

Infrastructure Compliance Report for PowerEdge Servers, Azure Stack HCI Clusters using the OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC)

Abstract

This white paper describes the process to generate update compliance report for PowerEdge servers, Microsoft Azure Stack HCI clusters, and Hyper-V based failover clusters by using OMIMSWAC.

November 2019

Revisions

Date	Description
April 2020	Initial release

Acknowledgements

This paper was produced by the following:

Authors:

- Kiranreddy Ballela — Software Senior Engineer, Server and Infrastructure Systems
- Karthik Sethuramalingam — Principal Engineering Technologist, Server and Infrastructure Systems

Support:

Other:

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © April 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [4/7/2020] [Dell EMC Technical White paper]

Table of contents

Revisions.....	2
Acknowledgements.....	2
Table of contents	3
Executive summary.....	4
Intended audience	4
1 Introduction.....	5
2 Step 1: Creating a baseline catalog by using Dell EMC Repository Manager (DRM)	6
3 Step 2: Downloading Dell EMC System Update and Dell EMC Inventory Collector tools	10
4 Step 3: Generating update compliance in OMIMSWAC by using the catalog generated by DRM.....	11

Executive summary

Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) provides a centralized management experience for IT administrators in managing their Microsoft Azure Stack Hyper-Converged Infrastructure (HCI) clusters, Hyper-V based failover clusters, and PowerEdge Servers running. OMIMSWAC simplifies the tasks of IT administrators by remotely managing the PowerEdge servers and clusters throughout their life cycle. Using OMIMSWAC, you can generate a hardware compliance report against a baseline catalog for all the firmware, BIOS and drivers

Intended audience

The intended audience of this document are IT administrators who are using OMIMSWAC to manage Dell EMC 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.

1 Introduction

Dell EMC provides validated catalogs (firmware, driver, application, and BIOS) for PowerEdge Servers, Microsoft Azure Stack HCI Solutions, and Hyper-V based failover solutions. By using OMIMSWAC, you can view the update compliance information against these catalogs for Windows Servers, Azure Stack HCI and Hyper-V based Failover clusters. To view the update compliance details, perform the following actions:

Step 1: [Creating a baseline catalog by using Dell EMC Repository Manager \(DRM\)](#). To generate the compliance report of Dell EMC Solutions for Microsoft Azure Stack HCI, it is recommended that Azure Stack HCI Solution catalog files are used.

Step 2: [Downloading Dell EMC System Update Utility and Dell EMC Inventory Collector tools](#).

Step 3: [Create update compliance report by using OMIMSWAC](#).

The following sections explain each of these steps in detail.

2 Step 1: Creating a baseline catalog by using Dell EMC Repository Manager (DRM)

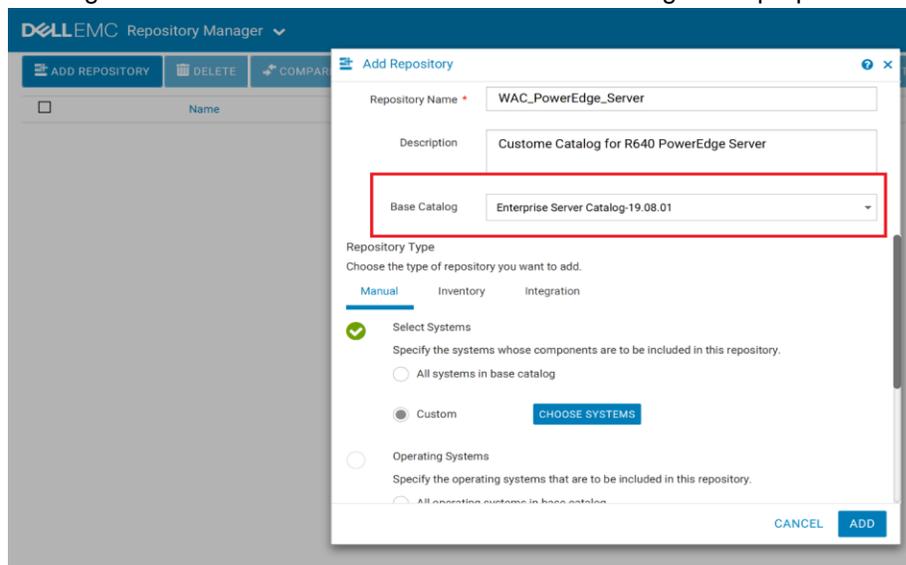
You can use Dell EMC Repository Manager (DRM) to create custom baseline catalogs for your solution (PowerEdge servers, Azure Stack HCI clusters, and Hyper-V based Failover clusters) to generate update compliance report by using OMIMSWAC.

