選択したコンポーネントのアップデートなど、サーバーのアップデートを実行する機能。
- 次のように、検証されたベースライン（BIOS、ドライバー、ファームウェア、システム管理アプリケーション）に対してクラスター対応アップデートを実行する機能。
  - PowerEdge サーバーベースのフェールオーバー クラスター
  - Microsoft Azure Stack HCI の Dell EMC ソリューション

    メモ: クラスター対応アップデート機能を使用するには、クラスター内の各ノードにプレミアム ライセンスをインストールする必要があります。
- 物理ディスクの探索や故障した物理ディスクの特定のために、点滅/点滅解除できる物理ディスクの発光ダイオード（LED）をサポート。
- より新しいプラットフォームのサポート：
  - AX ノードをベースにしたプラットフォーム - Microsoft Azure Stack HCI ノード向け Dell EMC ソリューション（AX-640、AX-6515、AX-740xd）。
  - Dell EMC の Storage Spaces Direct Ready Nodes に基づいたプラットフォーム - Microsoft Azure Stack HCI 向け Dell EMC ソリューション（R440、R640、R740xd、R740xd2）。
- Microsoft Windows Admin Center バージョン 1910.2 のサポート。
- 最新の iDRAC9 ベース PowerEdge サーバーでのアクセラレーター（GPU）の正常性とインベントリーを監視する機能。
- Intel Persistent Memory の正常性監視とインベントリーに対応したユーザー インターフェイスの機能拡張。
- アップデート コンプライアンスのパフォーマンスの向上。
- 関連付けられているディスクを表示するストレージ コントローラーと物理ディスクの相関。
- 管理対象ターゲット ノードの正常性、インベントリー、iDRAC 情報を更新して、最新のインベントリー情報が表示されるようにする機能。
- コンポーネントのアップデートに必要な DSU および IC の自動ダウンロードによる、操作性の向上。

- コンプライアンス レポートを生成するために、プロキシ設定を使用して、インターネットからカタログ、DSU、および IC の各ユーティリティーをダウンロードする機能。
- AX ノードまたは Storage Spaces Direct Ready Node で構成される Microsoft Azure Stack HCI クラスター向け Dell EMC ソリューションに対して、「**Azure Stack HCI 認定**」の Dell EMC ソリューション バッジを表示。

追加リソース

表 1. 追加リソース

文書	説明	入手先
『Dell EMC OpenManage Integration with Microsoft Windows Admin Center インストール ガイド』	OpenManage Integration with Microsoft Windows Admin Center のインストールと設定に関する情報が記載されています。	1. Dell.com/OpenManageManuals にアクセスします。 2. [**OpenManage Integration with Microsoft Windows Admin Center**] を選択します。 3. これらのドキュメントにアクセスするには、**[マニュアル]** > **[マニュアルと文書]** をクリックします。
Dell EMC OpenManage Integration with Microsoft Windows Admin Center リリースノート	OpenManage Integration with Microsoft Windows Admin Center の新機能、既知の問題、回避策に関する情報が記載されています。	
OMIMSWAC による PowerEdge サーバーおよび Azure Stack HCI クラスターの Dell EMC インフラストラクチャー コンプライアンス レポート	このホワイト ペーパーでは、OMIMSWAC を使用して、PowerEdge サーバー、Microsoft Azure Stack HCI クラスター、および Hyper-V ベースのフェールオーバー クラスターのアップデート コンプライアンス レポートを生成するプロセスが説明されています。	
Microsoft Windows Admin Center のマニュアル	Microsoft Windows Admin Center の使用の詳細が説明されています。	https://www.microsoft.com/en-us/cloud-platform/windows-admin-center

2

OpenManage Integration with Microsoft Windows Admin Center をお使いになる前に

Windows Admin Center で Dell EMC OpenManage Integration 拡張機能を起動する前に、次のことを確認します。

- Windows Admin Center にゲートウェイ管理者としてログインしている。

OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) をインストールした後、次の手順を実行してこの拡張機能を起動します。

1. Windows Admin Center の左上隅で、次を選択します。
   - Windows Admin Center の 1910.2 GA リリース、2007 GA リリース、または 2009 GA リリースの場合：ドロップダウン メニューの [**サーバー マネージャー**] または [**クラスター マネージャー**] のいずれか。
2. リストからサーバーまたはクラスター接続を選択し、[**接続**] をクリックします。
3. サーバーまたはクラスターの認証情報を入力します。

   メモ: 認証情報の入力を求めるプロンプトが表示されない場合は、[管理に使用する資格情報] を選択し、適切なサーバー管理者またはクラスター管理者のアカウントを入力します。

   メモ: OMIMSWAC は、シングル サインオンやスマート カード認証方式をサポートしていません。
4. Microsoft Windows Admin Center の左ペインで、[**拡張機能**] の下の [**Dell EMC OpenManage Integration**] をクリックします。

OpenManage Integration を初めて起動すると、USB NIC を有効化し、ターゲット ノードで iDRAC ユーザーを作成するなど、OpenManage Integration によって実行される操作を示すカスタマー通知が表示されます。OpenManage Integration を使用して PowerEdge サーバーの管理を続行するには、**同意する** をクリックします。

メモ: 管理対象ノードの情報が収集されると、以前に作成された iDRAC ユーザーは OMIMSWAC によって削除されます。

OpenManage Integration with Microsoft Windows Admin Center を正常に機能させるには、次のことを確認します。

- 所属するエンタープライズ環境のファイアウォールが SMB ポート 445 を介した通信を許可している。
- ターゲット ノード上で Redfish サービスが有効になっている。
- ターゲット ノードに使用可能な iDRAC ユーザー スロットがある。
- ターゲット ノードが Lifecycle Controller で起動されていないようにする。
- ターゲット ノードが再起動状態でない、または電源がオフになっている。
- USB NIC アダプターが、ターゲット ノード OS で無効になっていない。
- ターゲット ノードでロックダウン モードが無効になっている。
- PowerShell 実行ポリシーは、Windows Admin Center がインストールされているシステムとターゲット ノードの OS で RemoteSigned に設定されています。詳細については、https://www.dell.com/support/article/sln318718/dell-emc-openmanage-integration-with-microsoft-windows-admin-center-omimswac-fails-to-query-host-information を参照してください。

メモ: PowerEdge サーバーを管理するため、OMIMSWAC は OS から iDRAC への内部パススルー インターフェイスを使用します。デフォルトでは、iDRAC には IP アドレス 169.254.0.1/<サブネット>、または 169.254.1.1/<サブネット>を使用してアクセスできます。ただし、ホストに同じサブネット内に別のネットワーク インターフェイスがある場合 (たとえば、VMFleet などのツールがインストールされている場合)、OMIMSWAC はホスト OS から iDRAC に通信できない場合があります。競合を解決するには、iDRAC にログインし、[OS から iDRAC へのパススルー] セクションで、USB NIC IP アドレスを変更します。この IP アドレスの割り当てに関する詳細については、Dell EMC サポート サイトにある iDRAC のマニュアルを参照してください。

管理方法：

- PowerEdge サーバーについては、「Dell EMC PowerEdge サーバーの管理 、p. 10」を参照してください。
- PowerEdge サーバーで作成された Microsoft フェールオーバー クラスター、または Dell EMC の AX ノードまたは Storage Spaces Direct Ready Nodes で作成された Azure Stack HCI については、「フェールオーバー クラスターと Azure Stack HCI の管理 、p. 13」を参照してください。

3

Dell EMC OpenManage Integration with Microsoft Windows Admin Center に必要なポート

表 2. Dell EMC OpenManage Integration with Microsoft Windows Admin Center に必要なポート

OpenManage Integration with Windows Admin Center の機能	Windows Admin Center がインストールされているシステム	ターゲット ノード/クラスター ノード	DRM カタログが使用可能なシステム	DSU および IC ユーティリティーが使用可能なシステム	ターゲット ノード/クラスター ノードの iDRAC
インストール	該当なし	該当なし	該当なし	該当なし	該当なし
アンインストール	該当なし	該当なし	該当なし	該当なし	該当なし
正常性、ハードウェア、iDRAC インベントリー	445：アウトバウンド	445：インバウンド	該当なし	該当なし	443(デフォルトポート)
アップデート ソース設定：テスト接続	445：アウトバウンド	該当なし	該当なし	445：インバウンド	該当なし
アップデート コンプライアンス	該当なし	445：インバウンド	445：アウトバウンド	445：アウトバウンド	該当なし
コンプライアンス通知のアップデート	445：アウトバウンド	該当なし	445：インバウンド	該当なし	該当なし
ターゲット ノード アップデートとクラスター対応アップデート	該当なし	Microsoft によって提供されるデフォルト WinRM ポート	445：アウトバウンド	445：アウトバウンド	443(デフォルトポート)

SMB ポート 445 の詳細については、https://go.microsoft.com/fwlink/?linkid=2101556 を参照してください。

WinRM ポートの詳細については、『https://docs.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management』を参照してください。

4

Dell EMC PowerEdge サーバーの管理

前提条件：

- Microsoft Windows Admin Center に、ゲートウェイ管理者としてログインしている必要があります。
- Dell EMC OpenManage Integration with Microsoft Windows Admin Center（OMIMSWAC）拡張機能がインストールされている必要があります。インストール手順の詳細については、『*Dell EMC OpenManage Integration with Microsoft Windows Admin Center インストール ガイド*』を参照してください。
- サーバー接続は Microsoft Windows Admin Center に追加されます。サーバー接続の追加に関する詳細については、https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center を参照してください。

PowerEdge サーバーを管理するには、次のようにします。

1. Windows Admin Center の左上隅で、ドロップダウン メニューから [**サーバーマネージャー**] を選択します。
2. リストからサーバー接続を選択し、[**接続**] をクリックします。

   メモ: 接続の追加時にサーバーの資格情報を入力していない場合は、サーバーに接続するときに、[管理に使用する資格情報] を選択して資格情報を入力する必要があります。

3. Microsoft Windows Admin Center の左ペインで、[**拡張機能**] の下の [**Dell EMC OpenManage Integration**] をクリックします。
4. 次を選択します。
   - **正常性** - ターゲット ノード コンポーネントの正常性状態が表示されます。ステータス アイコンは、ターゲット ノードの全体的な正常性状態を表します。「正常性状態 - サポートされているターゲット ノード コンポーネント 、p. 11」を参照してください。
   - **インベントリー** - ターゲット ノード コンポーネントのハードウェア インベントリーの詳細情報が表示されます。「ハードウェア インベントリー - サポートされているターゲット ノード コンポーネント 、p. 11」を参照してください。
   - **アップデート** - コンプライアンス レポートが表示され、コンポーネントをベースライン バージョンにアップデートできます。「HCI およびフェールオーバー クラスターの PowerEdge サーバーとノードのアップデート 、p. 17」を参照してください。
   - **iDRAC** - ターゲット ノードの iDRAC の詳細が表示されます。OpenManage Integration を使用して、Windows Admin Center から iDRAC コンソールを直接起動することができます。「HCI およびフェールオーバー クラスターの PowerEdge サーバーおよびノードの iDRAC の詳細の表示 、p. 16」を参照してください。

メモ: 正常性、ハードウェア インベントリー、および iDRAC の詳細はキャッシュされ、拡張機能が読み込まれるたびには読み込まれません。最新の正常性、インベントリーのステータス、および iDRAC の詳細を表示するには、[正常性状態] の右上隅にある [**更新**] をクリックします。

メモ: モジュラー型サーバー（YX2X、YX3X、YX4X、YX5X の各モデルおよびそれ以降のモデルの PowerEdge サーバー）では、ファンおよび電源装置に関連する次の情報が表示されません。

