# Dell EMC OpenManage Integration Version 1.0.0 with Microsoft Windows Admin Center

User's Guide

DELL EMC

## 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.**



2019 - 08

Rev. A00

# Contents

# 1

# Overview of OpenManage Integration with Microsoft Windows Admin Center

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, and Hyper-Converged Infrastructure (HCI) created by using the Dell EMC Microsoft Storage Spaces Direct (S2D) Ready Nodes. 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.

**Key features of OMIMSWAC**

- OMIMSWAC provides a simplified solution to IT administrators to efficiently manage the following:
  - Dell EMC PowerEdge servers.
  - Azure Stack HCI created with Dell EMC Microsoft Storage Spaces Direct Ready Nodes.
  - Microsoft failover clusters created with Dell EMC PowerEdge servers.
- A unified view of health, hardware, and firmware inventory information of the device components.
- Provides update compliance report of PowerEdge servers and clusters against update repository that is created with Dell EMC Repository Manager (DRM).
- Provides notifications on availability of new update catalogs.
- View iDRAC information of PowerEdge servers. For out-of-band management, you can directly launch the iDRAC console from Windows Admin Center.
- Availability of OMIMSWAC extension and documentation localized in English, French, German, Spanish, Simplified Chinese, and Japanese languages.

**Topics:**



# Additional resources

**Table 1. Additional resources**

| Document | Description | Availability |
|---|---|---|
| *Dell EMC OpenManage Integration with Microsoft Windows Admin Center Installation Guide* | Provides information about installing and configuring OpenManage Integration with Microsoft Windows Admin Center. | 1. Go to Dell.com/OpenManageManuals.<br>2. Select **OpenManage Integration with Microsoft Windows Admin Center**.<br>3. Click **DOCUMENTATION** > **MANUALS AND DOCUMENTS** to access these documents. |
| *Dell EMC OpenManage Integration with Microsoft Windows Admin Center Release Notes* | Provides information about new features, known issues and workarounds in OpenManage Integration with Microsoft Windows Admin Center . | |
| *Microsoft Windows Admin Center documentation* | For more information about using Microsoft Windows Admin Center. | https://www.microsoft.com/en-us/cloud-platform/windows-admin-center |

# 2

# Getting started with OpenManage Integration with Microsoft Windows Admin Center

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 Windows Admin Center, select **Server Manager**, **Hyper-Converged Cluster Manager**, or **Failover Cluster Manager** from the drop-down menu.
2. From the list, select a server or cluster connection, and then click **Connect**.
3. Enter the server or cluster credentials.

   **NOTE: If you are not prompted to enter the credentials, ensure that you select "Manage as" and enter appropriate Server Administrator or Cluster Administrator accounts.**
4. In the left pane of the Microsoft Windows Admin Center, under **EXTENSIONS**, click **Dell EMC OpenManage Integration**.

**NOTE: If Microsoft Windows Admin Center is installed on a target node and the target node is managed by OMIMSWAC, the inventory collection functionality of OMIMSWAC may result in failures.**

**Before connecting to the target node, ensure that you select "Manage as" and provide appropriate Server Administrator or Cluster Administrator accounts. For more information about selecting "Manage as", see the "Get Started with Windows Admin Center" section in the Microsoft documentation.**

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, if the USB NIC is enabled by OMIMSWAC then it is disabled and the previously created iDRAC user is deleted by 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.

**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.
- Azure Stack HCI created with Dell EMC Microsoft Storage Spaces Direct Ready Nodes, see Manage Azure Stack HCI created with Dell EMC Microsoft Storage Spaces Direct Ready Nodes.
- Microsoft failover clusters created with PowerEdge servers, see Manage Microsoft Failover Clusters created with PowerEdge servers.

# 3

# 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 |
| Hardware inventory | 445—Outbound | 445—Inbound | NA | NA | 443 (Default port) |
| Health inventory | 445—Outbound | 445—Inbound | NA | NA | 443 (Default port) |
| iDRAC inventory | 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 |

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

# 4

# Manage Dell EMC PowerEdge Servers

Ensure that:

- 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* at Dell.com/OpenManageManuals.
- You have added server connections 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.
- The Redfish service is enabled in the iDRAC before connecting to a server from OMIMSWAC.

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 you have not entered the server credentials while adding the connection, you must enter the credentials when you are connecting to the server by selecting "Manage as".**
3. In the left pane of the Microsoft Windows Admin Center, under EXTENSIONS, click **OpenManage Integration**.
4. To manage the servers, select:
   - **Health Status** to view the health status of the server components. See Health status—Supported server components.
   - **Hardware Inventory** to view the detailed hardware inventory information of the component. See Hardware inventory—Supported server components.
   - **Update Compliance** to view the compliance chart and compliance report of the server components. See Viewing the update compliance of PowerEdge servers and node components of HCI and Failover clusters.
   - **iDRAC** to view the iDRAC details of the server. 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.

