

Dell EMC OpenManage Integration Version 2.1 with Microsoft Windows Admin Center

User's Guide

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Chapter 1: Overview of OpenManage Integration with Microsoft Windows Admin Center.....	5
Additional resources.....	6
Chapter 2: Getting started with OpenManage Integration with Microsoft Windows Admin Center.....	8
Chapter 3: Ports required by Dell EMC OpenManage Integration with Microsoft Windows Admin Center.....	10
Chapter 4: Manage Dell EMC PowerEdge Servers.....	11
Health status—Supported target node components.....	12
Hardware inventory—Supported target node components.....	12
Chapter 5: Manage Failover clusters, Azure Stack HCI, and Windows Server HCI clusters.....	14
Health status—Supported target node components in Failover Clusters, Windows Server HCI, and Azure Stack HCI.....	15
Hardware inventory—Supported target node components in Failover Clusters, Windows Server HCI, and Azure Stack HCI.....	16
Chapter 6: View iDRAC details of the PowerEdge servers and nodes of HCI and Failover clusters.....	18
Chapter 7: Update PowerEdge servers and nodes of Windows Server HCI, Azure Stack HCI, and Failover clusters using OpenManage Integration extension.....	19
Configure DSU and IC settings in Update Tools.....	20
Configure proxy settings.....	20
Update target nodes using OpenManage Integration extension.....	21
Update nodes of Windows Server HCI, Azure Stack HCI, and Failover clusters using OpenManage Integration extension.....	23
View compliance report.....	25
Chapter 8: Integrated deploy and update of Azure Stack HCI clusters.....	27
Integrated deploy and update an Azure Stack HCI cluster using OpenManage Integration snap-in.....	27
HCI configuration profile.....	30
Chapter 9: Full Stack Cluster-Aware Updating for Azure Stack HCI clusters using OpenManage Integration snap-in.....	34
Update an Azure Stack HCI cluster using OpenManage Integration snap-in.....	34
Chapter 10: Manage CPU cores in clusters or individual nodes.....	37
Chapter 11: Add nodes to existing clusters.....	39
Prepare nodes for Windows Server HCI and Azure Stack HCI cluster expansion.....	39
Prepare nodes for Failover cluster expansion.....	41

View Recommendations check.....	42
Chapter 12: Troubleshooting and Frequently asked questions	44
Upgrading.....	44
Licensing.....	45
Logs.....	45
Health, hardware, and iDRAC inventory.....	46
Blink and Unblink.....	48
Cluster-Aware Updating.....	48
Full Stack Cluster-Aware Updating.....	52
Manage CPU core.....	53
Cluster Expansion.....	54
Others.....	54
Chapter 13: Identifying the generation of your Dell EMC PowerEdge server	56
Chapter 14: Contacting Dell EMC.....	57
Appendix A: Glossary.....	58
Appendix B: Appendix.....	60

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 below YX5X PowerEdge servers.
 - R450, R550, R650, R650xs, R750xs, R750, R750XA, XR11, XR12, C6520, MX750c, and XE8545.
- Supports below AX nodes.
 - AX-650 and AX-750
- 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.

Revision history

Date	Document revision	Description of changes
July 2021	A00	Initial release for OMIMSWAC 2.1.
August 2021	A01	Added support for R450, R550, R650xs, R750xs, XR11, XR12 PowerEdge servers.
September 2021	A02	Added support for AX-650 and AX-750

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.

Topics:

- [Additional resources](#)

Additional resources

Table 1. Additional resources

Document	Description	Availability
<i>Dell EMC OpenManage Integration with Microsoft Windows Admin Center Installation Guide</i>	Provides information about installing and configuring OpenManage Integration with Microsoft Windows Admin Center.	<ol style="list-style-type: none"> 1. Go to Dell.com/OpenManageManuals. 2. Select OpenManage Integration with Microsoft Windows Admin Center. 3. Click DOCUMENTATION > MANUALS AND DOCUMENTS to access these documents.
<i>Dell EMC OpenManage Integration with Microsoft Windows Admin Center Release Notes</i>	Provides information about new features, known issues and workarounds in OpenManage Integration with Microsoft Windows Admin Center.	
<i>Dell EMC Infrastructure Compliance Report for PowerEdge Servers and</i>	This white paper describes the process to generate update compliance report for PowerEdge servers, Microsoft Azure Stack	

Table 1. Additional resources (continued)

Document	Description	Availability
<i>Azure Stack HCI Clusters using the OMIMSWAC</i>	HCI clusters, and Hyper-V based failover clusters by using OMIMSWAC.	
<i>Dell EMC OpenManage Integration with Microsoft Windows Admin Center Security Configuration Guide</i>	Provides information about security features and capabilities of Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC).	
<i>Microsoft Windows Admin Center documentation</i>	For more information about using Microsoft Windows Admin Center.	https://www.microsoft.com/en-us/cloud-platform/windows-admin-center
<i>Integrated System for Azure Stack HCI</i>	For more information about Dell EMC Integrated System for Microsoft Azure Stack HCI.	https://infohub.delltechnologies.com/t/microsoft-hci-solutions-from-dell-technologies-1/

Getting started with OpenManage Integration with Microsoft Windows Admin Center

Before you launch Dell EMC OpenManage Integration extension in Windows Admin Center, ensure that you have:

- Logged in to Windows Admin Center as a gateway administrator.

After installing the OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC), perform the following actions to launch the extension:

1. In the upper left corner of the Windows Admin Center, select **Server Manager** or **Cluster Manager** from the drop-down menu.

The supported WAC version is Windows Admin Center 2103.2 GA.

2. From the list, select a server or cluster connection, and then click **Connect**.
3. Enter the server or cluster credentials.

NOTE: If "Manage as" credentials are not provided while connecting to a target node or cluster or not available to the extension, you will be prompted to specify the "Manage as" credentials inside the extension when you try to manage the target node or cluster.

NOTE: OMIMSWAC does not support single sign-on and smart card authentication methods.

4. In the left pane of the Microsoft Windows Admin Center, under **EXTENSIONS**, click **Dell EMC OpenManage Integration**.

When you launch the OpenManage Integration for the first time, a customer notice is displayed to indicate the operations performed by the OpenManage Integration such as enabling the USB NIC and creating an iDRAC user on the target node. Click **Accept** to continue to manage the PowerEdge servers by using the OpenManage Integration.

NOTE: After the information from the managed nodes is collected, the previously created iDRAC user is deleted by OMIMSWAC.

Best practices for proper functioning of OMIMSWAC

To ensure proper functioning of OpenManage Integration with Microsoft Windows Admin Center, ensure that:

- Firewall in your enterprise environment enables communication through SMB port 445.
- Redfish service is enabled on the target node.
- An iDRAC user slot is available on the target node.
- Ensure that the target node is not booted to Lifecycle Controller.
- Target node is not in the reboot state, or is powered off.
- The USB NIC adapter is not disabled on the target node OS.
- The lockdown mode is disabled on target node.
- The PowerShell execution policy is set to RemoteSigned on the system with Windows Admin Center installed and on the target node OS. For more information, see <https://www.dell.com/support/article/sln318718/dell-emc-openmanage-integration-with-microsoft-windows-admin-center-omimswac-fails-to-query-host-information>.

NOTE: For management of PowerEdge servers, OMIMSWAC uses an internal OS to iDRAC Pass-through interface. By default, iDRAC can be accessed by using the IP address 169.254.0.1/<Subnet> or 169.254.1.1/<Subnet>. However, if the host has another network interface in the same subnet (for example, when tool such as VMFleet is installed), OMIMSWAC might not be able to communicate to the iDRAC from the host OS. To resolve the conflict, log in to iDRAC and change the USB NIC IP address under the OS to iDRAC passthrough section. For more information about assigning this IP address, see the iDRAC documentation on the Dell EMC support site.

To manage:

- PowerEdge servers, see [Manage Dell EMC PowerEdge Servers](#) on page 11.
- Microsoft failover clusters created with PowerEdge servers, Dell EMC HCI Solutions for Microsoft Windows Server created with AX nodes and/or Storage Spaces Direct Ready Nodes, or Dell EMC Integrated System for Microsoft Azure Stack HCI created with AX nodes, see [Manage Failover clusters, Azure Stack HCI, and Windows Server HCI clusters](#) on page 14.

Ports required by Dell EMC OpenManage Integration with Microsoft Windows Admin Center

Table 2. Ports required by Dell EMC OpenManage Integration with Microsoft Windows Admin Center

Functionality of OpenManage Integration with Windows Admin Center	System with Windows Admin Center installed	Target node/cluster node	System where DRM catalog is available	System where DSU and IC utilities are available	iDRAC of target node/cluster node
Installation	NA	NA	NA	NA	NA
Uninstallation	NA	NA	NA	NA	NA
Health, Hardware, and iDRAC inventory	445—Outbound	445—Inbound	NA	NA	443 (Default port)
Prerequisites for OpenManage Integration snap-in and HCI Configuration Profile Checks	445—Outbound	445—Inbound	NA	NA	443 (Default port)
Update tools settings—Test connection	445—Outbound	NA	NA	445—Inbound	NA
Update compliance	NA	445—Inbound	445—Outbound	445—Outbound	NA
Update compliance notifications	445—Outbound	NA	445—Inbound	NA	NA
Target node update (Standalone node update, CPU core management, and cluster expansion) Cluster nodes update (Cluster-Aware update and CPU core management)	NA	Default WinRM ports provided by Microsoft	445—Outbound	445—Outbound	443 (Default port)

For more information about the SMB port 445, see <https://go.microsoft.com/fwlink/?linkid=2101556>.

For more information about WinRM ports, see <https://docs.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management>.

Manage Dell EMC PowerEdge Servers

You can use OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) to view and manage health, hardware inventory, update, and iDRAC of PowerEdge servers.

Prerequisites

- You have installed Windows Admin Center 2103.2 GA.
- You must be logged in to Microsoft Windows Admin Center as a Gateway Administrator.
- You must have installed the OMIMSWAC extension. For more information about the installation procedure, see the [Dell EMC OpenManage Integration with Microsoft Windows Admin Center Installation Guide](#).
- Server connections are added in Microsoft Windows Admin Center. For more information about adding server connections, see <https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center>.
- Ensure to access the Windows Admin Center remotely using domain administrator credentials. For more information, refer to [Microsoft documents](#).

NOTE: If NICs are disabled in BIOS settings, health and hardware inventory information for certain iDRAC firmware versions will be delayed. Therefore, ensure all the NICs are enabled in BIOS settings.

Steps

To manage PowerEdge servers:

1. In the upper left corner of Windows Admin Center, select **Server Manager** from the drop-down menu.
2. From the list, select a server connection, and then click **Connect**.

NOTE: If "Manage as" credentials are not provided while connecting to a target node or cluster or not available to the extension, you will be prompted to specify the "Manage as" credentials inside the extension when you try to manage the target node or cluster.
3. In the left pane of the Microsoft Windows Admin Center, under **EXTENSIONS**, click **Dell EMC OpenManage Integration**.
4. Select:
 - **Health**—to view the health status of the target node components. A status icon represents the overall health status of the target node. See [Health status—Supported target node components](#) on page 12.
 - **Inventory**—to view the detailed hardware inventory information of the target node components. See [Hardware inventory—Supported target node components](#) on page 12.
 - **iDRAC**—to view the iDRAC details of the target node. You can directly launch the iDRAC console from Windows Admin Center by using the OpenManage Integration. See [View iDRAC details of the PowerEdge servers and nodes of HCI and Failover clusters](#) on page 18.
 - **Configure**—In Compute Resources, you can view CPU core distribution summary and manage CPU core counts. See [Manage CPU cores in clusters or individual nodes](#) on page 37.
 - **Update**—to view compliance report and to update components to baseline version. See [Update PowerEdge servers and nodes of Windows Server HCI, Azure Stack HCI, and Failover clusters using OpenManage Integration extension](#) on page 19.

The health, hardware inventory, and iDRAC details are cached and will not be loaded each time the extension is loaded. To view the latest health and inventory status and iDRAC details, in the upper-right corner of the Health Status, click **Refresh**.

NOTE: For modular servers (YX2X, YX3X, YX4X, YX5X, and above models of PowerEdge servers), the following information that is related to fans and power supplies are not displayed:

- Health status
- Attribute values in the hardware inventory table

NOTE: For YX2X and YX3X models of PowerEdge servers with firmware version earlier than 2.60.60.60, information about the following components are not displayed:

- Health status—Accelerators, memory, storage controllers, storage enclosures, and physical disks.



- Hardware inventory—Accelerators, memory, storage controllers, storage enclosures, physical disks, network devices, and firmware.

Topics:

- [Health status—Supported target node components](#)
- [Hardware inventory—Supported target node components](#)


Health status—Supported target node components

Health status of the following target node components is displayed:

- CPUs
- Accelerators
 -  **NOTE:** Health status information is available for Accelerators in YX4X models of PowerEdge servers and above with iDRAC version 4.00.00.00 or newer.
- Memory
 -  **NOTE:** Intel **DIMM** memory is identified as **IntelPersistent** with an icon.
- Storage Controllers
- Storage Enclosures
- Physical Disks
- iDRAC
- Power Supplies
- Fans
- Voltages
- Temperatures

The health statuses are represented by using a doughnut chart. You can select different sections in the doughnut chart to filter the health status of the components. For example, when you select the red section, components with critical health status are only displayed.



To view the latest health status, in the upper-right corner of the **Health** tab, click **Refresh**.

-  **NOTE:** For software storage controllers and physical disks that are attached to embedded SATA controller, the health inventory status is displayed as "Unknown".

Hardware inventory—Supported target node components

You can view information about the hardware and firmware components installed on the target nodes. To do this, in Dell EMC OpenManage Integration, select **Inventory**. To view the latest hardware inventory information, in the upper-right corner of the **Inventory** tab, click **Refresh**.

The Inventory section displays the information for the following components available on the target nodes:

- System
- Firmware
 -  **NOTE:** Under Firmware inventory, for few network devices with multiple ports, since the applicable firmware version is same for all ports, only a single port with the firmware version will be displayed.
- CPUs
- Accelerators
- Memory
 -  **NOTE:** Intel **DIMM** memory is identified as **IntelPersistent** with an icon.
- Storage Controllers

To view the physical disks in a storage controller, under **Related Disks**, click the **View Disks** link. The physical disks are listed in the **Physical Disks** tab.
- Storage Enclosures

NOTE:

- Information about a few attributes of storage enclosures, firmware inventory, and memory components might not be available for:
 - YX2X and YX3X models of PowerEdge servers.
 - YX4X models of PowerEdge servers with iDRAC version lesser than 3.30.30.30.
- You may find the hardware inventory attribute for a storage enclosure empty. This is because the information may not be available on the target node iDRAC.
- For PCIe SSD Backplane of storage enclosures, few attribute values might not be available.

- Network Devices
- Physical Disks

To view the additional properties of a disk, select the disk, and then click **Advanced Properties**. To view the associated storage controller, click the storage controller link under **Advanced Properties**. The associated storage controller is displayed in the **Storage Controllers** tab. If physical disks are attached to the CPU, then the storage controller link will not be available under **Advanced Properties**.

To identify physical disks you can blink or unblink the disks LED. For more information, see [LED blink and unblink physical disks](#).

- Power Supplies
- Fans

To view iDRAC details of target node, see [View iDRAC details of the PowerEdge servers and nodes of HCI and Failover clusters](#) on page 18.

- NOTE:** Under **Inventory**, the attribute values of a few target node components are displayed as blank because the value might not be available in the target node.

To blink and unblink physical disks

Select a physical disk, click **Blink** to enable the blinking of the LEDs on the physical disk. The LEDs represent the state of physical disks. When the physical disks are blinking, it helps to locate and also to identify the faulty physical disks in your data center. To disable the blinking of the physical disks, select a disk and click **Unblink**.

- NOTE:** The blink and unblink operations are not available for:

- Disks associated to Boot Optimized Storage Subsystem (BOSS) cards.
- Devices with iDRAC firmware version less than 3.30.30.30. Update the iDRAC firmware to the latest version to enable blink and unblink operations.