- 正常性状態
- ハードウェア インベントリー テーブル内の属性値

メモ: ファームウェアのバージョンが 2.60.60.60 より前の YX2X および YX3X モデルの PowerEdge サーバーでは、次のコンポーネントに関する情報は表示されません。

- 正常性状態 - アクセラレーター、メモリー、ストレージ コントローラー、ストレージ エンクロージャ、物理ディスク。
- ハードウェア インベントリー - アクセラレーター、メモリー、ストレージ コントローラー、ストレージ エンクロージャ、物理ディスク、ネットワーク デバイス、ファームウェア。

トピック：

正常性状態 - サポートされているターゲット ノード コンポーネント

次のターゲット ノード コンポーネントの正常性状態が表示されます。

- CPU
- アクセラレーター
- メモリ
- ストレージコントローラ
- ストレージ エンクロージャ
- 物理ディスク
- iDRAC
- 電源装置
- ファン
- 電圧
- 温度

メモ: 正常性状態情報は、iDRAC バージョンの 4.00.00.00 以降を搭載した PowerEdge サーバーの YX4X モデルのアクセラレーターで使用できます。

メモ: Intel **DIMM** メモリーはアイコンで **IntelPersistent** として識別されます。

正常性状態は、ドーナツ グラフを使用して表示されます。ドーナツ グラフのさまざまなセクションを選択して、コンポーネントの正常性状態をフィルタリングできます。たとえば、赤色のセクションを選択すると、重大な正常性ステータスのコンポーネントのみが表示されます。

最新の正常性状態を表示するには、[**正常性**] タブの右上隅にある [**更新**] をクリックします。

メモ: 内蔵 SATA コントローラーに接続されているソフトウェア ストレージ コントローラーと物理ディスクの場合、正常性インベントリーのステータスは「不明」と表示されます。

ハードウェア インベントリー - サポートされているターゲット ノード コンポーネント

次のターゲット ノード コンポーネントのハードウェア インベントリーが表示されます。

- システム
- ファームウェア
- CPU
- アクセラレーター
- メモリ
- ストレージコントローラ

  ストレージ コントローラー内の物理ディスクを表示するには、[**関連するディスク**] で、[**ディスクの表示**] リンクをクリックします。物理ディスクは [**物理ディスク**] タブに表示されます。

- ストレージ エンクロージャ
- ネットワークデバイス
- 物理ディスク

  ディスクの追加プロパティを表示するには、ディスクを選択し、[**詳細なプロパティ**] をクリックします。関連付けられているストレージ コントローラーを表示するには、[**詳細なプロパティ**] の下にあるストレージ コントローラーのリンクをクリックします。関連づけられているストレージ コントローラーが [**ストレージ コントローラー**] タブに表示されます。物理ディスクが CPU に接続されている場合、[**詳細なプロパティ**] でストレージ コントローラーのリンクが使用できなくなります。

  物理ディスクの点滅および点滅解除

  物理ディスクを選択し、[**点滅**] をクリックして物理ディスク上の LED の点滅を有効にします。LED は物理ディスクの状態を表します。物理ディスクの点滅によって、データ センター内の故障した物理ディスクを特定したり、識別したりすることができます。物理ディスクの点滅を無効にするには、ディスクを選択して [**点滅解除**] をクリックします。

メモ: 点滅および点滅解除の操作は以下では利用できない場合があります。

- Boot Optimized Storage Subsystem（BOSS）カードに関連付けられているディスク。
- iDRAC ファームウェア バージョンが 3.30.30.30 未満のデバイス。点滅および点滅解除操作を有効にするには、iDRAC ファームウェアを最新バージョンにアップデートします。

メモ:

- 点滅または点滅解除操作の実行中は、最新の正常性とハードウェア インベントリー情報を読み込む [**更新**] ボタンは無効です。また、OMIMSWAC で正常性とハードウェア インベントリーが読み込まれているときには、点滅および点滅解除の操作は無効になっています。
- 内蔵 SATA コントローラーに接続されている物理ディスクでの点滅および点滅解除操作は、「点滅と点滅解除は<ディスク名>でサポートされていない可能性があります。」というエラーが表示されて失敗します。

- 電源装置
- ファン

最新のハードウェア インベントリー情報を表示するには、[**インベントリー**] タブの右上隅にある [**更新**] をクリックします。

ターゲット ノードの iDRAC 詳細を表示するには、「HCI およびフェールオーバー クラスターの PowerEdge サーバーおよびノードの iDRAC の詳細の表示 、p. 16」を参照してください。

メモ: [**インベントリー**] の下では、ターゲット ノードで 2、3 個のコンポーネントの値が使用できなくなる可能性があるため、そのターゲット ノード コンポーネントの属性値が空白で表示されます。

メモ: ファームウェア インベントリーの下では、複数のポートを使用する一部のネットワーク デバイスに対して、該当するファームウェア バージョンがすべてのポートで同一であるため、そのファームウェア バージョンの 1 ポートのみが表示されます。

メモ: ストレージ エンクロージャ、ファームウェア インベントリー、およびメモリー コンポーネントのいくつかの属性についての情報は、次の場合は利用できないことがあります。

- YX2X および YX3X モデルの PowerEdge サーバー。
- 3.30.30.30 より前のバージョンの iDRAC を搭載した YX4X モデルの PowerEdge サーバー。

メモ: ストレージ エンクロージャの PCIe SSD バックプレーンでは、ほとんどの属性値を使用できます。

メモ: 正常性状態情報は、iDRAC バージョンの 4.00.00.00 以降を搭載した PowerEdge サーバーの YX4X モデルのアクセラレーターで使用できます。

メモ: Intel **DIMM** メモリーはアイコンで **IntelPersistent** として識別されます。

5

フェールオーバー クラスターと Azure Stack HCI の管理

前提条件：

- Microsoft Windows Admin Center に、ゲートウェイ管理者としてログインします。
- Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) 拡張機能がインストールされている必要があります。インストール手順の詳細については、『*Dell EMC OpenManage Integration with Microsoft Windows Admin Center インストール ガイド*』を参照してください。
- Microsoft Windows Admin Center で、フェールオーバーまたはハイパーコンバージド クラスター接続が追加されています。フェールオーバーまたはハイパーコンバージド クラスター接続の追加の詳細については、https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center を参照してください。
- OMIMSWAC でクラスターを管理する前に、IP アドレス、ホスト名、または完全修飾ドメイン名 (FQDN) を使用して、すべてのクラスター ノードに到達可能であることを確認します。

PowerEdge サーバーで作成された Microsoft フェールオーバー クラスター、および Dell EMC の AX ノードまたは Storage Spaces Direct Ready Nodes で作成された Azure Stack HCI を管理するには、次の手順を実行します。

1. Windows Admin Center の左上隅で、次を選択します。
   - Windows Admin Center の 1910.2 GA リリース、2007 GA リリース、または 2009 GA リリースの場合：ドロップダウン メニューの [**クラスター マネージャー**]。
2. リストから、フェールオーバーまたはハイパーコンバージド クラスター接続を選択して、**接続**をクリックします。
3. Microsoft Windows Admin Center の左ペインで、**拡張機能**の下の **Dell EMC OpenManage Integration** をクリックします。
4. フェールオーバーまたはハイパーコンバージド クラスターを管理するには、次を選択します。
   - **正常性** - クラスターの個々のノードのサーバー コンポーネントの正常性状態が表示されます。
     - **全体的な正常性状態**セクションには、クラスターの全体的な正常性が表示されます。クラスター ノードのコンポーネントの正常性状態をフィルタリングするには、ドーナツ グラフの個々のセクションを選択します。

       メモ: Windows Admin Center に表示されているノードのコンポーネントが「正常」であるにもかかわらず、クラスターの全体的な正常性状態が「重大」または「警告」として表示されることがあります。重大な正常性状態のコンポーネントの詳細については、それぞれの iDRAC コンソールにアクセスしてください。

     正常性状態 - フェールオーバー クラスターと Azure Stack HCI でサポートされるターゲット ノード コンポーネント 、p. 14 を参照してください。
   - **インベントリー** - コンポーネントのハードウェア インベントリーの詳細情報が表示されます。**概要**ページには、フェールオーバーまたはハイパーコンバージド クラスターのノードの基本的な詳細が表示されます。必要なノードを選択して、サーバー コンポーネントのハードウェア インベントリーの詳細を表示します。ハードウェア インベントリー - フェールオーバー クラスターと Azure Stack HCI でサポートされるターゲット ノード コンポーネント 、p. 14 を参照してください。
   - **アップデート** - ノードおよびコンポーネントのコンプライアンス グラフが表示されます。必要なノードを展開して、コンポーネントの詳細なコンプライアンスレポートを表示します。HCI およびフェールオーバー クラスターの PowerEdge サーバーとノードのアップデート 、p. 17 を参照してください。
   - **iDRAC** - 個々のノードの iDRAC の詳細が表示されます。OpenManage Integration を使用して、Windows Admin Center から iDRAC コンソールを直接起動することができます。HCI およびフェールオーバー クラスターの PowerEdge サーバーおよびノードの iDRAC の詳細の表示 、p. 16 を参照してください。

メモ: 正常性、ハードウェア インベントリー、および iDRAC の詳細はキャッシュされ、拡張機能が読み込まれるたびには読み込まれません。最新の正常性、インベントリーのステータス、および iDRAC の詳細を表示するには、[正常性状態] の右上隅にある**更新**をクリックします。

トピック：

正常性状態 - フェールオーバー クラスターと Azure Stack HCI でサポートされるターゲット ノード コンポーネント

[**クラスター - Azure Stack HCI**] ページで [**正常性**] タブを選択すると、フェールオーバーまたは HCI クラスターの全体的な正常性状態、およびフェールオーバー クラスターまたは Azure Stack HCI のノードの次のターゲット ノード コンポーネントの正常性状態が表示されます。全体的な正常性状態ドーナツ チャートの重大または警告のセクションを選択すると、対応するノードとコンポーネントがそれぞれ重大または警告状態に表示されます。

- CPU
- アクセラレーター
- メモリ
- ストレージコントローラ
- ストレージ エンクロージャ
- 物理ディスク
- iDRAC
- 電源装置
- ファン
- 電圧
- 温度

メモ: 正常性状態情報は、iDRAC バージョンの 4.00.00.00 以降を搭載した PowerEdge サーバーの YX4X モデルのアクセラレーターで使用できます。

メモ: Intel **DIMM** メモリーはアイコンで **IntelPersistent** として識別されます。

正常性状態は、ドーナツ グラフを使用して表示されます。ドーナツ グラフのさまざまなセクションを選択して、コンポーネントの正常性状態をフィルタリングできます。たとえば、赤色のセクションを選択すると、重大な正常性ステータスのコンポーネントのみが表示されます。

フェールオーバーまたは HCI クラスターでは、個々のコンポーネントに対してドーナツ グラフのさまざまなセクションが選択されている場合、一覧になったそれぞれのノードにコンポーネントの正常性ステータスが表示されます。ノードを展開すると、特定の正常性状態のコンポーネントが表示されます。

最新の正常性状態を表示するには、[**正常性**] タブの右上隅にある [**更新**] をクリックします。

メモ: 内蔵 SATA コントローラーに接続されているソフトウェア ストレージ コントローラーと物理ディスクの場合、正常性インベントリーのステータスは常に「不明」と表示されます。

ハードウェア インベントリー - フェールオーバー クラスターと Azure Stack HCI でサポートされるターゲット ノード コンポーネント

フェールオーバー クラスターまたは Azure Stack HCI のノードの、次のターゲット ノード コンポーネントのハードウェア インベントリーが表示されます。

- システム
- ファームウェア
- CPU
- アクセラレーター
- メモリ
- ストレージコントローラ

  ストレージ コントローラー内の物理ディスクを表示するには、[**関連するディスク**] で、[**ディスクの表示**] リンクをクリックします。物理ディスクは [**物理ディスク**] タブに表示されます。