To create a baseline catalog:

1. Download and install the DRM utility from [here](#). For more information about downloading and using DRM, see the *Dell EMC Repository Manager User's Guide*.

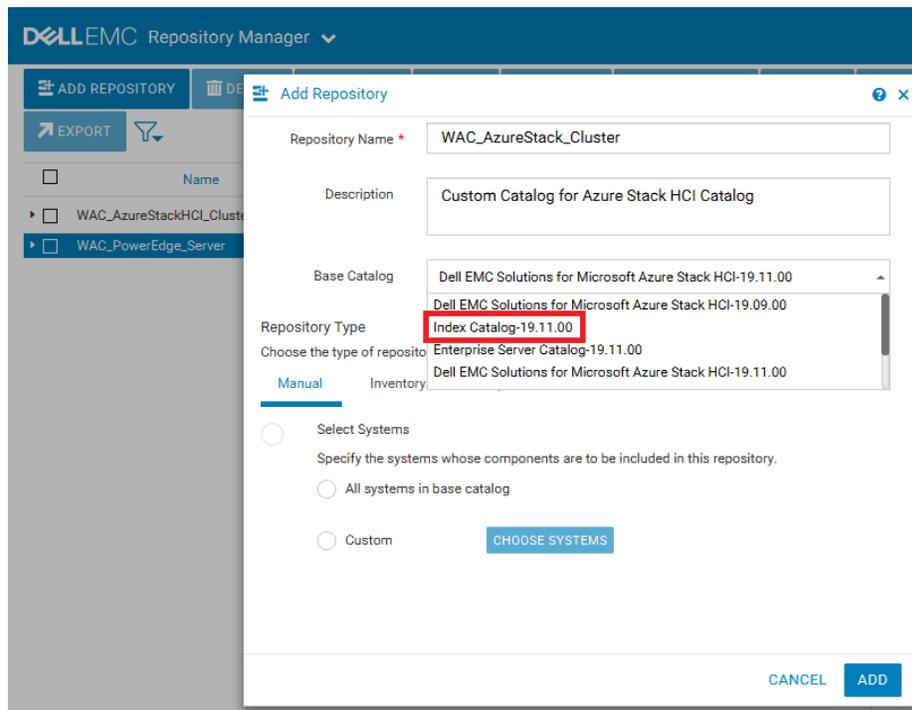
Note: Ensure that the system you are using to download the DRM utility has Internet connectivity.

2. From the **Start** menu, select **Dell EMC Repository Manager**.
3. To create a new repository, click **Add Repository**.
4. Enter a name and description for the new repository.
 - a. For PowerEdge Servers and Hyper-V based failover clusters, use **Enterprise Server Catalog**, which is selected by default in the **Base Catalog** drop-down list. Enterprise Server Catalog contains recommended firmware and driver for general purpose PowerEdge servers.