NOTE:

- When the blink or unblink operation is running, **Refresh** button to load the latest health and hardware inventory information is disabled. Also, when the health and hardware inventory is being loaded in OMIMSWAC, blink and unblink operations is disabled.
- Blink or unblink operation fails on physical disks that are attached to an embedded SATA controller with an error
Blink/Unblink May not be supported with - <disk_name>.

Manage Failover clusters, Azure Stack HCI, and Windows Server HCI clusters

You can use OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) extension to view and manage health, hardware inventory, update, and iDRAC of Microsoft Failover Clusters created with PowerEdge servers, Dell EMC HCI Solutions for Microsoft Windows Server (Windows Server HCI), and Dell EMC Integrated System for Microsoft Azure Stack HCI (Azure Stack HCI).

Prerequisites

- You have installed Windows Admin Center 2103.2 GA.
- You are logged in to Microsoft Windows Admin Center as a Gateway Administrator.
- You must have installed the Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) extension. For more information about the installation procedure, see the [Dell EMC OpenManage Integration with Microsoft Windows Admin Center Installation Guide](#).
- You have added failover or hyper-converged cluster connections in Microsoft Windows Admin Center. For more information about adding failover or hyper-converged cluster connections, see <https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center>.
- Ensure that all the cluster nodes are reachable using IP address, hostname, or Fully Qualified Domain Name (FQDN) before managing the cluster with OMIMSWAC.
- Ensure to access the Windows Admin Center remotely using domain administrator credentials. For more information, refer to [Microsoft documents](#).

NOTE: If NICs are disabled in BIOS settings, health and hardware inventory information for certain iDRAC firmware versions will be delayed. Therefore, ensure all the NICs are enabled in BIOS settings.

About this task

To manage the Microsoft Failover Clusters created with PowerEdge servers, Azure Stack HCI created with AX nodes, and Windows Server HCI created with Storage Spaces Direct Ready Nodes or combinations of AX nodes and Storage Spaces Direct Ready Nodes:

Steps

1. In the upper left corner of the Windows Admin Center, select **Cluster Manager** from the drop-down menu.
2. From the list, select a failover or hyper-converged cluster connection, and then click **Connect**.

NOTE: If the extension prompts you to specify the "Manage as" credentials, ensure that you select Manage as and provide appropriate cluster administrator credentials to authenticate the managed nodes, and then select the **use these credentials for all connections** check box. Ensure that the user is part of the local user group of gateway administrators. For more information about selecting "Manage as", see the "Get Started with Windows Admin Center" section in the Microsoft documentation.
3. In the left pane of the Microsoft Windows Admin Center, under **EXTENSIONS**, click **Dell EMC OpenManage Integration**.
4. To manage a failover or hyper-converged cluster, select:
 - **Health**—to view the health status of the server components of the individual nodes in the cluster.
 - The **Overall Health Status** section displays the overall health of the cluster. Select different sections in the doughnut chart to filter the health status of the components of the cluster nodes.

NOTE: The overall health status of the cluster might be displayed as critical or warning even though the components of the nodes displayed on the Windows Admin Center are healthy. For more details on the components in critical health state, go to the respective iDRAC console.

See [Health status—Supported target node components in Failover Clusters, Windows Server HCI, and Azure Stack HCI](#) on page 15.
 - **Inventory**—to view the detailed hardware inventory information of the component. On the **Overview** page, the basic details of the nodes of the failover or hyper-converged cluster are listed. Select the required node to view detailed

hardware inventory of the server components. See [Hardware inventory—Supported target node components in Failover Clusters, Windows Server HCI, and Azure Stack HCI](#) on page 16.

- **iDRAC**—to view the iDRAC details of the individual nodes. You can directly launch the iDRAC console from Windows Admin Center by using the OpenManage Integration. See [View iDRAC details of the PowerEdge servers and nodes of HCI and Failover clusters](#) on page 18.
- **Configure**—In Compute Resources, you can view CPU core distribution summary and manage CPU core counts. In Expand Cluster, you can identify and prepare nodes for cluster expansion. See [Manage CPU cores in clusters or individual nodes](#) on page 37 and [Add nodes to existing clusters](#) on page 39
- **Update**—to view and update the compliance charts of the nodes and components. Expand the required node to view a detailed compliance report of the components. See [Update PowerEdge servers and nodes of Windows Server HCI, Azure Stack HCI, and Failover clusters using OpenManage Integration extension](#) on page 19.



The health, hardware inventory, and iDRAC details are cached and will not be loaded each time the extension is loaded. To view the latest health and inventory status and iDRAC details, in the upper-right corner of the Health Status, click **Refresh**.

Topics:

- [Health status—Supported target node components in Failover Clusters, Windows Server HCI, and Azure Stack HCI](#)
- [Hardware inventory—Supported target node components in Failover Clusters, Windows Server HCI, and Azure Stack HCI](#)

Health status—Supported target node components in Failover Clusters, Windows Server HCI, and Azure Stack HCI


On the **Cluster - Azure Stack HCI** page, select the **Health** tab to view the overall health status of the Failover or HCI cluster and the health status of the following target node components of the nodes in Failover Cluster, Windows Server HCI, or Azure Stack HCI. Selecting critical or warning section in the overall health status doughnut chart displays corresponding nodes and the components in the critical or warning state respectively.

- CPUs
- Accelerators
 -  **NOTE:** Health status information is available for Accelerators in YX4X models of PowerEdge servers and above with iDRAC version 4.00.00.00 or newer.
- Memory
 -  **NOTE:** Intel **DIMM** memory is identified as **IntelPersistent** with an icon.
- Storage Controllers
- Storage Enclosures
- Physical Disks
- iDRAC
- Power Supplies
- Fans
- Voltages
- Temperatures

The health statuses are represented by using a doughnut chart. You can select different sections in the doughnut chart to filter the health status of the components. For example, when you select the red section, components with critical health status are only displayed.

In a Failover or HCI cluster, if the different sections of the doughnut chart for individual components are selected, the respective nodes with the component health status are listed. Expand the nodes to view the components in a particular health state.

To view the latest health status, in the upper-right corner of the **Health** tab, click **Refresh**.

-  **NOTE:** For software storage controllers and physical disks attached to embedded SATA controller, the health inventory status will always be displayed as "Unknown".

Hardware inventory—Supported target node components in Failover Clusters, Windows Server HCI, and Azure Stack HCI

You can view information about the hardware and firmware components installed on nodes in Failover Cluster, Windows Server HCI, or Azure Stack HCI. To do this, in Dell EMC OpenManage Integration, select **Inventory**. To view the latest hardware inventory information, in the upper-right corner of the **Inventory** tab, click **Refresh**.

Hardware inventory of the following target node components of the nodes in Failover Cluster, Windows Server HCI, or Azure Stack HCI are displayed:

- System
- Firmware
 - NOTE:** Under Firmware inventory, for few network devices with multiple ports, since the applicable firmware version is same for all ports, only a single port with the firmware version will be displayed.
- CPUs
- Accelerators
- Memory
 - NOTE:** Intel **DIMM** memory is identified as **IntelPersistent** with an icon.
- Storage Controllers

To view the physical disks in a storage controller, under **Related Disks**, click the **View Disks** link. The physical disks are listed in the **Physical Disks** tab.

- Storage Enclosures
 - NOTE:**
 - Information about a few attributes of storage enclosures, firmware inventory, and memory components might not be available for:
 - YX2X and YX3X models of PowerEdge servers.
 - YX4X models of PowerEdge servers with iDRAC version lesser than 3.30.30.30.
 - You may find the hardware inventory attribute for a storage enclosure empty. This is because the information may not be available on the target node iDRAC.
 - For PCIe SSD Backplane of storage enclosures, few attribute values might not be available.
- Network Devices
- Physical Disks

To view the additional properties of a disk, select the disk, and then click **Advanced Properties**. To view the associated storage controller, click the storage controller link under **Advanced Properties**. The associated storage controller is displayed in the **Storage Controllers** tab. If physical disks are attached to the CPU, then the storage controller link will not be available under **Advanced Properties**.

To identify physical disks you can blink or unblink the disks LED. For more information, see [LED blink and unblink physical disks](#).

- Power Supplies
- Fans

To view iDRAC details of target node, see [View iDRAC details of the PowerEdge servers and nodes of HCI and Failover clusters](#) on page 18.

- NOTE:** Under **Inventory**, the attribute values of a few target node components are displayed as blank because the value might not be available in the target node.

To blink and unblink physical disks

Select a node and then select a physical disk, click **Blink** to enable the blinking of the LEDs on the physical disk. The LEDs represent the state of physical disks. When the physical disks are blinking, it helps to locate and also to identify the faulty physical disks in your data center. To disable the blinking of the physical disks, select a disk and click **Unblink**. In a cluster, the blink or unblink operation of a selected node must complete before using the blink or unblink operation on a different node.

The blink and unblink operations are not available for:

- Disks associated to Boot Optimized Storage Subsystem (BOSS) cards.
- Devices with iDRAC firmware version less than 3.30.30.30. Update the iDRAC firmware to the latest version to enable blink and unblink operations.
 - If blink and unblink operation is unavailable for selected supported disks even with iDRAC firmware version 3.30.30.30 and above, then upgrade the iDRAC firmware to the latest version to enable blink and unblink operations.

NOTE:

- When the blink or unblink operation is running, **Refresh** button to load the latest health and hardware inventory information is disabled. And, when the health and hardware inventory is loaded in OMIMSWAC, blink and unblink operations is disabled.
- Blink or unblink operation fails on physical disks that are attached to an embedded SATA controller with an error `Blink/Unblibk May not be supported with - <disk_name>.`

View iDRAC details of the PowerEdge servers and nodes of HCI and Failover clusters

To view the following iDRAC details of the target node, select **Server Manager** or **Cluster Manager** from the upper left corner of Microsoft Windows Admin Center, and then select a server or cluster connection from the list. In the left pane, under **EXTENSIONS**, click **Dell EMC OpenManage Integration** and navigate to the **iDRAC** tab.

For failover and hyper-converged clusters, expand the nodes to view the following details

- DNS Domain name
- URL String: This contains the iDRAC IP address. You can launch the iDRAC console directly from Microsoft Windows Admin Center.
- IPMI version.
- iDRAC firmware version.
- MAC address of the device.
- Licenses: You can see various licenses available on the node. For example, OMIWAC Premium License for MSFT HCI Solutions, iDRAC9 Enterprise License, and so on.

Click the license name to view the license details.

To manage a cluster by using Dell EMC OpenManage Integration, you must have the OMIWAC Premium License installed on each target node. For more information about licensing, see the licensing section in the *OMIMSWAC Installation Guide*.

i **NOTE:** The premium license name for HCI solutions shown in OMIMSWAC iDRAC inventory is "OMIWAC Premium License for MSFT HCI Solutions". However, the same license name shown in the iDRAC is "OMIWAC Premium License for Azure Stack HCI".

Update PowerEdge servers and nodes of Windows Server HCI, Azure Stack HCI, and Failover clusters using OpenManage Integration extension

OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) allows you to generate compliance details and update components, such as BIOS, driver, firmware, and/or system management applications of target nodes and nodes in an HCI and failover clusters. You can use either an online or offline catalog to generate compliance details and update components.

In OMIMSWAC, click **Update**. The update window is displayed.

On this page, you can generate a compliance report and update the components as follows:

1. **Generate compliance report:** Select update source catalog (online or offline catalog) to fetch the update details for each device and generate a compliance report.
2. **Verify compliance report and confirm component selection:** Verify the generated compliance report. By default, all the non-compliant components (excluding downgradable component) are selected. Select or clear any components you want to update and then confirm the components selection.
3. **Update:** Update the target node or cluster.

To generate compliance report and update a target node, see [update target node](#). To generate compliance report and update nodes of HCI and Failover cluster, see [update nodes of HCI and failover clusters](#).

OpenManage Integration uses online or offline catalog to create baselines. The catalog contains latest BIOS, driver, firmware, and/or system management applications. The system management application might include IC, Driver Pack, iSM, OMSA and so on. OpenManage Integration also uses the Dell EMC System Update Utility (DSU) and Dell EMC Inventory Collector (IC) tools to fetch the update details for each device. The DSU and IC tools help to generate compliance report and remediate the non-compliant devices by updating them.

When offline or online catalog is selected, OMIMSWAC collects the DSU and IC tools configured in **Settings > Update Tools**. To configure Update Tools, see [Configure the update compliance tools setting](#). If DSU and IC tools are not configured in the Settings, then OMIMSWAC with Internet access will download them from www.downloads.dell.com.

In the **Notifications** section of the Windows Admin center, you are notified when a new online or offline catalog file is available. To generate the latest compliance report, on the **Update** tab, run Update Compliance Report.

NOTE: Cluster-Aware Updating (CAU) feature is supported on the following platforms with valid licenses:

- YX4X models of Dell EMC PowerEdge server and above with iDRAC firmware 4.00.00.00 or newer.
- Dell EMC HCI Solutions for Microsoft Windows Server with iDRAC firmware 4.00.00.00 or newer.
- Dell EMC Integrated System for Microsoft Azure Stack HCI with iDRAC firmware 4.00.00.00 or newer.

For more information about licenses, see *OpenManage Integration with Windows Admin Center Licensing* in the [OMIMSWAC Installation Guide](#).

Topics:

- [Configure DSU and IC settings in Update Tools](#)
- [Update target nodes using OpenManage Integration extension](#)
- [Update nodes of Windows Server HCI, Azure Stack HCI, and Failover clusters using OpenManage Integration extension](#)

Configure DSU and IC settings in Update Tools

About this task


To generate the latest compliance report and update components, OpenManage Integration extension without Internet access requires you to configure the DSU and IC settings available in **Settings > Update Tools**. The DSU and IC settings can also be configured when selecting a catalog in **Update > Update source**, by selecting **Advance setting**. The supported versions of the Dell System Update (DSU) and Dell Inventory Collector (IC) utilities for OpenManage Integration are:

- DSU version: 1.9.0. Download the DSU from <https://downloads.dell.com/OMIMSWAC/DSU/>.
- IC version: 21_04_202_1093. Download the IC from <https://dl.dell.com/OMIMSWAC/IC/>.

Steps

In the OpenManage Integration extension, click **Settings > Update Tools** tab to enter the followings:

1. Enter the share location where the DSU utility is placed.
DSU is used to apply the Dell update packages to target nodes.
2. Enter the share location where the IC utility is placed.
The IC utility is used to collect the hardware inventory information from target nodes.
3. Enter the user credentials to access the share location.

 **NOTE:** When OMIMSWAC is uninstalled, the data present in the Settings page is not deleted. If the OMIMSWAC is later reinstalled, previously configured data in the Settings page is still available to it. However, the password remains unavailable.

4. To confirm if the utilities are accessible, click **Test Connection**.
5. Click **Save** to save the update tools setting.

The passwords for the update tool settings are retained only for the current browser session. Ensure that you reenter the password after opening a new browser session for the Update compliance feature of OpenManage Integration with Microsoft Windows Admin Center to function properly.

Next steps

To generate compliance report and update target nodes, see [update target nodes](#).


To generate compliance report and update nodes of HCI and Failover cluster, see [update HCI and Failover cluster](#).

Configure proxy settings

OpenManage Integration extension provides an option to download catalog, DSU, and IC utilities from the Internet using proxy settings to generate compliance report. However, OMIMSWAC, which is connected to the Internet by proxy, does not support updating target nodes or clusters using online catalogs. In this case, compliance and updates using the offline catalog are supported.

About this task

You can configure the proxy settings to connect to a proxy server that acts as an intermediary between your gateway system and the Internet. If OMIMSWAC **Update Tools** settings are not configured and the gateway system is not connected to the Internet, it will check the Internet connectivity using the proxy settings.

 **NOTE:** Proxy settings are not supported in OpenManage Integration snap-in.

To connect to a proxy server:

Steps

1. Enter the IP address of the proxy server in the below format:
https://<IP address> or **http://<IP address>**

2. Enter the Port number of the proxy server, and click **Save**.

For example, for https: 443 or for http: 80

Next steps

To generate compliance report and update target nodes, see [update target nodes](#).

To generate compliance report and update nodes of HCI and Failover cluster, see [update HCI and Failover cluster](#).

Update target nodes using OpenManage Integration extension

By using OpenManage Integration with Windows Admin Center extension, you can view the compliance report (BIOS, driver, firmware, and/or system management application) and update the components of a target node.

