

Dell EMC OpenManage Integration with Microsoft Windows Admin Center バージョン 2.1 ユーザーズ ガイド

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。

章 1: Overview of OpenManage Integration with Microsoft Windows Admin Center.....	5
追加リソース.....	6
章 2: OpenManage Integration with Microsoft Windows Admin Center をお使いになる前に.....	7
章 3: Dell EMC OpenManage Integration with Microsoft Windows Admin Center に必要なポート.....	9
章 4: Dell EMC PowerEdge サーバーの管理.....	10
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.....	11
ハードウェア インベントリ - サポートされているターゲット ノード コンポーネント.....	11
章 5: フェールオーバー クラスタ、Azure Stack HCI、Windows Server HCI クラスタの管理.....	13
正常性状態 - フェールオーバー クラスタ、Windows Server HCI、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.....	14
ハードウェア インベントリ - フェールオーバー クラスタ、Windows Server HCI、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.....	15
章 6: HCI およびフェールオーバー クラスタの PowerEdge サーバーおよびノードの iDRAC の詳細の 表示	17
章 7: OpenManage Integration 拡張機能による、PowerEdge サーバー、および Windows Server HCI クラスタ、Azure Stack HCI クラスタ、フェールオーバー クラスタのノードのアップデート.....	18
アップデート ツールでの DSU および IC 設定の構成.....	19
プロキシ設定の構成.....	19
OpenManage Integration 拡張機能を使用したターゲット ノードのアップデート.....	20
OpenManage Integration 拡張機能による Windows Server HCI クラスタ、Azure Stack HCI クラスタ ー、フェールオーバー クラスタのノードのアップデート.....	22
コンプライアンス レポートの表示.....	25
章 8: Azure Stack HCI クラスタの統合された展開とアップデート.....	27
OpenManage Integration スナップインを使用した Azure Stack HCI クラスタの統合された展開とア ップデート.....	27
HCI 構成プロファイル.....	30
章 9: OpenManage Integration スナップインを使用した、Azure Stack HCI クラスタ向けのフル スタ ック クラスタ対応アップデート.....	34
OpenManage Integration スナップインを使用した Azure Stack HCI クラスタのアップデート.....	34
章 10: クラスタまたは個別のノードの CPU コアを管理する.....	37
章 11: 既存のクラスタへのノードの追加.....	39
Windows Server HCI および Azure Stack HCI クラスタ拡張のためのノードの準備.....	39
フェールオーバー クラスタ拡張のためのノードの準備.....	41
推奨事項の表示チェック	42

章 12: トラブルシューティングとよくある質問 (FAQ)	44
アップグレード.....	44
ライセンス.....	45
ログ.....	45
正常性、ハードウェア、iDRAC インベントリー.....	46
点滅および点滅解除.....	48
クラスター対応アップデート.....	48
フルスタック クラスター対応アップデート.....	52
CPU コアの管理.....	53
クラスターの拡張.....	55
その他.....	55
 章 13: Dell EMC PowerEdge サーバーの世代の特定.....	57
 章 14: Dell EMC へのお問い合わせ.....	58
 付録 A: 用語集.....	59
 付録 B: 付録.....	61

Overview of OpenManage Integration with Microsoft Windows Admin Center

Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) enables IT administrators to manage PowerEdge servers as hosts, Microsoft Failover Clusters created with PowerEdge servers, and Hyper-Converged Infrastructure (HCI) created by using Dell EMC HCI Solutions for Microsoft Windows Server or Dell EMC Integrated System for Microsoft Azure Stack HCI. OMIMSWAC simplifies the tasks of IT administrators by remotely managing the PowerEdge servers and clusters throughout their life cycle. For more information about the features and benefits of OMIMSWAC, see the documentation at Dell.com/OpenManageManuals.

What is new in this release

- 'CPU core management' feature enables CPU cores for distributions in an HCI (AS HCI and WS HCI) cluster or individual nodes. This feature gives you the ability to configure the CPU core count to achieve the right balance between power and performance optimal for workloads. This feature helps you to keep the Total Cost of Ownership for Hybrid cloud at an optimal level.
- 'Expand Cluster' feature that enables you to prepare nodes for cluster expansion. This feature helps you to identify and prepare right nodes for a cluster that follow Dell EMC recommendations, which can be later added into the cluster. This feature is supported in Failover clusters and HCI clusters.
- Hardware symmetry check has been renamed as HCI configuration profile check.
- Supports YX5X PowerEdge servers with Intel platforms.
- Enhancements:
 - Updating firmware, BIOS, and drivers of individual nodes part of an Azure Stack HCI cluster using the server extension tool is suboptimal and not recommended by Dell Technologies. This version has introduced this restriction to help maintain the cluster homogeneity.
 - Supports health and inventory retrieval when the port number other than the default port 443.
 - Enhanced HCI configuration policy checks to ensure a minimum of 5% of cache capacity available in clusters to improve cluster performance.

Key features of OMIMSWAC

- OMIMSWAC provides a simplified solution for IT administrators to efficiently manage the following:
 - Dell EMC PowerEdge Servers running on supported Windows operating systems.
 - Dell EMC Integrated System for Microsoft Azure Stack HCI (also known as Azure Stack HCI or AS HCI) created using AX nodes from Dell Technologies.
 - Dell EMC HCI Solutions for Microsoft Windows Server (also known as Windows Server HCI or WS HCI) created using Storage Spaces Direct Ready Nodes or combinations of AX nodes and Storage Spaces Direct Ready Nodes.
 - Microsoft Failover Clusters created with Dell EMC PowerEdge servers running supported Windows Server operating system.
- Inventory/Monitoring—Provides information about overall Health, Hardware inventory, and iDRAC inventory of nodes including component-level information of all supported Dell EMC platforms.
- iDRAC console—View iDRAC information of PowerEdge servers. For out-of-band management, you can directly launch the iDRAC console from Windows Admin Center.
- Cluster creation (Integrated Cluster Deploy and Update)—Supports integrated Firmware, BIOS, and Drivers installation while creating Azure Stack HCI cluster. Also, performs HCI configuration profile check to keep hardware configuration of cluster nodes inline with Dell EMC recommended hardware configuration.
- Update management—
 - Online catalogs—Support for creating firmware baselines by using the following online catalogs when OMIMSWAC is connected to the Internet:
 - **Dell EMC Enterprise Catalog**—Contains firmware updates for PowerEdge servers and PowerEdge server nodes in a cluster.
 - **Update Catalog for Microsoft HCI solutions**—Contains firmware updates for AX nodes and Storage Spaces Direct Ready Nodes and nodes in Windows Server HCI and Azure Stack HCI clusters.
 - **Dell EMC MX Solution Catalog** for PowerEdge MX Modular.

- Offline catalog—Support for creating local firmware baselines by using Dell EMC Repository Manager (DRM).
- Compliance report—Generate update compliance report against Dell EMC verified update catalogs and provide notifications when a new catalog version is available.
- Server update—Supports PowerEdge server update against baseline – Firmware, BIOS, Drivers, and system management applications.
- Cluster-Aware Update—Supports cluster update against validated baseline (Firmware, BIOS, and Drivers) for PowerEdge server-based Failover cluster, Dell EMC HCI Solutions for Microsoft Windows Server, and Dell EMC Integrated System for Microsoft Azure Stack HCI.
- Full Stack Cluster-Aware Updating—Supports integrated cluster-aware update for Azure Stack HCI clusters that include both operating system and hardware updates (Firmware, BIOS, and Drivers).
- Dell EMC Solutions badge—
 - Displays Dell EMC Solutions badge [Azure Stack HCI Certified] for Dell EMC Integrated System for Microsoft Azure Stack HCI consisting of AX nodes from Dell Technologies.
 - Displays Dell EMC Solutions badge [Windows Server HCI Certified] for Dell EMC HCI Solutions for Microsoft Windows Server created using Storage Spaces Direct Ready Nodes or combinations of AX nodes and Storage Spaces Direct Ready Nodes.
- Availability of OMIMSWAC extension and documentation localized in English, French, German, Spanish, Simplified Chinese, and Japanese languages.

トピック：

- [追加リソース](#)

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] > [マニュアルおよび文書] の順にクリックします。
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。	
Dell EMC OpenManage Integration with Microsoft Windows Admin Center セキュリティ設定ガイド	Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC)のセキュリティ機能と性能についての情報が記載されています。	
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
Azure Stack HCI 用統合システム	Microsoft Azure Stack HCI 用の Dell EMC 統合システムの詳細が説明されています。	https://infohub.delltechnologies.com/t/microsoft-hci-solutions-from-dell-technologies-1/

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 の左上隅のドロップダウン メニューで [サーバー マネージャー] または [クラスター マネージャー] を選択します。

サポートされている WAC バージョンは、Windows Admin Center 2103.2 GA です。

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: ターゲット ノードまたはクラスターへの接続中に [管理に使用する認証情報] が提供されていない場合、またはその認証情報を拡張機能で使用できない場合は、ターゲット ノードまたはクラスターを管理しようとするときに、拡張機能内で [管理に使用する認証情報] を指定するよう求められます。

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。

OMIMSWAC を正しく機能させるためのベスト プラクティス

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、AX ノードまたは Storage Spaces Direct Ready Node をで作成された Dell EMC HCI Solutions for Microsoft Windows Server、または AX ノードで作成された Dell EMC Integrated System for Microsoft Azure Stack HCI については、「[フェールオーバー クラスター](#)、[Azure Stack HCI](#)、[Windows Server HCI クラスターの管理](#)、p. 13」を参照してください。

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	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)
OpenManage Integration スナップインと HCI 構成プロファイル チェックの前提条件	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 ツール 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
ターゲットノードのアップデート(スタンダードノードのアップデート、CPU コア管理、クラスター拡張) クラスター ノードのアップデート(クラスター対応アップデートおよび CPU コア管理)	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。

Dell EMC PowerEdge サーバーの管理

OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) を使用して、PowerEdge サーバーの正常性、ハードウェア インベントリ、アップデート、iDRAC を表示および管理することができます。

前提条件

- Windows Admin Center 2103.2 GA がインストールされている。
- 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る。
- OMIMSWAC 拡張機能がインストールされている必要がある。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。
- サーバー接続が Microsoft Windows Admin Center に追加されている。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。
- ドメイン管理者の認証情報を使用して、Windows Admin Center にリモートでアクセスできるようになっている。詳細については、[Microsoft のドキュメント](#)を参照してください。

メモ: BIOS 設定で NIC が無効になっている場合、特定の iDRAC ファームウェア バージョンの正常性とハードウェア インベントリ情報が遅延します。したがって、BIOS 設定で NIC がすべて有効になっていることを確認してください。

手順

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: ターゲット ノードまたはクラスターへの接続中に [管理に使用する認証情報] が提供されていない場合、またはその認証情報を拡張機能で使用できない場合は、ターゲット ノードまたはクラスターを管理しようとするときに、拡張機能内で [管理に使用する認証情報] を指定するよう求められます。
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] - ターゲット ノード コンポーネントのハードウェア インベントリの詳細情報が表示されます。[ハードウェア インベントリ - 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。
 - [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. 17 を参照してください。
 - [設定] - [コンピューティング リソース] では、CPU コア分散サマリーを表示し、CPU コア数を管理することができます。[クラスターまたは個別のノードの CPU コアを管理する](#)、p. 37 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。[OpenManage Integration 拡張機能による、PowerEdge サーバー、および Windows Server HCI クラスター、Azure Stack HCI クラスター、フェールオーバー クラスターのノードのアップデート](#)、p. 18 を参照してください。

正常性、ハードウェア インベントリ、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ときには読み込まれません。最新の正常性、インベントリのステータス、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 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](#)
- [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](#)

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
 - ① **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。
- メモリ
 - ① **メモ:** Intel [DIMM] メモリーはアイコンで [IntelPersistent] として識別されます。
- 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

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。

- ① **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

このページには、ターゲット ノードにインストールされているハードウェアおよびファームウェア コンポーネントの情報が表示されます。これを表示するには、Dell EMC OpenManage Integration で、[インベントリー] を選択します。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。

インベントリー セクションには、ターゲット ノードで利用可能な以下のコンポーネントの情報が表示されます。

- システム
- ファームウェア
 - ① **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 バージョンのシングル ポートのみが表示されます。
- CPU
- アクセラレーター
- メモリ
 - ① **メモ:** Intel [DIMM] メモリーはアイコンで [IntelPersistent] として識別されます。
- 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

- ① **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、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、次の場所では利用できない場合があります。
 - 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。
 - ストレージ エンクロージャが空の場合は、ハードウェア インベントリ属性を確認できます。これは、ターゲット ノードの iDRAC で情報が使用できない場合があるためです。
 - 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。

- 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] のストレージ コントローラーのリンクは使用できません。

物理ディスクを識別するには、ディスク LED を点滅したり、点滅解除したりすることができます。詳細については、「[物理ディスクの LED 点滅および点滅解除](#)」を参照してください。

- 電源装置

- ファン

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. 17」を参照してください。

- ① **メモ:** [インベントリ] 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。

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。

- ① **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。

- ① **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。
- 物理ディスクが接続されている内蔵 SATA コントローラーにエラーがあると、点滅または点滅解除の操作が失敗します
Blink/Unblink May not be supported with - <disk_name>.