  ストレージ エンクロージャ
- ネットワークデバイス
- 物理ディスク

ディスクの追加プロパティを表示するには、ディスクを選択し、[**詳細なプロパティ**] をクリックします。関連付けられているストレージ コントローラーを表示するには、[**詳細なプロパティ**] の下にあるストレージ コントローラーのリンクをクリックします。関連づけられているストレージ コントローラーが [**ストレージ コントローラー**] タブに表示されます。物理ディスクが CPU に接続されている場合、[**詳細なプロパティ**] でストレージ コントローラーのリンクが使用できなくなります。

物理ディスクの点滅および点滅解除

ノードを選択してから物理ディスクを選択し、[**点滅**] をクリックして物理ディスク上の LED の点滅を有効にします。LED は物理ディスクの状態を表します。物理ディスクの点滅によって、データ センター内の故障した物理ディスクを特定したり、識別したりすることができます。物理ディスクの点滅を無効にするには、ディスクを選択して [**点滅解除**] をクリックします。クラスターでは、選択したノードの点滅または点滅解除操作は、別のノードで点滅または点滅解除操作を使用する前に完了している必要があります。

メモ: 点滅および点滅解除の操作は以下では利用できない場合があります。

- Boot Optimized Storage Subsystem (BOSS) カードに関連付けられているディスク。
- iDRAC ファームウェア バージョンが 3.30.30.30 未満のデバイス。点滅および点滅解除操作を有効にするには、iDRAC ファームウェアを最新バージョンにアップデートします。
  - iDRAC ファームウェア バージョン 3.30.30.30 以降を使用していても、選択した対応ディスクの点滅および点滅解除操作を使用できない場合は、iDRAC ファームウェアを最新バージョンにアップグレードして、点滅および点滅解除操作を有効にします。

メモ:

- 点滅または点滅解除操作の実行中は、最新の正常性とハードウェア インベントリー情報を読み込む [**更新**] ボタンは無効です。また、正常性とハードウェア インベントリーが OMIMSWAC で読み込まれているときには、点滅および点滅解除の操作は無効になっています。
- 内蔵 SATA コントローラーに接続されている物理ディスクでの点滅および点滅解除操作は、「点滅と点滅解除は<ディスク名>でサポートされていない可能性があります。」というエラーが表示されて失敗します。

- 電源装置
- ファン

最新のハードウェア インベントリー情報を表示するには、[**インベントリー**] タブの右上隅にある [**更新**] をクリックします。

ターゲット ノードの iDRAC 詳細を表示するには、「HCI およびフェールオーバー クラスターの PowerEdge サーバーおよびノードの iDRAC の詳細の表示 、p. 16」を参照してください。

メモ: [**インベントリー**] の下では、ターゲット ノードで 2、3 個のコンポーネントの値が使用できなくなる可能性があるため、そのターゲット ノード コンポーネントの属性値が空白で表示されます。

メモ: ファームウェア インベントリーの下では、複数のポートを使用する一部のネットワーク デバイスに対して、該当するファームウェア バージョンがすべてのポートで同一であるため、そのファームウェア バージョンの 1 ポートのみが表示されます。

メモ: ストレージ エンクロージャ、ファームウェア インベントリー、およびメモリー コンポーネントのいくつかの属性についての情報は、次の場合は利用できないことがあります。

- YX2X および YX3X モデルの PowerEdge サーバー。
- 3.30.30.30 より前のバージョンの iDRAC を搭載した YX4X モデルの PowerEdge サーバー。

メモ: ストレージ エンクロージャの PCIe SSD バックプレーンでは、ほとんどの属性値を使用できます。

メモ: 正常性状態情報は、iDRAC バージョンの 4.00.00.00 以降を搭載した PowerEdge サーバーの YX4X モデルのアクセラレーターで使用できます。

メモ: Intel **DIMM** メモリーはアイコンで **IntelPersistent** として識別されます。

6

HCI およびフェールオーバー クラスターの PowerEdge サーバーおよびノードの iDRAC の詳細の表示

ターゲット ノードの次の iDRAC の詳細情報を表示するには、Microsoft Windows Admin Center の左上隅で [**サーバー マネージャー**] または [**クラスター マネージャー**] を選択して、リストからサーバーまたはクラスターを選択します。左ペインの [拡張機能] で、[**Dell EMC OpenManage Integration**] をクリックして、[**iDRAC**] タブに移動します。

メモ: フェールオーバー クラスターおよびハイパーコンバージド クラスターの場合、ノードを展開すると次の詳細情報が表示されます。

- iDRAC の IP アドレス IDRAC コンソールは、Microsoft Windows Admin Center から直接起動することができます。
- IPMI バージョン
- iDRAC ファームウェア バージョン

7

HCI およびフェールオーバー クラスターの PowerEdge サーバーとノードのアップデート

OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) では、HCI およびフェールオーバー クラスター内のターゲット ノードや HCI ノードの BIOS、ドライバー、ファームウェア、システム管理アプリケーションなど、コンプライアンスの詳細を生成し、コンポーネントをアップデートすることができます。オンラインまたはオフラインのカタログを使用して、コンプライアンスの詳細を生成し、コンポーネントをアップデートすることができます。

OMIMSWAC で、**アップデート**をクリックします。アップデート ウィンドウが表示されます。

このページでは、コンプライアンス レポートを生成して、次のようにコンポーネントをアップデートすることができます。

1. コンプライアンス レポートの生成：アップデート ソース カタログ (オンラインまたはオフラインのカタログ) を選択して、各デバイスのアップデートの詳細を取得し、コンプライアンス レポートを生成します。
2. コンプライアンス レポートの検証とコンポーネントの選択の確認：生成されたコンプライアンス レポートを確認します。デフォルトでは、非対応コンポーネント (ダウングレード可能のコンポーネントを除く) がすべて選択されています。アップグレードするコンポーネントを選択または選択解除し、コンポーネントの選択を確認します。
3. アップデート：ターゲット ノードまたはクラスターをアップデートします。

コンプライアンス レポートを生成し、ターゲット ノードをアップデートするには、「ターゲット ノードのアップデート」を参照してください。コンプライアンス レポートを生成し、HCI およびフェールオーバー クラスターのノードをアップデートするには、「HCI およびフェールオーバー クラスターのノードのアップデート」を参照してください。

OpenManage Integration は、オンラインまたはオフラインのカタログを使用してベースラインを作成します。カタログには、最新の BIOS、ドライバー、ファームウェア、システム管理アプリケーションのいずれかまたはすべてが含まれています。システム管理アプリケーションには、IC、ドライバー パック、iSM、OMSA などがあります。OpenManage Integration では、各デバイスのアップデートの詳細を取得するために、Dell EMC System Update Utility (DSU) ツールと、Dell EMC Inventory Collector (IC) ツールを使用します。DSU ツールおよび IC ツールは、コンプライアンス レポートを生成し、非対応デバイスをアップデートして修正するのに使用されます。

オフラインまたはオンライン カタログを選択した場合、OMIMSWAC は**設定** > **アップデート ツール**で設定された DSU ツールおよび IC ツールを収集します。アップデート ツールを設定するには、「アップデート コンプライアンス ツール設定の構成」を参照してください。DSU ツールおよび IC ツールが設定で構成されていない場合、OMIMSWAC がインターネットに接続されていれば、`www.downloads.dell.com` からこれらのツールがダウンロードされます。

Windows Admin Center の**通知**セクションで、新しいオンラインまたはオフラインのカタログ ファイルが使用可能になったときに通知されます。最新のコンプライアンス レポートを生成するには、**アップデート**タブで、[コンプライアンス レポートのアップデート] を実行します。

メモ: クラスター対応アップデート (CAU) 機能は、有効なライセンスを持つ次のプラットフォームでサポートされています。

- iDRAC ファームウェア 4.00.00.00 以降がインストールされた Dell EMC PowerEdge サーバーの YX4X モデルおよびそれ以降。
- iDRAC ファームウェア 4.00.00.00 以降がインストールされた Microsoft Azure Stack HCI 向け Dell EMC ソリューション。

ライセンスの詳細については、『OMIMSWAC インストール ガイド』の「*OpenManage Integration with Windows Admin Center のライセンス*」を参照してください。

トピック：

- アップデート コンプライアンス ツール設定の構成
- ターゲット ノードのアップデート
- HCI およびフェールオーバー クラスターのノードのアップデート

アップデート コンプライアンス ツール設定の構成

最新のアップデート コンプライアンス レポートおよびデバイス コンポーネントの詳細を生成するには、OpenManage Integration がインターネットに接続されていない場合は、アップデート コンプライアンス ツールの設定を行う必要があります。OpenManage Integration バージョン 1.1.1 に対応する Dell System Update (DSU) および Dell Inventory Collector (IC) ユーティリティーのバージョンは次のとおりです。

- DSU バージョン：1.8.1。https://downloads.dell.com/OMIMSWAC/DSU/から、DSU をダウンロードします。
- IC バージョン：https://downloads.dell.com/OMIMSWAC/IC/から IC をダウンロードします。

Offline-Dell EMC Repository Manager（DRM）カタログを使用してコンプライアンス レポートを生成してコンポーネントをアップデートするが、OMIMSWAC がインターネットに接続されていない場合は、次の設定が必要です。

1. [**設定**] タブで、DSU ユーティリティーが保存されている共有の場所を入力します。
   DSU は、Dell Update Packages をターゲット ノードに導入するために使用されます。
2. IC ユーティリティーが保存されている共有の場所を入力します。
   IC ユーティリティーは、ターゲット ノードからのハードウェア インベントリー情報の収集に使用されます。
3. 共有の場所をアクセスするためのユーザー資格情報を入力します。

   メモ: OMIMSWAC をアンインストールしても、[設定] ページにあるデータは削除されません。OMIMSWAC を後で再インストールした場合、[設定] ページで以前に設定されたデータは引き続き使用できます。ただし、パスワードは使用できません。

4. ユーティリティーがアクセス可能かどうかを確認するには、[**テスト接続**] をクリックします。
5. [**保存**] をクリックして、アップデート ツールの設定を保存します。

   アップデート ツール設定のパスワードは、現在のブラウザー セッションに対してのみ保持されます。OpenManage Integration with Microsoft Windows Admin Center のアップデート コンプライアンス機能を正しく動作させるには、新しいブラウザー セッションを開いた後にパスワードを再入力する必要があります。

   最新のアップデート コンプライアンス レポートを生成するには、「コンプライアンス レポートの生成 - ターゲット ノードおよび「コンプライアンス レポートの生成 - フェールオーバー クラスターおよび Azure Stack HCI 内のターゲット ノード コンポーネント」を参照してください。

プロキシ設定の構成

OMIMSWAC には、コンプライアンス レポートを生成するために、プロキシ設定を使用して、インターネットからカタログ、DSU、および IC の各ユーティリティーをダウンロードするオプションが用意されています。ただし、プロキシによってインターネットに接続されている OMIMSWAC では、オンライン カタログを使用したターゲット ノードまたはクラスターのアップデートはサポートされていません。この場合、オフライン カタログを使用したコンプライアンスとアップデートがサポートされています。

プロキシの設定を行って、ゲートウェイ システムとインターネット間の仲介として機能するプロキシ サーバーに接続することができます。OMIMSWAC のアップデート コンプライアンス ツールの設定が行われておらず、ゲートウェイ システムがインターネットに接続されていない場合、OMIMSWAC はプロキシ設定を使用してインターネットへの接続性をチェックします。

プロキシ サーバーに接続するには、次のようにします。

1. プロキシ サーバーの IP アドレスを以下の形式で入力します。
   https://<IP アドレス>または **http://<IP アドレス>**
2. プロキシ サーバーのポート番号を以下の形式で入力し、[**保存**] をクリックします。
   <ポート番号>（https）または**<ポート番号>（http）**