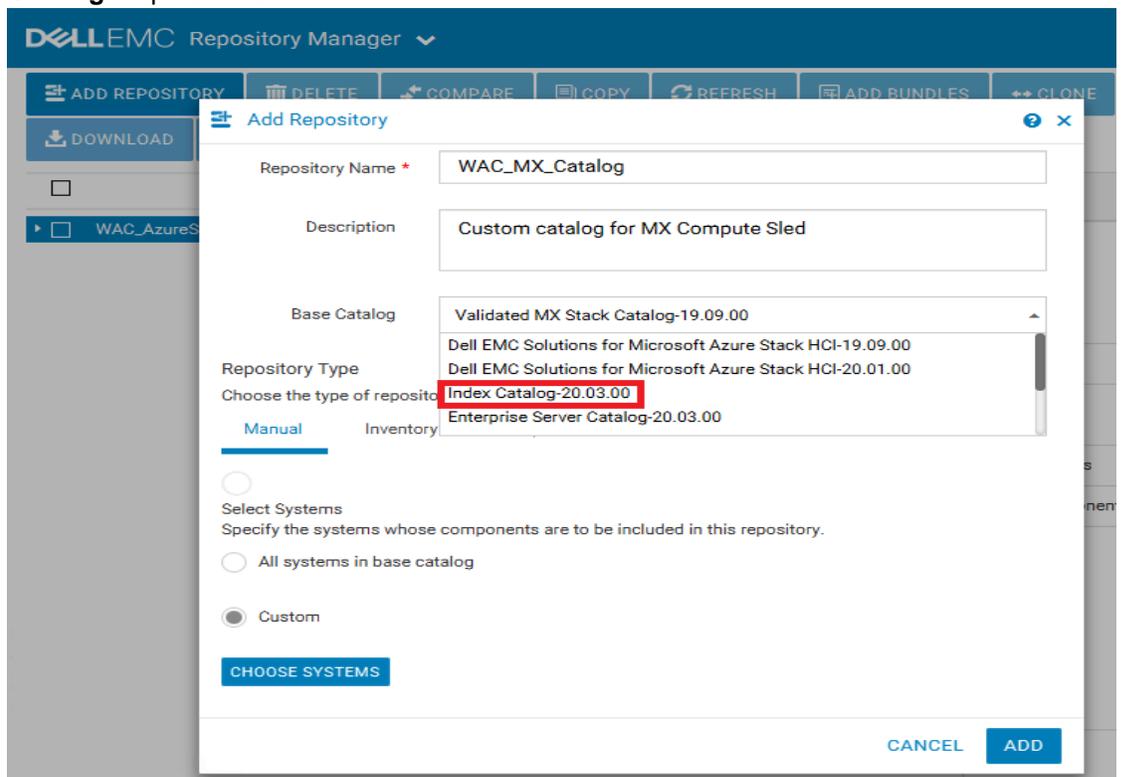
- b. For Azure Stack HCI clusters, Dell EMC provides validated firmware and drivers for Dell EMC Microsoft Storage Spaces Direct (S2D) Ready Nodes. To create validated ASHCI catalog, select **Index Catalog** from the **Base Catalog** drop-down list.

Step 1: Creating a baseline catalog by using Dell EMC Repository Manager (DRM)



Select **Catalog Groups** as **Dell EMC Solutions for Microsoft Azure Stack HCI**.
Select the latest catalog from **Catalogs**, and then click **Save**.

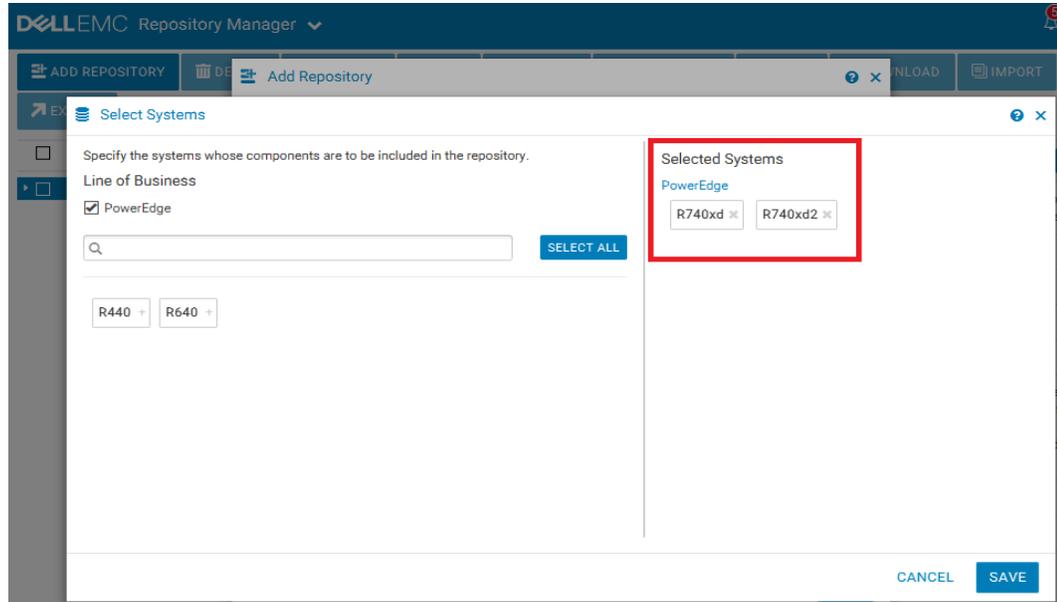
- c. For Modular (MX) PowerEdge servers, Dell EMC provides validated firmware for MX Compute Sleds. To create validated MX catalog, select **Index Catalog** from the **Base Catalog** drop-down list.