フェールオーバー クラスター、Azure Stack HCI、Windows Server HCI クラスターの管理

OpenManage Integration for Microsoft Windows Administration Center (OMIMSWAC) 拡張機能を使用して、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、Dell EMC HCI Solutions for Microsoft Windows Server (Windows Server HCI)、Dell EMC Integrated System for Microsoft Azure Stack HCI (Azure Stack HCI) の正常性、ハードウェア インベントリ、アップデート、iDRAC を表示し、管理することができます。

前提条件

- Windows Admin Center 2103.2 GA がインストールされている。
- 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。
- 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る。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る。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が確認されている。
- ドメイン管理者の認証情報を使用して、Windows Admin Center にリモートでアクセスできるようになっている。詳細については、[Microsoft のドキュメント](#)を参照してください。

① メモ: BIOS 設定で NIC が無効になっている場合、特定の iDRAC ファームウェア バージョンの正常性とハードウェア インベントリ情報が遅延します。したがって、BIOS 設定で NIC がすべて有効になっていることを確認してください。

このタスクについて

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、AX ノードで作成された Azure Stack HCI、Storage Spaces Direct Ready Node で、または AX ノードと Storage Spaces Direct Ready Node の組み合わせで作成された Windows Server HCI を管理するには、次の手順に従います。

手順

1. Windows Admin Center の左上隅のドロップダウン メニューで [クラスター マネージャー] を選択します。
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。

① メモ: 拡張機能により、「管理に使用する認証情報」の指定を求められた場合は、[管理に使用する認証情報] を選択し、管理下ノードの認証に適切なクラスター管理者認証情報を入力してから、[これらの認証情報をすべての接続に使用] チェック ボックスを選択します。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。[管理に使用する認証情報] 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。
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。

① 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、Windows Server HCI、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] - コンポーネントのハードウェア インベントリ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 インベントリの詳細を表示します。ハードウェア インベントリ - フェールオーバー クラスタ、Windows Server HCI、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. 15 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 クラスタの PowerEdge サーバーおよびノードの iDRAC の詳細の表示、p. 17 を参照してください。
- [設定] - [コンピューティング リソース] では、CPU コア分散サマリーを表示し、CPU コア数を管理することができます。[クラスタの拡張] では、クラスタの拡張用にノードを特定し、準備することができます。クラスタまたは個別のノードの CPU コアを管理する、p. 37 および を参照してください。既存のクラスタへのノードの追加、p. 39
- [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。OpenManage Integration 拡張機能による、PowerEdge サーバー、および Windows Server HCI クラスタ、Azure Stack HCI クラスタ、フェールオーバー クラスタのノードのアップデート、p. 18 を参照してください。

正常性、ハードウェア インベントリ、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ときには読み込まれません。最新の正常性、インベントリのステータス、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、Windows Server HCI、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
- ハードウェア インベントリ - フェールオーバー クラスタ、Windows Server HCI、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

正常性状態 - フェールオーバー クラスタ、Windows Server HCI、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 - 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、Windows Server HCI、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:** 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。
- メモリ
 -  **メモ:** Intel [DIMM] メモリはアイコンで [IntelPersistent] として識別されます。
- 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

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、Windows Server HCI、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、Windows Server HCI、Azure Stack HCI のノードにインストールされているハードウェアおよびファームウェア コンポーネントに関する情報を表示できます。これを表示するには、Dell EMC OpenManage Integration で、[インベントリー] を選択します。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。

フェールオーバー クラスター、Windows Server HCI、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

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 バージョンのシングル ポートのみが表示されます。

- CPU
- アクセラレーター
- メモリ

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

- ストレージコントローラ

ストレージ コントローラ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

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、次の場所では利用できない場合があります。
 - 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。
- ストレージ エンクロージャが空の場合は、ハードウェア インベントリー属性を確認できます。これは、ターゲット ノードの iDRAC で情報が使用できない場合があるためです。
- 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。

- 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 コントローラのリンクをクリックします。関連付けられているストレージ コントローラが [ストレージ コントローラ] 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] のストレージ コントローラのリンクは使用できません。

物理ディスクを識別するには、ディスク LED を点滅したり、点滅解除したりすることができます。詳細については、「[物理ディスクの LED 点滅および点滅解除](#)」を参照してください。

- 電源装置
- ファン

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. 17」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。

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。

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。
- 物理ディスクが接続されている内蔵 SATA コントローラーにエラーがあると、点滅または点滅解除の操作が失敗します
Blink/Unblink May not be supported with - <disk_name>.

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。

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 クラスターの場合は、ノードを展開して、次の詳細を表示します。

- DNS ドメイン名
- URL 文字列：これには、iDRAC IP アドレスが含まれます。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
- デバイスの MAC アドレスです。
- ライセンス：ノードで使用可能なさまざまなライセンスが表示されます。たとえば、OMIWAC Premium License for MSFT HCI Solutions、iDRAC9 Enterprise License などです。

ライセンス名をクリックすると、ライセンスの詳細が表示されます。

Dell EMC OpenManage Integration を使用してクラスターを管理するには、各ターゲットノードに OMIWAC Premium ライセンスがインストールされている必要があります。ライセンスの詳細については、『OMIMSWAC インストール ガイド』のライセンスのセクションを参照してください。

メモ: OMIMSWAC iDRAC インベントリに表示される HCI ソリューションのプレミアム ライセンス名は、「OMIWAC Premium License for MSFT HCI Solutions」です。ただし、iDRAC では、同じライセンス名が「OMIWAC Premium License for Azure Stack HCI」と表示されます。

OpenManage Integration 拡張機能による、PowerEdge サーバー、および Windows Server HCI クラスター、Azure Stack HCI クラスター、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 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備えた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 Dell EMC HCI Solutions for Microsoft Windows Server。
 - 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 Integrated System for Microsoft Azure Stack HCI。
- 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 ツールでの DSU および IC 設定の構成
- OpenManage Integration 拡張機能を使用したターゲット ノードのアップデート
- OpenManage Integration 拡張機能による Windows Server HCI クラスタ、Azure Stack HCI クラスタ、フェールオーバー クラスタのノードのアップデート

アップデート ツールでの DSU および IC 設定の構成

このタスクについて

インターネット アクセスのない OpenManage Integration 拡張機能で、最新のコンプライアンス レポートを生成し、コンポーネントをアップデートするには、[設定] > [アップデート ツール] に用意されている DSU および IC 設定を構成する必要があります。DSU および IC 設定は、[アップデート] > [ソース] の順にカタログを選択するときに、[詳細設定] を選択して構成することもできます。OpenManage Integration に対応する Dell System Update (DSU) および Dell Inventory Collector (IC) ユーティリティのバージョンは次のとおりです。

- DSU バージョン : 1.9.0。 <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 : 21_04_202_1093。 <https://dl.dell.com/OMIMSWAC/IC/> から IC をダウンロードします。

手順

OpenManage Integration 拡張機能で [設定] > [アップデート ツール] タブをクリックし、以下を入力します。

1. DSU ユーティリティ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 ユーティリティは、ターゲット ノードからのハードウェア インベントリ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。

次の手順

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 クラスタのノードのアップデート](#)」を参照してください。

プロキシ設定の構成

OpenManage Integration 拡張機能には、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atalogを使用したターゲット ノードまたはクラスタ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atalog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。

このタスクについて

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 ツール] 設定が構成されておらず、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。

-  **メモ:** プロキシ設定は、OpenManage Integration スナッピンではサポートされていません。

プロキシ サーバーに接続するには、次のようにします。

手順

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`)

次の手順

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 拡張機能を使用したターゲット ノードのアップデート

OpenManage Integration with Windows Admin Center 拡張機能を使用して、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。

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の要件に準拠していることを確認します。
- この拡張機能で「管理に使用する資格情報」を指定するように求められた場合は、[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指定します。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。[管理に使用する認証情報] 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。
 - ターゲット ノードに対して、コンプライアンス/アップデートは一度に1つのみ実行することを強くお勧めします。複数のコンプライアンス/アップデートを同時に実行すると、既存のコンプライアンス/アップデートでエラーが発生する可能性があります。

手順

コンプライアンスレポートを生成し、ターゲットノードのファームウェア、BIOS、ドライバのアップデートを実行するには、次の手順を実行します。

1. 検証されたカタログに対して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] の順に選択し、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。

- [オンライン (HTTPs) - <カタログ名>] を選択して、カタログを dell.com から自動的にダウンロードします。オンラインカタログは、デフォルトで選択されています。オンラインカタログは、OMIMSWAC がインターネットに接続されている場合に使用できます。また、プロキシ設定を使用してインターネットにアクセスすることもできます。[[プロキシ設定の構成](#)] を参照してください。

使用可能なカタログは次のとおりです。

- PowerEdge サーバーの場合 : 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。
 - AX ノードおよび Storage Spaces Direct Ready Node の場合 : Microsoft HCI ソリューションのアップデート カタログ。
- CIFS の場所に構成された DRM カタログを使用するには、[オフライン - Dell EMC Repository Manager カタログ] を選択します。

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。インターネットを使用できない場合、またはカスタマイズされた DRM カタログを使用する場合はこのカタログを使用できます。

- a. オフライン DRM カタログを使用するには、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が生成されていることを確認します。サポートされている DRM アプリケーションのバージョンは、[Dell EMC Repository Manager](#) からダウンロードできます。DRM カタログを作成するには、[技術に関する記事](#) を参照してください。
- b. DRM カタログを作成し、共有パスに保存したら、[DRM 設定] を選択し、DRM カタログがある CIFS 共有パスを指定して、共有パスにアクセスするための資格情報を入力します。

メモ:

- Azure Stack HCI および Windows Server HCI 用の「Microsoft HCI ソリューションのアップデート カタログ」を使用することをお勧めします。
- 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。

2. Dell EMC System Update (DSU) ツールおよび Inventory Collector (IC) ツールを使用するには、[詳細設定] を選択し、次のいずれかを選択します。

- OMIMSWAC がインターネットに接続されている場合は、[Dell EMC System Update (DSU) および Inventory Collector (IC) を自動的にダウンロードして設定] を選択。これがデフォルトで選択されています。
- 共有の場所にある DSU ツールおよび IC ツールを手動でダウンロードして設定するには、[DSU および IC を手動設定] を選択して、[設定] を選択。OMIMSWAC がインターネットに接続されていない場合は、このオプションを使用することをお勧めします。

OpenManage Integration 拡張機能の [アップデート ツール] 設定を使用して設定された DSU と IC の設定は、[詳細設定] でも使用できます。

終了したら、[次へ : コンプライアンス レポート] をクリックします。

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 <https://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。

3. [コンプライアンス レポート] タブで、[コンプライアンス レポートを表示](#) します。

- デフォルトでは、ファームウェア、BIOS、またはドライバがアップデートされる、「非対応」で「アップグレード可能」なすべてのコンポーネントが選択されます。

選択したコンポーネントの選択を解除するか、または「非対応」の「ダウングレード可能」なコンポーネントを選択してアップデートすることができます。ただし、デフォルトの選択内容を変更するには、対応するコンポーネントのファームウェアとドライバ間の依存関係が満たされていることを確認します。

- さらに具体的に選択するには、棒グラフの下にある各色コードを選択するか、検索ボックスを使用して必要なコンポーネントを除外することができます。[コンプライアンス レポート] ペインの右上にある [クリア] を選択して、色コードフィルターを削除します。

終了したら、[次へ : サマリー] をクリックします。

4. [サマリー] タブで、アップデートするコンポーネントを確認し、[次へ : アップデート] をクリックします。

- コンポーネントの選択を変更するには、[戻る] をクリックして [コンプライアンス レポート] タブに移動し、コンポーネント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。

[アップデート] タブでアップデートが進行中の場合は、ブラウザを終了または閉じないことをお勧めします。ブラウザを閉じたり、終了したりすると、ノードのアップデートに失敗し、アップデートのステータスが表示されないことがあります。

① 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。

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、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 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
- 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。

タスクの結果

コンポーネントのアップデートで再起動が必要な場合は、ノードが再起動されます。

OpenManage Integration 拡張機能による Windows Server HCI クラスター、Azure Stack HCI クラスター、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) 拡張機能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 (ファームウェア、BIOS、ドライバ) 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。

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。

- ドメイン管理者の認証情報を使用して、リモートで Microsoft Windows 管理センターにログインします。ゲートウェイ管理者としての認証情報であることを確認します。詳細については、[Microsoft のマニュアル](#)を参照してください。
- OMIMSWAC は、Microsoft クラスター対応アップデート機能フレームワークを使用してクラスターのアップデートを実行するため、CAU をトリガーする前に、すべてのターゲットノードに**フェールオーバー クラスターリング機能とフェールオーバー クラスターリング ツール**がインストールされていることを確認してください。詳細については、[Microsoft の文書の「クラスター対応アップデートの要件とベストプラクティス」](#)を参照してください。
- ① **メモ:** CAU をトリガーする前に、クラスターの準備状況をテストすることをお勧めします。詳細については、[Microsoft のマニュアルに記載されたクラスター アップデートの準備状況のテスト](#)を参照してください。
- [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の要件に準拠していることを確認します。
- CAU 機能を使用するには、OMIWAC 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、OpenManage Integration 拡張機能の [iDRAC] タブをクリックして、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 ドメイン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。詳細については、[Microsoft の文書の「クラスター対応アップデートの要件とベスト プラクティス」](#)を参照してください。
- ターゲット ノードのインベントリ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。

このタスクについて

CAU 機能は、有効な OMIWAC プレミアム ライセンスを備えた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 以降を搭載した AX ノードと Storage Space Direct Ready Node。

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。
- 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。
- ターゲット ノードまたはクラスターに対して、一度に 1 つのコンプライアンス/アップデートのみを実行することを強くお勧めします。複数のコンプライアンス/アップデートを同時に実行すると、既存のコンプライアンス/アップデートでエラーが発生する可能性があります。
- 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

コンプライアンス レポートを生成し、Windows Server HCI クラスター、Azure Stack HCI クラスター、フェールオーバー クラスターのファームウェア、BIOS、ドライバーのアップデートを実行するには、次の手順を実行します。

1. 検証済みカタログに対するコンプライアンス レポートを生成するには、[アップデートソース] タブで、次の手順を実行します。
 - a. カタログ ファイルをダウンロードする方法を 1 つ選択します。
 - [オンライン (HTTPs) - <カタログ名>] で、dell.com からカタログを自動的にダウンロードします。オンライン カタログは、デフォルトで選択されています。
 使用可能なカタログは次のとおりです。
 - 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 モジュール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。
 - Windows Server HCI および 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 のコンポーネントの検証済みバージョンが含まれている Microsoft HCI ソリューションのカタログをアップデートします。

オンライン カタログのサポートには、Windows Admin Center ゲートウェイから直接インターネット接続が必要です。カタログの全体的なダウンロード時間は、ネットワーク帯域幅とアップデート対象のコンポーネントの数によって異なります。また、プロキシ設定を使用してインターネットにアクセスすることもできます。「[プロキシ設定の構成](#)」を参照してください。

- [オフライン - Dell EMC Repository Manager カタログ] を選択すると、CIFS の場所で設定された DRM カタログを使用します。