   例：443（https）または 80（http）

   最新のアップデート コンプライアンス レポートを生成するには、「コンプライアンス レポートの生成 - ターゲット ノードおよび「コンプライアンス レポートの生成 - フェールオーバー クラスターおよび Azure Stack HCI 内のターゲット ノード コンポーネント」を参照してください。

ターゲット ノードのアップデート

OpenManage Integration for Windows Administration Center を使用して、コンプライアンス レポート（BIOS、ドライバー、ファームウェア、システム管理アプリケーション）を表示し、ターゲット ノードのコンポーネントをアップデートすることができます。

コンプライアンスとアップデートの前提条件

コンプライアンス レポートを生成し、コンポーネントをアップデートする前に、次のことを行ってください。

- 『インストール ガイド』の*互換性マトリックス*に記載されているソフトウェアおよびハードウェア要件が満たされていることを確認します。
- ターゲット ノードを管理するには、[**管理に使用する資格情報**] オプションを使用してターゲット ノードに接続し、適切なターゲット ノード管理者の認証情報を入力します。また、ユーザーがゲートウェイ管理者のローカル ユーザー グループに属している

ことを確認します。[管理に使用する資格情報] の選択に関する詳細については、Microsoft のマニュアルの「Windows 管理センターを使ってみる」を参照してください。

- ターゲット ノードをアップデートする前に、ワークロードを十分に考慮します。
- ターゲット ノードのインベントリー情報が取得されていることを確認します。
- iDRAC ロックダウン モードが無効になっていることを確認します。iDRAC システム ロックダウン モードを無効にするには、iDRAC ドキュメントを参照してください。
- SAS-RAID_Driver については、次のことを確認してください。
  - SATA コントローラーが RAID モードに設定されている。
  - NVMe PCIe SSD が RAID モードに設定されている。

  RAID モードの設定の詳細については、「付録」を参照してください。
- アップデートするターゲット ノードに WAC がインストールされていないことを確認します。
- ターゲット ノードの IP アドレス、ホスト名、および完全修飾ドメイン名 (FQDN) を使用してターゲット ノードに到達可能であることを確認します。

  メモ: ターゲット ノードに到達できない場合、ターゲット ノードのアップデートが実行されると、アップデート ステータスが失敗と表示されることがあります。この場合、アップデートの直後にターゲット ノードを再起動してコンプライアンスを再実行すると、ターゲット ノード コンポーネントの状態が対応と表示される一方、ターゲット ノード全体のアップデート ステータスが失敗として表示される場合があります。

メモ: WAC がインストールされているターゲット ノードのアップデートは推奨されません。このシナリオをサポートするには、別の (WAC に関連しない) ターゲット ノードに WAC をインストールして、アップデートを完了します。

メモ: コンプライアンスまたはアップデートの進行中は、同一のターゲット ノードに MS WAC Update ツールからのアップデート リクエストを含む場合は、そのターゲット ノードでそれ以上のコンプライアンス タスクまたはアップデート タスクを実行することはできません。

手順 1: コンプライアンス レポートの生成 - ターゲット ノード コンポーネント

ターゲット ノードのコンプライアンス レポートを生成するには [**アップデート**] > [**アップデート ソース**] を選択し、次の手順に従って、使用可能なオフラインまたはオンラインのカタログ オプションのいずれかを選択します。

オンライン カタログを使用したコンプライアンス レポートの生成

オンライン カタログを使用するには、プロキシ設定の有無にかかわらず、OMIMSWAC がインターネットに接続されている必要があります。インターネットに接続されている OMIMSWAC で、[**アップデート ソース**] ドロップダウン リストのオンライン カタログ オプションを使用して、カタログを自動的にダウンロードすることができます。

コンプライアンスの詳細を表示するには、次のアクションを実行する必要があります。

1. [**アップデート**] > [**アップデート ソース**] で、使用可能なオンライン カタログ オプションのいずれかを選択します。

   ターゲット ノードに基づいて、対応するオンライン カタログがデフォルトで選択されています。

   次のように、使用可能なオンライン カタログは接続されているターゲット ノード/クラスターによって異なります。
   - PowerEdge サーバーおよび PowerEdge サーバーを含むクラスターの場合 : PowerEdge サーバーの検証済みバージョンのコンポーネントが含まれている Dell EMC エンタープライズ カタログ。
   - MX サーバーの場合 : PowerEdge MX モジュラーの検証済みバージョンのコンポーネントが含まれている Dell EMC MX ソリューション カタログ。
   - Azure Stack HCI クラスター ノードの場合 : AX ノードおよび Storage Spaces Direct Ready Node の検証済みバージョンのコンポーネントが含まれている Dell EMC Azure Stack HCI ソリューション カタログ。

   使用可能なカタログの詳細については、「付録」を参照してください。

2. [**次 : コンプライアンスの詳細**] を選択して、コンプライアンス レポートを生成します。

OMIMSWAC はカタログをダウンロードし、[**設定**] タブで構成された DSU ツールおよび IC ツールを収集して、コンプライアンス レポートを生成します。DSU ツールおよび IC ツールが [**設定**] で構成されていない場合、OMIMSWAC が `www.downloads.dell.com` からダウンロードし、コンプライアンス レポートを生成します。

コンプライアンスの詳細が割り出され、[**アップデート**] > [**コンプライアンスの詳細**] の下にあるレポートが使用可能になります。コンプライアンス レポートの詳細については、「コンプライアンス レポートの表示」を参照してください。

オフライン カタログを使用したコンプライアンス レポートの生成

OMIMSWAC がインターネットに接続されている場合でもされていない場合でも、オフライン - Dell EMC Repository Manager カタログを選択して、コンプライアンス レポートを生成することができます。

ターゲット ノード コンポーネントの最新のコンプライアンス レポートを生成する前に、以下を確認してください。OMIMSWAC がインターネットに接続されていない場合は、次の前提条件を満たし、Offline-Dell EMC Repository Manager (DRM) カタログを使用して、コンプライアンス レポートを生成し、コンポーネントをアップデートする必要があります。

- DSU および IC アプリケーションが配置されている共有の場所の詳細を設定します。「アップデート コンプライアンス ツール設定の構成」を参照してください。
- Dell EMC Repository Manager (DRM) アプリケーションを使用して、最新のカタログ ファイルを生成していること。サポートされている DRM のバージョンは、Dell EMC Repository Manager からダウンロードできます。

コンプライアンスの詳細を表示するには、次のアクションを実行します。

1. **[アップデート]** > **[アップデート ソース]** の下で、ドロップダウン リストから [**オフライン - Dell EMC Repository Manager カタログ**] を選択します。デフォルトでは、オンライン カタログが選択されています。

   オフライン - Dell EMC Repository Manager カタログ : DRM リポジトリーが共有された場所にあり、データ センターのインターネットに接続されていない OMIMSWAC 管理下のすべてのノードに適用できる場合。

2. カタログ ファイルが置かれている CIFS 共有パスとその CIFS 共有パスにアクセスするためのユーザー資格情報を入力して、[**次 : コンプライアンスの詳細**] を選択します。

   カタログ ファイルは、Dell EMC Repository Manager (DRM) アプリケーションを使用して生成できます。共有カタログ リポジトリーで、必要なすべての Dell Update Packages (DUP) がターゲット ノードで使用可能であることを確認します。

   新しいカタログ パスを指定した場合は、アップデート コンプライアンスを割り出すために使用された以前のパスが使用できなくなります。

OMIMSWAC は、共有パスからカタログを収集し、[**設定**] タブで構成された DSU ツールおよび IC ツールを収集して、コンプライアンス レポートを生成します。DSU ツールおよび IC ツールが [**設定**] で構成されていない場合は、インターネットに接続されている OMIMSWAC は、`www.downloads.dell.com` からこれらのツールをダウンロードし、コンプライアンス レポートを生成します。

メモ: 個別のカタログ ファイルには、それぞれサーバー マネージャーとクラスター マネージャーのユーザー資格情報を使用してアクセスする必要があります。

コンプライアンスの詳細が割り出され、**[アップデート]** > **[コンプライアンスの詳細]** の下にあるレポートが使用可能になります。コンプライアンス レポートの詳細については、「コンプライアンス レポートの表示」を参照してください。

手順 2 : コンプライアンス レポートの表示とコンポーネントの選択 — ターゲット ノード コンポーネント

アップデート コンプライアンスの詳細が割り出され、コンプライアンス レポートが表示されます。ドーナツ グラフは、カラー コードを使用して、対応、緊急、推奨、オプション状態にあるコンポーネントの数を表します。コンプライアンス レポートには、コンポーネント名、現在のバージョン、タイプ、ベースライン バージョン、コンプライアンス ステータス、重要度、コンプライアンス タイプを含む、すべてのコンポーネントの詳細なビューが表示されます。

属性名	説明
コンポーネント名	コンポーネント名を指定します。 例 : `Serial-ATA_Firmware_6FGD4_WN64_E012_A00`
対応性	対応または非対応のどちらかの、コンプライアンス タイプを指定します。 • **対応** - このカテゴリのターゲット ノードには、インポートされたカタログと同じバージョンの BIOS、ドライバー、ファームウェア、システム管理アプリケーションがあります。 • **非対応** - このカテゴリのターゲット ノードには、BIOS、ドライバー、ファームウェア、システム管理アプリケーションのいずれかのアップデートが必要です。
重大度	コンプライアンスが緊急、推奨、またはオプションかを指定します。

	• 緊急 - このアップデートには、Dell EMC システムまたは関連コンポーネントの信頼性および可用性を向上させる変更が含まれています。そのため、このアップデートをただちに適用してください。 • 推奨 - このアップデートには、システム ソフトウェアを最新に保ち、他のシステム モジュール (ファームウェア、BIOS、ドライバー、システム管理アプリケーションなど) との互換性を維持するための機能強化や機能変更が含まれています。 • オプション - このアップデートには、特定の設定を行っている場合にのみ適用される変更、または環境によっては適用されない可能性のある新機能が含まれています。お使いのシステムに適用されるかどうかを判断するために、アップデートの仕様を確認してください。
現在のバージョン	現在のコンポーネントのバージョンを指定します。 例：E012
ベースライン バージョン	インポートされたカタログに属するバージョンを指定します。 例：E013
タイプ	コンポーネント タイプを指定します。例：ファームウェア、BIOS、ドライバー、アプリケーション
コンプライアンス タイプ	コンポーネントがアップグレード可能、ダウングレード可能、同一かを指定します。 • アップグレード可能 - コンポーネントは現在のバージョンからアップグレードすることができます。 • ダウングレード可能 - コンポーネントは、現在のバージョンからダウングレードすることができます。 • 同一 - コンポーネントの現在のバージョンはベースライン バージョンと同じです。

1. デフォルトでは、すべての非対応アップグレード可能コンポーネントが選択されています。

   選択したコンポーネントをクリアするか、アップデートする非対応のダウングレード可能コンポーネントを選択します。ただし、デフォルトの選択内容を変更する場合は、対応するコンポーネントのファームウェアとドライバー間の依存関係が満たされていることを確認します。

2. アップデートするコンポーネントを選択したら、[**コンプライアンスの詳細**] で [**次：サマリ**] をクリックして、確認のためにサマリ レポート ページに進みます。

   メモ: コンポーネントを選択して確認しても、ターゲット ノード上の iDRAC でロックダウン モードが有効になっていると、エラーが発生し、アップデートを続行できません。ターゲット ノードをアップデートする前に、OMIMSWAC によって管理されているターゲット ノードでロックダウン モードを無効にします。iDRAC システム ロックダウン モードを無効にするには、iDRAC ドキュメントを参照してください。