Prerequisites

Before you generate a compliance report and update components, ensure the following:

- Ensure to comply with the software and hardware requirements listed in the *compatibility matrix* of the [Installation Guide](#).
- If the extension prompts to specify the "Manage as" credentials, ensure that you select **Manage as** and provide appropriate Server Administrator or Cluster Administrator accounts. And ensure that the user is part of the local user group of gateway administrators. For more information about selecting "Manage as", see the "Get Started with Windows Admin Center" section in the Microsoft documentation.
- Take care of the workload before updating the target node.
- Ensure that inventory information for the target node has been retrieved.
- Ensure that iDRAC lockdown mode is disabled. To disable iDRAC system lockdown mode, see iDRAC documents.
- For SAS-RAID_Driver, ensure the followings:
 - Set the SATA controller to RAID mode.
 - Set the NVMe PCIe SSDs to RAID mode.

For more information about setting the RAID mode, see [Appendix](#)

- Ensure that the WAC is not installed on the target node you want to update.
- Ensure that the target node is reachable using IP address, hostname, and Fully Qualified Domain Name (FQDN) of the target node.

NOTE: If the target node is not reachable, and the target node update is performed, the update status may show failed. In this case, if you reboot the target node immediately after update and rerun the compliance, the target node components status may show compliant, whereas the overall target node update status may still show failed.

NOTE:

- Updating a target node where WAC is installed is not recommended. To support this scenario, install the WAC on another target node (non WAC related) and complete the update.
- We highly recommend to run only one compliance/update for a target node at a time. Running multiple compliance/updates at the same time might cause failures to the existing compliance/updates.

Steps

To generate compliance report and perform firmware, BIOS, and drivers update for target nodes, do the following:

1. To generate a compliance report against a validated catalog, select **Update > Update Source**, and choose any of the available offline or online catalog options as follows. The corresponding online catalog is selected by default based on the target node.

- Choose 'Online (HTTPs) - <catalog name>' to download the catalog automatically from dell.com. Online catalog is selected by default. You can use the online catalog when the OMIMSWAC is connected to the Internet. You can also access the Internet using proxy settings. See [configure proxy settings](#).

The available catalogs are:

- For PowerEdge servers: Dell EMC Enterprise Catalog which contains the validated versions of components for PowerEdge servers.
 - For MX servers: Dell EMC MX Solution Catalog which contains the validated versions of components for PowerEdge MX Modular.
 - For AX nodes and Storage Spaces Direct Ready Nodes: Update Catalog for Microsoft HCI solutions.
- Choose "Offline - Dell EMC Repository Manager Catalog" to use the DRM catalog configured in a CIFS location.

OMIMSWAC with or without Internet access allows you to select the Offline - Dell EMC Repository Manager Catalog to generate a compliance report. You may use this catalog when the Internet is not available or to use a customized DRM catalog.

- a. To use offline DRM catalog, ensure the latest catalog files are generated by using the Dell EMC Repository Manager (DRM) application. The supported version of DRM application can be downloaded from [Dell EMC Repository Manager](#). To create a DRM catalog, refer to the [Technical article](#).
- b. After the DRM catalog is created and stored in a share path, select **DRM Settings** and specify the CIFS share path where DRM catalog is located and provide credentials to access the share path.



NOTE:

- We recommend to use 'Update Catalog for Microsoft HCI solutions' catalog for Azure Stack HCI and Windows Server HCI.
- You must provide individual catalog files with the user credentials for server manager, and cluster manager respectively.

2. To use Dell EMC System Update (DSU) and Inventory Collector (IC) tools, select **Advance settings** and then choose one of the following:
 - "Automatically downloads and configures the Dell EMC System Update (DSU) and Inventory Collector (IC)." when OMIMSWAC is connected to the Internet. This is selected by default.
 - "Manually configure DSU and IC" and then select **Settings** to manually download and configure DSU and IC tools in a share location. We recommend using this option when OMIMSWAC is not connected to the Internet.

The DSU and IC settings, configured using the **Update Tool** settings in OpenManage Integration extension will also be available under **Advance setting**.

When finished, click **Next: Compliance report**.

OMIMSWAC downloads the catalog, collects the DSU and IC tools that are configured in the Settings tab, and generates a Compliance Report. If DSU and IC tools are not configured in the Settings, then OMIMSWAC downloads them from <https://downloads.dell.com> to generate the compliance report.

3. On the **Compliance report** tab, [view the compliance report](#).
 - By default, all the 'non-compliant' 'upgradable' components are selected whose firmware, BIOS, or drivers will be updated.

You may deselect the selected components or select the 'non-compliant' 'downgradable' components for update. However, to change any of the default selections, ensure that the dependencies between the corresponding component firmware and drivers are met.
 - For more specific selection, you can select each color code present under the bar chart or use the search box to filter out the required components. Select 'clear' at the upper right of the **Compliance Report** pane to remove the color code filter.

When finished, click **Next: Summary**.

4. On the **Summary** tab, review the components to be updated and click **Next: Update**.
 - To change the components selection, click **Back** to go to the **Compliance report** tab, and select or clear the component selections.
 - If you want to change the update source and rerun the compliance, click **Exit** to go to the **Update Source**.

While the update is in progress on the **Update** tab, it is recommended not to exit or close the browser. If you close or exit the browser, node updates may fail and the update status may not be shown.



NOTE: When components are selected and confirmed, if lockdown mode is enabled in iDRAC on the target node, an error occurs and you cannot proceed to update. Disable the lockdown mode on the target node that is being managed by OMIMSWAC before updating the target node. To disable iDRAC system lockdown mode, see iDRAC documents.

The update job continues in the background regardless of whether the UI session is alive or not. If the UI session is alive, node level progress status is displayed. OMIMSWAC notifies once the update job is finished.

- After successful update, compliance report (based on the previous selections) will be recomputed automatically and displayed in the **Update** tab.
- If the update operation fails, check the log files stored at the following path for more details.
 - Gateway system: <Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs
 - Windows 10 gateway system: <Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs
- To run the compliance report again, click **Re-run Compliance** and provide the compliance settings details.

Results

If any of the component update requires a restart, the node will be restarted.

Update nodes of Windows Server HCI, Azure Stack HCI, and Failover clusters using OpenManage Integration extension

The Cluster-Aware Updating (CAU) feature in OpenManage Integration with Windows Admin Center (OMIMSWAC) extension allows you to view the compliance report (firmware, BIOS, and drivers) and update the components of nodes of HCI and failover clusters without affecting the workloads.

Prerequisites

Before you generate a compliance report and update components, ensure the following:

- You are logged in to Microsoft Windows Admin Center remotely using domain administrator credentials. Ensure the credentials are part of Gateway Administrator. For more information, see [Microsoft documents](#).
- As OMIMSWAC uses the Microsoft Cluster-Aware Updating feature framework to perform cluster updates, ensure the **Failover Clustering feature** and **Failover Clustering Tools** are installed on all the target nodes before triggering CAU. For more information, see [Cluster-Aware Updating requirements and best practices in Microsoft document](#).
- **NOTE:** It is recommended to test the cluster readiness before triggering CAU. For more information, see [Tests for cluster updating readiness in Microsoft document](#).
- Ensure to comply with the software and hardware requirements listed in the *compatibility matrix* of the [Installation Guide](#).
- Ensure that OMIWAC premium licenses are installed on all cluster nodes to use the CAU feature. To verify licensing, click the **iDRAC** tab in the OpenManage Integration extension to view licenses installed on each node.
- Ensure that the cluster service is up before running the update compliance. When the cluster service is down, an update compliance report for a target node may not be generated.
- To manage a cluster, connect to the cluster using **Manage as** option and provide appropriate cluster domain administrator credentials. And ensure that the user is part of the local user group of gateway administrators. For more information, see [Cluster-Aware Updating requirements and best practices in Microsoft document](#).
- Ensure that inventory information for the target node has been retrieved.
- Ensure both physical, and virtual disks are in healthy state before triggering CAU.
- Ensure that iDRAC lockdown mode is disabled. To disable iDRAC system lockdown mode, see [iDRAC documents](#).
- For SAS-RAID_Driver, ensure the followings:
 - Set the SATA controller to RAID mode.
 - Set the NVMe PCIe SSDs to RAID mode.

For more information about setting the RAID mode, see [Appendix](#)

- Ensure that the target node is reachable using IP address, hostname, and Fully Qualified Domain Name (FQDN) of the target node.

NOTE: If the target node is not reachable, and the target node update is performed, the update status may show failed. In this case, if you reboot the target node immediately after update and rerun the compliance, the target node components status may show compliant, whereas the overall server update status may still show failed.

About this task

The CAU feature is supported for the following platforms with valid OMIWAC Premium Licenses:

- YX4X models of Dell EMC PowerEdge Server and above with iDRAC firmware 4.00.00.00 or newer.
- AX nodes and Storage Space Direct Ready Nodes with iDRAC firmware 4.00.00.00 or newer.

NOTE:

- We recommend to validate the cluster before triggering the CAU. For more information about validating a cluster, see [Microsoft documents Validate Hardware for a cluster](#).
- Updating a cluster where WAC is installed on a cluster node is not recommended. To support this scenario, install the WAC on another system that is not part of the cluster and complete the update.
- We highly recommend to run only one compliance/update for a target node or cluster at a time. Running multiple compliance/updates at the same time might cause failures to the existing compliance/updates.

- The CAU feature is not supported for YX2X and YX3X models of Dell EMC PowerEdge servers.

Steps

To generate compliance report and perform firmware, BIOS, and drivers update for Windows Server HCI, Azure Stack HCI, and Failover clusters, do the following:

1. To generate compliance report against the validated catalog, on the **Update source** tab, do the following:

- a. Select one of the methods to download catalog files:

- **Online (HTTPs) - <catalog name>** catalog to download the catalog automatically from dell.com. Online catalog is selected by default.

The available catalogs are:

- For PowerEdge servers and clusters containing PowerEdge servers: Dell EMC Enterprise Catalog which contains the validated versions of components for PowerEdge servers.
- For MX servers: Dell EMC MX Solution Catalog which contains the validated versions of components for PowerEdge MX Modular.
- For Windows Server HCI and Azure Stack HCI cluster nodes: Update Catalog for Microsoft HCI solutions which contains the validated versions of components for AX nodes and Storage Spaces Direct Ready Nodes.

Online catalog support requires direct internet connectivity from the Windows Admin Center gateway. The overall download time of a catalog depends on the network bandwidth and number of components being updated. You can also access the Internet using proxy settings. See [configure proxy settings](#).

- **Offline - Dell EMC Repository Manager Catalog** to use the DRM catalog configured in a CIFS location.

OMIMSWAC with or without Internet access allows you to select the Offline - Dell EMC Repository Manager Catalog to generate compliance report. You may use this option when the Internet is not available or to use a customized DRM catalog.

- To use offline catalog, select **DRM Settings** to ensure the CIFS share path is configured with the DRM catalog. The supported version of DRM application can be downloaded from [Dell EMC Repository Manager](#). To create a DRM catalog, refer to the [Technical article](#).



NOTE:

- We recommend to use 'Update Catalog for Microsoft HCI solutions' catalog for Azure Stack HCI and Windows Server HCI.
- You must provide individual catalog files with the user credentials for server manager, and cluster manager respectively.

- b. To use the Dell EMC System Update (DSU) and Inventory Collector (IC) tools, select **Advance setting**, and then select one of the following:

- "Automatically downloads and configures the Dell EMC System Update (DSU) and Inventory Collector (IC)." when OMIMSWAC is connected to the Internet. This is selected by default.
- "Manually configure DSU and IC" and then select **Settings** to manually download and configure DSU and IC tools in a share location. We recommend using this option when OMIMSWAC is not connected to the Internet.

DSU and IC settings, configured using **Update Tool** settings in OpenManage Integration extension will also be available under **Advance setting** in OpenManage Integration snap-in.

When finished, click **Next: Compliance report**.

OMIMSWAC downloads the catalog, collects the DSU and IC tools that are configured in the **Settings** tab, and generates a Compliance Report. If DSU and IC tools are not configured in the **Settings**, then OMIMSWAC downloads them from <https://downloads.dell.com> to generate the compliance report.

2. On the **Compliance report** tab, view the compliance report. For more information about the compliance report, [view the compliance report](#).

- The 'upgradable' components that are 'non-compliant' are selected by default for update.

You may deselect the selected components or select the 'non-compliant' 'downgradable' components for update. However, if you want to change any of the default selections, ensure that the dependencies between the corresponding component firmware and drivers are met.

- For more specific selection, you can select each color code present under the bar chart or use the search box to filter out the required components. Select 'clear' at the upper right of the **Compliance Report** pane to remove the color code filter.

You can also click 'Expand all' icon at the upper right of the **Compliance Report** pane to expand the nodes where you can select or deselect components.

When finished, click **Next: Summary**.

3. On the **Summary** tab, review the components to be updated and choose to run the update now or schedule for later:
 - **Run now:** This will execute the cluster update immediately and reboot nodes if required.
 - **Schedule later:** Select a future date and time when the cluster update will be performed. This will download and copy the required files and keep the cluster ready for update at the specified time.

At any given time, only one CAU job can be scheduled per cluster. Any new CAU job (Run now or Schedule later) will replace the existing scheduled job.

To change the components selection, select **Back** to go to the **Compliance report** tab, and select or clear the component selections. If you want to change the update source and rerun the compliance, click **Exit** to go to the **Update Source**.

NOTE: If a catalog does not contain updates to a component, then the component will not be displayed in the compliance report generated by using OpenManage Integration with Microsoft Windows Admin Center integration.

4. When finished, click **Next: Cluster Aware Update**.

A message is prompted to enable CredSSP. Click **Yes** to enable the CredSSP and continue updating the selected components. You will be directed to the **Cluster aware update** tab to see the update status. To improve security, disable the CredSSP after the update operation is complete.

NOTE: While the update is in progress on the **Cluster aware update** tab, it is recommended not to exit or close the browser. If you close or exit the browser, node updates may fail and the update status may not be shown.

The update job continues in the background regardless of whether the UI session is alive or not. If the UI session is alive, node level progress status is displayed. OMIMSWAC notifies once the update job is finished.

- If the update operation fails, check the log files that are stored at the following path for troubleshooting purposes.
 - Gateway system: <Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs
 - Windows 10 gateway system: <Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs
 - After the scheduled cluster update is over, DSU logs for individual nodes can be found in <Windows Directory>\Temp\OMIMSWAC folder on the respective nodes.
- To run the compliance report again, click **Re-run Compliance** and provide the compliance settings details if required.

Results

If any of the component update requires a restart, nodes will be restarted one at a time, moving cluster roles such as VMs between nodes to prevent downtime.

View compliance report

The update compliance details are computed, and the compliance report is displayed. The bar chart represents the number of components in compliant, urgent, recommended, and optional states using color codes. The Compliance Report provides a detailed view of all the components that contains component name, current version, type, baseline version, compliance status, criticality, and compliance type.

You can click **Expand all** or **Collapse all** icon (available only for Cluster-Aware Update in OpenManage Integration extension) at the upper right of the **Compliance Report** pane to expand the nodes where you can select or deselect components. For more specific selection, you can select each color code present under the bar chart or use the search box to filter out the required components. Select clear at the upper right of the **Compliance Report** pane to remove the color code filter.

To analyze further, check the individual nodes in the Compliance Report to get the current version, baseline versions and compliance type of the components, and to view all the nodes and components in non-compliant, urgent, recommended, and optional states respectively. Along with compliance information, the license status (OMIWAC Premium License) for each node is also displayed.

NOTE: All target nodes participating in the cluster must have valid licenses, otherwise, you cannot proceed to update the cluster. For more information about OMIMSWAC licensing, refer to [OMIMSWAC Installation Guide](#).

NOTE: If a catalog does not contain updates to a component, then the component is not displayed in the generated compliance report.