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。インターネットを使用できない場合、またはカスタマイズされた DRM カタログを使用する場合は、このオプションを使用できます。

- オフライン カタログを使用するには、[DRM 設定] を選択して、DRM カタログとともに CIFS 共有パスが設定されていることを確認します。サポートされている DRM アプリケーションのバージョンは、[Dell EMC Repository Manager](#) からダウンロードできます。DRM カタログを作成するには、[技術に関する記事](#)を参照してください。

メモ:

- Azure Stack HCI および Windows Server HCI 用の「Microsoft HCI ソリューションのアップデート カタログ」を使用することをお勧めします。
- 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。

- b. Dell EMC System Update (DSU) および Inventory Collector (IC) ツールを使用するには、[詳細設定] を選択し、次のいずれかを選択します。

- OMIMSWAC がインターネットに接続されている場合は、[Dell EMC System Update (DSU) および Inventory Collector (IC) を自動的にダウンロードして設定] を選択。これがデフォルトで選択されています。
- 共有の場所にある DSU ツールおよび IC ツールを手動でダウンロードして設定するには、[DSU および IC を手動設定] を選択して、[設定] を選択。OMIMSWAC がインターネットに接続されていない場合は、このオプションを使用することをお勧めします。

OpenManage Integration 拡張機能の [アップデート ツール] 設定を使用して設定された DSU および IC の設定は、OpenManage Integration スナップインの [詳細設定] でも使用できます。

終了したら、[次へ : コンプライアンス レポート] をクリックします。

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 <https://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。

2. [コンプライアンス レポート] タブで、コンプライアンス レポートを表示します。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 レポートを表示](#)してください。

- 「非対応」で「アップグレード可能」なコンポーネントは、デフォルトで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の選択を解除するか、または「非対応」の「ダウングレード可能」なコンポーネントを選択してアップデートすることができます。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。

- さらに具体的に選択するには、棒グラフの下にある各色コードを選択するか、検索ボックスを使用して必要なコンポーネントを除外することができます。[コンプライアンス レポート] ペインの右上にある [クリア] を選択して、色コードフィルターを削除します。

また、[コンプライアンス レポート] パネルの右上にある「すべて展開」アイコンをクリックしてノードを展開し、コンポーネントを選択したり、選択を解除したりすることもできます。

終了したら、[次へ : サマリー] をクリックします。

3. [サマリー] タブで、アップデートするコンポーネントを確認し、今すぐアップデートを実行するか、後で実行するスケジュールを設定するかを選択します。

- [今すぐ実行]: これにより、クラスターのアップデートがすぐに実行され、必要に応じてノードが再起動されます。
- [スケジュールを設定]: クラスターのアップデートが実行される将来の日時を選択します。これにより、指定した時間にクラスターがアップデートされるよう、必要なファイルのダウンロードとコピーが行われます。

特定の時点にスケジュールできる CAU ジョブは、クラスターごとに1つのみです。新しい CAU ジョブ ([今すぐ実行] または [スケジュールを設定]) を選択すると、既存のスケジュール設定されたジョブがキャンセルされます。

コンポーネントの選択を変更するには、[戻る] を選択して [コンプライアンス レポート] タブに移動し、コンポーネントを選択し直すか、選択をクリアします。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は、OpenManage Integration with Microsoft Windows Admin Center の統合を使用して生成されたコンプライアンス レポートにコンポーネントが表示されません。

4. 終了したら、[次へ : 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。[はい] をクリックして CredSSP を有効にし、選択したコンポーネントのアップデートを続行します。[クラスター対応アップデート] タブに移動すると、アップデート ステータスが表示されます。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: [クラスター対応アップデート] タブでのアップデートの進行中は、ブラウザを終了したり、閉じたりしないことをお勧めします。ブラウザを閉じたり、終了したりすると、ノードのアップデートに失敗し、アップデートのステータスが表示されないことがあります。

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 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
 - スケジュール設定されたクラスターのアップデートが完了した後は、個々のノードの DSU ログが、それぞれのノードの <Windows Directory>\Temp\OMIMSWAC フォルダで見つかります。
- 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、必要に応じてコンプライアンス設定の詳細を入力します。

タスクの結果

コンポーネントのアップデートのいずれかで再起動が必要になった場合は、ノードが一度に1つずつ再起動され、ダウンタイムを回避するために、VM などのクラスターの役割がノード間で移動されます。

コンプライアンス レポートの表示

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。棒グラフは、カラー コードを使用して、対応、緊急、推奨、オプションの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。

[コンプライアンス レポート] パネルの右上にある [すべて展開] または [すべて折りたたむ] アイコン (OpenManage Integration 拡張機能のクラスター対応アップデートでのみ使用可能) をクリックしてコンポーネントを選択するか、選択を解除することができます。さらに具体的に選択するには、棒グラフの下にある各色コードを選択するか、検索ボックスを使用して必要なコンポーネントを除外することができます。[コンプライアンス レポート] パネルの右上にある「クリア」を選択してカラー コードフィルターを削除します。

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 (OMIWAC プレミアム ライセンス) も表示されます。

メモ: 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。

メモ: コンポーネントのアップデートがカタログに含まれていない場合は、生成されたコンプライアンス レポートにコンポーネントが表示されません。

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 ノードのファームウェア、BIOS、ドライバは、インポートされたカタログのものと同一バージョンです。

	Non-Compliant - このカテゴリーのターゲット ノードには、ファームウェア、BIOS、ドライバー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（ファームウェア、BIOS、ドライバー）との互換性を維持するために役立つ機能の拡張または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。

メモ: コンプライアンス レポートで、[Microsoft 基本ディスプレイ アダプター ドライバー] のコンプライアンス タイプがダウングレード可能として表示されることがあります。アップデート（ダウングレード）後は、ドライバーの名前が [Matrox G200eW3 (Nuvoton) WDDM <バージョン No.> ドライバー] に変更されます。これは想定内の動作です。

Azure Stack HCI クラスターの統合された展開とアップデート

このセクションでは、OpenManage Integration スナップインを使用して、Azure Stack (AS HCI) クラスターの統合された展開とアップデートを実行する方法について説明します。

Windows Admin Center の AX ノードを使用して Azure Stack HCI クラスターを展開する際は、OpenManage Integration スナップインを使用して、クラスターの最適なパフォーマンスとサポートのために、次のことを確認してください。

- HCI 構成プロファイルのチェック：Azure Stack HCI クラスター用に選択されたノードがサポート対象であり、Dell EMC が推奨する対称型ハードウェア構成であることを確認します。
- アップデート：選択されたノードのファームウェア、BIOS、およびドライバーが最新であることを確認します。

この機能は Azure Stack HCI クラスター作成ワークフローと統合されているため、オペレーティングシステムとハードウェアの両方のアップデートが完了した後、必要に応じて、ノードが一度だけ再起動されます。

トピック：

- [OpenManage Integration スナップインを使用した Azure Stack HCI クラスターの統合された展開とアップデート](#)
- [HCI 構成プロファイル](#)

OpenManage Integration スナップインを使用した Azure Stack HCI クラスターの統合された展開とアップデート

OpenManage Integration で統合されたクラスターの展開およびアップデート機能を使用すると、Windows Admin Center を使用して Azure Stack HCI クラスターを作成しながら、ターゲット ノードをアップデートすることができます。この機能は、選択したノードのハードウェア構成を、Dell EMC が推奨するハードウェア構成に準拠させるのにも役立ちます。

前提条件

作業を開始する前に、次のことを確認します。

- Windows Admin Center 2103.2 GA がインストールされていることを確認します。
- ドメイン管理者の認証情報を使用して、リモートで Microsoft Windows 管理センターにログインします。ゲートウェイ管理者としての認証情報であることを確認します。詳細については、[Microsoft のマニュアル](#)を参照してください。
- Microsoft のマニュアルの「[Windows Admin Center を使用して Azure Stack HCI クラスターを作成する](#)」に記載されている前提条件がすべて満たされていることを確認します。
- 選択されたすべてのノードが、Azure Stack HCI バージョン 20H2 オペレーティングシステムを実行している AX ノードであることを確認します。サポートされているハードウェアの詳細については、OMIMSWAC のインストールガイドの「[互換性マトリックス](#)」を参照してください。
- クラスターを作成するには、適切なノード管理者の認証情報を指定して、ノードに接続します。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。[管理に使用する認証情報] 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。
- ノードが既存のクラスターに含まれていないことを確認します。
- HCI 構成プロファイルのチェックのために、MSFT HCI ソリューション向け OMIWAC プレミアム ライセンスが各ノードで利用できることを確認します。
- 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ことを確認します。また、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、IC の各ユーティリティをダウンロードし、コンプライアンスレポートのみを生成することもできます。プロキシ設定の詳細については、「[プロキシ設定の構成](#)」を参照してください。
- オフライン DRM カタログを使用するには、設定が[アップデート ツール設定の構成](#)に記載されているように設定されていることを確認します。

このタスクについて

メモ:

- 上記のいずれかの前提条件を満たしていない場合は、必要に応じて確認して解決するようにしてください。OpenManage Integration スナップイン フローをスキップして、Microsoft のクラスター作成ワークフローを続行することもできます。ただし、ハードウェア アップデートのインストール ワークフローをスキップすると、クラスターのパフォーマンスに影響する可能性があります。したがって、クラスターを作成する際には、ハードウェア アップデートをインストールすることをお勧めします。
- Dell EMC OpenManage Integration with Windows Admin Center は、ストレッチ クラスターの作成をサポートしていません。

手順

Azure Stack HCI クラスターを展開するときに、対称型ハードウェア構成を維持し、Azure Stack HCI クラスター ノードのファームウェア/ドライバーをアップデートするには、次の手順を実行します。

- Windows Admin Center に Azure Stack HCI クラスターを展開するときに、[作業の開始] ウィザードを使用して、必要に応じて、[1.1 前提条件の確認]、[1.2 サーバーの追加]、[1.3 ドメインに参加]、[1.4 機能のインストール]、および [1.5 アップデートのインストール] タブで手順を実行します。

- メモ:** [1.3 ドメインに参加] タブでのノード名の変更はサポートされていません。名前を変更すると、ハードウェア アップデートのインストール時に必須条件エラーが発生する可能性があります。サーバーの名前を変更するには（必要な場合）、クラスターの導入ワークフローの外で実行することをお勧めします。たとえば、Azure Stack HCI OS サーバー構成ツール（Sconfig）または Windows Admin Center を使用して、ノードの名前を変更します。クラスター作成ウィザードを起動する前に、新しいノード名が有効であることを確認してください。

- [ハードウェア アップデートのインストール] タブで、[インストール] をクリックして、OpenManage Integration スナップインをインストールします。OpenManage Integration 拡張機能バージョン 2.1 をすでにインストールしている場合は、[アップデートのチェック] をクリックして、[ハードウェア アップデートのインストール] ページに移動します。

- メモ:** スナップインで「管理に使用する認証情報」を指定するように求められた場合は、[管理に使用する認証情報] を選択して、管理下ノードでの認証に適切なクラスター管理者の認証情報を入力します。次に、[これらの認証情報をすべての接続に使用] チェック ボックスを選択します。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。[管理に使用する認証情報] 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」セクションを参照してください。

OpenManage Integration スナップインがインストールされている場合は、Windows Admin Center の [ツール] メニューの下に、OpenManage Integration スタンドアロン拡張機能が表示されます。OpenManage Integration 拡張機能のすべての機能が、スナップイン固有の機能とともに使用できるようになります。

- ページに一覧表示されている前提条件を確認して、すべてのノードで HCI 構成プロファイルのチェックとアップデートを実行する準備ができていることを確認します。
 - いずれかのノードが有効なモデルではない場合は、次のステップに進むことはできません。サポートされているモデルの詳細については、[AS HCI のサポート マトリックス](#)を参照してください。
 - いずれのノードにも OMIWAC プレミアム ライセンスが含まれていない場合、ノードのアップデートを続行することはできませんが、HCI 構成プロファイルのチェックを実行することはできません。

[再実行] をクリックして、前提条件を再度実行します。

終了したら、[次へ : HCI 構成プロファイル] をクリックします。

- [HCI 構成プロファイル] では、各カテゴリに表示されている設定を確認して、すべてのノードの設定が Dell EMC が推奨する設定に従っていることを確認します。HCI 構成プロファイルに必要なハードウェア構成の詳細については、「[HCI 構成プロファイル](#)」を参照してください。

- （オプション）インターネットに接続できない場合は、次の手順を実行して、HCI 構成プロファイルのチェックをオフラインモードで実行します。
 - <http://downloads.dell.com/omimswac/supportmatrix/> から `asHCISolutionSupportMatrix.json` および `asHCISolutionSupportMatrix.json.sign` ファイルをダウンロードします。
 - これらのファイルを、Windows Admin Center がインストールされているゲートウェイ システムの `C:\Users\Dell\SymmetryCheck` フォルダーに配置します。
 - HCI 構成プロファイルのチェックを実行します。

- メモ:** 必要な設定のいずれかが「重大」エラーで失敗した場合、HCI 構成プロファイルのチェックは正常に行われません。問題を解決するための推奨事項と詳細を確認して HCI 構成プロファイルを実現し、次の手順に進みます。

設定が「警告」で失敗した場合、その設定はクラスターの導入には対応していますが、クラスターのパフォーマンスが最適なレベルになる可能性があります。したがって、確認する必要があります。

[再実行] をクリックして、HCI 構成プロファイルのチェックを再度実行します。

終了したら、[次へ : アップデートソース] をクリックします。

5. 検証済みの Azure Stack HCI カタログに対してコンプライアンス レポートを生成するには、[アップデートソース] ページで次の手順を実行します。

a. カタログ ファイルをダウンロードする方法を 1 つ選択します。

- [オンライン (HTTPs) - Microsoft HCI ソリューションのアップデート カタログ] を使用すると、dell.com からカタログが自動的にダウンロードされます。オンライン カタログは、デフォルトで選択されています。

オンライン カタログのサポートには、Windows Admin Center ゲートウェイから直接インターネット接続が必要です。カタログの全体的なダウンロード時間は、ネットワーク帯域幅とアップデート対象のコンポーネントの数によって異なります。

 **メモ:** プロキシ設定を使用したインターネットへのアクセスはサポートされていません。

- [オフライン - Dell EMC Repository Manager カタログ] を選択すると、CIFS の場所で設定された DRM カタログを使用します。