   - アップデート操作中にコンポーネントの選択を変更するには、[**サマリ**] タブで [**戻る**] をクリックして [**コンプライアンスの詳細**] タブに移動し、コンポーネントの選択を選択または選択解除します。
   - アップデート ソースを変更してコンプライアンスを再実行するには、[**終了**] をクリックして [**アップデート ソース**] に移動します。

メモ: カタログにコンポーネントへのアップデートが含まれていない場合、コンポーネントは、OpenManage Integration with Microsoft Windows Admin Center 統合を使用して生成されたコンプライアンス レポートに表示されません。

手順 3：アップデート - ターゲット ノード コンポーネント

[**コンプライアンスの詳細**] タブでコンプライアンス レポートを生成し、[**サマリ**] タブでコンポーネントの選択を確認したら、次の手順を実行して、ターゲット ノード コンポーネントをアップデートします。

1. PowerEdge サーバーの BIOS、ドライバー、ファームウェア、システム管理アプリケーションのいずれかまたはすべてを最新バージョンにアップデートするには、[**サマリ**] の下で [**次：アップデート**] をクリックします。[**アップデート ステータス**] ウィンドウが表示されます。

   メモ: アップデートの進行中は、ブラウザーを終了または閉じることは推奨されません。ブラウザーを閉じたり、終了したりすると、ターゲット ノードのアップデートが失敗する場合があります。

2. OMIMSWAC は、アップデート ジョブが完了すると通知します。
   - アップデートが正常に完了すると、コンプライアンス レポート (以前の選択に基づく) が自動的に再計算され、[**アップデート**] タブに表示されます。
   - アップデート操作が失敗した場合は、次のパスに格納されているログ ファイルで詳細を確認してください。
     - ゲートウェイ システム：<Windows ディレクトリ >\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs
     - Windows 10 ゲートウェイ システム：<Windows インストール ドライブ>\Users\<ユーザー名 >\AppData\Local\Temp\generated\logs
   - 再度コンプライアンス レポートを実行するには、[**コンプライアンスを再実行**] をクリックして、コンプライアンス設定の詳細を入力します。

HCI およびフェールオーバー クラスターのノードのアップデート

OpenManage Integration for Windows Admin Center (OMIMSWAC) でのクラスター対応アップデート (CAU) 機能を使用すると、ワークロードに影響を与えることなく、コンプライアンス レポート (BIOS、ドライバー、ファームウェア、システム管理アプリケーション) を表示し、HCI およびフェールオーバー クラスターのノードのコンポーネントをアップデートすることができます。

メモ: CAU 機能は、有効なライセンスを持つ次のプラットフォームでサポートされています。

- iDRAC ファームウェア 4.00.00.00 以降がインストールされた Dell EMC PowerEdge サーバーの YX4X モデルおよびそれ以降。
- iDRAC ファームウェア 4.00.00.00 以降がインストールされた Microsoft Azure Stack HCI 向け Dell EMC ソリューション。

コンプライアンスとアップデートの前提条件

コンプライアンス レポートを生成し、コンポーネントをアップデートする前に、次のことを行ってください。

- 『インストール ガイド』の*互換性マトリックス*に記載されているソフトウェアおよびハードウェア要件が満たされていることを確認します。
- アップデート コンプライアンスを実行する前に、クラスター サービスが実行されていることを確認します。クラスター サービスが実行されていないと、ターゲット ノードのアップデート コンプライアンス レポートが生成されない場合があります。
- クラスターを管理するには、**管理に使用する資格情報**オプションを使用してクラスターに接続し、適切なクラスター管理者の認証情報を入力します。また、ユーザーがゲートウェイ管理者のローカル ユーザー グループに属していることを確認します。[管理に使用する資格情報] の選択に関する詳細については、Microsoft のマニュアルの「Windows 管理センターを使ってみる」を参照してください。
- フェールオーバー クラスター管理ツール (RSAT-Clustering-Mgmt) がターゲット ノードにインストールされていることを確認します。
- ターゲット ノードのインベントリー情報が取得されていることを確認します。
- CAU をトリガーする前に、物理ディスクと仮想ディスクの両方が正常な状態であることを確認します。
- iDRAC ロックダウン モードが無効になっていることを確認します。iDRAC システム ロックダウン モードを無効にするには、iDRAC ドキュメントを参照してください。
- SAS-RAID_Driver については、次のことを確認してください。
  - SATA コントローラーが RAID モードに設定されている。
  - NVMe PCIe SSD が RAID モードに設定されている。

  RAID モードの設定の詳細については、「付録」を参照してください。
- ターゲット ノードの IP アドレス、ホスト名、および完全修飾ドメイン名 (FQDN) を使用してターゲット ノードに到達可能であることを確認します。

  メモ: ターゲット ノードに到達できない場合、ターゲット ノードのアップデートが実行されると、アップデート ステータスが失敗と表示されることがあります。この場合、アップデートの直後にターゲット ノードを再起動してコンプライアンスを再実行すると、ターゲット ノード コンポーネントの状態が対応と表示される一方、サーバー全体のアップデート ステータスが失敗として表示される場合があります。
- CAU 機能を使用するには、OMIMSWAC プレミアム ライセンスがすべてのクラスター ノードにインストールされていることを確認します。ライセンスを確認するには、コンプライアンス レポートを生成して、各ノードにインストールされているライセンスを表示することができます。

メモ: CAU をトリガーする前に、クラスターの妥当性検査を行うことをお勧めします。クラスターの検証の詳細については、Microsoft ドキュメント『クラスターのハードウェアの検証』を参照してください。

メモ: クラスター ノードに WAC がインストールされているクラスターのアップデートは推奨されません。このシナリオをサポートするには、クラスターの一部ではない別のシステムに WAC をインストールして、アップデートを完了します。

メモ: コンプライアンスまたはアップデートの進行中は、同一のクラスターに MS WAC Update ツールからのアップデート リクエストを含む場合は、そのクラスターでそれ以上のコンプライアンス タスクまたはアップデート タスクを実行することはできません。

メモ: CAU 機能は Dell EMC PowerEdge サーバーの YX2X および YX3X モデルではサポートされていません。

手順 1 : コンプライアンス レポートの生成 - フェールオーバー クラスターおよび Azure Stack HCI 内のターゲット ノード コンポーネント

フェールオーバー クラスターおよび Azure Stack HCI でターゲット ノード コンポーネントのコンプライアンス レポートを生成するには、[**アップデート**] > [**アップデート ソース**] を選択し、次の手順に従って、使用可能なオフラインまたはオンラインのカタログ オプションのいずれかを選択します。

オンライン カタログを使用したコンプライアンス レポートの生成

オンライン カタログを使用するには、OMIMSWAC がインターネットに接続されている必要があります。インターネットに接続されている OMIMSWAC で、[**アップデート ソース**] ドロップダウン リストのオンライン カタログ オプションを使用して、カタログを自動的にダウンロードすることができます。

コンプライアンスの詳細を表示するには、次のアクションを実行する必要があります。

1. [**アップデート**] > [**アップデート ソース**] で、使用可能なオンライン カタログ オプションのいずれかを選択します。クラスターに基づいて、対応するオンライン カタログがデフォルトで選択されています。

   次のように、使用可能なオンライン カタログは接続されているクラスター/ターゲット ノードによって異なります。

   - PowerEdge サーバーおよび PowerEdge サーバーを含むクラスターの場合 : PowerEdge サーバーの検証済みバージョンのコンポーネントが含まれている Dell EMC エンタープライズ カタログ。
   - MX サーバーの場合 : PowerEdge MX モジュラーの検証済みバージョンのコンポーネントが含まれている Dell EMC MX ソリューションカタログ。
   - Azure Stack HCI クラスター ノードの場合 : AX ノードおよび Storage Spaces Direct Ready Node の検証済みバージョンのコンポーネントが含まれている Dell EMC Azure Stack HCI ソリューション カタログ。

   使用可能なカタログの詳細については、「付録」を参照してください。

2. [**次 : コンプライアンスの詳細**] を選択して、コンプライアンス レポートを生成します。

OMIMSWAC はカタログをダウンロードし、[**設定**] タブで構成された DSU ツールおよび IC ツールを収集して、コンプライアンス レポートを生成します。DSU ツールおよび IC ツールが [**設定**] で構成されていない場合、OMIMSWAC が `www.downloads.dell.com` からダウンロードし、コンプライアンス レポートを生成します。

[**コンプライアンスの詳細**] ウィンドウで生成されたコンプライアンス レポートに自動的に移動します。コンプライアンス レポートの詳細については、「コンプライアンス レポートの表示」を参照してください。

オフライン カタログを使用したコンプライアンス レポートの生成

OMIMSWAC がインターネットに接続されている場合でもされていない場合でも、オフライン - Dell EMC Repository Manager カタログを選択して、コンプライアンス レポートを生成することができます。

クラスターの最新のコンプライアンス レポートを生成する前に、以下を確認してください。OMIMSWAC がインターネットに接続されていない場合は、次の前提条件を満たし、Offline-Dell EMC Repository Manager (DRM) カタログを使用して、コンプライアンス レポートを生成し、コンポーネントをアップデートする必要があります。

- DSU および IC アプリケーションが配置されている共有の場所の詳細を設定します。「アップデート コンプライアンス ツール設定の構成」を参照してください。
- Dell EMC Repository Manager (DRM) アプリケーションを使用して、最新のカタログ ファイルを生成していること。サポートされている DRM のバージョンは、Dell EMC Repository Manager からダウンロードできます。

コンプライアンスの詳細を表示するには、次のアクションを実行します。

1. [**アップデート**] > [**アップデート ソース**] の下で、ドロップダウン リストから [**オフライン - Dell EMC Repository Manager カタログ**] を選択します。デフォルトでは、オンライン カタログが選択されています。

   オフライン - Dell EMC Repository Manager カタログ : DRM リポジトリーが共有の場所で使用可能であり、データ センターのインターネットに接続されていない OMIMSWAC 管理下のすべてのデバイスに適用できる場合。

メモ: Azure stack HCI のコンプライアンス レポートを生成するには、Azure Stack HCI カタログ ファイルを使用することをお勧めします。

2. カタログ ファイルが置かれている CIFS 共有パスとその CIFS 共有パスにアクセスするためのユーザー資格情報を入力して、[**次：コンプライアンスの詳細**] を選択し、コンプライアンス レポートを生成します。

   カタログ ファイルは、Dell EMC Repository Manager (DRM) アプリケーションを使用して生成できます。共有カタログ リポジトリーで、必要なすべての Dell Update Packages (DUP) がターゲット ノードで使用可能であることを確認します。

   新しいカタログ パスを指定した場合は、アップデート コンプライアンスを割り出すために使用された以前のパスが使用できなくなります。

OMIMSWAC は、共有パスからカタログを収集し、[**設定**] タブで構成された DSU ツールおよび IC ツールを収集して、コンプライアンス レポートを生成します。DSU ツールおよび IC ツールが [**設定**] で構成されていない場合は、インターネットに接続されている OMIMSWAC は、`www.downloads.dell.com` からこれらのツールをダウンロードし、コンプライアンス レポートを生成します。

メモ: 個別のカタログ ファイルには、それぞれサーバー マネージャーとクラスター マネージャーのユーザー資格情報を使用してアクセスする必要があります。

[**コンプライアンスの詳細**] ウィンドウで生成されたコンプライアンス レポートに自動的に移動します。コンプライアンス レポートの詳細については、「コンプライアンス レポートの表示」を参照してください。

手順 2：コンプライアンス レポートの表示とコンポーネントの選択 - フェールオーバー クラスターおよび Azure Stack HCI 内のターゲット ノード コンポーネント