Attribute names	Description
Component Name	Specifies component name. For example: Serial-ATA_Firmware_6FGD4_WN64_E012_A00
Compliance	Specifies compliance type whether compliant or non-compliant. <ul style="list-style-type: none"> Compliant - Target nodes in this category have the same versions of Firmware, BIOS, and Driver as that of the imported catalog. Non-Compliant - Target nodes in this category require Firmware, BIOS, and Drivers updates.
Criticality	Specifies whether compliance is urgent, recommended, or optional. <ul style="list-style-type: none"> Urgent - The update contains changes to improve the reliability and availability of the Dell EMC system or related component. Therefore, apply this update immediately. Recommended - The update contains feature enhancements or changes that help keep the system software current and compatible with other system modules (Firmware, BIOS, and Drivers). Optional - The update contains changes that impact only certain configurations, or provides new features that may/may not apply to the environment. Review the update specifications to determine if it applies to the system.
Current Version	Specifies the current component version. For example: E012
Baseline Version	Specifies the version belongs to the imported catalog. For example: E013
Type	Specifies the component type. For example: Firmware, BIOS, Driver, Application
Compliance Type	Specifies whether the component is Upgradable, Downgradable, or Same. <ul style="list-style-type: none"> Upgradable: Component can be upgraded from the current version. Downgradable: Component can be downgraded from the current version. Same: Component current version is same as the baseline version.

NOTE: In the compliance report, the compliance type of **Microsoft basic display adapter Driver** may show as downgradable. After you update (downgrade), the name of the driver will change to **Matrox G200eW3 (Nuvoton) WDDM <version no.> Driver**. This an expected behavior.

Integrated deploy and update of Azure Stack HCI clusters

In this section, you will learn how to use OpenManage Integration snap-in to perform integrated deploy and update of Azure Stack (AS HCI) clusters.

While deploying an Azure Stack HCI cluster using AX nodes in Windows Admin Center, use OpenManage Integration snap-in to ensure the followings for optimal cluster performance and support:

- HCI Configuration Profile checks: ensures nodes selected for an Azure Stack HCI cluster are supported and have symmetrical hardware configurations as recommended by Dell EMC.
- Update: ensures Firmware, BIOS, and Drivers of selected nodes are the latest.

Because this feature is integrated with the Azure Stack HCI cluster creation workflow, this restarts the nodes only once if necessary after both operating system and hardware updates are complete.

Topics:

- [Integrated deploy and update an Azure Stack HCI cluster using OpenManage Integration snap-in](#)
- [HCI configuration profile](#)

Integrated deploy and update an Azure Stack HCI cluster using OpenManage Integration snap-in

The Integrated cluster deploy and update feature in OpenManage Integration enables you to update target nodes while creating an Azure Stack HCI cluster using Windows Admin Center. This feature also helps you to comply hardware configurations of selected nodes with Dell EMC recommended hardware configurations.

Prerequisites

Before you begin, verify the followings:

- Ensure that you have installed the Windows Admin Center 2103.2 GA.
- You are logged in to Microsoft Windows Admin Center remotely using domain administrator credentials. Ensure the credentials are part of Gateway Administrator. For more information, see [Microsoft documents](#).
- Ensure that all the prerequisites mentioned in the [Create an Azure Stack HCI cluster using Windows Admin Center](#) in the Microsoft documents are met.
- Ensure that all the selected nodes are of AX nodes running Azure Stack HCI version 20H2 operating system. For more information about the supported hardware, see *Compatibility matrix* in OMIMSWAC Installation Guide.
- To create a cluster, connect to the nodes by specifying appropriate node administrator credentials. And ensure that the user is part of the local user group of gateway administrators. For more information about selecting "Manage as", see the "Get Started with Windows Admin Center" section in the Microsoft documentation.
- Ensure that nodes are not part of any existing cluster.
- For HCI Configuration Profile checks, ensure OMIWAC Premium License for MSFT HCI Solutions is available on each node.
- To use online catalogs, ensure that OMIMSWAC is connected to the Internet. You may also use proxy settings to download catalog, DSU, and IC utilities from the Internet to generate compliance reports only. For more information about proxy settings, see [Configure proxy settings](#).
- To use the offline DRM catalog, ensure that settings are configured as mentioned in the [Configure update tool settings](#).

About this task

NOTE:

- If any of the above prerequisites are not met, ensure to review and resolve as needed. You can also skip the OpenManage Integration snap-in flow and continue with the cluster creation workflow of Microsoft. However, skipping

the Install hardware updates workflow may impact the cluster performance. Therefore, it is recommended to install hardware updates while creating clusters.

- Dell EMC OpenManage Integration with Windows Admin Center does not support the creation of a Stretched Cluster.

Steps

When deploying an Azure Stack HCI cluster, to maintain symmetrical hardware configuration and update firmware/drivers for Azure Stack HCI cluster nodes, do the following:

1. When deploying an Azure Stack HCI cluster in Windows Admin Center, using **Get started** wizard, complete the operations on the **1.1 Check the prerequisites**, **1.2 Add servers**, **1.3 Join a domain**, **1.4 Install features**, and **1.5 Install updates** tabs as required.

NOTE: Renaming nodes in **1.3 Join a domain** tab is not supported and may cause prerequisites failure when installing hardware updates. To rename the servers (if required), it is recommended to do it outside of cluster deployment workflow. For example, use Azure Stack HCI OS Server Configuration tool (Sconfig) or Windows Admin Center to rename a node. Before launching the cluster create wizard, ensure the new node name is effective.

2. On **Install hardware updates** tab, click **Install** to install OpenManage Integration snap-in. If you have already installed the OpenManage Integration extension version 2.1, click **Check for updates** to move to the install hardware updates page.

NOTE: If the snap-in prompts to specify the "Manage as" credentials, ensure that you select Manage as and provide appropriate cluster administrator credentials to authenticate to the managed node, and then select "use these credentials for all connections" check box. Ensure that the user is part of the local user group of gateway administrators. For more information about selecting "Manage as", see the *Get Started with Windows Admin Center* section in the Microsoft documentation.

When the OpenManage Integration snap-in is installed, the OpenManage Integration standalone extension appears under the **Tools** menu in the Windows Admin Center. You will be able to use all the features of OpenManage Integration extension along with the snap-in specific features.

3. Review the prerequisites listed in the page to ensure that all nodes are ready to perform HCI configuration profile checks and update.
 - If any of the nodes is not a valid model, you cannot proceed to the next step. For more information about supported models, refer to [AS HCI support matrix](#).
 - If any of the nodes do not contain OMIWAC Premium License, you can continue to update nodes; however, you cannot run HCI Configuration Profile checks.

Click **Re-Run** to run the prerequisites again.

When finished, click **Next: HCI Configuration Profile**.

4. For **HCI Configuration Profile**, review the configurations listed under each category to ensure all nodes configurations are as per Dell EMC recommended configurations. For more information about hardware configurations required for HCI Configuration Profile, see [HCI configuration profile](#).
 - (optional) If internet connection is not available, perform the below steps to run HCI configuration profile checks in offline mode:
 - a. Download the *asHCISolutionSupportMatrix.json* and *asHCISolutionSupportMatrix.json.sign* files from <http://downloads.dell.com/omimswac/supportmatrix/>.
 - b. Place these files in C:\Users\Dell\SymmetryCheck folder in the gateway system where Windows Admin Center is installed.
 - c. Run the HCI configuration profile check.

NOTE: HCI configuration profile will fail if any of the required configurations fail with a "Critical" error. Review the recommendations and details to resolve any issues to achieve HCI configuration profile and proceed to the next step.


When the configuration fails with a "Warning", this means the configuration can be supported for cluster deployment, but could result in sub-optimal cluster performance. Therefore, it should be reviewed.

click **Re-Run** to run the HCI configuration profile check again.

When finished, click **Next: Update source**.

5. To generate compliance report against the validated Azure Stack HCI catalog, on the **Update source** page, do the following:
 - a. Select one of the methods to download catalog files:
 - **Online (HTTPs) - Update Catalog for Microsoft HCI Solutions** catalog to download the catalog automatically from dell.com. Online catalog is selected by default.

Online catalog support requires direct internet connectivity from the Windows Admin Center gateway. The overall download time of a catalog depends on the network bandwidth and number of components being updated.

 **NOTE:** Accessing to the Internet using proxy settings are not supported.

- **Offline - Dell EMC Repository Manager Catalog** to use the DRM catalog configured in a CIFS location.

OMIMSWAC with or without Internet access allows you to select the Offline - Dell EMC Repository Manager Catalog to generate compliance report. You may use this option when the Internet is not available or to use a customized DRM catalog.

- To use offline catalog, select **DRM Settings** to ensure the CIFS share path is configured with the DRM catalog. To create a DRM catalog, see the [Technical article](#).

- b. To use the Dell EMC System Update (DSU) and Inventory Collector (IC) tools, select **Advance setting**, and then select one of the following:

- **Automatically downloads and configures the Dell EMC System Update (DSU) and Inventory Collector (IC)**, when OMIMSWAC is connected to the Internet.
- **Manually configure DSU and IC** and then select **Settings** to manually download and configure DSU and IC tools in a share location. We recommend using this option when OMIMSWAC is not connected to the Internet.

DSU and IC settings, configured using **Update Tool** settings in OpenManage Integration extension will also be available under **Advance setting** in OpenManage Integration snap-in.

When finished, click **Next: Compliance report**.

OMIMSWAC downloads the catalog, collects the DSU and IC tools that are configured in the **Settings** tab, and generates a Compliance Report. If DSU and IC tools are not configured in the **Settings**, then OMIMSWAC downloads them from <https://downloads.dell.com> to generate the compliance report.

6. On the **Compliance report** tab, view the compliance report. For more information about the compliance report, see [view compliance report](#).


- The 'upgradable' components that are 'non-compliant' are selected by default for update.

You may deselect the selected components or select the 'non-compliant' 'downgradable' components. However, if you want to change any of the default selections, ensure that the dependencies between the corresponding component firmware and drivers are met.

When finished, click **Next: Summary**.

7. On the **Summary** tab, review the components to be updated, and then click **Next: Update** to update the cluster nodes. A message is prompted to enable CredSSP.

- a. Click **Yes** to enable the CredSSP to continue updating the selected components. You will be directed to the **Update** page. To improve security, disable the CredSSP after the update operation is complete.

 **NOTE:** While the update is in progress on the **Update** page, it is recommended not to exit or close the browser. If you close or exit the browser, node updates may fail and the update status may not be shown.

The update job continues in the background regardless of whether the UI session is alive or not. If the UI session is alive, node level progress status is displayed. OMIMSWAC notifies once the update job is finished.

- If the update operation fails, check the log files that are stored at the following path for troubleshooting purposes.
 - Gateway system: <Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs
 - Windows 10 gateway system: <Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs
- To run the compliance report again, click **Re-run Compliance** and provide the compliance settings details if required.

Results

After hardware updates are complete, you may continue to follow the instructions shown on the Windows Admin Center to create the Azure Stack HCI cluster.

HCI configuration profile

HCI configuration profile check ensures nodes selected for an Azure Stack HCI cluster are supported and have symmetrical hardware configurations as recommended by Dell EMC.

Azure stack HCI cluster works best when the hardware configurations of all the selected nodes are compliant with Dell EMC recommendations.

The Integrated Deploy and Update feature in OMIMSWAC helps you to maintain HCI configuration profile and update nodes while creating an Azure Stack HCI cluster using AX nodes (running Azure Stack HCI OS) in Windows Admin Center. The HCI configuration profile check runs a set of rules on nodes and helps you to align their hardware configurations with Dell EMC recommendations.

Before you create an Azure Stack HCI cluster, ensure to run and comply with all the rules of HCI configuration profile checks.

HCI configuration profile checks are intended to do the following:

- Find hardware or configuration issues before an Azure stack HCI cluster goes into production.
- Ensure that the Azure stack HCI cluster you deploy is reliable and the cluster performance is optimal.

This topic explains the HCI configuration profile rules and provides examples of supported and unsupported configurations. For information about supported and validated components required for HCI configuration profile, see [AS HCI support matrix](#). If any of the HCI configuration profile checks fail with a "Critical" or "Warning" error, review the recommendations and show details and contact the [Dell support team](#) to resolve the issue before proceeding to the next step.

The critical error states that this aspect of nodes configuration is not supported. You must correct the issue before you can deploy an symmetric Azure Stack HCI cluster. And Warning states that this aspect of nodes configuration can be supported for cluster deployment, but might result in sub-optimal cluster performance. Therefore, it should be reviewed.

Configuration rules

Processor

- It is recommended for all nodes to have processors from the same model. Using nodes with different processor models results in a warning.

For example: if one node has a processor of X model, they should all have processors from the X model.

- All nodes must have same number of processor sockets. Using nodes with different processor sockets results in HCI configuration profile failure.

For example, if one node has 2 processor sockets, then they should all have 2 processor sockets.

Memory

- If one node has persistent memory, it is recommended they should all have the persistent memory of same number and capacity. Using nodes with different numbers or capacities of persistent memory results in a warning.
- It is recommended to have the same amount of physical memory for all nodes. Using physical memory of different capacity results in a warning.

Platform

- All nodes must have a BOSS adapter. Using nodes without a BOSS adapter results in HCI configuration profile failure.

Storage

- It is recommended to have compatible drives of same media type such as SSD, NVMe, and HDD for all nodes. Using nodes with incompatible drives results in a warning.
- All nodes must have the same Host Bus Adapter (HBA) except for all NVMe configurations. Using nodes with different HBA results in HCI configuration profile failure.

For example, if one node has HBA 330, they should all have the same HBA 330.

Network

- It is recommended that all nodes should have compatible network adapters. Using nodes with incompatible network adapters results in a warning.
- At least one RDMA network adapters must be common across all nodes. Using nodes without any common network adapters results in HCI configuration profile failure.

For example, if one node has Qlogic network adapter and other nodes have Mellanox network adapter, then this configuration is not supported. In this case, at least one common RDMA network adapter(Qlogic or Mellanox) should be present in all nodes.


Disks

- It is recommended that all nodes should contain compatible disks as mentioned in the [AS HCI support matrix](#). Using nodes with incompatible disks results in a warning.
- It is recommended that all nodes should contain up to two media types. Supported media type combinations are as follows:
 - Persistent Memory and NVMe
 - Persistent Memory and SSD
 - NVMe and SSD
 - NVMe and HDD
 - SSD and HDD
 - ALL NVMe
 - ALL SSDUsing combination of three media types such as NVMe, SSD and HDD results in HCI configuration profile failure.
- It is recommended that all nodes should have minimum number of drives required per media type.

For example, if a node has only 1 media type of SSD, then at least 4 capacity drives of SSD are required. If a node has 2 media types such as SSD and HDD, then 2 SSD drives for cache and 4 HDD drives for capacity are required.

Using media types with different drives results in a warning.
- All nodes must have the same drive types. For example, if one node has SATA drives they should all have SATA drives. Using combination of SATA and SAS drives in a cluster results in HCI configuration failure.
- It is recommended that all drives of each media type such as SSD, NVMe, and HDD across all cluster nodes have the same bus protocol such as SAS, SATA, or PCIe.

For example, if one node has SSD and HDD drives with SAS bus protocol, other nodes should also have SSD and HDD drives with SAS bus protocol. Using drives of different bus protocols results in a warning.

 **NOTE:** It is recommended that drives across selected nodes have the same bus protocol to achieve symmetrical configuration. For example, nodes with drives such as SSD and HDD with SATA and SAS bus protocols respectively are not a supported configuration.
- It is recommended that all nodes should have drives of equal size and count per media type.

For example, If one node has 4 SSD drives of 2 TB size, other nodes should also have 4 SSD drives of 2 TB size. Using nodes with different count and capacity results in a warning.
- It is recommended for each node having drives of SSD or NVMe media type to have the same endurance.

For example, If one node has 4 Mixed Use SSD drive type, other nodes should also have 4 Mixed Use SSD drive type.

Using nodes with drives of different endurance such as Read intensive, Mixed Use, and Write Intensive results in a warning.
- If persistent memory is present on at least one node, all the remaining nodes selected for the cluster should also contain the same number and capacity of persistent memory modules. Using nodes with different persistent memory modules results in a warning.
- The total raw capacity of the cache drives should not be less than 5% of the raw capacity of the capacity drives.

Example configurations

Here are some supported and unsupported configurations:

Not supported: different models between nodes

The first two nodes use AX-640 model but the third node uses AX-740xd.

Node 1	Node 2	Node 3
AX-640	AX-640	AX-740xd

This is not supported. All nodes should have the same model node.