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。インターネットを使用できない場合、またはカスタマイズされた DRM カタログを使用する場合は、このオプションを使用できます。

- オフライン カタログを使用するには、[DRM 設定] を選択して、DRM カタログとともに CIFS 共有パスが設定されていることを確認します。DRM カタログを作成するには、[技術に関する記事](#)を参照してください。

b. Dell EMC System Update (DSU) および Inventory Collector (IC) ツールを使用するには、[詳細設定] を選択し、次のいずれかを選択します。

- [Dell EMC System Update (DSU) および Inventory Collector (IC) を自動的にダウンロードして設定]。OMIMSWAC がインターネットに接続されている場合に選択します。
- 共有の場所にある DSU ツールおよび IC ツールを手動でダウンロードして設定するには、[DSU および IC を手動設定] を選択して、[設定] を選択。OMIMSWAC がインターネットに接続されていない場合は、このオプションを使用することをお勧めします。

OpenManage Integration 拡張機能の [アップデート ツール] 設定を使用して設定された DSU および IC の設定は、OpenManage Integration スナプインの [詳細設定] でも使用できます。

終了したら、[次へ : コンプライアンス レポート] をクリックします。

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 <https://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。

6. [コンプライアンス レポート] タブで、コンプライアンス レポートを表示します。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。

- 「非対応」で「アップグレード可能」なコンポーネントは、デフォルトで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の選択を解除するか、または「非対応」の「ダウングレード可能」なコンポーネントを選択することができます。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。

終了したら、[次へ : サマリー] をクリックします。

7. [サマリー] タブで、アップデートするコンポーネントを確認し、[次へ : アップデート] をクリックしてクラスター ノードをアップデートします。

CredSSP を有効にするためのメッセージが表示されます。

- a. [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] ページが表示されます。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] ページでアップデートが進行中の場合は、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、ノードのアップデートに失敗し、アップデートのステータスが表示されないことがあります。

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 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
- 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、必要に応じてコンプライアンス設定の詳細を入力します。

タスクの結果

ハードウェア アップデートが完了した後、Windows Admin Center に表示される指示に従って、Azure Stack HCI クラスターを作成することができます。

HCI 構成プロファイル

HCI 構成プロファイルのチェックにより、Azure Stack HCI クラスター用に選択されたノードがサポート対象であり、Dell EMC が推奨する対称型ハードウェア構成であることが確認されます。

Azure Stack HCI クラスターは、選択されたすべてのノードのハードウェア構成が Dell EMC の推奨事項に準拠している場合に最大の機能を発揮します。

OMIMSWAC の統合された導入およびアップデート機能は、Windows 管理センターで AX ノード (Azure Stack HCI OS を実行する) を使用して Azure Stack HCI クラスターを構築する際に、HCI 構成プロファイルを維持し、ノードをアップデートできるようにします。HCI 構成プロファイルのチェックは、一連のルールをノードで実行し、Dell EMC の推奨事項にハードウェア構成を合わせるために役立ちます。

Azure Stack HCI クラスターを作成する前に、HCI 構成プロファイルのチェックのすべてのルールを実行し、このルールに準拠していることを確認してください。

HCI 構成プロファイルのチェックは、次のことを実施します。

- Azure Stack HCI クラスターを本番環境に移行する前に、ハードウェアまたは構成の問題を検出する。
- 導入する Azure Stack HCI クラスターの信頼性が高く、クラスターのパフォーマンスが最適であることを確認する。

このトピックでは、HCI 構成プロファイルのルールについて説明し、サポート対象およびサポート対象外の構成の例を示します。HCI 構成プロファイルに必要なサポート対象コンポーネントおよび検証済みコンポーネントの詳細については、[「AS HCI のサポート マトリックス」](#) を参照してください。HCI 構成プロファイルのチェックのいずれかが「重大」または「警告」のエラーで失敗した場合は、推奨事項を確認し、詳細を表示した後、[Dell サポート チーム](#)に連絡して問題を解決してから、次の手順に進んでください。

重大なエラーは、ノード構成のその側面がサポートされていないことを示しています。対称型 Azure Stack HCI クラスターを導入する前に、この問題を修正する必要があります。警告の状態は、ノード構成のその側面がクラスター導入でサポートされる可能性はあるものの、クラスターのパフォーマンスが最大化されない可能性を示します。したがって、確認する必要があります。

構成ルール

プロセッサ

- すべてのノードで、同じモデルのプロセッサを使用することをお勧めします。プロセッサ モデルの異なるノードを使用すると、警告が表示されます。

たとえば、1つのノードのプロセッサが X モデルである場合は、すべてのノードのプロセッサが X モデルである必要があります。

- すべてのノードでプロセッサ ソケット数が同じである必要があります。異なるプロセッサ ソケットのノードを使用すると、HCI 構成プロファイルの障害が発生します。

たとえば、1つのノードのプロセッサ ソケット数が 2 個の場合は、すべてのノードのプロセッサ ソケット数が 2 個である必要があります。

メモリ

- 1つのノードにパーシステント メモリーがある場合は、すべてのノードに、同じ数と容量のパーシステント メモリーがあることが推奨されます。パーシステント メモリーの数または容量が異なるノードを使用すると、警告が表示されます。
- すべてのノードで、同じ容量の物理メモリーを使用することをお勧めします。容量の異なる物理メモリーを使用すると、警告が表示されます。

プラットフォーム

- すべてのノードには、Boot Optimized Storage Subsystem (BOSS) アダプターが必要です。BOSS アダプターなしでノードを使用すると、HCI 構成プロファイルの障害が発生します。

保管時

- すべてのノードで、同じメディア タイプ (SSD、NVMe、HDD など) で互換性のあるドライブを使用することをお勧めします。互換性のないドライブのノードを使用すると、警告が表示されます。
- すべての NVMe 構成を除き、すべてのノードが、同じホスト バス アダプター (HBA) を使用している必要があります。HBA が異なるノードを使用すると、HCI 構成プロファイルの障害が発生します。

たとえば、1つのノードが HBA 330 を使用している場合は、すべてのノードが HBA 330 を使用する必要があります。

ネットワーク

- すべてのノードで、互換性のあるネットワーク アダプターを使用することをお勧めします。互換性のないネットワーク アダプターのノードを使用すると、警告が表示されます。
- すべてのノードで、少なくとも1つの RDMA ネットワーク アダプターが共通である必要があります。一般的なネットワーク アダプターのないノードを使用すると、HCI 構成プロファイルの障害が発生します。

たとえば、1つのノードに QLogic ネットワーク アダプターがあり、他のノードに Mellanox ネットワーク アダプターがある場合、この構成はサポートされません。この場合は、すべてのノードに少なくとも1つの共通 RDMA ネットワーク アダプター (QLogic または Mellanox) が存在する必要があります。

ディスク

- AS HCI サポート マトリックスに記載されているように、すべてのノードに、互換性のあるディスクが含まれることが推奨されます。互換性のないディスクのノードを使用すると、警告が表示されます。
- すべてのノードで、使用するメディア タイプは2つまでにすることをお勧めします。サポートされているメディア タイプの組み合わせは、次のとおりです。
 - パーシステント メモリーと NVMe
 - パーシステント メモリーと SSD
 - NVMe と SSD
 - NVMe と HDD
 - SSD と HDD
 - NVMe のみ
 - SSD のみ

NVMe、SSD、HDD など、3つのメディア タイプの組み合わせを使用すると、HCI 構成プロファイルの障害が発生します。

- すべてのノードのドライブ数を、メディア タイプごとに必要な最小限に収めることをお勧めします。

たとえば、1つのノードに1つのメディア タイプの SSD のみがある場合は、少なくとも4台の容量用 SSD ドライブが必要です。SSD と HDD のように、ノードのメディア タイプが2つの場合は、2台のキャッシュ用 SSD ドライブと4台の容量用 HDD ドライブが必要です。

複数のメディア タイプの複数のドライブを使用すると、警告が表示されます。

- すべてのノードで同じドライブ タイプを使用する必要があります。たとえば、1つのノードに SATA ドライブがある場合、すべてのノードで SATA ドライブを使用する必要があります。クラスター内で SATA および SAS ドライブを組み合わせると、HCI 構成の障害が発生します。
- すべてのクラスター ノードで、SSD、NVMe、HDD などのメディア タイプごとにすべてのドライブが、同じバス プロトコル (SAS、SATA、または PCIe など) を使用することをお勧めします。

たとえば、1つのノードの SSD ドライブと HDD ドライブで SAS バス プロトコルを使用している場合は、他のノードにも、SSD ドライブと HDD ドライブがあり、SAS バス プロトコルを使用している必要があります。複数のドライブで異なるバス プロトコルを使用すると、警告が表示されます。

メモ: 対称性構成を実現するために、選択した各ノードのドライブで同じバス プロトコルを使用することをお勧めします。たとえば、SATA バス プロトコルの SSD と、SAS バス プロトコルの HDD など、複数のドライブがノードに搭載されている構成はサポートされていません。

- すべてのノードでドライブのサイズと数を、メディア タイプごとに同じにすることをお勧めします。

たとえば、1つのノードに4台の2TBのSSDドライブがある場合は、他のノードにも、4台の2TBのSSDドライブが必要です。ドライブの数と容量の異なる複数のノードを使用すると、警告が表示されます。

- SSD または NVMe メディア タイプのドライブを持つ各ノードは、同じ耐久性であるようにすることをお勧めします。

たとえば、1つのノードで4つの混合使用型 SSD ドライブ タイプを使用している場合は、他のノードでも、4つの混合使用型 SSD ドライブ タイプを使用する必要があります。

読み取り集中型、混合使用型、書き込み集中型など、異なる耐久性の複数のドライブを持つノードを使用すると、警告が表示されます。

- 少なくとも1つのノードにパーシステント メモリーが存在する場合は、そのクラスター用に選択されている残りのすべてのノードにも、同じ数と容量のパーシステント メモリー モジュールが含まれる必要があります。パーシステント メモリー モジュールの数と容量の異なる複数のノードを使用すると、警告が表示されます。
- キャッシュ ドライブの raw 容量の合計は、キャパシティ ドライブの raw 容量の 5%以上である必要があります。

構成の例

サポート対象とサポート対象外の構成の例を以下に示します。

サポート対象外：ノード間での異なるモデルの使用

最初の2つのノードは AX-640 モデルを使用していますが、3 番目のノードは AX-740xd を使用しています。

ノード 1	ノード 2	ノード 3
AX-640	AX-640	AX-740xd

これはサポートされていません。すべてのノードが、同じモデルを使用する必要があります。

サポート対象：2つ以下のメディア タイプ

メディア タイプが2つの、サポート対象の構成は次のとおりです。

ノード 1	ノード 2	ノード 3	ノード 4	ノード 5
NVMe+SSD	NVMe+HDD	SSD+HDD	NVMe のみ	SSD のみ

サポート対象外：最小数以上のドライブ数

次の例では、2つのメディア タイプがあります。

ノード 1	ノード 2	ノード 3
2 x キャッシュ用 SSD	2 x キャッシュ用 SSD	2 x キャッシュ用 SSD
3 x 容量用 HDD	3 x 容量用 HDD	3 x 容量用 HDD

これはサポートされていません。2つのメディア タイプのドライブを持つノードには、2 台のキャッシュ用 SSD ドライブと 4 台の容量用 HDD ドライブが必要です。

サポート対象：最小数以上のドライブ数

メディア タイプが2つの場合、サポートされている構成は次のとおりです。

ノード 1	ノード 2	ノード 3
2 x キャッシュ用 SSD	2 x キャッシュ用 SSD	2 x キャッシュ用 SSD
4 x 容量用 HDD	4 x 容量用 HDD	4 x 容量用 HDD

これはサポートされています。2つのメディア タイプのドライブを持つノードには、2 台のキャッシュ用ドライブ (SSD/ NVMe/AEP) と 4 台の容量用ドライブ (HDD/SSD/NVMe) が必要です。

サポート対象外：異なるバス プロトコルの複数のドライブ

最初の2つのノードは、SAS バス プロトコルの SSD ドライブを使用していますが、3 番目のノードは、SATA バス プロトコルの SSD ドライブを使用しています。

ノード 1	ノード 2	ノード 3
SAS プロトコルを使用する SSD	SAS プロトコルを使用する SSD	SATA プロトコルを使用する SSD

最初の2つのノードは、SAS バス プロトコルの SSD ドライブと HDD ドライブを使用していますが、3 番目のノードは、SATA バス プロトコルの HDD ドライブを使用しています。

ノード 1	ノード 2	ノード 3
SAS プロトコルを使用する SSD	SAS プロトコルを使用する HDD	SATA プロトコルを使用する HDD

これらはサポートされていません。各ノードのドライブが、対称性構成のために、同じバス プロトコルを使用する必要があります。

サポート対象外：容量が同じで数が異なる複数のドライブ

最初の 2 つのノードは 2 TB の SSD を使用していますが、3 番目のノードは 3 TB の SSD を使用しています。すべてのノードに合計 4 台の SSD があります。

ノード 1	ノード 2	ノード 3
4 x 2 TB SSD	4 x 2 TB SSD	4 x 3 TB SSD

これはサポートされていません。メディア タイプ (SSD/NVMe/HDD) ごとに、すべてのドライブの数と容量が同じである必要があります。

サポート対象外：ノード全体で同一の RDMA ネットワーク アダプターが 1 つ以上使われている

最初の 2 つのノードは QLogic ネットワーク アダプターを使用していますが、3 番目のノードは Mellanox ネットワーク アダプターを使用しています。

ノード 1	ノード 2	ノード 3
QLogic ネットワーク アダプター	QLogic ネットワーク アダプター	Mellanox ネットワーク アダプター

これはサポートされていません。すべてのノードで、1 つのネットワーク アダプターが共通して使われている必要があります。

HCI 構成プロファイルのチェック結果の表示

HCI 構成プロファイルのチェックが完了すると、サマリー レポートが表示されます。すべてのルールに、正常終了を示す緑のチェックマーク、または、場合によっては黄色の三角形 (警告) が付いている必要があります。次の表は、サマリーに含まれる記号とその意味を示しています。