アップデート コンプライアンスの詳細が割り出され、コンプライアンス レポートが表示されます。ドーナツ グラフは、カラー コードを使用して、対応、緊急、推奨、オプション状態にあるコンポーネントの数を表します。コンプライアンス レポートには、コンポーネント名、現在のバージョン、タイプ、ベースライン バージョン、コンプライアンス ステータス、重要度、コンプライアンス タイプを含む、すべてのコンポーネントの詳細なビューが表示されます。

HCI およびフェールオーバー クラスターでは、個々のターゲット ノードとコンポーネントのアップデート コンプライアンスは、2 つのドーナツ グラフ (ノードの概要とコンポーネントの概要) を使用して表されます。さらに詳細を分析するには、コンプライアンス レポート内の個々のノードを確認して、コンポーネントの現在のバージョンとベースライン バージョン、およびコンプライアンス タイプを取得し、非対応、緊急、推奨、オプションの状態にあるすべてのノードとコンポーネントをそれぞれ表示します。

コンプライアンス情報とともに、各ノードのライセンス ステータス (OMIMSWAC プレミアム ライセンス) も表示されます。クラスターに参加しているすべてのターゲット ノードには、有効なライセンスが必要です。有効なライセンスがない場合は、クラスターのアップデートに進むことはできません。OMIMSWAC のライセンスの詳細については、『OMIMSWAC インストール ガイド』を参照してください。

属性名	説明
コンポーネント名	コンポーネント名を指定します。 たとえば、次のとおりです。 `Serial-ATA_Firmware_6FGD4_WN64_E012_A00`
対応性	対応または非対応のどちらかの、コンプライアンス タイプを指定します。 ● `Compliant` - このカテゴリーのターゲット ノードには、インポートされたカタログと同じバージョンの BIOS、ドライバー、ファームウェア、システム管理アプリケーションが含まれます。 ● `Non-Compliant` - このカテゴリーのターゲット ノードには、BIOS、ドライバー、ファームウェア、システム管理アプリケーションのいずれかのアップデートが必要です。
重大度	コンプライアンスが緊急、推奨、またはオプションかを指定します。 ● `Urgent` - このアップデートには、Dell EMC システムまたは関連コンポーネントの信頼性および可用性を向上させる変

	更が含まれています。そのため、このアップデートをただちに適用してください。 • Recommended - このアップデートには、システム ソフトウェアを最新に保ち、その他のシステム モジュール (BIOS、ドライバー、ファームウェア、システム管理アプリケーション)との互換性を維持するための機能強化や機能変更が含まれています。 • Optional - このアップデートには、特定の設定を行っている場合にのみ適用される変更、またはお使いの環境によっては適用されない可能性のある新機能が含まれています。お使いのシステムに適用されるかどうかを判断するために、アップデートの仕様を確認してください。
現在のバージョン	現在のコンポーネントのバージョンを指定します。 たとえば、次のとおりです。 E012
ベースライン バージョン	インポートされたカタログに属するバージョンを指定します。たとえば、次のとおりです。 E013
タイプ	コンポーネント タイプを指定します。例：Firmware、BIOS、Driver、 Application
コンプライアンス タイプ	コンポーネントがアップグレード可能、ダウングレード可能、同一かを指定します。 • Upgradable：コンポーネントを現在のバージョンからアップグレードできます。 • Downgradable：コンポーネントを現在のバージョンからダウングレードできます。 • Same:コンポーネントの現在のバージョンはベースライン バージョンと同じです。

1. デフォルトでは、すべての非対応アップグレード可能コンポーネントがアップデート用に選択されています。

   選択したコンポーネントをクリアするか、アップデートする非対応のダウングレード可能コンポーネントを選択します。ただし、デフォルトの選択内容を変更する場合は、対応するコンポーネントのファームウェアとドライバー間の依存関係が満たされていることを確認します。

2. コンポーネントが選択されたら、[**コンプライアンスの詳細**] で、[**次：サマリ**] をクリックして、確認のためにサマリ レポート ページに進みます。

   メモ: コンポーネントを選択して確認しても、ターゲット ノード上の iDRAC でロックダウン モードが有効になっていると、エラーが発生し、アップデートを続行できません。クラスターをアップデートする前に、OMIMSWAC によって管理されているターゲット ノードでロックダウン モードを無効にします。iDRAC システム ロックダウン モードを無効にするには、iDRAC ドキュメントを参照してください。

   - アップデート操作中にコンポーネントの選択を変更するには、[**サマリ**] タブで [**戻る**] をクリックして [**コンプライアンスの詳細**] タブに移動し、コンポーネントの選択を選択または選択解除します。
   - アップデート ソースを変更してコンプライアンスを再実行するには、[**終了**] をクリックして [**アップデート ソース**] に移動します。

メモ: カタログにコンポーネントへのアップデートが含まれていない場合、コンポーネントは、OpenManage Integration with Microsoft Windows Admin Center 統合を使用して生成されたコンプライアンス レポートに表示されません。

手順 3：アップデート - フェールオーバー クラスターおよび Azure Stack HCI 内のターゲット ノード コンポーネント

[**コンプライアンスの詳細**] タブでコンプライアンス レポートを生成し、[**サマリ**] タブでコンポーネントの選択を確認した後、次の手順を実行して、フェールオーバー クラスターと Azure Stack HCI のターゲット ノード コンポーネントをアップデートします。

1. Azure Stack HCI およびフェールオーバー クラスター内のターゲット ノード コンポーネントの BIOS、ドライバー、ファームウェア、システム管理アプリケーションのいずれかまたはすべてを最新バージョンにアップデートするには、[**サマリ**] の下で [**次：クラスター対応アップデート**] をクリックします。

   CredSSP を有効にするためのメッセージが表示されます。

2. [**はい**] をクリックして CredSSP を有効にして、選択したコンポーネントのアップデートを続行します。[**アップデート ステータス**] ウィンドウが表示されます。

   セキュリティを向上させるには、アップデート操作が完了した後で CredSSP を無効にします。

   メモ: [**アップデート ステータス**] ウィンドウでアップデートが進行中である間は、ブラウザーを終了または閉じないことをお勧めします。ブラウザーを閉じたり、終了したりすると、クラスターのアップデートが失敗する場合があります。

   UI セッションがアクティブであるかどうかに関係なく、アップデート ジョブはバックグラウンドで継続されます。UI セッションがアクティブな場合は、ノード レベルの進行状況ステータスが表示されます。OMIMSWAC は、アップデート ジョブが完了すると通知します。

   - アップデートが正常に完了すると、コンプライアンス レポート (以前の選択に基づく) が自動的に再計算され、[**アップデート**] タブに表示されます。
   - アップデート操作が失敗した場合は、トラブルシューティングのために、次のパスに格納されているログ ファイルを確認します。
     - ゲートウェイ システム：`<Windows ディレクトリ >\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs`
     - Windows 10 ゲートウェイ システム：`<Windows インストール ドライブ>\Users\<ユーザー名 >\AppData\Local\Temp\generated\logs`
   - 再度コンプライアンス レポートを実行するには、[**コンプライアンスを再実行**] をクリックして、コンプライアンス設定の詳細を入力します。

メモ: アップデート ジョブが失敗した場合、アップデートされたコンポーネントは古いバージョンにロールバックされません。そのため、クラスター内のノード間で BIOS、ファームウェア、またはドライバーのバージョンが同じレベルではないことがあります。この場合は、アップデートされたコンポーネントを除外してアップデートを再度実行してください。

8

トラブルシューティング

トピック：

OMIMSWAC 拡張ログの可用性

ターゲット ノードとクラスター ノードの OpenManage Integration with Microsoft Windows Admin Center（OMIMSWAC）拡張機能のログは、ターゲット ノードの`<Windows Directory>\Temp\OMIMSWAC` で入手できます。このログは、OMIMSWAC 機能が実行されたときに情報を収集し、OMIMSWAC 操作の実行中に発生したエラーに関するデバッグ情報も提供します。各種 OMIMSWAC 機能のログには、次の命名規則を使用して簡単にアクセスできます。

- ハードウェアおよび正常性インベントリーの場合： `Inventory<ID*>`
- 更新コンプライアンスの場合： `FirmwareCompliance<ID*>`
- 更新通知の場合： `Notification<ID*>`

アップデート操作ログの可用性

アップデート コンプライアンス機能のアプリケーション ログは、次のパスから入手できます。

- ゲートウェイ システム： `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs`
- Windows 10 ゲートウェイ システム： `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs`

オンライン カタログのダウンロード ステータスは、アプリケーション ログに記録され、オンライン カタログのダウンロード エラーをトラブルシューティングするために参照することができます。

オンライン カタログ ソースが選択されていて、DSU と IC が事前に設定されていない場合、OMIMSWAC は次のパスにあるカタログ、DSU、および IC の各ユーティリティーをダウンロードします。

- ゲートウェイ システム： `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\Share\temp\<server/cluster_name>`
- Windows 10 ゲートウェイ システム： `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\Share\temp\<server/cluster_name>`

ダウンロードしたカタログ ファイル、DSU、および IC が、コンプライアンスの生成およびアップデート時に変更されていないことを確認します。カタログ ファイル、DSU、および IC の各ユーティリティーは、コンプライアンス レポートが生成され、アップデートされた後に自動的に削除されます。

ストレージをメンテナンス モードにするために HCI クラスターでアップデート前に実行されるスクリプトのログは、各ノード上の `<Windows Directory>\Temp\precau.log` にあります。また、メンテナンス モードからストレージをリストアするために HCI クラスターでアップデート後に実行されるスクリプトのログは、各ノード上の`<Windows Directory>\Temp\postcau.log` にあります。

インベントリー情報をフェッチするために必要なファイルをターゲット ノードにコピーすることはできません。

次の点を確認します。

- ターゲット ノードが再起動状態になっていないこと、また、電源がオンになっていること。
- ファイアウォールによって、SMB ポート 445 を介した通信がブロックされていないこと。詳細については、「Windows Admin Center の環境の準備」を参照してください。

iDRAC から正常性およびハードウェア インベントリーを取得できません。

iDRAC から正常性およびハードウェア インベントリー情報を取得するには、次のことを確認します。

- PowerEdge サーバーを管理するために、OMIMSWAC はオペレーティング システムから iDRAC への内部パススルー インターフェイスを使用します。デフォルトでは、iDRAC は IP アドレス 169.254.0.1/<*サブネット*>、または 169.254.1.1/<*サブネット*>を使用して到達可能になります。ただし、ホストに同じサブネット内に別のネットワーク インターフェイスがある場合 (たとえば、VMFleet などのツールがインストールされている場合)、OMIMSWAC はホスト オペレーティング システムから iDRAC に通信できない場合があります。

  競合を解決するには、iDRAC にログインし、オペレーティング システムから iDRAC へのパススルーのセクションで USB NIC の IP アドレスを変更します。この IP アドレスの割り当てに関する詳細については、サポート サイトにある iDRAC のマニュアルを参照してください。

- クラスターを管理するには、OMIMSWAC でクラスターを管理する前に、IP アドレス、ホスト名、および完全修飾ドメイン名 (FQDN) を使用して、すべてのクラスター ノードに到達できるようにします。
- Redfish サービスが無効になっている場合は、iDRAC UI を使用して Redfish サービスを有効にします。詳細な情報については、Dell EMC のサポート サイトにある iDRAC のマニュアルを参照してください。
- ユーザーを作成するために、iDRAC でユーザー スロットを使用できます。

点滅または点滅解除操作用のディスクを完了または選択できません。

- **原因**：Redfish サービスが有効になっていません。

  対応処置：iDRAC UI を使用して Redfish サービスを有効化します。詳細な情報については、Dell EMC のサポート サイトにある iDRAC のマニュアルを参照してください。