**NOTE: A status icon represents the overall health status of the server.**

**NOTE: The health and hardware inventory details are fetched from the devices each time the OpenManage Integration with Windows Admin Center extension is loaded. This might cause a delay in displaying the information.**

**NOTE: For modular servers (12th, 13th, and 14th generation 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 12th and 13th generation of PowerEdge servers with firmware version earlier than 2.60.60.60, information about the following components are not displayed:**

- **Health status—Memory, storage controllers, storage enclosures, and physical disks.**
- **Hardware inventory—Memory, storage controllers, storage enclosures, physical disks, network devices, and firmware.**

### Topics:



# Health status—Supported server components

Health status of the following server components are displayed:

- CPUs
- Memory
- 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.

**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 server components

Hardware inventory of the following server components are displayed:

- System
- Firmware
- CPUs
- Memory
- Storage Controllers
- Storage Enclosures
- Network Devices
- 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.

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

**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.**

**NOTE: Information of few attributes of storage enclosures, firmware inventory, and memory component might not be available for:**

- **12th and 13th generation of PowerEdge servers.**
- **14th generation of PowerEdge servers with iDRAC version lesser than 3.30.30.30.**

# 5

# Manage Azure Stack HCI created with Dell EMC Microsoft Storage Spaces Direct Ready Nodes

Prerequisites:

- 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* at Dell.com/OpenManageManuals.
- You have added hyper-converged cluster connections in Microsoft Windows Admin Center. For more information about adding hyper-converged cluster connections, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center.
- You must ensure that the Redfish service is enabled in the iDRAC before connecting to a server from OMIMSWAC.

To manage the Azure Stack HCI created with Dell EMC Microsoft Storage Spaces Direct Ready Nodes:

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

   **NOTE: If you have not entered the hyper-converged cluster credentials while adding the connection, you must enter the credentials when you are connecting to the hyper-converged cluster by selecting "Manage as".**
3. In the left pane of the Microsoft Windows Admin Center, under EXTENSIONS, click **OpenManage Integration**.
4. To manage the hyper-converged cluster, select:
   - **Health Status** to view the health status of the server components of the individual nodes in the hyper-converged cluster.
     - The **Overall Health Status** section displays the overall health of the Azure Stack HCI cluster. Select different sections in the doughnut chart to filter the health status of the components of the HCI cluster nodes.

       **NOTE: The overall health status of the HCI 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 server components in Azure Stack HCI.
   - **Hardware Inventory** to view the detailed hardware inventory information of the component. On the Overview page, the basic details of the nodes of the hyper-converged cluster are listed. Select the required node to view detailed hardware inventory of the server components. See Hardware inventory—Supported server components in Azure Stack HCI.
   - **Update Compliance** to view the compliance charts of the nodes and components. Expand the required node to view a detailed compliance report of the components. See Viewing the update compliance of PowerEdge servers and node components of HCI and Failover clusters.
   - **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.

**NOTE: The health and hardware inventory details are fetched from the devices each time the OpenManage Integration with Windows Admin Center extension is loaded. This might cause a delay in displaying the details.**

## Topics:

# Health status—Supported server components in Azure Stack HCI

On the Cluster - Azure Stack HCI page, select the **Health Status** tab to view the overall health status of the HCI cluster and the health status of the following server components of the nodes in Azure Stack HCI created with Dell EMC Microsoft Storage Spaces Direct Ready Nodes. 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
- Memory
- 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 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.

**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 server components in Azure Stack HCI

Hardware inventory of the following server components of the nodes in Azure Stack HCI are displayed:

- System
- Firmware
- CPUs
- Memory
- Storage Controllers
- Storage Enclosures
- Network Devices
- 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.

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

**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.**

**NOTE: Information of few attributes of storage enclosures, firmware inventory, and memory component might not be available for:**

- **12th and 13th generation of PowerEdge servers.**
- **14th generation of PowerEdge servers with iDRAC version lesser than 3.30.30.30.**

# 6

# Manage Microsoft Failover Clusters created with PowerEdge servers

Prerequisites:

- 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* at Dell.com/OpenManageManuals.
- You have added failover cluster connections in Microsoft Windows Admin Center. For more information about adding failover cluster connections, see https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center.
- You must ensure that the Redfish service is enabled in the iDRAC before connecting to a server from OMIMSWAC.