記号	説明
	HCI 構成プロファイルのチェックが正常に終了しました。つまり、ノード構成のその側面は、クラスター導入でサポートされています。
	HCI 構成プロファイルのチェックで警告が生成され、ノード構成のその側面がクラスター導入でサポートされる可能性はあるものの、クラスターのパフォーマンスが準最適なレベルになる可能性を示します。したがって、確認する必要があります。
	HCI 構成プロファイルのチェックでエラーが生成され、ノード構成のその側面がサポートされていません。対称型 Azure Stack HCI クラスターを導入する前に、この問題を修正する必要があります。

OpenManage Integration スナップインを使用した、Azure Stack HCI クラスター向けのフル スタック クラスター対応アップデート

OpenManage Integration スナップインのフル スタック クラスター対応アップデート機能を使用すると、Windows Admin Center で使用可能なオペレーティングシステムのアップデートに加えて、Microsoft Azure Stack HCI (Azure Stack HCI と呼ばれます) クラスター ノード用の Dell EMC 統合システム上でハードウェアのアップデート (ファームウェア、BIOS、およびドライバ) を実行することができます。

最新の機能を利用するには、最新のセキュリティ フィックスを適用し、インフラストラクチャーの不具合がない状態を維持し、オペレーティングシステムおよびファームウェア、BIOS、ドライバなどのハードウェアの最新のアップデートでターゲット ノードがアップデートされていることを確認する必要があります。オペレーティングシステムおよびハードウェアのアップデートの多くは、変更を適用するためにノードの再起動が必要になる場合があります。再起動プロセスは、ノードで実行されているワークロードやアプリケーションに影響を与える可能性があります。

OpenManage Integration スナップインを Windows Admin Center クラスターのアップデート ワークフローと統合して使用すると、WAC で使用可能なオペレーティングシステムのアップデートに加えて、ターゲット ノード上のファームウェア、BIOS、およびドライバをシームレスにアップデートすることができます。また、フル スタック CAU 機能を使用したアップデートの後に必要な再起動の回数も減ります。

フル スタック アップデート機能にアクセスするには、Windows Admin Center で、[ツール] メニューから [アップデート] を選択します。

クラスター上でハードウェアのアップデートを個別に実行するには、OpenManage Integration with Windows Admin Center 拡張機能 ツールで使用可能なクラスター対応アップデート機能を使用します。OpenManage Integration 拡張機能による、PowerEdge サーバー、および Windows Server HCI クラスター、Azure Stack HCI クラスター、フェールオーバー クラスターのノードのアップデート、p. 18 を参照してください。

トピック：

- [OpenManage Integration スナップインを使用した Azure Stack HCI クラスターのアップデート](#)

OpenManage Integration スナップインを使用した Azure Stack HCI クラスターのアップデート

前提条件

ファームウェア、BIOS、ドライバのアップデートを開始する前に、次の前提条件を満たしていることを確認します。

- Windows Admin Center 2103.2 GA がインストールされていることを確認します。
- ドメイン管理者の認証情報を使用して、リモートで Microsoft Windows 管理センターにログインします。ゲートウェイ管理者としての認証情報であることを確認します。詳細については、[Microsoft のマニュアル](#)を参照してください。
- Microsoft Azure Stack HCI (Azure Stack HCI と呼ばれます) クラスター用の Dell EMC 統合システムが、Azure Stack HCI バージョン 20H2 オペレーティングシステムを実行している AX ノードから作成されていることを確認します。
- OMIWAC プレミアム ライセンスが各 AX ノードにインストールされていることを確認します。
- クラスターの役割の一部として、アップデート前のスクリプトとアップデート後のスクリプトが存在しないことを確認します。存在する場合は、アップデートをトリガーする前にそのスクリプトを削除することをお勧めします。詳細については、「トラブルシューティング」セクションの「[\[テスト サマリー \] ページ](#)」を参照してください。
- 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ことを確認します。また、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、IC の各ユーティリティをダウンロードし、コンプライアンス レポートのみを生成することもできます。プロキシ設定の詳細については、「[プロキシ設定の構成](#)」を参照してください。
- オフライン DRM カタログを使用するには、設定が[アップデート ツール設定の構成](#)に記載されているように設定されていることを確認します。

- スナップインで「管理に使用する認証情報」を指定するように求められた場合は、管理下ノードの認証に適切なクラスタードメイン管理者の認証情報を入力し、「これらの認証情報をすべての接続に使用」チェックボックスを選択します。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。詳細については、[Microsoft の文書の「クラスター対応アップデートの要件とベストプラクティス」](#)を参照してください。

このタスクについて

フルスタック クラスター対応アップデート機能は、Azure Stack HCI バージョン 20H2 オペレーティングシステムを実行している Microsoft Azure Stack HCI 用の Dell EMC 統合システムでサポートされています。

手順

Azure Stack HCI クラスター ノードでオペレーティングシステムとハードウェアの両方のアップデートを実行するには、次の手順を実行します。

1. Windows Admin Center で、「ツール」メニューから「アップデート」を選択します。
 - a. Credential Security Service Provider (CredSSP) を有効にして、明示的な認証情報を指定する必要があります。CredSSP を有効にするかどうか確認が求められたら、「はい」をクリックします。
「アップデート」ページが表示されます。
2. オペレーティングシステムのアップデートについては、[Microsoft の Azure Stack HCI のマニュアル](#)を参照してください。
3. 「アップデートのインストール」ページで、オペレーティングシステムのアップデートを確認した後、「次へ：ハードウェアのアップデート」を選択します。
4. Windows Admin Center は、サポートされている Dell EMC OpenManage Integration 拡張機能がインストールされているかどうかを確認します。
 - 拡張機能がインストールされていない場合は、「インストール」をクリックして、ライセンス条項に同意し、OpenManage Integration スナップインをインストールします。
 - OpenManage Integration 拡張機能バージョン 2.1 がすでにインストールされている場合、または OpenManage Integration スナップインをインストールした後に、「アップデートの入手」をクリックして、「ハードウェアのアップデート」ページに移動します。

OpenManage Integration スナップインがインストールされると、Windows 管理センターの「ツール」メニューに OpenManage Integration 拡張機能バージョン 2.1 が表示されます。OpenManage Integration 拡張機能のすべての機能が、スナップイン固有の機能とともに使用できるようになります。

5. 「ハードウェアのアップデート」ページで、リストされている前提条件を確認し、すべてのノードでハードウェアのアップデートの準備ができていないことを確認します。終了したら、「次へ：アップデートソース」をクリックします。「再実行」をクリックして、前提条件を再度実行します。

「前提条件」タブに表示されているすべての前提条件を満たしている必要があります。そうでない場合は、次の手順に進むことができません。

6. 検証済みの Azure Stack HCI カタログに対してコンプライアンス レポートを生成するには、「アップデートソース」ページで次の手順を実行します。
 - a. カタログ ファイルをダウンロードする方法を 1 つ選択します。

- 「オンライン (HTTPs) - Microsoft HCI ソリューションのアップデート カタログ」を選択すると、dell.com からこのカタログを自動的にダウンロードします。オンライン カタログ オプションがデフォルトで選択されています。

オンライン カタログのサポートには、Windows Admin Center ゲートウェイから直接インターネット接続が必要です。カタログの全体的なダウンロード時間は、ネットワーク帯域幅とアップデート対象のコンポーネントの数によって異なります。

 **メモ:** プロキシ設定を使用したインターネットへのアクセスはサポートされていません。

- 「オフライン - Dell EMC Repository Manager カタログ」を選択すると、CIFS の場所で設定された DRM カタログを使用します。

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。インターネットを使用できない場合、またはカスタマイズされた DRM カタログを使用する場合は、このオプションを使用できます。

- オフライン カタログを使用するには、「DRM 設定」を選択して、DRM カタログとともに CIFS 共有パスが設定されていることを確認します。DRM カタログを作成するには、[技術に関する記事](#)を参照してください。

- b. Dell EMC System Update (DSU) および Inventory Collector (IC) ツールを使用するには、「詳細設定」を選択し、次のいずれかを選択します。

- OMIMSWAC がインターネットに接続されている場合は、「Dell EMC System Update (DSU) および Inventory Collector (IC)」を自動的にダウンロードして設定」を選択。

- 共有の場所にある DSU ツールおよび IC ツールを手動でダウンロードして設定するには、[DSU および IC を手動設定] を選択して、[設定] を選択。OMIMSWAC がインターネットに接続されていない場合は、このオプションを使用することをお勧めします。

OpenManage Integration 拡張機能の [アップデート ツール] 設定を使用して設定された DSU および IC の設定は、OpenManage Integration スナップインの [詳細設定] でも使用できます。

終了したら、[次へ：コンプライアンス レポート] をクリックします。

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 <https://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 レポート] タブで、コンプライアンス レポートを表示します。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。

- 「非対応」で「アップグレード可能」なコンポーネントは、デフォルトで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の横にあるチェック ボックスをオフにするか、または「非対応」で「ダウングレード可能」な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間の依存関係が満たされていることを確認します。

終了したら、[次へ：サマリー] をクリックします。

- [サマリー] タブで、アップデートするコンポーネントを確認し、[次へ：アップデートのダウンロード] をクリックして、選択したコンポーネントのアップデートをダウンロードします。

メモ: ダウンロードの進行中は、ブラウザを終了または閉じることは推奨されません。ブラウザを閉じたり、終了したりすると、アップデート操作のダウンロード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、ダウンロード 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、ダウンロード ジョブが完了すると通知します。

- ダウンロード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 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
 - クラスターのアップデートが完了した後、個々のノードの DSU ログは、それぞれのノード上の<Windows Directory>\Temp\OMIMSWAC フォルダーにあります。
- コンプライアンス レポートを再度実行するには、[コンプライアンスを再実行] をクリックして、手順 4~7 を繰り返します。

- アップデートがダウンロードされたら、Windows Admin Center で表示される指示に従ってオペレーティング システムとハードウェアの両方のアップデートをインストールします。

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。アップデートが完了すると、Windows Admin Center から通知があります。

タスクの結果

アップデートで再起動を必要とするものがあれば、ノードは一度に1つずつ再起動され、ダウンタイムを回避するために、VM などのクラスターの役割がノード間で移動します。

次の手順

- メモ:** CAU のクラスター化された役割はデフォルトでは、毎月第3週の火曜日にクラスターの自動アップデート機能をトリガーするように設定されています。したがって、アップデートが完了したら、クラスターの自動アップデート機能が動作しないように、いずれかのクラスター ノードで CAU のクラスター化された役割を無効にするようにしてください。CAU のクラスター化された役割を無効化する方法の詳細については、次を参照してください： <https://docs.microsoft.com/en-us/powershell/module/clusterawareupdating/disable-cauclusterrole?view=win10-ps>

クラスターまたは個別のノードの CPU コアを管理する

前提条件

- OMIMSWAC の適切な機能については、「OpenManage Integration の準備」の項でベスト プラクティスを参照してください。
- クラスターに同種のノードが含まれていることを確認します。たとえば、ノードには、インテルまたは AMD からの、同じプロセッサ ファミリーの CPU が必要です。インテルと AMD の両方、または異なるプロセッサ ファミリーの CPU を含むノードはサポートされていません。
- クラスター内の CPU コアを管理するには、各クラスター ノードに「OMIWAC Premium License for MSFT HCI Solutions」をインストールする必要があります。個別のノード (AX、S2D、PowerEdge ノード) 内の CPU コアを管理するには、「OMIWAC Premium License for MSFT HCI Solutions」を AX/S2D ノードにインストールし、「OMIWAC Premium License for PowerEdge」を PowerEdge ノードにインストールする必要があります。

このタスクについて

ワークロードの要求と電力消費を管理するために、「CPU コア管理」機能を使用して、ノードまたはクラスターに割り当てられている CPU コアの量を変更できます。この機能は、電力とパフォーマンスのバランスを適切に維持するために役立ちます。この機能を使用すると、クラスターの CPU コアを最適化して、総所有コストを最適なレベルに維持することもできます。

CPU コア管理機能は、Azure Stack HCI クラスター、Windows Server ベースの HCI クラスター、各ノードに OMIWAC Premium License がインストールされている個別のノードでサポートされています。

メモ: CPU コア管理機能は、フェールオーバー クラスターと、Azure Stack HCI または Windows Server HCI クラスターの一部である個別のノードではサポートされていません。

手順

Windows 管理センターで、クラスターまたは個別のノードに接続し、次の手順を実行します。

1. Windows 管理センターの [拡張機能] で、[Dell EMC OpenManage Integration] をクリックします。
2. [Dell EMC OpenManage Integration] で、[構成] タブをクリックします。
3. [CPU コア管理] では、クラスター ノードまたは個別のノードの CPU コア ディストリビューションの概要が次のように表示されます。
 - [CPU コア構成サマリー] の横の横棒グラフには、クラスターまたは個別のノードで現在有効になっているコアの数と、使用可能なコアの数が表示されます。ノードまたはクラスター内に存在する CPU コアの最大数は、棒グラフの下に記載されています。
 - [現在の構成] では、ノードの合計数、CPU、および現在有効なコアが CPU モデル番号とともに表示されます。
 - ノード名、ノードで使用されている CPU モデル、CPU 数、CPU あたりのコア数、コア スピードなどのノードの詳細を表示または非表示にするには、[ノードレベルの詳細の表示] をオンまたはオフに切り替えます。
- a. [ノードレベルの詳細の表示] で、ノードを選択して、次のようなノードの [詳細情報] を表示します。
 - Dell Controlled Turbo
 - Logical Processor (論理プロセッサ)
 - Configurable TDP (設定可能 TDP)
 - 仮想化テクノロジー
 - X2APIC モード
4. CPU コアを管理するには、[CPU コアのアップデート] をクリックします。
CPU コアのアップデート ウィザードが右側に表示されます。
5. CPU コアのアップデート ウィザードで、スライダーを左右に動かして、ワークロードに基づいて使用されるコアの数を増減します。

CPU コア メーカー (インテルまたは AMD) に基づいて、コアを次のように構成することができます。クラスターの均一性を維持するために、OMIMSWAC はすべてのノードで同じ構成を適用します。

メモ: コア数を変更すると、クラスターの全体的なコアの数に影響します。電力とパフォーマンスのバランスを維持するために、適切な数のコアを使用していることを確認します。