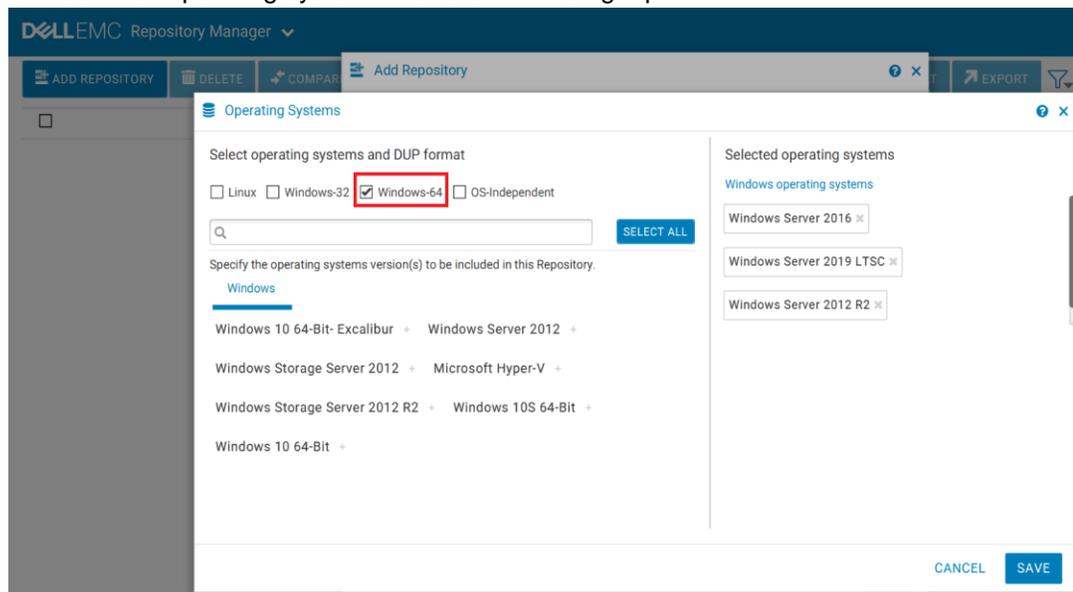
Select **Catalog Groups** as **Validated MX Stack Catalog**.
Select the latest catalog from **Catalogs**, and then click **Save**.

Note: For Azure Stack HCI clusters, it is recommended to use a corresponding catalog with validated firmware, BIOS and drivers.

5. On the **Manual** tab, select **Custom**, and then click **Choose Systems** to include the system models that are to be included in the new repository.
The selected systems are listed on the right pane.