To manage the Microsoft failover clusters created with PowerEdge servers:

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

   **NOTE: If you have not entered the failover cluster credentials while adding the connection, you must enter the credentials when you are connecting to the failover cluster by selecting "Manage as".**
3. In the left pane of the Microsoft Windows Admin Center, under EXTENSIONS, click **OpenManage Integration**.
4. To manage the failover cluster, select:
   - **Health Status** to view the health status of the server components of the individual nodes in the failover cluster.
     - The **Overall Health Status** section displays the overall health of the failover cluster. Select different sections in the doughnut chart to filter the health status of the components of the failover cluster nodes.

       **NOTE: The overall health status of the failover 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 server components in Microsoft failover clusters.
   - **Hardware Inventory** to view the detailed hardware inventory information of the component. On the Overview page, the basic details of the nodes of the failover cluster are listed. Select the required node to view detailed hardware inventory of the server components. See Hardware inventory—Supported server components in Microsoft failover clusters.
   - **Update Compliance** to view the compliance charts of the nodes and components. Expand the required node to view a detailed compliance report of the components. See Viewing the update compliance of PowerEdge servers and node components of HCI and Failover clusters.
   - **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.

**NOTE: The health and hardware inventory details are fetched from the devices each time the OpenManage Integration with Windows Admin Center extension is loaded. This might cause a delay in displaying the details.**

## Topics:

# Health status—Supported server components in Microsoft failover clusters

On the Cluster - Dell EMC PowerEdge Server page, select the **Health Status** tab to view the overall health status of the Microsoft failover cluster created with PowerEdge servers and the health status of the following server components of the nodes in Microsoft failover clusters created with PowerEdge servers. 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
- Memory
- 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 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.

**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 server components in Microsoft failover clusters

On the Cluster - Dell EMC PowerEdge Server page, select the **Hardware Inventory** tab to view the hardware inventory details of the following server components of the nodes in Microsoft failover clusters.

- System
- Firmware
- CPUs
- Memory
- Storage Controllers
- Storage Enclosures
- Network Devices
- 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.

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

**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.**

**NOTE: Information of few attributes of storage enclosures, firmware inventory, and memory component might not be available for:**

- **12th and 13th generation of PowerEdge servers.**
- **14th generation of PowerEdge servers with iDRAC version lesser than 3.30.30.30.**

# 7

# 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**, **Hyper-Converged Cluster Manager**, or **Failover 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 **OpenManage Integration** and navigate to the **iDRAC** tab.

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

- iDRAC IP address. You can launch the iDRAC console directly from Microsoft Windows Admin Center.
- IPMI version.
- iDRAC firmware version.

# 8

# Viewing the update compliance of PowerEdge servers and node components of HCI and Failover clusters

By using OpenManage Integration with Windows Admin Center, you can view the update compliance details (firmware, driver, application, and BIOS) of the PowerEdge servers and nodes in a HCI and failover clusters. To view the update compliance details, you must perform the following actions:

1. In the **Settings** tab, specify the system update location information. The OpenManage Integration uses the Dell EMC System Update Utility (DSU) and Dell EMC Inventory Collector (IC) to fetch the firmware details of the devices. For more information on downloading the required applications and configuring the update tools setting, see Configure the update compliance tools setting. The supported versions of the DSU and IC utilities for OpenManage Integration version 1.0 are:
   - DSU version: 1.7.0
   - IC version: 19_04_200_472
2. Under **Update Compliance** > **Update Source**, specify the share location path where the catalog files are placed. The catalog files can be generated by using the Dell EMC Repository Manager (DRM) application. To generate the compliance report of S2D ready nodes, it is recommended that WSSD catalog files are used. For more information on latest update compliance information of the devices, see Generate the update compliance information of PowerEdge servers and node components of HCI and Failover clusters.

In the **Notifications** section of the Windows Admin Center, you are notified if a new catalog file is available in the provided share location. To get the latest update compliance report, run the compliance again by clicking the **Re-run Compliance** button. If a new catalog path is provided, the previous path used to compute the update compliance will not be available.

**Topics:**



# Configure the update compliance tools setting

To view the latest update compliance report and details of the device components, OpenManage Integration requires that you configure the settings for the update compliance tools.

1. In the **Settings** tab, enter the share location where the Dell System Update (DSU) utility is placed. DSU is used to deploy the Dell update packages to PowerEdge servers.
2. Enter the share location where the Dell Inventory Collector (IC) utility is placed. The IC utility is used to collect the hardware inventory information from PowerEdge servers.
3. Enter the user credentials of the share location.