CPU Type	手順
インテル CPU	● CPU あたりの有効にするコア数を選択します。 ● 有効にできるコアの最小数は 4 です。ワークロードを管理するすべてのコアを有効にすることができます。
AMD CPU	● 最初のスライダーを使用して、有効にするプロセッサあたりの CCD の数を選択します。 ● 2 番目のスライダーを使用して、有効にする CCD あたりのコア数を選択します。 ● 少なくとも、任意の数のコアを有効にすることができます。ワークロードを管理するすべてのコアを有効にすることもできます。

6. 次のいずれかのオプションを選択して、変更を適用してノードを再起動します。

- **個別のノードの場合：**
 - [適用して今すぐ再起動]: 変更を適用してすぐにノードを再起動するには、このオプションを選択します。変更を適用する前に、ワークロードを十分に考慮してください。
 - [次の再起動時に適用]: このオプションを選択すると、変更を今すぐ適用し、後でノードを再起動します。CPU コアの変更が正常に適用されるように、後でノードを再起動するようにしてください。また、ノードを再起動する前に、ワークロードを十分に考慮してください。
- **クラスターの場合：**
 - [適用して今すぐ再起動]: 変更を適用してクラスター ノードを今すぐ再起動する場合は、このオプションを選択します。ワークロードを処理することによってノードが自動的に再起動されるため、Dell EMC ではこのオプションを使用することを推奨します。
[適用して今すぐ再起動] をクリックする前に、次のことを確認してください。
 - OMIMSWAC は、Microsoft クラスター対応アップデート機能フレームワークを使用してクラスターのアップデートを実行するため、クラスターを再起動する前に、すべてのクラスター ノードに**フェールオーバー クラスターリング機能とフェールオーバー クラスターリング ツール**がインストールされていることを確認してください。詳細については、[Microsoft の文書の「クラスター対応アップデートの要件とベストプラクティス」](#)を参照してください。
 - クラスターを再起動する前に、クラスターの準備状況をテストすることをお勧めします。詳細については、[Microsoft のマニュアルに記載されたクラスター アップデートの準備状況のテスト](#)を参照してください。
 - [次の再起動時に適用]: このオプションを選択すると、変更を今すぐ適用し、後でノードを再起動します。CPU コアの変更が正常に適用されるように、後でクラスター ノードを再起動するようにしてください。また、ノードを再起動する前に、ワークロードを十分に考慮してください。

メモ: [適用して今すぐ再起動] 処理では、CredSSP を有効にする必要があります。セキュリティを向上させるには、CPU 構成の変更が完了した後に CredSSP を無効にします。

7. 変更を適用するには、[確認] をクリックします。

[コンピューティング リソース] の下で、変更のステータスが表示されます。ノード レベルでの進行状況を表示するには、[詳細の表示] をクリックします。

次の手順

CPU 構成のアップデートに関する問題については、「トラブルシューティング」の項を参照してください。

既存のクラスターへのノードの追加

OMIMSWAC を使用することにより、既存の Windows Server HCI、Azure Stack HCI、フェールオーバー クラスターに追加するノードを準備し、容量を向上させることができます。

この作業は、クラスター管理者がクラスターを対称に維持し、Dell EMC の推奨事項に準拠するために常に重要です。クラスターの拡張時に、プロセスを自動化し、お客様が Dell EMC の推奨事項に従うことを支援するために、OMIMSWAC に「クラスターの拡張」という機能が導入されました。「クラスターの拡張」機能を使用すると、管理者はノードに互換性があることを確認し、Dell EMC の推奨事項に従ってノードを準備し、既存のクラスターに追加することができます。

クラスターの拡張プロセスには、次の3つの主要なステップがあります。

- 高レベルの互換性チェック：クラスターに追加する互換性のあるノードを特定するのに役立ちます。
- ライセンスの可用性のチェック：新しいノードおよびクラスター ノードで使用可能な OMIWAC プレミアム ライセンスがあるかをチェックします。
- HCI 構成プロファイルのチェック：Dell EMC の推奨事項に基づいて、新しいノードおよびクラスター ノードの HCI 構成を確認するのに役立ちます。このプロセスは、Windows Server HCI および Azure Stack HCI クラスターにのみ適用されます。
- アップデート コンプライアンス：新しいノードとクラスター ノードの両方のコンプライアンス レポートを生成し、新しいノードについてのみコンプライアンスを修正するのに役立ちます。

これらのステップをすべて正常に完了した後で、既存のクラスターに新しいノードを追加することができます。

トピック：

- [Windows Server HCI および Azure Stack HCI クラスター拡張のためのノードの準備](#)
- [フェールオーバー クラスター拡張のためのノードの準備](#)

Windows Server HCI および Azure Stack HCI クラスター拡張のためのノードの準備

前提条件

- 「OMIWAC Premium License for MFHCI Solutions」がクラスター ノードと新しいノードにインストールされていることを確認します。
- 新しいノードがクラスターに含まれていないことを確認します。
- SAS RAID_Driver の新しいノードについては、次のことを確認します。
 - 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。

クラスター拡張のためのノードを準備する前に、次を計画します。

- 新しいノードをラックに設置し、適切にケーブル接続します。
- 新しいノードに、既存のクラスター ノードと同じオペレーティング システムがインストールされていることを確認します。
- Windows 管理センターを使用してノードを接続し、ユーザー名、ドメインなどの基本設定を構成します。
- 新しいノードがクラスター ノードと同じドメインにあることを確認します。
- クラスター管理者が新しいノードにローカル管理者権限でアクセスできることを確認します。

手順

クラスター拡張用にノードを準備するには、次の手順を実行します。

1. Windows 管理センターを使用してクラスターに接続し、OpenManage Integration の拡張機能を起動します。
2. [設定] タブに移動し、左側の [クラスターの拡張] をクリックします。
3. [クラスターの拡張] ウィンドウで、[ノードの追加] をクリックします。
4. [クラスターの拡張] ウィンドウの [互換性のあるノードの選択] で、ノードのリストが表示されます。リストは、Windows 管理センターの [Server Manager] ページで使用可能なすべてのノードを取得します。

- a. クラスタに追加するノードを選択します。検索ボックスを使用して任意のノードを検索するか、[すべて選択] チェックボックスをクリックしてすべてのノードを選択することもできます。新しいノードがクラスタに含まれていないことを確認します。

メモ: クラスタでサポートされているノードの合計数は 16 です。たとえば、既存の 4 つのノードを持つクラスタの場合、最大 12 個のノードを選択してクラスタを拡張することができます。

- b. ノードが選択されたら、[高レベルの互換性] の [チェック] をクリックして、Dell EMC の推奨事項に従って新しいノードとクラスタ ノードを検証します。

検証は、次のように高レベルで行われます。

- 新しいノードとクラスタ ノードの両方が Dell Technologies 製である必要があります。

メモ: HCI クラスタの拡張では、AX-640、AX-740XD、AX-6515、AX-7525 ノードなどの Dell Technologies の AX ノードのみがサポートされています。Storage Space Direct Ready Nodes は、HCI クラスタの拡張ではサポートされていません。

- 対称クラスタでは、新しいノードとクラスタ ノードは同じモデルである必要があります。
- 新しいノードにインストールされているオペレーティング システムがサポートされ、クラスタ ノードと同じである必要があります。

以下は、高レベルの互換性の説明です。

- 非準拠: 選択されたノードはいずれも Dell EMC の推奨事項に準拠していません。
- 一部準拠: 選択されたノードのいくつかは Dell EMC の推奨事項に準拠しています。準拠ノードに対してのみ [ライセンスの可用性] チェックを続行することができます。
- 準拠: 選択されたすべてのノードは Dell EMC の推奨事項に準拠しており、すべての準拠ノードの [ライセンスの可用性] チェックを続行することができます。

高レベルの互換性が「非準拠」または「一部準拠」である場合は、[詳細の表示] をクリックして、ノードと、コンプライアンス違反のタイプについて詳しく知ることができます。

- c. 新しいノードとクラスタ ノードに「OMIWAC Premium License for MSFT HCI Solutions」がインストールされているかどうかを確認するには、[ライセンス可用性] の [チェック] をクリックします。

[HCI 構成プロファイル] のチェックに進む前に、新しいノードとクラスタ ノードに OMIWAC Premium License がインストールされていることを確認します。

- d. [HCI 構成プロファイル] の [チェック] をクリックして、Dell EMC からの対称的な推奨事項に基づいて、新しいノードとクラスタ ノードを検証します。インターネット接続が使用できない場合は、「[トラブルシューティング](#)」の項を参照して、HCI 構成プロファイルのチェックをオフライン モードで実行します。

ノードのいずれにも互換性がない場合は、[詳細の表示] をクリックすると、ノードに関する詳細情報が表示され、非準拠の理由および推奨事項が表示されます。HCI 構成プロファイルのルールの詳細については、「[HCI 構成プロファイル](#)、p. 30」を参照してください。

メモ: 必要な構成のいずれかが「Critical」エラーで失敗した場合、HCI 構成プロファイルは失敗します。問題を解決するための推奨事項と詳細を確認して HCI 構成プロファイルを実現し、次の手順に進みます。

構成が「Warning」で失敗した場合、その構成はクラスタの導入には対応していますが、クラスタのパフォーマンスが準最適なレベルになる可能性があります。したがって、確認する必要があります。

次の手順に進む前に、すべてのノードの HCI 構成が Dell EMC の推奨事項に従っていることを確認します。

5. 高レベルの互換性チェック、ライセンス チェック、HCI 構成プロファイルのチェックを正常に完了した後、[次: コンプライアンスのアップデート] をクリックして、新しいノードとクラスタ ノードのファームウェア、BIOS、ドライバの準拠を確認します。「クラスタ拡張」フローを使用すると、新しいノードに対してファームウェア、BIOS、ドライバをアップデートすることのみができます。新しいノードとクラスタ ノードの両方のコンプライアンス レポートを生成するには、次の手順を実行します。

- a. カタログ ファイルをダウンロードするいずれかの方法を選択します。

- [オンライン] カタログを使用して、dell.com から PowerEdge サーバーのカタログを自動的にダウンロードします。オンライン カタログは、デフォルトで選択されています。
- [オフライン] カタログ: CIFS の場所に構成された DRM カタログを使用します。

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。インターネットを使用できない場合、またはカスタマイズされた DRM カタログを使用する場合は、このオプションを使用できます。インターネットが使用できない場合は、オフライン カタログを使用する前に、[設定] ページに、[DSU および IC 設定が構成されている](#)ことを確認します。

- オフライン カタログを使用するには、[DRM 設定] を選択して、Microsoft HCI ソリューションの DRM カタログとともに CIFS 共有パスが設定されていることを確認します。DRM カタログを作成するには、[技術に関する記事](#)を参照してください。

終了したら、[コンプライアンスのチェック]をクリックします。

6. [コンプライアンス結果] セクションでは、クラスター ノードと新しいノードのコンプライアンス レポートが表示されます。[詳細の表示] をクリックしてコンプライアンス レポートを表示するか、[エクスポート] をクリックして CSV 形式でレポートをエクスポートします。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](#)、p. 25 を参照してください。
- クラスター ノードが非準拠になっている場合は、クラスター内の新しいノードを追加する前に、クラスター ノードが準拠していることを確認します。クラスター ノードをアップデートするには、ウィザードを終了し、クラスター対応アップデート方法を使用してクラスター アップデートの [アップデート] タブに移動します。
 - 新しいノードが非準拠になっている場合は、[コンプライアンス結果] の [詳細の表示] をクリックして非準拠コンポーネントを検証し、[完了] をクリックして新しいノードをアップデートして、クラスター拡張の準備ができた状態にします。アップデートのステータスを表示するには、[アップデート進行中 - 表示] をクリックします。
 - 新しいノードが準拠している場合は、[サマリー] の [詳細の表示] をクリックして、クラスター拡張の準備が完了しているノードのリストを表示し、[終了] をクリックします。

次の手順

新しいノードとクラスター ノードの両方がアップデートされた後、Windows 管理センターのワークフローに移動して、既存のクラスターに新しいノードを追加します。

-  **メモ:** クラスターにノードを追加する前に、クラスター ノードと同じ新しいノードにホスト OS ネットワークを構成するようにしてください。ホスト OS ネットワークの構成に関する詳細については、『[Azure Stack HCI 用 Dell EMC ソリューションの拡張性のあるアーキテクチャ](#)』を参照してください。

フェールオーバー クラスター拡張のためのノードの準備

前提条件

- クラスター ノードおよび新しいノードに、[OMIWAC Premium License for PowerEdge] がインストールされていることを確認します。
 - SAS RAID_Driver の新しいノードについては、次のことを確認します。
 - 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。

クラスター拡張のためのノードを準備する前に、次を計画します。

- 新しいノードをラックに設置し、適切にケーブル接続します。
- 新しいノードに、既存のクラスター ノードと同じオペレーティング システムがインストールされていることを確認します。
- Windows 管理センターからノードを接続し、ユーザー名、ドメインなどの基本設定を構成します。
- 新しいノードがクラスター ノードと同じドメインにあり、ドメイン管理者がアクセスできることを確認します。

手順

クラスター拡張用にノードを準備するには、次の手順を実行します。

1. Windows 管理センターを使用してクラスターに接続し、OpenManage Integration の拡張機能を起動します。
2. [設定] タブに移動し、左側の [クラスターの拡張] をクリックします。
3. [クラスターの拡張] ウィンドウで、[ノードの追加] をクリックします。
4. [クラスターの拡張] ウィンドウの [互換性のあるノードの選択] で、ノードのリストが表示されます。リストは、Windows 管理センターの [Server Manager] ページで使用可能なすべてのノードを取得します。
 - a. クラスターに追加するノードを選択します。検索ボックスを使用して任意のノードを検索するか、[すべて選択] チェックボックスをクリックしてすべてのノードを選択することもできます。新しいノードがクラスターに含まれていないことを確認します。

 **メモ:** クラスターでサポートされているノードの合計数は 16 です。たとえば、既存の 2 つのノードを持つクラスターでは、クラスターの拡張用に最大 14 個のノードを選択できます。
 - b. ノードを選択した後、[推奨事項] の [チェック]、[詳細の表示] の順にクリックして、クラスターの拡張に推奨されるノードと推奨されないノードを確認します。推奨事項のチェックの詳細については、[推奨事項の表示チェック](#)、p. 42 を参照してください。