- **原因**：ハードウェア インベントリーが OMIMSWAC で読み込まれた後で物理ディスクが削除されると、「`Blink may not be supported with <Disk_Name>`」エラーが発生して点滅および点滅解除の操作が失敗します。

  対応処置：物理ディスクを挿入し、[**更新**] をクリックして OMIMSWAC でインベントリー情報を再読み込みし、点滅および点滅解除操作を再度実行します。

- **原因**：iDRAC のファームウェア バージョンが 3.30.30.30 未満の場合、物理ディスクを点滅または点滅解除するように選択することはできません。

  対応処置：iDRAC ファームウェアを最新バージョンにアップデートし、点滅および点滅解除操作を再試行します。

- 物理ディスクが内蔵 SATA コントローラーに接続されていて正常性状態が [`Unknown`] である場合、点滅や点滅解除の操作は失敗します。これは、ディスクでの点滅や点滅解除操作がサポートされていない場合があることを示します。

ライセンスのステータスが不明またはライセンスなし

ライセンスのステータスが [`Unknown`] であるか [`Non-licensed`] の場合は、次のことを確認します。

- ライセンスの有効期限が切れていないこと。
- ライセンスが各ターゲット ノードに存在すること。
- ターゲット ノードが再起動状態になっていないこと、また、電源がオンになっていること。

- Redfish が有効になっていること。
- Azure Stack HCI ライセンスまたは PowerEdge サーバー ライセンスが、それぞれのハードウェアにインポートされていること。Azure Stack HCI ライセンスの PowerEdge サーバーへのインポート、または PowerEdge サーバー ライセンスの Azure Stack HCI へのインポートはサポートされません。

問題が解決しない場合は、次の操作を実行します。

1. iDRAC に移動します。
2. Redfish サービスが有効になっていることを確認します。
3. OS to iDRAC パススルーを無効にしてから有効にします。

   OS to iDRAC パススルーの有効化/無効化の詳細に関しては、『iDRAC ユーザー ガイド』を参照してください。

ライセンス ログの可用性

ライセンス関連のログは次のパスから入手でき、[*クリーンアップ*] ファイルで「*DellLicenseCollection*」を検索することによって見つけることができます。

- ゲートウェイ システム：`<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\CleanupXXXXXXXXXXXXXX.log`
- Windows 10 ゲートウェイ システム：`<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\CleanupXXXXXXXXXXXXXX.log`

サーバー操作およびクラスター対応アップデート操作に必要なコンポーネントをダウンロード中にジョブが失敗しました。

原因：Dell EMC Repository Manager (DRM) を使用してリポジトリーをエクスポートするときに、エクスポート ジョブが「部分的に成功しました」のステータスで完了する場合があります。この場合、1 つまたは複数の DUP がリポジトリーから失われている可能性があります。

対応処置：DRM でリポジトリーのエクスポートを再試行し、ジョブが正常に完了したことを確認します。

原因：アップデート ソースがオンライン ソースとして選択されているときに、1 つまたは複数のコンポーネントがダウンロードされない場合があります。

対応処置：インターネットに接続されていることを確認し、オンライン ソースからカタログのダウンロードを再試行します。詳細については、『Dell EMC Repository Manager ユーザー ガイド』を参照してください。

アップデート中に CredSSP が失敗しました

- **原因**：クラスターのアップデート中に、CredSSP を使用した資格情報の委任が失敗する場合があります。

  対応処置：完全修飾ドメイン名を使用してクラスターを再接続し、[**すべてのサーバーにこの資格情報を使用する**] チェック ボックスをクリックします。

  例えば、ドメイン名が test.dev.com の場合は、ドメイン名として **test.dev.com\administrator** を使用し、[**すべてのサーバーにこの資格情報を使用する**] チェック ボックスをクリックします。

- **原因**：リモート マシンで CredSSP 認証を使用してスクリプトを実行すると、アップデート ジョブがエラーで失敗する場合があります。

  この問題は、ゲートウェイ マシンで CredSSP が無効になっているために発生します。

  対応処置：この問題を解決するには、次の手順を実行します。

  1. PowerShell ウィンドウから次を実行します：`gpedit`
  2. [グループ ポリシー エディター] ウィンドウで、**[PC 設定]** > **[管理用テンプレート]** > **[システム]** > **[資格情報の委任]** に移動します。
  3. [**NTLM のみのサーバー認証での新しい資格情報の委任を許可する**] を選択し、有効にします。
  4. PowerShell で、`gpupdate /force` を実行します。

コンプライアンス レポートの生成中にジョブが失敗しました

原因：[管理に使用する資格情報] ではなくシングル サインオンを使用してターゲット ノードまたはクラスターに接続し、OMIMSWAC を使用してコンプライアンス レポートを生成すると、コンプライアンスの生成が失敗する場合があります。

対応処置：ターゲット ノードまたはクラスターに接続する前に、[管理に使用する資格情報] を選択し、適切なサーバー管理者またはクラスター管理者のアカウントを指定するようにしてください。

原因：コンプライアンス レポートの生成時に、コンプライアンス レポートの生成が失敗し、次のエラーがログに記録されることがあります。

```
Starting a command on the remote server failed with the following error message : The WinRM
client sent a request to the remote WS-Management service and was notified that the request
size exceeded the configured MaxEnvelopeSize quota. For more information, see the
about_Remote_Troubleshooting Help topic.
```

対応処置：以下を確認してください。

- ゲートウェイ システムとターゲット ノードの間のネットワーク接続が損なわれていない。
- ゲートウェイ システムとターゲット ノード間でファイルのコピーが機能している。これを確認するには、次のようにします。
  1. 次の PowerShell コマンドを実行して、ターゲット ノードの資格情報に基づいてセッションを作成します。

     ```
     $SecurePassword = convertto-securestring <password> -asplaintext -force

     $credential = New-Object System.Management.Automation.PSCredential -ArgumentList <userid>,
     $SecurePassword

     $session = New-PSSession -ComputerName <MN FQDN> -Credential $credential -ErrorAction
     SilentlyContinue
     ```

  2. 「Test.txt」が C:\ドライブにあることを前提として、障害の発生したターゲット ノードにテストファイルをコピーします。

     ```
     Copy-Item -Path "C:\Test.txt" -Destination "C:\" -Recurse -Force -ToSession $session
     ```

- 前述のアクションを実行した後も問題が解決しない場合は、ターゲット ノードで (ファイルコピーが失敗している) Windows リモート管理 (WS-MANAGEMENT) サービスを再開してから、コンプライアンスを再実行してみてください。

原因：クラスターのコンプライアンス レポートを生成するときに、クラスター ノードのコンプライアンス レポートの生成が失敗する場合があります。

対応処置：以下を確認してください。

- `Get-ClusterService` PowerShell コマンドを使用して、クラスター ノード上でクラスター サービスが実行されていること。
- クラスター ノードが再起動中でないこと、または、電源がオフの状態でないこと。
- Windows Admin Center にクラスターを追加するときには必ず、FQDN 形式でクラスター名を使用していること。

原因：Windows 10 の Microsoft Edge ブラウザーを使用してコンプライアンス レポートを生成すると、コンプライアンス レポートの生成に失敗し、次のエラーが表示される場合があります：`Unable to generate compliance report. The Manage As credentials have not been set or are not in domain\user format.`

対応処置：次のいずれかを実行します。

- 完全修飾ドメイン名 (例：**domain.lab\username**)、またはトップ レベルのドメイン (例：**domain\username**) を使用して、ターゲット ノードに資格情報を接続します。
- ブラウザーのキャッシュ メモリーをクリアして、コンプライアンスを再実行します。
- 正しい認証情報を使用してターゲット ノードに接続するために、WAC がインストールされているシステムで DNS が適切に構成されていることを確認します。

選択したコンポーネントのアップデート中にジョブが失敗しました。

場合によっては、CAU またはターゲット ノードのアップデートが失敗する可能性があります。原因と対応処置を以下に示します。

- CAU の場合、クラスター対応のアップデートをトリガーする前に、クラスターを検証します。クラスターの検証の詳細については、Microsoft ドキュメントの『クラスターのハードウェアの検証』を参照してください。

- **原因**：コンプライアンス インベントリー ファイルが一部のノードで使用できない、またはノードからゲートウェイへのファイルのコピーがコンプライアンスの生成後に失敗します。

  対応処置：コンプライアンスを再実行します。

- **原因**：インターネット接続の問題により、次の処理に失敗する可能性があります。
  - DSU または IC の署名検証
  - オンライン カタログのダウンロード
  - DUP のダウンロード

  上記のいずれかが失敗した場合、CAU またはサーバーのアップデートも失敗します。

  対応処置：インターネットに接続されていることを確認し、コンプライアンスを再実行してアップデートします。

- **原因**：インストーラー ファイルが Windows Admin Center プロセス (sme.exe) によってロックされることがあるため、DSU インストーラーはノードからクリアされません。

  対応処置：Windows Services コンソールから Windows Admin Center サービスを再起動します。

- **原因**：ディスクのいずれかが正常に稼働していない場合、CAU は失敗します。

  対応処置：CAU をトリガーする前に、物理および仮想ディスクが正常な状態であることを確認してください。正常ではない状態のディスクがある場合は、Microsoft のマニュアルを参照して、正常な状態にします。

- **原因**：クラスター ノードのいずれかが一時停止されている場合、CAU は失敗します。

  対応処置：CAU をトリガーする前に、クラスター ノード (フェールオーバーの役割) を再開します。

アップデート後にコンポーネントが非対応と表示されます

アップデート後、コンポーネントが非対応として表示されることがあります。

対応処置：この場合、コンポーネントにエラーがあるかどうかを確認するために、DSU ログを含むクリーンアップ ログを確認してください。アップデートの前にコンポーネントに必要な前提条件がある場合は、必要条件を満たしてからアップデートを再実行します。

OpenManage Integration へのアクセスが拒否されました

原因：管理者権限のないゲートウェイ ユーザー資格情報を使用して Windows Admin Center (WAC) にログインし、WAC コンソールから OpenManage Integration を起動しようとすると、アクセス拒否エラーが表示される場合があります。

対応処置：Windows Admin Center で Dell EMC OpenManage Integration 拡張機能を起動する前に、ゲートウェイ管理者として WAC にログインしていることを確認してください。

Dell Update Package の障害

アップデートをトリガーした後、Dell EMC Update Package (DUP) はコンポーネントのアップデートに失敗する場合があります。アップデート中に DUP が失敗する理由はさまざまです。問題を解決するには、次の可能なソリューションを確認してください。

- Windows Admin Center (WAC) がインストールされているマシンで、ログ ファイルを確認して、DUP ダウンロードの失敗およびコンポーネント マッピングに関する詳細情報を取得します。コンポーネント マッピングは、DUP カタログで、アップデートが選択されたコンポーネントを識別するために用意されています。ログ ファイルは次のパスにあります。

  ゲートウェイ システム：

  - サーバー アップデート：`<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\<PrepareUpdate XXXX>`
  - CAU：`<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\Update XXXX`

  Windows 10 ゲートウェイ システム：

  - サーバー アップデート：`<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\<PrepareUpdate XXXX>`
  - CAU：`<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\Update XXXX`

- サンプル ログ メッセージは次のとおりです。
  - DUP ダウンロード失敗エラー ログ

    ```
    28-Apr-2020 12:19:18 AM::: Error >>> Message : DUPs for some of the selected components are not present in DRM repository.
    ```

  - コンポーネント マッピング ログ ファイル

    ```
    ## Format: :>> Component Name -> Package Name

    :>> [0001] Broadcom NetXtreme Gigabit Ethernet ->
    Network_Firmware_RG25N_WN64_21.60.2_01.EXE
    ```