Supported: no more than two media types

Supported configuration for two media types are as follows:

Node 1	Node 2	Node 3	Node 4	Node 5
NVMe+SSD	NVMe+HDD	SSD+HDD	All NVMe	All SSD

Not supported: at least minimum number of drives

If two media types exist:

Node 1	Node 2	Node 3
2 × SSD for cache	2 × SSD for cache	2 × SSD for cache
3 × HDD for capacity	3 × HDD for capacity	3 × HDD for capacity

This is not supported. Nodes with two media types drives should have 2 SSD drives for cache and 4 HDD drives for capacity.

Supported: at least minimum number of drives

If two media types exist, supported configurations are:

Node 1	Node 2	Node 3
2 × SSD for cache	2 × SSD for cache	2 × SSD for cache
4 × HDD for capacity	4 × HDD for capacity	4 × HDD for capacity

This is supported. Nodes with two media types drives should have 2 cache drives (SSD/NVMe/AEP) and 4 capacity drives (HDD/SSD/NVMe).

Not supported: drives with different bus protocol

The first two nodes use SSD drive with SAS bus protocol but the third node uses SSD drive with SATA bus protocol.

Node 1	Node 2	Node 3
SSD with SAS protocol	SSD with SAS protocol	SSD with SATA protocol

The first two nodes use SSD and HDD drives with SAS bus protocol but the third node uses HDD drive with SATA bus protocol.

Node 1	Node 2	Node 3
SSD with SAS protocol	HDD with SAS protocol	HDD with SATA protocol

These are not supported. Drives across nodes should have the same bus protocol for symmetrical configuration.

Not supported: drives with same capacity and different count

The first two nodes use 2TB SSD and the last node uses 3TB SSD. Every node has total 4 SSD.

Node 1	Node 2	Node 3
4 × 2 TB SSD	4 × 2 TB SSD	4 × 3 TB SSD

This is not supported. All drives of each media type (SSD/NVMe/HDD) should be of the same count and capacity.

Not supported: at least one same RDMA network adapter present in all nodes




The first two nodes use Qlogic network adapter and the last node uses Mellanox network adapter.

Node 1	Node 2	Node 3
Qlogic network adapter	Qlogic network adapter	Mellanox network adapter

This is not supported. One network adapters should be common across all nodes.

View HCI configuration profile check results

After the HCI configuration profile check has completed, the summary report is displayed. All rules must pass with a green check mark, or in some cases, a yellow triangle (warning). The following table shows the symbols in the summary and explains what they mean:

Symbols	Description
	The HCI configuration profile check passed, indicating that this aspect of nodes configuration is supported for the cluster deployment.
	The HCI configuration profile check produced a warning, indicating that this aspect of nodes configuration can be supported for cluster deployment, but might result in sub-optimal cluster performance. Therefore, it should be reviewed.
	The HCI configuration profile check failed, and this aspect of nodes configuration is not supported. You must correct the issue before you can deploy an symmetric Azure Stack HCI cluster.

Full Stack Cluster-Aware Updating for Azure Stack HCI clusters using OpenManage Integration snap-in

With the use of Full Stack Cluster-Aware Updating capability in OpenManage Integration snap-in, you can perform hardware updates (firmware, BIOS, and drivers) on Dell EMC Integrated System for Microsoft Azure Stack HCI (also known as Azure Stack HCI) cluster nodes in addition to the operating system update available in the Windows Admin Center.

To get the latest features, apply the latest security fixes, and keep the infrastructure defect free, you must ensure that the target nodes are updated with the latest operating system and hardware updates such as Firmware, BIOS, and Drivers. Many operating system and hardware updates may require rebooting nodes to apply the changes. The reboot process may impact the workload or applications running on the node.

With the use of OpenManage Integration snap-in integrated with the Windows Admin Center cluster update workflow, you can seamlessly update the firmware, BIOS, and drivers on target nodes in addition to the operating system update available in the WAC. It also reduces the number of reboots required after the update using the Full Stack CAU feature.

To access full stack update feature, in Windows Admin Center, select **Updates** from the **Tools** menu.

To perform hardware updates on the cluster separately, use the Cluster-Aware Updating feature available in the OpenManage Integration with Windows Admin Center extension tool. See [Update PowerEdge servers and nodes of Windows Server HCI, Azure Stack HCI, and Failover clusters using OpenManage Integration extension](#) on page 19.

Topics:

- [Update an Azure Stack HCI cluster using OpenManage Integration snap-in](#)

Update an Azure Stack HCI cluster using OpenManage Integration snap-in

Prerequisites

Before you begin Firmware, BIOS, and Drivers update, verify the following prerequisites are met:

- Ensure that you have installed the Windows Admin Center 2103.2 GA.
- You are logged in to Microsoft Windows Admin Center remotely using domain administrator credentials. Ensure the credentials are part of Gateway Administrator. For more information, see [Microsoft documents](#).
- Ensure that the Dell EMC Integrated System for Microsoft Azure Stack HCI (also known as Azure Stack HCI) cluster is created from AX nodes running Azure Stack HCI version 20H2 operating system.
- Ensure OMIWAC Premium License is installed on each AX nodes.
- Ensure that pre-update script and post-update script are not present as part of the cluster role. If it's present, it's recommended to remove the script before triggering Updates. For more information, see [Tests Summary page](#) in the *Troubleshooting* section.
- To use online catalogs, ensure that OMIMSWAC is connected to the Internet. You may also use proxy settings to download catalog, DSU, and IC utilities from the Internet to generate compliance reports only. For more information about proxy settings, see [Configure proxy settings](#).
- To use the offline DRM catalog, ensure that settings are configured as mentioned in the [Configure update tool settings](#).
- If the snap-in prompts to specify the "Manage as" credentials, provide appropriate cluster domain administrator credentials to authenticate to the managed node, and then select **use these credentials for all connections** check box. Ensure that the user is part of the local user group of gateway administrators. For more information, see [Cluster-Aware Updating requirements and best practices in Microsoft document](#).

About this task

Full Stack Cluster-Aware Updating feature is supported for Dell EMC Integrated System for Microsoft Azure Stack HCI running Azure Stack HCI version 20H2 operating system.

Steps

To perform both operating system and hardware updates on Azure Stack HCI cluster nodes:

1. In Windows Admin Center, select **Updates** from the **Tools** menu.
 - a. You must enable Credential Security Service Provider (CredSSP) and provide explicit credentials. When asked if CredSSP should be enabled, click **Yes**.
The **Updates** page is displayed.

2. For operating system update, see the [Azure Stack HCI documentation in Microsoft](#).

3. On the **Install updates** page, after you review the operating system updates, select **Next: Hardware updates**.

4. Windows Admin Center will check if the supported Dell EMC OpenManage Integration extension has been installed.
 - If the extension is not installed, click **Install** to accept the license terms and install the Openmanage Integration snap-in.
 - If OpenManage Integration extension version 2.1 is already installed or after the OpenManage Integration snap-in is installed, click **Get updates** to move to the Hardware updates page.

After the OpenManage Integration snap-in is installed, the OpenManage Integration extension version 2.1 appears under the **Tools** menu in the Windows Admin Center. You will be able to use all the features of OpenManage Integration extension along with the snap-in specific features.


5. On the **Hardware updates** page, review the prerequisites listed to ensure all nodes are ready for hardware updates. When finished, click **Next: Update Source**. Click **Re-Run** to run the prerequisites again.

You must meet all the prerequisites mentioned on the **Prerequisites** tab, otherwise you cannot proceed to the next step.

6. To generate compliance report against the validated Azure Stack HCI catalog, on the **Update source** page, do the following:
 - a. Select one of the methods to download catalog files:

- **Online (HTTPs) - Update Catalog for Microsoft HCI Solutions** to download the catalog automatically from the dell.com. Online catalog option is selected by default.

Online catalog support requires direct internet connectivity from the Windows Admin Center gateway. The overall download time of a catalog depends on the network bandwidth and number of components being updated.

 **NOTE:** Accessing to the Internet using proxy settings are not supported.

- **Offline - Dell EMC Repository Manager Catalog** to use the DRM catalog configured in a CIFS location.

OMIMSWAC with or without Internet access allows you to select the Offline - Dell EMC Repository Manager Catalog to generate compliance report. You may use this option when the Internet is not available or to use a customized DRM catalog.

- To use offline catalog, select **DRM Settings** to ensure the CIFS share path is configured with the DRM catalog. To create a DRM catalog, see the [Technical article](#).

- b. To use the Dell EMC System Update (DSU) and Inventory Collector (IC) tools, select **Advance setting**, and then select one of the following:

- "Automatically downloads and configures the Dell EMC System Update (DSU) and Inventory Collector (IC)." when OMIMSWAC is connected to the Internet.
- "Manually configure DSU and IC" and then select **Settings** to manually download and configure DSU and IC tools in a share location. We recommend using this option when OMIMSWAC is not connected to the Internet.

DSU and IC settings, configured using **Update Tool** settings in OpenManage Integration extension will also be available under **Advance setting** in OpenManage Integration snap-in.

When finished, click **Next: Compliance report**.

OMIMSWAC downloads the catalog, collects the DSU and IC tools that are configured in the **Settings** tab, and generates a Compliance Report. If DSU and IC tools are not configured in the **Settings**, then OMIMSWAC downloads them from <https://downloads.dell.com> to generate the compliance report.

7. On the **Compliance report** tab, view the compliance report. For more information about the compliance report, see [view compliance report](#).
 - The 'upgradable' components that are 'non-compliant' are selected by default for update.

You may clear the check box beside to the selected components or select the 'non-compliant' 'downgradable' components. However, if you want to change any of the default selections, ensure that the dependencies between the corresponding component firmware and drivers are met.

When finished, click **Next: Summary**.

8. On the **Summary** tab, review the components to be updated, and then click **Next: Download updates** to download the updates for the selected components.

NOTE: While the download is in progress, it is recommended not to exit or close the browser. If you close or exit the browser, download of update operation may fail.

The download job continues in the background regardless of whether the UI session is alive or not. If the UI session is alive, node level progress status is displayed. OMIMSWAC notifies once the download job is finished.

- If the download operation fails, check the log files stored at the following path for troubleshooting.
 - Gateway system: <Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs
 - Windows 10 gateway system: <Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs
 - After the cluster update is over, DSU logs for individual nodes can be found in <Windows Directory>\Temp\OMIMSWAC folder on the respective nodes.
- To run the compliance report again, click **Re-run Compliance** and repeat steps 4 to 7.

9. After the updates are downloaded, follow the instructions on the Windows Admin Center to install both operating system and hardware updates.

If the UI session is alive, node level progress status is displayed. Windows Admin Center notifies once the update is completed.

Results

If any of the updates require a restart, nodes will be restarted one at a time, moving cluster roles such as VMs between nodes to prevent downtime.

Next steps

NOTE: The CAU clustered role is configured by default to trigger the self-updating functionality of the cluster on Tuesdays on the third week of each month. Therefore, after the update is complete, ensure to disable the CAU clustered role in one of the cluster node to prevent the self-updating functionality of the cluster. For more information about disabling CAU clustered role, see <https://docs.microsoft.com/en-us/powershell/module/clusterawareupdating/disable-cauclusterrole?view=win10-ps>

Manage CPU cores in clusters or individual nodes


Prerequisites

- See [best practices for proper functioning of OMIMSWAC in the 'Getting started with OpenManage Integration' section](#).
- Ensure that the cluster contains homogenous nodes. For example, the nodes should have the CPUs either from Intel or AMD and from the same processor family. Having nodes that include CPUs from both Intel and AMD or from different processor family is not supported.
- To manage CPU core in a cluster, "OMIWAC Premium License for MSFT HCI Solutions" must be installed on each cluster nodes. To manage CPU core in an individual node (AX, S2D, or PowerEdge node), 'OMIWAC Premium License for MSFT HCI Solutions' must be installed in AX/S2D node and 'OMIWAC Premium License for PowerEdge' must be installed in PowerEdge node.

About this task

To manage workload demands and power consumption, you can change the amount of CPU cores allocated to a node or cluster by using the 'CPU core management' feature. This feature helps you to maintain the right balance between power and performance. This feature also helps you to optimize CPU cores in clusters to keep the Total Cost of Ownership at an optimal level.

The CPU core management feature is supported in Azure Stack HCI clusters, Windows Server based HCI clusters, and individual nodes with OMIWAC Premium License installed on each node.

 **NOTE:** CPU core management feature is not supported in Failover clusters and individual node that is part of an Azure Stack HCI or Windows Server HCI cluster.

Steps

In the Windows Admin Center, connect to a cluster or individual node and then perform the following steps:

1. In Windows Admin Center, under Extensions, click **Dell EMC OpenManage Integration**.
2. In **Dell EMC OpenManage Integration**, click the **Configure** tab.
3. Under **CPU Core Management**, a summary of CPU core distributions of the cluster nodes or individual node is displayed as follows:
 - The horizontal bar chart under **CPU Core Configuration Summary** displays the number of cores that are currently enabled in the cluster or individual node and the number cores available for use. The maximum number of CPU cores present in the node or cluster is mentioned below the bar chart.
 - Under **Current Configuration**, total number of nodes, CPUs, and currently enabled cores along with CPU model number are displayed.
 - Switch the **Show Node Level Details** on or off to show or hide the node details such as node name, CPU model used in the node, number of CPUs, number of cores per CPU, and core speed.
- a. In the **Show Node Level Details**, select a node to see the **Advanced Details** of the node as follows:
 - Dell Controlled Turbo
 - Logical Processor
 - Configurable TDP
 - Virtualization technology
 - X2APIC mode
4. To manage CPU cores, click **Update CPU Core**.
Update CPU Core wizard is displayed on the right.
5. In the Update CPU Core wizard, move the slider left or right to decrease or increase the number of cores to be used based on workloads.

Based on the CPU core manufacturer (Intel or AMD) you can configure the cores as follows. To maintain cluster homogeneity, OMIMSWAC will apply the same configuration across all nodes.

NOTE: Changing the number of cores impact the overall core count of the cluster. Ensure that you are using the right number of cores to maintain the balance between power and performance.

CPU Type	Instructions
Intel CPU	<ul style="list-style-type: none"> Select number of cores you want to enable per CPU. Minimum number of cores that can be enabled is four. You can enable all the cores that you want to manage workloads.
AMD CPU	<ul style="list-style-type: none"> Using the first slider, select the number of CCDs per processor you want to enable. Using the second slider, select the number of cores per CCD you want to enable. You can enable any numbers of cores at a minimum. You can also enable all the cores that you want to manage workloads.

6. Select one of the following options to apply the changes and reboot nodes.

- For an **individual node**:
 - Apply and Reboot Now:** Select the option if you want to apply the changes and reboot the node now. Ensure to take care of the workloads before applying the changes.
 - Apply at Next Reboot:** Select this option if you want to apply the changes now and reboot the node later. Ensure that you reboot the node later to successfully apply the CPU core changes. Also, ensure to take care of the workload before rebooting the node.
- For a **cluster**:
 - Apply and Reboot Now:** Select the option if you want to apply the changes and reboot the cluster nodes now. Dell EMC recommends using this option as the nodes are rebooted automatically by taking care of the workloads.

Before clicking "Apply and Reboot Now", ensure the followings:

 - As OMIMSWAC uses the Microsoft Cluster-Aware Updating feature framework to perform cluster updates, ensure the **Failover Clustering feature** and **Failover Clustering Tools** are installed on all the cluster nodes before rebooting the cluster. For more information, see [Cluster-Aware Updating requirements and best practices in Microsoft document](#).
 - Dell EMC recommends to test the cluster readiness before rebooting the cluster. For more information, see [Tests for cluster updating readiness in Microsoft document](#).
 - Apply at Next Reboot:** Select this option if you want to apply the changes now and reboot the cluster nodes later. Ensure that you reboot the cluster nodes later to successfully apply the CPU core changes. Also, ensure to take care of the workload before rebooting the nodes.

NOTE: Apply and Reboot now process requires the CredSSP to be enabled. To improve security, disable CredSSP after the CPU configuration changes is complete.

7. To apply the changes, click **Confirm**.

Under **Compute Resources** the status of the changes is displayed. Click **View Details** to see the progress at a node level.

Next steps

For any issues with updating CPU configurations, see the Troubleshooting section.