- c. [ライセンスの可用性] の [チェック] をクリックして、新しいノードとクラスター ノードに「OMIWAC Premium License for PowerEdge」がインストールされているかどうかを確認します。

アップデート コンプライアンスに移行する前に、推奨事項チェックから検討される新しいノードとクラスター ノードに OMIWAC プレミアム ライセンスがインストール済みであることを確認します。

5. 推奨事項およびライセンスの可用性のチェックが正常に完了したら、[次へ：コンプライアンスのアップデート] をクリックして、新しいノードとクラスター ノードのファームウェア、BIOS、およびドライバー コンプライアンスを確認します。「クラスターの拡張」を使用して、新しいノードのみのファームウェア、BIOS、ドライバー、システム管理アプリケーションをアップデートすることができます。新しいノードとクラスター ノードの両方のコンプライアンス レポートを生成するには、次の手順を実行します。

- a. カタログ ファイルをダウンロードするいずれかの方法を選択します。

- [オンライン エンタープライズ] カタログ：PowerEdge サーバーのカタログを dell.com から自動的にダウンロードします。オンライン カタログは、デフォルトで選択されています。
- [オンライン - MX] カタログ：PowerEdge MX モジュラー用の検証済みバージョンのコンポーネントが含まれています。

オンライン カタログのサポートには、Windows Admin Center ゲートウェイから直接インターネット接続が必要です。カタログの全体的なダウンロード時間は、ネットワーク帯域幅とアップデート対象のコンポーネントの数によって異なります。

 **メモ:** プロキシ設定を使用したインターネットへのアクセスはサポートされていません。

- [オフライン] カタログ：CIFS の場所に構成された DRM カタログを使用します。

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。インターネットを使用できない場合、またはカスタマイズされた DRM カタログを使用する場合は、このオプションを使用できます。インターネットが使用できない場合は、オフライン カタログを使用する前に、[設定] ページに、[DSU および IS 設定が構成されている](#)ことを確認します。

- オフライン カタログを使用するには、[DRM 設定] を選択して、DRM カタログとともに CIFS 共有パスが設定されていることを確認します。DRM カタログを作成するには、[技術に関する記事](#)を参照してください。

終了したら、[コンプライアンスのチェック] をクリックします。

- b. [コンプライアンスの結果] には、クラスター ノードと新しいノードのコンプライアンスのサマリーが表示されます。[詳細の表示] をクリックしてコンプライアンス レポートを表示するか、[エクスポート] をクリックして CSV 形式でレポートをエクスポートします。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](#)、p. 25 を参照してください。

- クラスター ノードが非準拠である場合は、クラスター内に新しいノードを追加する前に、クラスター ノードが準拠しているようにしてください。クラスター ノードをアップデートするには、ウィザードを終了し、クラスター対応アップデート方法を使用してクラスター アップデートの [アップデート] タブに移動します。
- 新しいノードが非準拠である場合は、[コンプライアンス結果] の [詳細の表示] をクリックして非準拠コンポーネントを確認し、[完了] をクリックして新しいノード コンポーネントをアップデートして、クラスター拡張の準備ができた状態にします。アップデート ステータスを表示するには、[アップデート進行中 - 詳細の表示] をクリックします。
- クラスター ノードと新しいノードの両方が準拠している場合は、[終了] をクリックして、Microsoft 推奨の手順に従ってクラスターにノードを追加します。

次の手順

新しいノードとクラスター ノードの両方がアップデートされた後、Windows 管理センターのワークフローに移動して、既存のクラスターに新しいノードを追加します。

 **メモ:** クラスターにノードを追加する前に、クラスター ノードと同じ新しいノードにホスト OS ネットワークを構成するようにしてください。

推奨事項の表示チェック

推奨事項の全体のステータスは、個々のノードのステータスを統合したビューです。[詳細の表示] をクリックすると、各ノードの推奨事項が表示されます。次の表は、推奨事項の全体のステータスと個々のノードのステータスの詳細を示しています。

推奨事項の全体のステータス	個々のノードのステータス	ライセンスのチェックに進むことができる	備考
---------------	--------------	---------------------	----

推奨 ()	選択されたすべてのノードは Dell EMC の推奨事項に準拠しています。	はい。	すべての準拠ノードがライセンス チェックの対象です。
一部準拠 ()	一部のノードは準拠していますが、そうでない場合は非推奨または非対応です。	はい。	準拠しているが非推奨のノードは、ライセンス チェックの対象となります。ただし、クラスターの拡張に推奨されないノードを使用すると、クラスターのパフォーマンスが準最適なレベルになる可能性があります。 非対応ノードは、ライセンス チェックの対象外です。
非推奨 ()	ノードは非推奨ですが、クラスター拡張でサポートされています。	はい。	非推奨ノードはライセンス チェックの対象となります。ただし、クラスターの拡張に推奨されないノードを使用すると、クラスターのパフォーマンスが準最適なレベルになる可能性があります。
非対応 ()	選択されたすべてのノードが非対応になっています。	番号	非対応ノードは、ライセンス チェックの対象外です。

ノードは、次のチェック項目に基づいて推奨されます。

- 新しいノードとクラスター ノードの両方が Dell Technologies 製である必要があります。
- 新しいノードとクラスター ノードは、対称型クラスターの同じモデルである必要があります。混合型クラスターの場合、新しいノードは、既存のクラスター ノードの任意のモデルにすることができます。
- 新しいノードにインストールされたオペレーティング システムは、クラスター ノード (メジャー OS バージョン) と同じである必要があります。フェールオーバー クラスターの拡張は、OS バージョン Windows Server 2016 および 2019 を使用しているノードでサポートされています。

トラブルシューティングとよくある質問 (FAQ)

トピック：

- アップグレード
- ライセンス
- ログ
- 正常性、ハードウェア、iDRAC インベントリ
- 点滅および点滅解除
- クラスター対応アップデート
- フルスタック クラスター対応アップデート
- CPU コアの管理
- クラスターの拡張
- その他

アップグレード

拡張機能のインストールに失敗する

Azure Stack HCI クラスターの作成またはアップデート時に OpenManage Integration スナップインをインストールしようとする、拡張機能のインストールが失敗する場合があります。

原因：旧バージョンの拡張機能 (OMIMSWAC 1.1.1 以前) がインストールされている可能性があります。

解決策：

- 古いバージョンをアンインストールしてから、Azure Stack HCI クラスターの作成またはアップデート時に、OpenManage Integration スナップインをインストールします。OMIMSWAC のインストール ガイドの「*Dell EMC OpenManage Integration with Microsoft Windows Admin Center のインストール*」セクションを参照してください。
- 以前のバージョンから OpenManage Integration スナップインにアップグレードするには、[拡張機能] > [インストールされた拡張] タブに移動します。ステータスに [利用可能なアップデートがあります (バージョン)] と表示されている Dell EMC OpenManage Integration 拡張機能を選択し、[アップデート] をクリックします。

ローカル フィードを使用して拡張機能をインストールできないのはなぜですか。

ローカル フィードを使用した拡張機能のインストールは、次のエラーで失敗する可能性があります。

```
Couldn't install the extension: 'Dell EMC OpenManage Integration'. Error: Extension dell-emc.openmanage-integration <Version> was not available from any extension feed.
```

ファイル名が `dell-emc.openmanage-integration.<バージョン>.nupkg` に拡張子「OMIMSWAC」がついたものであることを確認してください。デフォルトのファイル名が変更されている場合、インストールは失敗します。

拡張機能をインストールできないのはなぜですか。

拡張機能のインストールは、次のエラーで失敗する可能性があります。

```
Couldn't install the extension: 'Dell EMC OpenManage Integration'. Error: Extension dell-emc.openmanage-integration <Version> was not available from any extension feed.
```

拡張機能をインストールする前に、次のことを確認してください。

- 拡張機能がサポート対象の WAC バージョンにインストールされている。サポート対象の WAC バージョンの詳細については、「互換性マトリックス」を参照してください。
- CredSSP が無効になっている。

拡張機能をインストールするための前提条件の詳細については、『OMIMSWAC インストールガイド』を参照してください。

ライセンス

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 ノードの電源がオンであるが、再起動の状態でない。また、ターゲット ノードの再起動が保留されていない。
- 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。

ログ

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の場合： Inventory<ID*>
- アップデート コンプライアンスの場合： FirmwareCompliance<ID*>
- アップデート通知の場合： 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。

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

正常性、ハードウェア、iDRAC インベントリ

インベントリ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。
- USB NIC アダプターが、ターゲット ノードのオペレーティング システムで無効になっていないこと。

iDRAC から正常性およびハードウェア インベントリを取得できない

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

- PowerEdge サーバーの YX3X モデルと YX2X モデルが、2.60.60.60 以降の最新の iDRAC バージョンでアップデートされていること。
- PowerEdge サーバーの YX4X モデルが、3.30.30.30 以降の最新の iDRAC バージョンでアップデートされていること。
- 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。

- クラスタを管理するには、OMIMSWAC でクラスタを管理する前に、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 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。

PowerEdge サーバーの YX2X、YX3X、および YX4X モデルの正常性とハードウェア インベントリが表示されない

- PowerEdge サーバーの YX3X および YX2X モデルが、2.60.60.60 以降の最新の iDRAC バージョンでアップデートされていることを確認します。
- PowerEdge サーバーの YX4X モデルが、3.30.30.30 以降の最新の iDRAC バージョンでアップデートされていることを確認します。

ノード コンポーネントの正常性状態は正常と示されるが、全体的な正常性状態が警告または重大と表示される

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場合でも、PowerEdge サーバー、フェールオーバー クラスター、および HCI クラスターの全体的な正常性状態が重大または警告と表示されることがあります。内蔵 SATA コントローラーに接続されている物理ディスクの正常性状態は、iDRAC がこれらのディスクの正常性情報を取得できないため、[不明] と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。

ターゲット iDRAC デバイスでユーザーを作成できない

PowerEdge サーバーの YX4X モデル以降でロックダウン モードが有効になっている場合、正常性、ハードウェア、および iDRAC のインベントリは、「ターゲット iDRAC デバイスでユーザーを作成できません」というエラーで失敗します。

対応処置 : Dell EMC OpenManage Integration によって管理されるターゲット ノード上のロックダウン モードを無効にします。

OMIMSWAC 拡張機能を初期化できない

サーバー ノードおよびクラスター ノードからインベントリを取得すると、「OMIMSWAC 拡張機能を初期化できません」というエラーで失敗することがあります。

対応処置 : IPMI ドライバーがインストールされており、ターゲット ノードで IPMI サービスが実行されていることを確認します。要件およびソリューションの詳細については、[Dell の情報センター](#)を参照してください。

インベントリの詳細情報が表示されないのはなぜですか。

インベントリの詳細情報が読み込まれていない場合は、次のことを確認してください。

- 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。
- USB NIC アダプターが、ターゲット ノードのオペレーティング システムで無効になっていないこと。
- Windows 管理センターで 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。
- PS-Remoting が有効になっている。
- 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。
- Lifecycle Controller がターゲット ノードで使用可能である。
- 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。
- IPMI ドライバーがターゲット ノードに存在し、IPMI サービスが実行されている。
- USB パススルーで IP アドレスが競合していない。
- CA および CN が、ターゲット ノードの iDRAC で無効になっている。

いくつかのクラスター ノードのインベントリーの詳細情報が表示されないのはなぜですか。

OMIMSWAC 拡張機能を使用して Storage Spaces Direct クラスターを監視している間、一部のサーバーのインベントリーおよび正常性データが読み込まれない場合があります。この場合、iDRAC をリセットし、インベントリー/正常性データを再実行します。

新しいブラウザー セッションで拡張機能を開いたときに、インベントリーの詳細情報が表示されないのはなぜですか。

認証情報は、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。新しいブラウザー セッションを開いた場合は、[manage as] を選択し、プロンプトが表示されたら管理者の認証情報を提供して、クラスター/ターゲット ノードに再接続するようにしてください。

いくつかのコンポーネントの正常性とインベントリーのステータスが [unknown] と表示されるのはなぜですか。

組み込み 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正常性とインベントリーのステータスは、iDRAC がこれらのディスクの正常性とインベントリー情報を取得できないために [unknown] と表示されます。

点滅および点滅解除

点滅または点滅解除操作のディスクを完了または選択できない

- **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実行します。
- 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。

クラスター対応アップデート

アップデート コンプライアンス操作に必要なコンポーネントのダウンロード中にジョブが失敗する

DSU ツールおよび IC ツールのダウンロード中に、さまざまな理由によりアップデート ジョブが失敗する場合があります。考えられる原因と解決策を以下に示します。

- **原因**：Dell EMC Repository Manager (DRM) を使用してリポジトリ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。

DUP をダウンロードできない

ドメイン認証情報を使用してローカルに Windows 管理センター (WAC) にアクセスすると、ターゲットノードまたはクラスターのアップデート中に DUP をダウンロードできない場合があります。

対応処置：次のことを確認します。

- ドメイン管理者の認証情報を使用して、リモートで Microsoft Windows 管理センターにログインします。ゲートウェイ管理者としての認証情報であることを確認します。詳細については、[Microsoft のマニュアル](#)を参照してください。
- インターネット接続またはプロキシ設定を確認します。

コンプライアンスレポートを生成できない

- **原因**：[管理に使用する認証情報] 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、[管理に使用する認証情報] 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認証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 ノードに認証情報を接続します。
- 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。

- **原因** : コンプライアンス レポートの生成が次のエラーによって失敗した可能性があります: Unable to install Dell System Update(DSU) package for the server/cluster because DSU installation operation is already in progress for another server/cluster. これは、1人のユーザーが2つの異なるインスタンス/セッションから同時にコンプライアンスを実行しようとしたために発生した可能性があります。たとえば、ポップアウト ボタンをクリックするという1つのインスタンスと、同じゲートウェイから同時にブラウザーを使用するという別のインスタンスです。最初にトリガーされたインスタンス/セッションの1つはコンプライアンス/アップデートを実行する処理を開始し、一方で別のインスタンスはエラーになります。