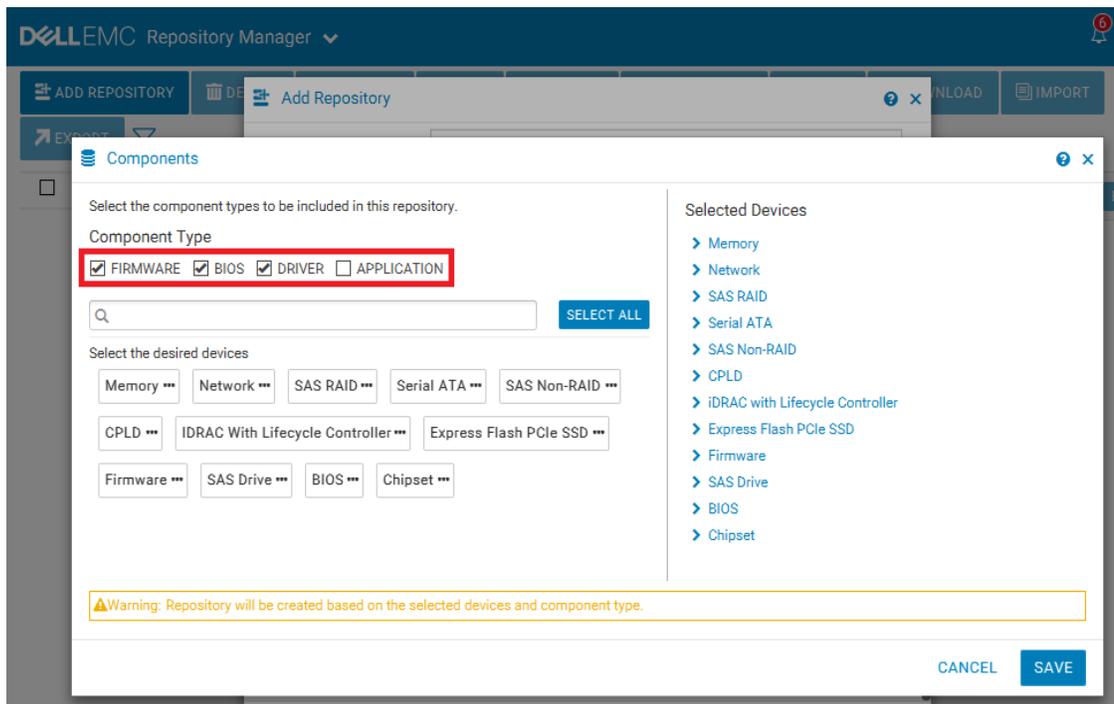


6. Click **Save**.
7. On the **Operating Systems** tab, select **Custom**, and then click **Choose Operating Systems** to include the operating systems that are to be included in the new repository.
The selected operating systems are listed on the right pane.

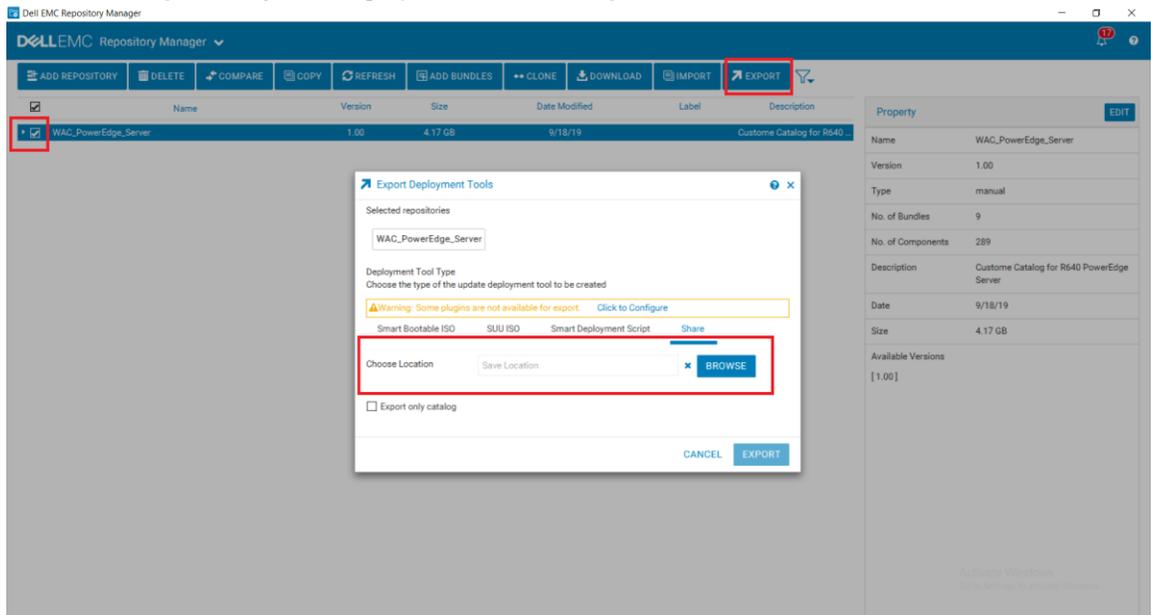


8. Click **Save**.
9. On the **Components** tab, select **Custom**, and then click **Choose Components** to include components that are to be included in the new repository.
The selected components are listed on right pane.