Add nodes to existing clusters

By using OMIMSWAC, you can prepare nodes to add to your existing Windows Server HCI, Azure Stack HCI, and Failover cluster to improve capacity.

It's always important for cluster administrators to keep the cluster symmetrical and adhere to Dell EMC recommendations. During cluster expansion, to automate the process and help customers comply with Dell EMC recommendations, OMIMSWAC has introduced a feature called "Expand Cluster". With the use of "Expand Cluster" feature, you as an administrator can prepare nodes ensuring the node is compatible and follow Dell EMC recommendations, which can then be added to the existing cluster.

The cluster expansion process involves three major steps:

- High Level Compatibility Check: Helps to identify compatible nodes to add to the cluster.
- License Availability Check: Checks for OMIWAC premium licenses available on new nodes as well as cluster nodes.
- HCI Configuration Profile check: Helps you to validate new node as well as cluster nodes HCI configurations based on Dell EMC recommendations. This process is only applicable for Windows Server HCI and Azure Stack HCI cluster.
- Update Compliance: Helps you to generate compliance report for both new nodes and cluster nodes and then fix the compliance only for new nodes.

After successfully completing all of these steps, you can add a new node to an existing cluster.

Topics:

- [Prepare nodes for Windows Server HCI and Azure Stack HCI cluster expansion](#)
- [Prepare nodes for Failover cluster expansion](#)

Prepare nodes for Windows Server HCI and Azure Stack HCI cluster expansion

Prerequisites

- Ensure that 'OMIWAC Premium License for MSFT HCI Solutions' is installed on cluster nodes as well as the new node.
- Ensure that new nodes are not part of any cluster.
- For new nodes with SAS-RAID_Driver, ensure the followings:
 - Set the SATA controller to RAID mode.
 - Set the NVMe PCIe SSDs to RAID mode.

For more information about setting the RAID mode, see [Appendix](#)

Planning before preparing a node for cluster expansion:


- Place the new node in a rack and cable it properly.
- Ensure the same operating system is installed on the new node as on the existing cluster nodes.
- Connect the node using the Windows Admin Center and configures the basic settings such as username, domain, and so on.
- Ensure new nodes are in the same domain as of cluster nodes.
- Ensure cluster administrators can access new nodes with local admin rights.

Steps

To prepare nodes for cluster expansion:

1. Connect to the cluster using Windows Admin Center and launch OpenManage Integration extension.
2. Go to **Configure** tab and then click **Expand Cluster** on the left side.
3. In the **Expand Cluster** window, click **Add Nodes**.
4. In the **Expand Cluster** window, under **Select compatible nodes**, list of nodes are displayed. The list fetches all nodes available on the **Server Manager** page in the Windows Admin Center.


- a. Select any nodes that you want to add to the cluster. You can also search any node using the search box or click **select all** check box to select all nodes. Ensure that new nodes are not part of the cluster.

 **NOTE:** Total number of nodes supported in a cluster is 16. For example, for a cluster with existing 4 nodes, you can select up to 12 nodes for cluster expansion.

- b. After nodes are selected, click **Check** for **High Level Compatibility** to validate the new nodes and cluster nodes as per Dell EMC recommendations.

The validation happens on a high level as below:

- Both new nodes and cluster nodes must be from Dell Technologies.

 **NOTE:** Only AX nodes from Dell Technologies such as AX-640, AX-740XD, AX-6515, AX-7525 nodes are supported for HCI cluster expansion. Storage Space Direct Ready Nodes are not supported for HCI cluster expansion.

- New nodes and cluster nodes must be of the same model for symmetrical cluster.
- Operating system installed on new nodes must be supported and same as cluster nodes.

If the high level compatibility shows

- Non-compliant: None of the selected nodes are compliant as per Dell EMC recommendations.
- Partially Compliant: Few of the selected nodes are compliant as per Dell EMC recommendations and you can proceed for **License Availability** check only for the compliant nodes.
- Compliant: All the selected nodes are compliant as per Dell EMC recommendations and you can proceed for **License Availability** check for all the compliant nodes.


If the high level compatibility shows Non-compliant or Partially Compliant, click **View Details** to learn more about the nodes and type of non-compliance.

- c. Click **Check** for **License Availability** to verify whether new nodes and cluster nodes have 'OMIWAC Premium License for MSFT HCI Solutions' installed.

Before moving for **HCI Configuration Profile** check, ensure new nodes and cluster nodes have OMIWAC premium license installed.

- d. Click **Check** for **HCI Configuration Profile** to validate new nodes as well as cluster nodes against symmetrical recommendations from Dell EMC. If internet connection is not available, see the [Troubleshooting](#) section to run HCI configuration profile check in offline mode.

If any of the node is not compatible, click **View Details** to see more information about the nodes, reason for non-compliant and recommendations. For more information about HCI configuration profile rules, see [HCI configuration profile](#) on page 30.

 **NOTE:** HCI configuration profile will fail if any of the required configurations fail with a "Critical" error. Review the recommendations and details to resolve any issues to achieve HCI configuration profile and proceed to the next step.

When the configuration fails with a "Warning", this means the configuration can be supported for cluster deployment, but could result in sub-optimal cluster performance. Therefore, it should be reviewed.

Before you proceed to the next step, ensure HCI configurations of all nodes are compliant as per Dell EMC recommendations.

5. After you successfully complete the high-level compatibility check, license check, and HCI configuration profile check, click **Next: Update compliance** to check for firmware, BIOS, and drivers compliance for new nodes and cluster nodes. Using 'Expand Cluster' flow, you can update firmware, BIOS, and drivers for new nodes only. To generate compliance report for both new nodes and cluster nodes:

- a. Select one of the methods to download catalog files.

- **Online** catalog to download the catalog automatically from dell.com for PowerEdge servers. Online catalog is selected by default.
- **Offline** catalog to use the DRM catalog configured in a CIFS location.

OMIMSWAC with or without Internet access allows you to select the Offline - Dell EMC Repository Manager Catalog to generate compliance report. You may use this option when the Internet is not available or to use a customized DRM catalog. When internet is not available, before using offline catalog ensure [DSU and IC settings are configured on the Settings page](#).


- To use offline catalog, select **DRM Settings** to ensure the CIFS share path is configured with Microsoft HCI solution DRM catalog. To create a DRM catalog, see the [Technical article](#).

When finished, click **Check Compliance**.

6. **Compliance Results** section shows compliance reports of cluster nodes and new nodes. Click **View Details** to see the compliance report or **Export** to export the report in CSV format. For more information about compliance report, see [View compliance report](#) on page 25.
- If cluster nodes are non-compliant, ensure that the cluster nodes are compliant before adding new nodes in the cluster. To update cluster nodes, exit the wizard and go to the **Update** tab for cluster update using cluster-aware updating method.
 - If new nodes are non-compliant, click **View Details** in the **Compliance Result** to verify the non-compliant components and then click **Finish** to update the new nodes and keep them ready for cluster expansion. Click **Update in progress-View** to see the update status.
 - If new nodes are compliant, click **View Details** in the **Summary** to see the list of nodes that will be prepared for cluster expansion and then click **Exit**.

Next steps

After both new nodes and cluster nodes are updated, navigate to the Windows Admin Center workflow to add new nodes to the existing cluster.

 **NOTE:** Before adding a node to the cluster, ensure that you configure the host OS network to the new nodes same as the cluster nodes. For more information about configuring host OS networks, see [Scalable Architecture for Dell EMC Solutions for Azure Stack HCI](#).

Prepare nodes for Failover cluster expansion

Prerequisites

- Ensure that 'OMIWAC Premium License for PowerEdge' is installed on cluster nodes as well as the new node.
- For new nodes with SAS-RAID_Driver, ensure the followings:
 - Set the SATA controller to RAID mode.
 - Set the NVMe PCIe SSDs to RAID mode.

For more information about setting the RAID mode, see [Appendix](#)


Planning before preparing a node for cluster expansion:

- Place the new node in a rack and cable it properly.
- Ensure the same operating system is installed on the new node as on the existing cluster nodes.
- Connect the node using the Windows Admin Center and configure the basic settings such as username, domain, and so on.
- Ensure new nodes are in the same domain as of cluster nodes and they are accessible by the domain administrator.

Steps

To prepare nodes for cluster expansion:

1. Connect to the cluster using Windows Admin Center and launch OpenManage Integration extension.
2. Go to **Configure** tab and then click **Expand Cluster** on the left side.
3. In the **Expand Cluster** window, click **Add Nodes**.
4. In the **Expand Cluster** window, under **Select compatible nodes**, list of nodes are displayed. The list fetches all nodes available on the **Server Manager** page in the Windows Admin Center.
 - a. Select any nodes that you want to add to the cluster. You can also search any node using the search box or click **select all** check box to select all nodes. Ensure that new nodes are not part of any cluster.

 **NOTE:** Total number of nodes supported in a cluster is 16. For example, for a cluster with existing 2 nodes, you can select up to 14 nodes for cluster expansion.
 - b. After nodes are selected, click **Check** in **Recommendations** and then click **View Details** to see recommended and not-recommended nodes for cluster expansion. For more information about Recommendations check, see [View Recommendations check](#) on page 42.
 - c. Click **Check** in **License Availability** to verify whether new nodes and cluster nodes have 'OMIWAC Premium License for PowerEdge' installed.


Before moving for update compliance, ensure new nodes considered from recommendations check and cluster nodes have OMIWAC premium license installed.

5. After you successfully complete the Recommendations and License Availability check, click **Next: Update compliance** to check for firmware, BIOS, and drivers compliance for new nodes and cluster nodes. Using 'Expand Cluster', you can update firmware, BIOS, drivers, and system management applications of new nodes only. To generate compliance report for both new nodes and cluster nodes:

a. Select one of the methods to download catalog files.

- **Online Enterprise** catalog to download the catalog automatically from dell.com for PowerEdge servers. Online catalog is selected by default.
- **Online - MX** catalog contains the validated versions of components for PowerEdge MX Modular.

Online catalog support requires direct internet connectivity from the Windows Admin Center gateway. The overall download time of a catalog depends on the network bandwidth and number of components being updated.

 **NOTE:** Accessing to the Internet using proxy settings are not supported.

- **Offline** catalog to use the DRM catalog configured in a CIFS location.

OMIMSWAC with or without Internet access allows you to select the Offline - Dell EMC Repository Manager Catalog to generate compliance report. You may use this option when the Internet is not available or to use a customized DRM catalog. When internet is not available, before using offline catalog ensure [DSU and IS settings are configured on the Settings page](#).


- To use offline catalog, select **DRM Settings** to ensure the CIFS share path is configured with the DRM catalog. To create a DRM catalog, see the [Technical article](#).

When finished, click **Check Compliance**.

- b. **Compliance Results** displays compliance summary of cluster nodes and new nodes. Click **View Details** to see the compliance report or **Export** to export the report in CSV format. For more information about compliance report, see [View compliance report](#) on page 25.
- If cluster nodes are non-compliant, ensure the cluster nodes are compliant before adding new nodes in the cluster. To update cluster nodes, exit the wizard and go to the **Update** tab for cluster update using cluster-aware updating method.
 - If new nodes are non-compliant, click **View Details** in the **Compliance Results** to verify the non-compliant components and then click **Finish** to update the new nodes components and keep them ready for cluster expansion. Click **Update in progress - View Details** to see the update status.
 - If both cluster nodes and new nodes are compliant, click exit and follow Microsoft recommended steps to add nodes to the cluster.



Next steps

After both new nodes and cluster nodes are updated, navigate to the Windows Admin Center workflow to add new nodes to the existing cluster.

 **NOTE:** Before adding a node to the cluster, ensure that you configure the host OS network to the new nodes same as the cluster nodes.

View Recommendations check

The overall status in Recommendations is a consolidated view of individual node status. Click **View Details** to see recommendations for individual nodes. The following table provides details about the overall Recommendations status and individual nodes status.

Overall Recommendation status	Individual nodes status	Can proceed for license check	Remarks
Recommended ()	All the selected nodes are compliant with Dell EMC recommendation.	Yes.	All compliant nodes are considered for license check.
Partially recommended ()	Few nodes are compliant while others are not (Non- recommended or non-compliant).	Yes.	Compliant and non-recommended nodes are considered for license check. However, using non-recommended nodes for

			cluster expansion may result in sub-optimal cluster performance. Non-compliant nodes are not considered for license check.
Non-recommended (⚠)	Nodes are non-recommended but are supported for cluster expansion.	Yes.	Non-recommended nodes are considered for license check. However, using non-recommended nodes for cluster expansion may result in sub-optimal cluster performance.
Non-compliant (❌)	All the selected nodes are non-compliant.	No.	Non-compliant nodes are not considered for license check

The nodes are recommended based on the following checks:

- Both new nodes and cluster nodes must be from Dell Technologies.
- New nodes and cluster nodes must be from the same model for symmetrical cluster. For mixed cluster, new nodes can be of any model of the existing cluster nodes.
- Operating system installed on new nodes must be same as cluster nodes (major OS version). Failover cluster expansion is supported in nodes using Windows Server 2016 and 2019 OS versions.

Troubleshooting and Frequently asked questions

Topics:

- [Upgrading](#)
- [Licensing](#)
- [Logs](#)
- [Health, hardware, and iDRAC inventory](#)
- [Blink and Unblink](#)
- [Cluster-Aware Updating](#)
- [Full Stack Cluster-Aware Updating](#)
- [Manage CPU core](#)
- [Cluster Expansion](#)
- [Others](#)

Upgrading

Extension installation failed

When you try to install OpenManage Integration snap-in during Azure Stack HCI cluster creation or update, the extension installation may fail.

Reason: An older version of the extension (OMIMSWAC 1.1.1 or earlier) may have already been installed.

Resolution:

- Uninstall the older version, and then install the OpenManage Integration snap-in during Azure Stack HCI cluster creation or update. See *Installing Dell EMC OpenManage Integration with Microsoft Windows Admin Center* section in OMIMSWAC installation Guide.
- To upgrade to OpenManage Integration snap-in from earlier versions, go to **Extensions > Installed extensions** tab. Select Dell EMC OpenManage Integration extension with the status "Update available (version)," and then click **Update**.

Why am I not able to install the extension using the local feed?

The installation of the extension using the local feed may fail with the below error:

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

Ensure that the file name is *dell-emc.openmanage-integration.<Version>.nupkg* while adding the OMIMSWAC extension. The installation fails if the default file name is changed.

Why am I not able to install the extension?

The installation of the extension may fail with the below error:

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

Before installing the extension, ensure the followings:

- The extension is installed on a supported WAC version. For information about supported WAC version, see the Compatibility Matrix.
- The CredSSP is disabled.

For more information about prerequisites for installing the extension, see the OMIMSWAC Installation Guide.

Licensing

Licensing status is Unknown or Non-licensed

If the license status is `Unknown` or `Non-licensed`, ensure that:

- License is not expired.
- Licenses are present on each target node.
- Target node is powered on and not in the reboot state. Also, no reboots are pending for the target node.
- Redfish is enabled.
- Azure stack HCI license or PowerEdge server license is imported onto the respective hardware. Importing Azure stack HCI license to a PowerEdge server or PowerEdge server license to an Azure stack HCI server is not supported.

If the problem persists:

1. Go to iDRAC.
2. Ensure that Redfish service is enabled.
3. Disable **OS to iDRAC Pass-through** and then enable it.

For more information about enabling or disabling OS to iDRAC Pass-through, see iDRAC user guide.

Logs

Availability of OMIMSWAC extension logs

The OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) extension logs of target nodes and cluster nodes are available at `<Windows Directory>\Temp\OMIMSWAC` on target nodes. The logs capture information when the OMIMSWAC functionalities are run and also provide debug information about any errors that occur while performing any OMIMSWAC operations. The logs of various OMIMSWAC functionalities can be easily accessed with the help of the following naming convention:

- For hardware and health inventory: `Inventory<ID*>`
- For update compliance: `FirmwareCompliance<ID*>`
- For update notifications: `Notification<ID*>`

Availability of update operation logs

The application logs for the update compliance feature is available at the following path:

- Gateway system: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs`
- Windows 10 gateway system: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs`

Online catalogs download status is captured in the application logs and can be referred to troubleshoot any download errors in the online catalogs.