- ターゲット ノードで、コンポーネント マッピングを参照し、コンポーネント関連の DUP ログ ファイルを見つけて、<Windows Directory>\Dell\UpdatePackage\log\<Package Name>で指定されたリターン コードを確認します。問題の原因と、考えられる解決策については、『Dell EMC Update Package ユーザー ガイド』を参照してください。

  DUP 障害シナリオのリターン コード サンプルを以下に示します。

  ```
  Exit code = 1 (Failure)

  2020-04-21 23:48:27

  Update Package finished. Exit code = 1
  ```

- ドライバー コンポーネントを下位のバージョンにダウングレードしようとすると、DUP が失敗する可能性があります。この場合は、オペレーティング システムからドライバーをアンインストールしてから、OMIMSWAC からコンポーネントのアップデートを再度実行します。ドライバーをアンインストールする方法の詳細については、Microsoft のマニュアルを参照してください。

または、次のように試行することもできます。

- iDRAC をリセットしてバージョン 4.20.20.20 以降にアップデートしてから、アップデートを再実行します。iDRAC をリセットまたはアップデートする方法の詳細については、iDRAC のマニュアルを参照してください。
- DUP ログで<Windows Directory>\Dell\UpdatePackage\log\<Package Name>に指定されたパスからダウンロードして、ターゲット ノードでアップデートを手動で実行します。ネットワーク ファームウェアの例は https://downloads.dell.com/FOLDER06091050M/1/Network_Firmware_TWFF6_WN64_16.26.60.00.EXE です。
- Dell サポート サイトでコンポーネント名を検索して、選択した DUP が選択したオペレーティング システムおよびプラットフォームでサポートされていることを確認します。Dell サポート サイト URL は、https://www.dell.com/support/home/in/en/inbsd1/?app=products です。

Test-Cluster がネットワーク通信エラーで失敗します

原因：iDRAC で USB NIC が有効になっている場合、クラスターの作成準備状況またはクラスターの正常性を検証するために Test-Cluster コマンドを実行すると、妥当性検査レポートにエラーが表示されることがあります。このエラーは、ホスト オペレーティング システム USB NIC に割り当てられている IPv4 アドレスが他のクラスター ネットワークと通信するために使用できないことを示しています。このエラーは無視しても問題ありません。

対応処置：Test-Cluster コマンドを実行する前に、USB NIC（デフォルトでは「Ethernet」とラベル付けされています）を無効にします。

USB NIC ネットワークがパーティション化されたクラスター ネットワークとして表示されます

原因：iDRAC で USB NIC が有効になっている場合、フェールオーバー クラスター マネージャーのクラスター ネットワークには、USB NIC に関連付けられているネットワークがパーティション分割されて表示されます。この問題は、すべてのネットワーク アダプター上でクラスター通信がデフォルトで有効になっていて USB NIC IPv4 アドレスを使用して外部と通信することはできないため、これらの NIC のクラスターの通信が中断されることによって発生します。このエラーは無視しても問題ありません。

対応処置：クラスター マネージャーから USB NIC に関連付けられているネットワークとのクラスター通信を無効にします。

9

Dell EMC PowerEdge サーバーの世代の特定

一連のサーバー モデルに対応するため、PowerEdge サーバーは世代ではなく汎用命名規則を使用して参照されるようになりました。

このトピックでは、汎用命名規則を使用して参照された PowerEdge サーバーの世代を識別する方法について説明します。

例：

R740 サーバー モデルは、インテル プロセッサー搭載第 14 世代サーバーの中の、ラック型、プロセッサー 2 基搭載のシステムです。この文書では、R740 を参照するために、汎用命名規則 **YX4X** サーバーが使用されています。ここで、

- 文字 **Y**（英文字）は、サーバーのタイプを表します（フォーム ファクター：クラウド（C）、フレキシブル（F）、モジュラー（M または MX）、ラック（R）、タワー（T））。
- 文字 **X**（数字）は、サーバーのクラス（プロセッサー数）を示します。
- 数字 **4** は、サーバーの世代を示します。
- 文字 **X**（数字）は、プロセッサーのモデルを示します。

表 3. PowerEdge サーバーの命名規則と例

YX5X サーバー	YX4X サーバー	YX3X サーバー
PowerEdge R7515	PowerEdge M640	PowerEdge M630
PowerEdge R6515	PowerEdge R440	PowerEdge M830
	PowerEdge R540	PowerEdge T130

10

Dell EMC へのお問い合わせ

Dell EMC では、オンラインおよび電話によるサポートとサービスオプションをいくつかご用意しています。これらのサービスは国および製品によって異なり、お住まいの地域では一部のサービスがご利用いただけない場合があります。

メモ: アクティブなインターネット接続がない場合は、ご購入時の納品書、出荷伝票、請求書、または Dell EMC 製品カタログで連絡先をご確認いただけます。

Dell EMC のセールス、テクニカルサポート、またはカスタマーサービスへは、次の手順でお問い合わせいただけます。

1. Dell.com/support にアクセスします。
2. ページの右下にあるリストで、国または地域を選択します。
3. [**サポートへのお問い合わせ**] をクリックして、該当するサポート リンクを選択します。

A

用語集

次の表では、このマニュアルで使用する略語について定義または識別します。

表 4. 用語集

略語/頭字語	定義
OMIMSWAC：OpenManage Integration with Microsoft Windows Admin Center	Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) を使用して、IT 管理者は、ホストとしての PowerEdge サーバー、PowerEdge サーバーで作成された Microsoft フェールオーバー クラスター、Microsoft Azure Stack HCI 向け Dell EMC ソリューションを使用して作成されたハイパーコンバージド インフラストラクチャー (HCI) を管理できます。OMIMSWAC は、PowerEdge サーバーやクラスターのライフサイクル全体を通してリモートに管理することにより、IT 管理者の作業をシンプルにします。
BIOS	基本入出力システム。 BIOS は、PC のシステム ボードまたはマザーボード上の小さいメモリー チップに組み込まれているファームウェアです。BIOS は、PC のハードウェアとオペレーティング システムの間のインターフェイスとして機能します。BIOS には、ネットワークまたはハード ディスク ドライブから起動するかどうかなどの基本的な手順を実行するために PC が使用する指示も含まれています。
コンソール	リモート プラットフォーム管理タスクを実行するためにユーザーが利用する管理アプリケーション。
DRM：Dell EMC Repository Manager	Dell EMC Repository Manager (DRM) は、Dell OpenManage ポートフォリオ内のアプリケーションで、IT 管理者はこれを使うことでシステム アップデートを容易に管理できます。Dell Repository Manager は、Dell Update Packages (DUP) のバンドルおよびリポジトリーと呼ばれる、カスタム ソフトウェアのコレクションの作成に使用される検索可能なインターフェイスを提供します。
DSU：Dell EMC System Update ユーティリティー	Dell EMC System Update (DSU) は、Dell Update Packages (DUP) を Dell EMC ターゲット ノードに適用するための、スクリプトによって最適化されたアップデート展開ツールです。
FQDN	完全修飾ドメイン名。
ゲートウェイ管理者	ゲートウェイ管理者は、ユーザーにアクセス権を付与したり、ユーザーのゲートウェイへの認証方法を設定したりすることができます。Windows Admin Center では、ゲートウェイ管理者のみがアクセス設定を表示して設定することができます。ゲートウェイ マシン上のローカル管理者は、常に Windows Admin Center ゲートウェイ サービスの管理者です。
ゲートウェイ システム	Windows サーバー上のゲートウェイとしてインストールされた Windows Admin Center。
ゲートウェイ ユーザー	ゲートウェイ ユーザーは、Windows Admin Center ゲートウェイ サービスに接続して、そのゲートウェイを介してサーバーを管理することができますが、アクセス権やゲートウェイの認証に使用する認証メカニズムは変更できません。
Windows 10 ゲートウェイ システム	Windows 10 OS でゲートウェイとしてインストールされた Windows Admin Center。
HCI	ハイパーコンバージド インフラストラクチャ。
IC：Dell EMC インベントリー コレクター	インベントリー コレクターは、ターゲット システムのインベントリーを実行し、結果をリポジトリーまたはカタログと比較して、必要なアップデートのみを導入する際に使用します。
iDRAC	Integrated Dell Remote Access Controller。
IPMI	Intelligent Platform Management Interface

表 4. 用語集（続き）

略語/頭字語	定義
LED	Light Emitting Diode
NIC	ネットワーク インターフェイス カード（別称ネットワーク インターフェイス コントローラー）
オフライン - Dell EMC Repository Manager カタログ	DRM リポジトリーが共有の場所で使用可能であり、データ センターのインターネットに接続されていない OMIMSWAC 管理下のすべてのデバイスに適用できる場合に推奨されます。
オンライン（HTTPs） - Dell EMC Azure Stack HCI ソリューション カタログ	Azure Stack HCI カタログの Dell EMC ソリューション用ファームウェアおよびドライバーのアップデート カタログは、Ready Node および AHCI コンポーネントのすべての検証済みバージョンのカタログを提供します。 Azure Stack の HCI クラスター(Dell EMC Microsoft Storage Spaces Direct Ready Nodes および Azure Stack HCI の Dell EMC アプライアンスによって作成) および Azure Stack HCI サーバーに対して推奨されます。
オンライン（HTTPs） - Dell EMC エンタープライズ カタログ	PowerEdge サーバーに推奨されます。
オンライン（HTTPs） - Dell EMC MX ソリューション カタログ	PowerEdge サーバーの MX モデルに推奨されます。
SATA	老朽化した **PATA** テクノロジーを置き換えることを目的とした Serial Advanced Technology Attachment インターフェイス
USB	ユニバーサル シリアル バス
UI	ユーザーインタフェース
<Windows ディレクトリー>	C:\Windows

B

付録

SAS-RAID_Driver

SAS RAID_Driver のアップデート コンプライアンス操作を実行している間は、*SATA コントローラー*および *NVMe PCIe SSD* が RAID モードに設定されていることを確認してください。RAID モードを設定するには、次のようにします。

1. [**Dell Power-On Self-Test (POST)**] 画面が表示されたら、F2 を押します。

   [**Dell PowerEdge システム セットアップ**] ウィンドウが表示されます。

   - [**システム BIOS 設定**] の下で、**[SATA 設定]** > **[内蔵 SATA]** で RAID モードを設定します。
   - [**システム BIOS 設定**] の下で、**[NVMe 設定]** > **[NVMe モード]** で RAID モードを設定します。

ターゲット ノードまたはクラスターに対する推奨カタログ

次の表では、[アップデート ソース] の下のターゲット ノードまたはクラスターに対して推奨するカタログを示します。

ターゲット ノードまたはクラスター	推奨カタログ
PowerEdge サーバー (ラック型、モジュラー型、タワー型)	オンライン (HTTPs) - Dell EMC エンタープライズ カタログ (PowerEdge サーバー用)
MX サーバー	オンライン (HTTPs) - Dell EMC MX ソリューション カタログ (PowerEdge サーバー用)
AHCI クラスター レディー ノード (S2D または Ax アプライアンス)	オンライン (HTTPs) - Dell EMC Azure Stack HCI ソリューション カタログ
MX および PowerEdge サーバーを含むクラスター	オンライン (HTTPs) - Dell EMC エンタープライズ カタログ (PowerEdge サーバー用)
AHCI レディー ノードおよび PowerEdge サーバーを含むクラスター	オンライン (HTTPs) - Dell EMC エンタープライズ カタログ (PowerEdge サーバー用)
PowerEdge、MX、および AHCI レディー ノード サーバーを含むクラスター	オンライン (HTTPs) - Dell EMC エンタープライズ カタログ (PowerEdge サーバー用)
PowerEdge XE2420 Edge サーバーまたはクラスター	オンライン (HTTPs) - Dell EMC エンタープライズ カタログ (PowerEdge サーバー用)