   **NOTE: After OpenManage Integration with Windows Admin Center is uninstalled, the update tool settings will be retained in the Windows Admin Center instance. However, the passwords are not retained.**
4. To confirm if the utilities are accessible, click **Test Connection**.
5. Click **Save** to save the update tools setting.

To view the latest update compliance details of the components, see Generate the update compliance information of PowerEdge servers and node components of HCI and Failover clusters.

**NOTE: The passwords for the update tool settings will be retained only for the current browser session. Ensure to re-enter the password again after you open a new browser session for the Update compliance feature of OpenManage Integration with Microsoft Windows Admin Center to function properly.**

# Generate the update compliance information of PowerEdge servers and node components of HCI and Failover clusters

Before you generate the latest update compliance information of PowerEdge server components and node components in a HCI and failover clusters, ensure that you have:

- Configured the share location details where the Dell EMC System Update Utility and Dell EMC Inventory Collector applications are placed. See Configure the update compliance tools setting.
- Generate the latest catalog files by using the Dell EMC Repository Manager (DRM) application.

To generate the update compliance details of the server components:

1. Under **Update Compliance** > **Update Source**, enter the share location where the .xml catalog files are placed.
2. Enter the user credentials of the share location for OpenManage Integration to access the catalog files.

   **NOTE: You must provide individual catalog files with the user credentials for server manager, hyper converged cluster manager, and failover cluster manager respectively.**
3. Click **Next**.

The update compliance details are computed and the report is available under **Update Compliance** > **Compliance Details**. The doughnut chart represents the number of components in compliant, urgent, recommended, and optional states. The Compliance Report provides a detailed view of all the components with the current and baseline versions of the update type.

For HCI and failover clusters, the update compliance of the individual nodes and the components are represented by using two doughnut charts—Node Summary and Component Summary. To drill down further, expand the individual nodes in the Compliance Report to get the current version and baseline versions of the components, and to view all the nodes and components in non compliant, urgent, recommended, and optional states respectively.

# 9

# Troubleshooting

1. The OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) extension logs of servers and cluster nodes are available at `<Windows Directory>\Temp\OMIMSWAC`. 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*>`

   *ID is an internal identifier assigned when the OMIMSWAC functionalities are run.
2. Unable to copy the required files to fetch inventory information to the target node.

   Possible reasons for failure:
   - Target node is in the reboot state or is powered off.
   - Firewall blocking communication through SMB port 445. For more information, see https://go.microsoft.com/fwlink/?linkid=2101556.
   - The user is not logged in with Gateway Administrative privileges. Before connecting to the target node, ensure that you select "Manage as" and provide appropriate Server Administrator or Cluster Administrator accounts. For more information about selecting "Manage as", see the "Get Started with Windows Admin Center" section in the Microsoft documentation.
3. Unable to fetch the health and hardware inventory from iDRAC.

   Possible reasons for failure:
   - For management of PowerEdge servers, OMIMSWAC uses an internal OS to iDRAC Pass-through interface. By default, iDRAC will be 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 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 support site.
   - The Redfish service is not enabled. Enable the Redfish service by using iDRAC UI. For more information, see the iDRAC documentation on Dell EMC support site.
   - No user slots are available on iDRAC to create new users.
4. The Redfish service might not be accessible because:
   - The USB NIC adapter is disabled on the target node OS.
   - The Redfish service is not enabled on iDRAC.

   To manage the target node by using OpenManage Integration with Microsoft Windows Admin Center, ensure that the USB NIC adapter and Redfish service are enabled on the target node.
5. To manage target nodes with Microsoft Windows Server 2012R2 and earlier versions of OS, see the following Microsoft documentation:
   - Prepare your environment for Windows Admin Center
   - Download and install Windows PowerShell 5.1
6. The update compliance report might not be generated for the cluster nodes.

   Workaround:
   - Ensure that the cluster service is running on the cluster node by using the `Get -ClusterService` PowerShell command.
   - Ensure that the cluster node is not rebooting or in the powered-off state.

# 10

# Contacting Dell EMC

**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.**

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

1. Go to **Dell.com/support.**
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.

# A

# Glossary

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

**Table 3. Glossary**

| Abbreviations/ Acronyms | Definition |
|---|---|
| OMIMSWAC—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, and Hyper-Converged Infrastructure (HCI) created by using the Dell EMC Microsoft Storage Spaces Direct (S2D) Ready Nodes. |
| 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 PowerEdge servers. |
| 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. |
| WSSD catalogs | The firmware and driver update catalogs for Dell EMC Solutions for Azure Stack HCI (S2D catalogs or WSSD catalogs) provides a catalog of all validated versions of the ready node components. |