When online catalog source is selected, and if DSU and IC are not configured in settings in advance, OMIMSWAC will download the catalog, DSU, and IC utilities in the following path:

- Gateway system: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\Share\temp\<server /cluster_name>`

- Windows 10 gateway system: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\Share\temp\<server/cluster_name>`

Ensure that the downloaded catalog file, DSU and IC are not modified during compliance generation and update. The catalog file, DSU, and IC utilities are automatically removed after the compliance report is generated and updated.

Logs for pre-update script running on HCI clusters to put storage into maintenance mode are available at `<Windows Directory>\Temp\precau.log` on each node. And logs for post update script running on HCI clusters to restore storage from maintenance mode are available at `<Windows Directory>\Temp\postcau.log` on each node.

Availability of licensing logs

The license related logs are available at the following path and can be found by searching *DellLicenseCollection* in the *Cleanup* file.

- Gateway system: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\CleanupXXXXXX XXXXXXXX.log`
- Windows 10 gateway system: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\CleanupXXXXXXXXXXXXXXXXX.log`

Health, hardware, and iDRAC inventory

Unable to copy the required files to the target node to fetch inventory information.

Ensure that:

- Target node is not in the reboot state and is powered on.
- Firewall is not blocking communication through SMB port 445. For more information, see [prepare your environment for Windows Admin Center](#).
- The USB NIC adapter is not disabled on the target node operating system.

Unable to fetch the health and hardware inventory from iDRAC

To fetch the health and hardware inventory information from iDRAC, ensure that:

- YX3X and YX2X models of PowerEdge servers are updated with latest iDRAC version of 2.60.60.60 or later.
- YX4X models of PowerEdge Servers are updated with latest iDRAC version of 3.30.30.30 or later.
- For management of PowerEdge servers, OMIMSWAC uses an internal operating system to iDRAC Pass-through interface. By default, iDRAC is reachable using the IP address `169.254.0.1/<Subnet>` or `169.254.1.1/<Subnet>`. However, if the host has another network interface in the same subnet (for example, when tool such as VMFleet is installed), OMIMSWAC might not be able to communicate to the iDRAC from the host operating system.

To resolve the conflict, log in to iDRAC and change the USB NIC IP address under the operating system to iDRAC passthrough section. For more information about assigning this IP address, see the iDRAC documentation on the support site.

- For management of Clusters, all the cluster nodes are reachable using IP address, Hostname, and Fully Qualified Domain Name (FQDN) before managing the cluster with OMIMSWAC.
- If the Redfish service is disabled, enable the Redfish service by using iDRAC UI. For more information, see the iDRAC documentation on Dell EMC support site.
- User slots are available on iDRAC to create new users.

Health and hardware inventory of YX2X, YX3X, and YX4X models of PowerEdge servers not displayed

- Ensure that YX3X and YX2X models of PowerEdge servers are updated with latest iDRAC version of 2.60.60.60 or later.
- Ensure that YX4X models of PowerEdge Servers are updated with latest iDRAC version of 3.30.30.30 or later.

Overall health status shows warning or critical while health status of node components shows healthy

The overall health status of PowerEdge servers, failover clusters, and HCI clusters might be displayed as critical or warning even if the components of the nodes displayed on the Windows Admin Center are healthy. Because the health status of physical disks that are attached to embedded SATA controller may be displayed as Unknown as iDRAC is unable to get the health information for these disks.

For more details on the components in critical health state, go to the respective iDRAC console.

Unable to create users on target iDRAC device

If the lockdown mode is enabled on YX4X model of PowerEdge Servers and above, inventory of health, hardware, and iDRAC fails with the error: "Unable to create users on target iDRAC device."

Resolution: Disable the lockdown mode on the target node managed by Dell EMC OpenManage Integration.

Unable to initialize the OMIMSWAC extension.

Retrieving inventory from servers and cluster nodes may fail with the error: Unable to initialize the OMIMSWAC extension.

Resolution: Ensure the IPMI driver is installed, and the IPMI service is running on the target node. For more information on the requirement and solution, see [OMIMSWAC fails to query host information KB article](#).

Why is the Inventory details not displayed?

If inventory details are not loading, ensure the followings:

- Target node is not in the reboot state and is powered on.
- Firewall is not blocking communication through SMB port 445. For more information, see [prepare your environment for Windows Admin Center](#).
- The USB NIC adapter is not disabled on the target node operating system.
- Before you launch Dell EMC OpenManage Integration extension in Windows Admin Center, ensure to log in to WAC as a gateway administrator.
- PS-Remoting is enabled.
- Redfish service is enabled on the target node.
- An iDRAC user slot is available on the target node.
- Lifecycle Controller is available on the target node.
- The lockdown mode is disabled on target node.
- The PowerShell execution policy is set to RemoteSigned on the system with Windows Admin Center installed and on the target node OS. For more information, see <https://www.dell.com/support/article/sln318718/dell-emc-openmanage-integration-with-microsoft-windows-admin-center-omimswac-fails-to-query-host-information>.
- IPMI drivers are present in the target node and the IPMI service is running.
- There is no IP address conflict in USB pass-through .
- There are no proxy settings configured on the target node that might conflict with the USB NIC IP address configured in OS to iDRAC Pass-through in the iDRAC. If the proxy setting is configured, do the following to exclude the USB NIC IP address:
 1. In the target node, open the **Proxy settings**.
 2. Under **Manual proxy setup**, type 169.254.* to exclude the USB NIC IP address configured in the OS to iDRAC Pass-through settings.
- CA and CN are disabled on the target node iDRAC.

Why is the inventory details not displayed for a few of the cluster nodes?

While monitoring Storage Spaces Direct cluster using OMIMSWAC extension, the inventory and health data for few of the servers may not load. In this case, reset the iDRAC and rerun the inventory/health data.

Why is the inventory details not displayed when the extension is opened in a new browser session?

The credentials are retained only for the current browser session. If you open a new browser session, ensure to reconnect the cluster/target node by selecting 'manage as' and provide administrator credentials when prompted.

Why does health and inventory status for a few components show as 'unknown'?

The health and inventory status for software storage controllers and physical disks attached to embedded SATA controller are displayed as "Unknown" as iDRAC is unable to get the health and inventory information for these disks.

Blink and Unblink

Unable to complete or select the disks for the blink or unblink operations

- **Cause:** The Redfish service is not enabled.
Resolution: Enable the Redfish service by using iDRAC UI. For more information, see the iDRAC documentation on Dell EMC support site.
- **Cause:** After the hardware inventory is loaded in OMIMSWAC, if the physical disk is removed then the blink and unblink operations fail with error: `Blink may not be supported with <Disk_Name>`.
Resolution: Insert the physical disk and click **Refresh** to reload the inventory information in OMIMSWAC, and rerun the blink and unblink operations.
- **Cause:** If the iDRAC firmware version is less than 3.30.30.30, the physical disks cannot be selected to blink or unblink.
Resolution: Update the iDRAC firmware to the latest version and retry the blink and unblink operations.
- Blink and unblink operations fail when a physical disk is attached to an embedded SATA controller and the health status is `Unknown`, indicating that blink or unblink operation may not be supported on the disk.

Cluster-Aware Updating

Job failed while downloading the required components for the update compliance operation

While downloading the DSU and IC tools, the update jobs may fail due to various reasons. Probable causes and solutions are given below:

- **Cause:** While exporting the repository by using Dell EMC Repository Manager (DRM), the export job may complete with status as "Partially succeeded." In this case, one or more DUPs may be missing from the repository.
Resolution: Retry exporting the repository in DRM and ensure that the job is successfully completed.
- **Cause:** One or more components may not be downloaded when the 'update source' is selected as an online source.
Resolution: Ensure that there is Internet connectivity and retry downloading the catalog from the online source. For more information, see Dell EMC Repository Manager user guide.

Unable to download the DUP(s)

When accessing Windows Admin Center (WAC) locally with domain credentials, DUP downloads may fail during target node or cluster updates.

Resolution: Ensure the followings:

- You are logged in to Microsoft Windows Admin Center remotely using domain administrator credentials. Ensure the credentials are part of Gateway Administrator. For more information, see [Microsoft documents](#).
- Check your Internet connection or proxy configuration.

Unable to generate compliance report

- **Cause:** When you connect to a target node or cluster using Single-Sign-on rather than 'Manage as' and generate compliance report using OMIMSWAC, the compliance generation may fail.

Resolution: Before connecting to the target node or cluster, ensure that you select "Manage as" and provide appropriate Server Administrator or Cluster Administrator accounts.

- **Cause:** When generating a compliance report, the compliance report generation may fail with the following error in the log:

```
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.
```

Resolution: Ensure that:

- Network connectivity between the gateway system and the target node is intact.
- File copying works between the gateway system and the target node. To check this:
 1. Create a session based on target node credential by executing the following PowerShell command:

```
$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. Copy a test file to the failed target node assuming "Test.txt" is in C:\ drive

```
Copy-Item -Path "C:\Test.txt" -Destination "C:\" -Recurse -Force -ToSession $session
```
- If the problem persists after performing the above actions, try restarting the Windows Remote Management (WS-Management) service in the target node (file copy is failing) then re-run the compliance.

- **Cause:** When generating a compliance report for a cluster, the compliance report generation may fail for cluster nodes.

Resolution: Ensure that:

- The cluster service is running on the cluster node by using the Get-ClusterService PowerShell command.
- The cluster node is not rebooting or in the powered-off state.
- When adding a cluster to the Windows Admin Center, ensure to use the cluster name in FQDN format.
- **Cause:** When generating a compliance report using Windows 10 Microsoft Edge browser, the compliance report generation may fail with the following error: Unable to generate compliance report. The Manage As credentials have not been set or are not in domain\user format.

Resolution: Do any of the followings:

- Connect the target node with credentials using Fully Qualified Domain Name (For example, **domain.lab\username**) or Top Level Domain (For example, **domain\username**).
- Clear the cache memory of the browser and rerun the compliance.
- Ensure that the DNS is configured properly in the WAC installed system to connect to the target node with right credentials.
- **Cause:** Compliance report generation may fail with the following error Unable to install Dell System Update (DSU) package for the server/cluster because DSU installation operation is already in progress for another server/cluster. This occurs because, a user may be trying to run compliance concurrently from two different instances/sessions. For example, one instance by clicking the pop-out button and another instance by using the browser from the same gateway at the same time. One of the instance/sessions that was triggered first proceeds for compliance/update; while another results in an error.

Resolution: Run only one compliance/update for a target node/cluster at a time using one gateway instance.

Compliance report page on loading state for a long time

While generating a compliance report, the compliance report page may show up in the loading state even after the notification of successfully generated update compliance report.

In this case, go to any of the other tabs such as "Settings", "Inventory", and so forth,, and then go back to the Update tab, where you will see the generated compliance report.

Job failed while updating the selected components

Sometimes, CAU or target node updates may fail due to various reasons. The causes and resolutions are given below:

- **Causes:** If target nodes are not validated before triggering CAU, the CAU may fail.
Resolution: For Cluster-Aware Updating, ensure to validate the cluster before triggering CAU. For more information about validating a cluster, see Microsoft document [Validate Hardware for a cluster](#).
- **Causes:** If Failover Clustering feature and Failover Clustering Tools are not installed on target nodes, the CAU may fail.
Resolution: As OMIMSWAC uses the Microsoft Cluster-Aware Updating feature framework to perform cluster updates, before updating a cluster using OMIMSWAC, ensure that the Failover Clustering feature and Failover Clustering Tools are installed on all the target nodes. For more information, see [CAU requirements and best practices in Microsoft documents](#).
To check whether failover clustering tools are running on all the target nodes, from the PowerShell window on the target node, run the `Get-CauClusterRole` PowerShell command.
- **Cause:** Compliance Inventory file is not available for some nodes or file copying from node to gateway is failed after compliance generation.
Resolution: Rerun the compliance.
- **Cause:** Due to Internet connectivity issue, the followings may fail:
 - Signature verification of DSU or IC
 - Downloading of online catalog
 - Downloading of DUPIf any of the above fails, CAU or server update also fails.
Resolution: Ensure that there is Internet connectivity and rerun compliance and update.
- **Cause:** DSU installer is not cleared from a node because the installer file sometimes gets locked by the Windows Admin Center process (sme.exe).
Resolution: Restart the Windows Admin Center service from Windows Services consoles.
- **Cause:** CAU fails if any of the disks is not in healthy state.
Resolution: Ensure both physical and virtual disks are in healthy state before triggering CAU. If any disk is in an unhealthy healthy state, see the [Microsoft document](#) to get it to a healthy state.
- **Cause:** CAU fails if any of the cluster nodes is paused.
Resolution: Resume cluster nodes (Failover roles) before triggering CAU.
- **Cause:** CAU fails when Failover Clustering feature and Failover Clustering Tools are not installed on all the target nodes.
Resolution: Ensure Failover Clustering feature and Failover Clustering Tools are installed on all the target nodes before performing CAU. For more information, see <https://docs.microsoft.com/en-us/windows-server/failover-clustering/cluster-aware-updating-requirements>.

CredSSP Failure

Check the event viewer logs in the gateway system to ensure that CredSSP has not failed during Cluster-Aware Updating. If the CredSSP fails, following are the probable causes and solutions:

- **Cause:** While updating a cluster, credential delegation using CredSSP may fail.
Resolution: Reconnect the cluster using fully qualified domain name, and click **Use this credential for all servers** check box.

For example, if the domain name is test.dev.com, use `test.dev.com\administrator` as the domain name, and then click **Use this credential for all servers** check box.

- **Cause:** When using CredSSP authentication to run scripts on a remote machine, the update job may fail with an error.

The issue is because CredSSP has been disabled in the gateway machine.

Resolution: To resolve the issue, follow the steps below:

1. From PowerShell window, run `gpedit`
2. In the Group Policy Editor window, **Computer Configurations > Administrative Templates > System > Credentials Delegation**
3. Select **Allow delegating fresh credentials with NTLM-only server authentication** and enable it.
4. Run `gpupdate /force` in the PowerShell.

Dell Update Package failures

The Dell EMC Update Package (DUP) may fail to update components after you trigger an update. There are various reasons for the DUP to fail during the update. Look at the following possible solutions to resolve the issue:

- In Windows Admin Center (WAC) installed machine, check the log files to get more information regarding DUP download failure and component mapping. The component mapping is provided to identify the component (selected for update) in the DUP catalog. The log files are at the following path.

Gateway system:

- Server update: `<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 gateway system:

- Server update: `<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`

- Sample log messages are given below:

- DUP download failure error log

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

- Component mapping log file

```
## Format: :>> Component Name -> Package Name
:>> [0001] Broadcom NetXtreme Gigabit Ethernet ->
Network_Firmware_RG25N_WN64_21.60.2_01.EXE
```

- In the target node, refer component mapping and find the component related DUP log file and check the return code that is specified in `<Windows Directory>\Dell\UpdatePackage\log\<Package Name>`. See Dell EMC Update Package user guide for cause and possible resolution.

A return code sample of a DUP failure scenario is given below:

```
Exit code = 1 (Failure)
```

```
2020-04-21 23:48:27
```

```
Update Package finished. Exit code = 1
```

- The DUP may fail when attempting to downgrade a driver component to a lower version. In this case, uninstall the driver from the operating system then rerun the component update from OMIMSWAC. For more information about how to uninstall drivers, see Microsoft document.
- After cluster update, you may see components showing as non-compliant. This happens because of DUP failure.

Resolution: In this case, check the cleanup logs having the DSU logs to see if there is any ERROR for those components. If there is any prerequisite that is required for the component before update, follow the prerequisite and then rerun the update.

Alternatively, you can also try the followings:

- Reset and update the iDRAC to version 4.20.20.20 or higher and then rerun the update. For more information about how to Reset or update iDRAC, see iDRAC documentation.

- Run the update manually in the target node by downloading from the path specified in <Windows Directory>\Dell\UpdatePackage\log\<Package Name> in the DUP log. Example for a network firmware is https://downloads.dell.com/FOLDER06091050M/1/Network_Firmware_TWFF6_WN64_16.26.60.00.EXE.
- Ensure that the selected DUP is supported on the selected operating system and platform by searching the component name in the Dell Support site. Dell support site URL: <https://www.dell.com/support/home/in/en/inbsd1/?app=products>.

Full Stack Cluster-Aware Updating

Couldn't configure cluster aware updates

Cause: To perform full stack updates, in Windows Admin Center, when you select **Updates** from the **Tools** menu, an error might occur: Couldn't configure cluster aware updates. This error occurs because CAU clustered role could not be added to the cluster for update.

Resolution: As a workaround, you can add the cluster role manually using the following PowerShell command before triggering the full stack update: `Add-CauClusterRole -StartDate "02-03-2021 3:00:00 AM" -DaysOfWeek Tuesday -WeeksOfMonth 3 -EnableFirewallRules -RequireAllNodesOnline -Force`

For more information, see [Configure the nodes for remote management](#) in Microsoft documents.

Couldn't query readiness for cluster aware updates

Cause: To perform full stack updates, in Windows Admin Center, when you select **Updates** from the **Tools** menu, an error might occur: Couldn't query readiness for cluster aware updates. This error occurs because of CredSSP failure.

Resolution: As a workaround, see [CredSSP failure](#) to find the cause and solution.

For more information, see the [Microsoft document](#).

Tests Summary page appears

While triggering full stack updates, Tests Summary page may appear.

Resolution: As a workaround, verify if pre-update or post-update script are part of the cluster role. If present, remove the scripts from the cluster node by running the following command in PowerShell: `Set-CauClusterRole -PreUpdateScript $null -PostUpdateScript $null`. For more information about prerequisites required for cluster update, see the [Microsoft document](#).

Update status takes longer to refresh

During full stack cluster updates, the update status that is shown in the **Updates** page may take longer to refresh. In this case, it is recommended to stay on the Updates page and wait for the update to complete. The update status will automatically be displayed once the update is complete. For more information about Microsoft recommendations, see the [Microsoft document](#).

Full stack update may fail with failover cluster tool extension 1.271.0 nupkg

During full stack cluster updates in Azure Stack HCI clusters, the update may fail with an exception Error: RemoteException: Exception calling "Add" with "2" argument(s): "Item has already been added. Key in dictionary: 'PreUpdateScript' Key being added: 'PreUpdateScript'". This issue occurs when Microsoft Failover Cluster Tool Extension 1.271.0 is installed. Due to this issue, both hardware and OS cluster-aware updates (Full stack update) cannot be performed together.

Resolution: Use the latest Microsoft Failover Cluster Tool Extension to perform full stack updates using OMIMSWAC.

Manage CPU core

Job failed while updating CPU core configuration

Applying CPU core configuration changes may fail due to various reasons. The causes and resolutions are given below:

- **Causes:** If the cluster is not validated as per Microsoft recommendations before applying CPU core changes, updating CPU core changes may fail.
Resolution: Before updating CPU core changes ensure to validate the cluster. For more information about validating a cluster, see Microsoft document [Validate Hardware for a cluster](#).
- **Causes:** If Failover Clustering feature and Failover Clustering Tools are not installed on target nodes, updating CPU core changes may fail.
Resolution: As OMIMSWAC uses the Microsoft Cluster-Aware Updating feature framework to perform cluster updates, before updating a cluster using OMIMSWAC, ensure that the Failover Clustering feature and Failover Clustering Tools are installed on all the target nodes. For more information, see [CAU requirements and best practices in Microsoft documents](#).
To check whether failover clustering tools are running on all the target nodes, from the PowerShell window on the target node, run the `Get-CauClusterRole` PowerShell command.
- **Cause:** After CPU core updates are applied in a cluster, rebooting of nodes may fail if any of the disks is not in healthy state.
Resolution: Ensure both physical and virtual disks are in healthy state before updating CPU core configurations. If any disk is in an unhealthy healthy state, see the [Microsoft document](#) to get it to a healthy state.
- **Cause:** CPU core update fails if any of the cluster nodes is paused.
Resolution: Resume cluster nodes (Failover roles) before updating CPU core configurations.
- **Cause:** While applying the CPU core changes, one of the cluster nodes may be forcefully or accidentally shut down.
- **Cause:** Health and hardware inventory from target node iDRAC could not be retrieved.
Resolution: For more information, see [unable to fetch the health and hardware inventory from iDRAC](#).

CredSSP Failure

Check the event viewer logs in the gateway system to ensure that CredSSP has not failed during CPU core configuration update. If the CredSSP fails, following are the probable causes and solutions:

- **Cause:** While updating CPU cores, credential delegation using CredSSP may fail.
Resolution: Reconnect the cluster using fully qualified domain name, and click **Use this credential for all servers** check box.
For example, if the domain name is test.dev.com, use `test.dev.com\administrator` as the domain name, and then click **Use this credential for all servers** check box.
- **Cause:** When using CredSSP authentication to run scripts on a remote machine, the update job may fail with an error.
The issue is because CredSSP has been disabled in the gateway machine.
Resolution: To resolve the issue, follow the steps below:
 1. From PowerShell window, run `gpedit`
 2. In the Group Policy Editor window, **Computer Configurations > Administrative Templates > System > Credentials Delegation**
 3. Select **Allow delegating fresh credentials with NTLM-only server authentication** and enable it.
 4. Run `gpupdate /force` in the PowerShell.

Applying CPU core changes failed

Applying CPU core changes status may show as failed in individual nodes because during CPU core changes:

- OMIMSWAC is unable to connect to the node.
- CPU core update session is disconnected.
- Rebooting of the node is stuck.

Can I update CPU core configurations in Failover cluster?

No, updating CPU core configurations is not supported in Failover clusters. It is supported only on Azure Stack HCI clusters and Windows Server based HCI clusters.

Can I update CPU core configurations in individual nodes?

Yes, you can update CPU core configurations in individual nodes. However, the node should not be part of an Azure Stack HCI cluster or Windows Server based HCI cluster. Nodes part of Failover clusters are supported for individual CPU core configuration update.

NOTE: Dell EMC highly recommends to keep hardware configuration same across all cluster nodes to achieve optimal performance. If you update CPU core configuration in one node in a failover cluster, ensure to maintain the same configurations across all nodes in the cluster.

Do I need a license installed to update the CPU core configuration?

Yes, "OMIWAC Premium License for MSFT HCI Solutions" must be installed on each cluster nodes to update CPU core configurations. For individual nodes, OMIWAC Premium License must be installed for individual CPU core update. For more information about licenses, see the licensing section in OMIMSWAC installation guide.

Cluster Expansion

Signature verification failed with the provided support matrix details

(optional) If internet connection is not available, perform the below steps to run HCI configuration profile checks in offline mode:

1. Download the *asHCISolutionSupportMatrix.json* and *asHCISolutionSupportMatrix.json.sign* files from <http://downloads.dell.com/omimswac/supportmatrix/>.
2. Place these files in C:\Users\Dell\SymmetryCheck folder in the gateway system where Windows Admin Center is installed.
3. Go to Windows Admin Center cluster connection home page, connect to the cluster and then launch to Dell EMC extension again.
4. In the OpenManage Integration, go to the **Configure** tab and then click **Expand Cluster** on the left side.

Node update fails during node preparation for cluster expansion

During node preparation for cluster expansion, if node update fails due to SAS-RAID_Driver, ensure the followings configurations are set:

- Set the SATA controller to RAID mode.
- Set the NVMe PCIe SSDs to RAID mode.

For more information about setting the RAID mode, see [Appendix](#)

Others

OpenManage Integration access denied

Cause: When you log in to Windows Admin Center (WAC) using gateway user credentials without admin privileges and try to launch OpenManage Integration from the WAC console, access denied error may appear.

Resolution: Before you launch Dell EMC OpenManage Integration extension in Windows Admin Center, ensure to log in to WAC as a gateway administrator.

Test-Cluster fails with network communication errors

Cause: With USB NIC enabled in iDRAC, if you run Test-Cluster command to verify the cluster creation readiness or cluster health, you may see an error in the validation report. The error states that the IPv4 addresses assigned to the host operating system USB NIC cannot be used to communicate with the other cluster networks. This error can be safely ignored.

Resolution: Disable the USB NIC (labeled as Ethernet by default) temporarily before running the Test-Cluster command.

USB NIC network shows as partitioned cluster network

Cause: When the USB NIC is enabled in iDRAC, cluster networks in the failover cluster manager show the networks that are associated with the USB NIC as partitioned. This issue occurs as cluster communications are enabled by default on all network adapters and USB NIC IPv4 addresses cannot be used to communicate externally, thus disrupting cluster communication on those NICs. This error can be safely ignored.

Resolution: Disable cluster communication with the networks associated with the USB NICs from the cluster manager.

Acceptance Failed to save: Dell EMC Software License Agreement and Customer Notice

Cause: Dell EMC Software License Agreement and Customer Notice acceptance may fail to save. This may happen when you launch multiple instances of the Dell EMC OpenManage Integration extension from the same gateway, and accept terms and conditions in one instance. In the remaining instances, if you attempt to accept the terms and conditions, you will encounter this error.

Resolution: Navigate away from the Dell EMC OpenManage Integration extension where this issue occurs, and then back in to resolve this issue.

Can I use the Single Sign-on or smart card authentication to log in to OMIMSWAC?

You cannot use Single Sign-on or smart card authentication to log in to OMIMSWAC. To connect to a cluster/server, use 'manage as' and then enter domain or gateway admin credentials.

Why am I not able to access the OMI extension using remote connection?

Without gateway administrator privileges, you will not be able to access the OMIMSWAC. You can launch the browser and connect to the gateway system using gateway administrator credentials from the remote workstation.

Identifying the generation of your Dell EMC PowerEdge server

To cover a range of server models, the PowerEdge servers are now be referred to using the generic naming convention and not their generation.

This topic explains how to identify the generation of a PowerEdge server that are referred to using the generic naming convention.

Example:

The R740 server model is a rack, two processor system from the 14th generation of servers with Intel processors. In the documentation, to refer to R740, generic naming convention **YX4X** server is used, where:

- The letter **Y** (alphabet) denotes the type (form factor: Cloud (C), Flexible(F), Modular (M or MX), Rack(R), Tower(T)) of the server.
- The letter **X** (digit) denotes the class (number of processors) of the server.
- The digit **4** denotes the generation of the server.
- The letter **X** (digit) denotes the make of the processor.


Table 3. PowerEdge servers naming convention and examples

YX5X servers	YX4X servers	YX3X servers
PowerEdge R7515	PowerEdge M640	PowerEdge M630
PowerEdge R6515	PowerEdge R440	PowerEdge M830
	PowerEdge R540	PowerEdge T130

Contacting Dell EMC

About this task

Dell EMC provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area.

 **NOTE:** If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell EMC product catalog.

To contact Dell EMC for sales, technical support, or customer service issues:

Steps

1. Go to Dell.com/support.
2. Select preferred country or region from the list at the bottom right of the page.
3. Click **Contact Us** and select the appropriate support link.

Glossary

The following table defines or identifies abbreviations and acronyms used in this document.

Table 4. Glossary

Abbreviations/ Acronyms	Definition
OMIMSWAC—OpenManage Integration with Microsoft Windows Admin Center extension (also known as OpenManage Integration extension)	Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) enables IT administrators to manage the PowerEdge servers as hosts, Microsoft Failover Clusters (created with PowerEdge servers), Dell EMC HCI Solutions for Microsoft Windows Server (created using AX nodes and/or Storage Spaces Direct Ready Nodes), and Dell EMC Integrated System for Microsoft Azure Stack HCI (created using AX nodes). OMIMSWAC simplifies the tasks of IT administrators by remotely managing the PowerEdge servers and clusters throughout their life cycle.
OpenManage Integration snap-in	OpenManage Integration snap-in is integrated with Windows Admin Center cluster creation or cluster update workflow to enhance the cluster creation and update experience and reduce the number of the reboots required to one while creating a cluster. After OpenManage Integration snap-in is installed, the OpenManage Integration extension appears under the Tools menu in the Windows Admin Center. You will be able to use all the features of OpenManage Integration extension along with the snap-in specific features.
BIOS	Basic Input or Output System. BIOS is firmware that is embedded on a small memory chip on the computer's system board or motherboard. It acts as an interface between the computer's hardware and the operating system. BIOS also contains instructions that the computer uses to perform basic instructions such as whether to boot from network or hard disk drive
Console	The management application a user utilizes to perform remote platform management tasks.
DRM—Dell EMC Repository Manager	Dell EMC Repository Manager (DRM) is an application within the Dell OpenManage portfolio that allows IT Administrators to easily manage system updates. Dell Repository Manager provides a searchable interface used to create custom software collections known as bundles and repositories of Dell Update Packages (DUPs).
DSU—Dell EMC System Update Utility	Dell EMC System Update (DSU) is a script-optimized update deployment tool for applying Dell Update Packages (DUP) to Dell EMC target nodes.
FQDN	Fully Qualified Domain Name.
Gateway administrators	Gateway administrators can configure who gets access as well as how users authenticate to the gateway. Only gateway administrators can view and configure the Access settings in Windows Admin Center. Local administrators on the gateway machine are always administrators of the Windows Admin Center gateway service.
Gateway system	Windows Admin Center installed as a gateway on a Windows server.
Gateway user	Gateway users can connect to the Windows Admin Center gateway service to manage servers through that gateway, but they can't change access permissions nor the authentication mechanism used to authenticate to the gateway.
Windows 10 gateway system	Windows Admin Center installed as a gateway on a Windows 10 OS.

Table 4. Glossary (continued)

Abbreviations/ Acronyms	Definition
HCI	Hyper-Converged Infrastructure.
IC—Dell EMC Inventory Collector	Inventory Collector is used to inventory the target system, compare the results against a Repository or Catalog and only deploy the updates that are required.
iDRAC	Integrated Dell Remote Access Controller.
IPMI	Intelligent Platform Management Interface
LED	Light Emitting Diode
NIC	Network Interface Card also known as Network Interface Controller
Offline - Dell EMC Repository Manager Catalog	Recommended when the DRM repositories are available in a shared location and is applicable for all managed devices by OMIMSWAC in data centers with no Internet connectivity.
Online (HTTPs) - Update Catalog for Microsoft HCI solutions	Recommended for Windows Server (created using AX nodes and/or Storage Spaces Direct Ready Nodes) and Azure Stack HCI clusters (created using AX nodes).
Online (HTTPs) - Dell EMC Enterprise Catalog	Recommended for PowerEdge servers.
Online (HTTPs) - Dell EMC MX Solution Catalog	Recommended for MX models of PowerEdge servers.
SATA	Serial Advanced Technology Attachment interface that is meant to replace the aging PATA technology.
USB	Universal Serial Bus
UI	User Interface
<Windows Directory>	C:\Windows

Appendix

SAS-RAID_Driver

While performing update compliance operation for SAS-RAID_Driver, ensure that *SATA controller* and *NVMe PCIe SSDs* are set to RAID mode. To configure RAID mode:

1. When the **Dell Power-On Self-Test (POST)** screen is displayed, press F2.

Dell PowerEdge System Setup window is displayed.

- Under **System BIOS setting**, configure RAID mode in **SATA settings** > **Embedded SATA**.
- Under **System BIOS setting**, configure RAID mode in **NVMe settings** > **NVMe mode**.

Recommended catalog for target nodes or clusters

The following table shows the recommended catalog for a target node or cluster under 'Update Source'.

Target nodes or cluster	Recommended catalog
PowerEdge server (Rack, Modular, and Tower)	Online (HTTPs) - Dell EMC Enterprise Catalog (for PowerEdge servers)
MX server	Online (HTTPs) - Dell EMC MX Solution Catalog (for PowerEdge servers)
AHCI cluster ready nodes (S2D or Ax appliance)	Online (HTTPs) - Update Catalog for Microsoft HCI solutions
Cluster containing MX and PowerEdge server	Online (HTTPs) - Dell EMC Enterprise Catalog (for PowerEdge servers)
Cluster containing AHCI ready nodes and PowerEdge server	Online (HTTPs) - Dell EMC Enterprise Catalog (for PowerEdge servers)
Cluster containing PowerEdge, MX, and AHCI ready node server	Online (HTTPs) - Dell EMC Enterprise Catalog (for PowerEdge servers)
PowerEdge XE2420 Edge server or cluster	Online (HTTPs) - Dell EMC Enterprise Catalog (for PowerEdge servers)