対応処置 : 1つのゲートウェイ インスタンスを使用して、一度に1つのターゲット ノード/クラスターに対して1つのコンプライアンス/アップデートのみを実行します。

コンプライアンス レポート ページでロード中の状態が続く

コンプライアンス レポートを生成している間に、アップデート コンプライアンス レポートが正常に生成されたことを通知した後も、コンプライアンス レポート ページがロード中の状態が表示されることがあります。

この場合、[設定]、[インベントリー] などの他のタブに移動してから、[アップデート] タブに戻り、生成されたコンプライアンス レポートを表示します。

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する

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、さまざまな理由で失敗する場合があります。原因と対応処置を以下に示します。

- **原因** : CAU をトリガーする前にターゲット ノードが検証されない場合、CAU が失敗することがあります。

対応処置 : クラスター対応アップデートでは、CAU をトリガーする前にクラスターを検証するようにしてください。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** : フェールオーバー クラスターリング機能およびフェールオーバー クラスターリング ツールがターゲット ノードにインストールされていない場合、CAU が失敗する場合があります。

対応処置 : OMIMSWAC ではクラスターのアップデートを実行するために Microsoft クラスター対応アップデート機能フレームワークを使用するため、OMIMSWAC を使用してクラスターをアップデートする前に、すべてのターゲット ノードにフェールオーバー クラスターリング機能とフェールオーバー クラスターリング ツールがインストールされていることを確認します。詳細については、[Microsoft のマニュアルで CAU の要件とベスト プラクティス](#)を参照してください。

フェールオーバー クラスターリング ツールがすべてのターゲット ノードで実行されているかどうかを確認するには、ターゲット ノードの PowerShell ウィンドウから `Get-CauClusterRole` PowerShell コマンドを実行します。

- **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 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 ノード (フェールオーバーの役割) を再開します。

- **原因** : フェールオーバー クラスタリング機能およびフェールオーバー クラスタリング ツールがすべてのターゲット ノードにインストールされていない場合、CAU は失敗します。

対応処置 : CAU を実行する前に、フェールオーバー クラスタリング機能とフェールオーバー クラスタリング ツールがすべてのターゲット ノードにインストールされていることを確認します。詳細については、<https://docs.microsoft.com/en-us/windows-server/failover-clustering/cluster-aware-updating-requirements> を参照してください。

CredSSP の障害

ゲートウェイ システムのイベント ビューアー ログを確認して、クラスタ対応アップデート中に CredSSP が失敗していないことを確認します。CredSSP が失敗する場合、考えられる原因と解決策は次のとおりです。

- **原因** : クラスタのアップデート中に、CredSSP を使用した認証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を再接続し、[すべてのサーバーにこの認証情報を使用する] チェック ボックスをクリックします。

たとえば、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認証情報を使用する] 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] > [認証情報の委任] に移動します。
3. [NTLM のみのサーバー認証での新しい認証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。

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、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。
- クラスターのアップデート後、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。これは、DUP の障害が原因で発生します。

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動作条件がある場合は、動作条件を満たしてからアップデートを再実行します。

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 に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。

フル スタック クラスター対応アップデート

クラスター対応アップデートを設定できない

原因：フル スタック アップデートを実行するために、Windows Admin Center の [ツール] メニューから [アップデート] を選択すると、Couldn't configure cluster aware updates というエラーが発生することがあります。このエラーは、アップデートのために、CAU のクラスター化された役割をクラスターに追加できなかったために発生します。

対応処置：この問題を回避するには、次の PowerShell コマンドを使用してクラスターの役割を手動で追加してから、フル スタック アップデートをトリガーすることができます。Add-CauClusterRole -StartDate "02-03-2021 3:00:00 AM" -DaysOfWeek Tuesday -WeeksOfMonth 3 -EnableFirewallRules -RequireAllNodesOnline -Force

詳細については、Microsoft のマニュアルの「[リモート管理のノードの構成](#)」を参照してください。

クラスター対応アップデートの準備状況をクエリーできない

原因：フル スタック アップデートを実行するために、Windows Admin Center の [ツール] メニューから [アップデート] を選択すると、Couldn't query readiness for cluster aware updates というエラーが発生することがあります。このエラーは、CredSSP の障害が原因で発生します。

対応処置：この問題を回避するには、「[CredSSP の障害](#)」を参照して原因と解決策を確認してください。

詳細については、[Microsoft のマニュアル](#)を参照してください。

[テスト サマリー] ページが表示される

フルスタック アップデートのトリガー中、[テスト サマリー] ページが表示される場合があります。

対応処置：この問題を回避するには、アップデート前またはアップデート後のスクリプトがクラスターの役割に含まれているかどうかを確認します。含まれている場合は、PowerShell で `Set-CauClusterRole -PreUpdateScript $null -PostUpdateScript $null` コマンドを実行して、クラスター ノードからスクリプトを削除します。クラスターのアップデートに必要な前提条件の詳細については、[Microsoft のマニュアル](#)を参照してください。

アップデート ステータスの表示更新に時間がかかる

フルスタックのクラスター アップデート中に、[アップデート] ページに表示されるアップデート ステータスの表示の更新に時間がかかる場合があります。この場合は、[アップデート] ページを表示したまま、アップデートが完了するまで待機することをお勧めします。アップデートが完了すると、アップデート ステータスが自動的に表示されます。Microsoft の推奨事項の詳細については、[Microsoft のマニュアル](#)を参照してください。

Failover Cluster Tool Extension 1.271.0 nupkg でフルスタック アップデートが失敗することがある

Azure Stack HCI クラスターでのフルスタック クラスター アップデート中に、次の例外エラーでアップデートが失敗する場合があります。RemoteException: Exception calling "Add" with "2" argument(s): "Item has already been added.Key in dictionary: 'PreUpdateScript' Key being added: 'PreUpdateScript'". この問題は、Microsoft Failover Cluster Tool Extension 1.271.0 がインストールされている場合に発生します。この問題により、ハードウェアと OS 両方のクラスター対応アップデート (フルスタック アップデート) を同時に実行することはできません。

対応処置：最新の Microsoft フェールオーバー クラスター ツール拡張機能を使用して、OMIMSWAC を使用したフルスタック アップデートを実行します。

CPU コアの管理

CPU コア構成のアップデート中にジョブが失敗しました

CPU コア構成の変更は、さまざまな理由によって適用できない場合があります。原因と対応処置を以下に示します。

- **原因**：CPU コアの変更を適用する前に Microsoft の推奨事項に従ってクラスターが検証されない場合、CPU コアの変更のアップデートが失敗する可能性があります。
対応処置：CPU コアの構成をアップデートする前に、クラスターの妥当性検査を行ってください。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**：フェールオーバー クラスタリング機能およびフェールオーバー クラスタリング ツールがターゲット ノードにインストールされていない場合、CPU コアの構成をアップデートできない場合があります。
対応処置：OMIMSWAC ではクラスターのアップデートを実行するために Microsoft クラスター対応アップデート機能フレームワークを使用するため、OMIMSWAC を使用してクラスターをアップデートする前に、すべてのターゲット ノードにフェールオーバー クラスタリング機能とフェールオーバー クラスタリング ツールがインストールされていることを確認します。詳細については、[Microsoft のマニュアル](#)で [CAU の要件とベスト プラクティス](#)を参照してください。
フェールオーバー クラスタリング ツールがすべてのターゲット ノードで実行されているかどうかを確認するには、ターゲット ノードの PowerShell ウィンドウから `Get-CauClusterRole` PowerShell コマンドを実行します。
- **原因**：CPU コアのアップデートがクラスターに適用された後、いずれかのディスクが正常に稼働していないと、ノードを再起動できない場合があります。
対応処置：CPU コアの構成をアップデートする前に、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、CPU コアのアップデートは失敗します。
対応処置：CPU コアの構成をアップデートする前に、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。

- **原因**：CPU コアの変更を適用するときに、クラスター ノードのいずれかが強制的にあるいは間違っ

CredSSP の障害

ゲートウェイ システムのイベント ビューアー ログを確認して、CPU コア構成のアップデート中に CredSSP が失敗していないことを確認します。CredSSP が失敗する場合、考えられる原因と解決策は次のとおりです。

- **原因**：CPU コアのアップデート中に、CredSSP を使用した認証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認証情報を使用する] チェック ボックスをクリックします。
- たとえば、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認証情報を使用する] 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] > [認証情報の委任] に移動します。
 3. [NTLM のみのサーバー認証での新しい認証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。

CPU コアの変更を適用できませんでした

CPU コアの変更時に、CPU コアの変更ステータスの適用は、個別のノードでエラーとして表示されることがあります。

- OMIMSWAC はノードに接続できません。
- CPU コア アップデート セッションは切断されています。
- ノードの再起動がスタックしています。

フェールオーバー クラスター内の CPU コア構成をアップデートすることはできますか。

いいえ、フェールオーバー クラスターでの CPU コア構成のアップデートはサポートされていません。Azure Stack HCI クラスターおよび Windows Server ベースの HCI クラスターのみがサポート対象です。

個別のノード内の CPU コア構成をアップデートすることはできますか。

はい、個別のノード内の CPU コア構成はアップデートすることができます。ただし、ノードが Azure Stack HCI クラスターまたは Windows Server ベースの HCI クラスターの一部ではないようにする必要があります。フェールオーバー クラスターのノード部分は、個別の CPU コア構成のアップデートに対してサポートされています。

- メモ**：最適なパフォーマンスを実現するために、Dell EMC はすべてのクラスター ノードでハードウェア構成を同じに維持することを強く推奨します。フェールオーバー クラスター内の 1 つのノードで CPU コア構成をアップデートする場合は、クラスター内のすべてのノードで同じ構成を維持するようにしてください。

CPU コア構成をアップデートするには、ライセンスがインストールされている必要がありますか。

はい、CPU コア構成をアップデートするには、OMIWAC Premium License for MFHCI Solutions が各クラスター ノードにインストールされている必要があります。個別のノードについては、個別の CPU コア アップデートのために OMIWAC Premium License をインストールする必要があります。ライセンスの詳細については、『OMIMSWAC インストール ガイド』の「ライセンス」セクションを参照してください。

クラスタの拡張

指定されたサポート マトリックスの詳細で署名を検証できませんでした

(オプション) インターネットに接続できない場合は、次の手順を実行して、HCI 構成プロファイルのチェックをオフライン モードで実行します。

1. <http://downloads.dell.com/omimswac/supportmatrix/> から *asHCISolutionSupportMatrix.json* および *asHCISolutionSupportMatrix.json.sign* ファイルをダウンロードします。
2. これらのファイルを、Windows Admin Center がインストールされているゲートウェイ システムの C:\Users\Dell\SymmetryCheck フォルダに配置します。
3. Windows 管理者センターのクラスタ接続ホームページに移動し、クラスタに接続してから、もう一度 Dell EMC 拡張機能を起動します。
4. OpenManage Integration で、[構成] タブに移動し、左側の [クラスタの拡張] をクリックします。

クラスタ拡張のためのノードの準備中にノードをアップデートできません

クラスタ拡張のためのノードの準備中に SAS-RAID_Driver のためにノードのアップデートが失敗した場合は、次の構成が設定されている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。

その他

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。

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、クラスタの作成準備状況またはクラスタ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 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 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 マネージャーのクラスタ 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できないときに発生し、このため、これらの NIC でクラスタの通信が中断されます。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 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通信を無効にします。

次に対する同意の保存に失敗します : Dell EMC ソフトウェア ライセンス 契約およびカスタマー通知

原因 : Dell EMC ソフトウェア ライセンス契約およびカスタマー通知への同意を保存できない場合があります。これは、同じゲートウェイから Dell EMC OpenManage Integration 拡張機能の複数のインスタンスを起動し、1つのインスタンスで契約条件に同意した場合に発生することがあります。残りのインスタンスで契約条件に同意しようとすると、このエラーが発生します。

対応処置 : この問題が発生している Dell EMC OpenManage Integration 拡張機能から移動し、再度戻ってこの問題を解決します。

OMIMSWAC にログインするには、シングル サインオンまたはスマートカード認証を使用できますか。

OMIMSWAC へのログインにシングル サインオンまたはスマートカード認証を使用することはできません。クラスター/サーバーに接続するには、「manage as」を使用して、ドメインまたはゲートウェイ管理者の認証情報を入力します。

リモート接続を使用して OMI 拡張機能にアクセスできないのはなぜですか。

ゲートウェイ管理者権限がない場合は、OMIMSWAC にアクセスできません。リモート ワークステーションからのゲートウェイ管理者認証情報を使用して、ブラウザーを起動し、ゲートウェイ システムに接続することができます。

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 プロセッサ搭載第 14 世代サーバーの中の、ラック型、プロセッサ 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

Dell EMC へのお問い合わせ

このタスクについて

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。

手順

1. [Dell.com/support](https://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。

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 拡張機能 (OpenManage Integration 拡張機能とも呼ばれます)	Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) により IT 管理者は、ホスト、Microsoft Failover Clusters (PowerEdge サーバーで作成)、Dell EMC HCI Solutions for Microsoft Windows Server (AX ノード、Storage Spaces Direct Ready Node、またはその両方を使用して作成)、Dell EMC Integrated System for Microsoft Azure Stack HCI (AX ノードを使用して作成) として PowerEdge サーバーを管理できます。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。
OpenManage Integration スナップイン	OpenManage Integration スナップインは、Windows Admin Center クラスター作成またはクラスター アップデート ワークフローに統合されており、クラスターの作成とアップデートの操作性を向上させ、クラスターの作成時に必要な再起動の回数を削減します。 OpenManage Integration スナップインをインストールすると、Windows Admin Center の [ツール] メニューに OpenManage Integration 拡張機能が表示されます。OpenManage Integration 拡張機能のすべての機能は、スナップイン固有の機能とともに使用することができます。
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。

表 4. 用語集（続き）

略語/頭字語	定義
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 Inventory Collector)	Inventory Collector は、ターゲット システムのインベントリを実行し、結果をリポジトリ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
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) - Microsoft HCI ソリューションのアップデート カタログ	Windows Server (AX ノードと Storage Spaces Direct Ready Node のいずれかまたは両方を使用して作成) および Azure Stack HCI クラスタ (AX ノードを使用して作成) に推奨されます。
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

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) - Microsoft HCI ソリューションのアップデート 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)