Step 1: Creating a baseline catalog by using Dell EMC Repository Manager (DRM)



10. Click **Save**, and then click **Add**.
11. To download the catalog, select the repository and click **Export**.
12. In the **Export Deployment Tools** window, enter a network file share location (CIFS or NFS).
13. Select the **Export only catalog** option and click **Export**.



Note: The gateway administrator of the Microsoft Windows Admin Center must have access to the selected network file share.

Recommendation: Based on your data center environment, you might require multiple baseline catalogs to compute the compliance. Therefore, it is recommended to name each catalog with an appropriate name to identify the catalogs at a later time.

3 Step 2: Downloading Dell EMC System Update and Dell EMC Inventory Collector tools

To compute the update compliance, OMIMSWAC uses the standard and supported Dell EMC Server Update tools: Dell EMC System Update (DSU) and Dell EMC Inventory Collector (IC). To download the DSU and IC tools:

Note: The following settings are a one-time job for a WAC instance.

1. Install the latest version of OMIMSWAC extension. For installation instructions, see the *Dell EMC OpenManage Integration with Microsoft Windows Admin Center Installation Guide* from [here](#).
2. In the left pane of Windows Admin Center, select **Dell EMC OpenManage Integration**.

DELL EMC OpenManage Integration with Microsoft Windows Admin Center

Cluster - Dell EMC S2D Ready Node (Nodes: 6)

Health Status | Hardware Inventory | iDRAC | Update Compliance | **Settings** | About

Update Tools

Update Tools

Dell EMC System Update Location * ⓘ

❗ Dell EMC System Update (DSU) is a script optimized update deployment tool for applying Dell EMC Update Packages (DUP) to Dell EMC PowerEdge servers. Please download this tool using this [link](#) to a Windows Share and provide the credentials. Ensure that you download DSU of the type: Update Package for Microsoft® Windows® 64-Bit. Supported Version for DSU: 1.7.

Inventory collector location * ⓘ

❗ Dell EMC Inventory Collector (IC) is a utility to collect hardware inventory from Dell EMC PowerEdge servers. Please download this tool using this [link](#) to a Windows Share and provide the credentials.

Username * ⓘ

Password * ⓘ

Test Connection

Save Discard

3. In the **Settings** tab, to download DSU and IC tools, click the corresponding download links and copy the files to a network share (CIFS or NFS) that Gateway Administrator in Windows Admin Center can access.
If required, rename the downloaded files.
4. On the **Update Tools** page, enter the network share paths (including file names) for DSU and IC files.
5. Click **Test connection**, and then click **Save**.
The network share path settings for catalog files are user specific and stored in Windows Admin Center (WAC). It is retained for the next session. The settings will be deleted only when WAC is uninstalled and not when OMIMSWAC extension is uninstalled.

Note: The passwords are encrypted and stored only for the current session in Windows Admin Center. You must enter the password for the next session.

4 Step 3: Generating update compliance in OMIMSWAC by using the catalog generated by DRM

To generate an update compliance report for firmware, BIOS and drivers in OMIMSWAC:

1. In the left pane of Windows Admin Center, click **Dell EMC OpenManage Integration**.
2. Click the **Update Compliance** tab. Under **Update Source**, enter the catalog file share location (suffixed with the catalog file name) and credentials to access the file share location.

For example:

The following screenshot displays Microsoft Azure Stack HCI with the supported Dell EMC S2D Ready Nodes depicting a 6-node cluster

DELL EMC OpenManage Integration with Microsoft Windows Admin Center

Cluster - Dell EMC S2D Ready Node (Nodes: 6)

Health Status | Hardware Inventory | iDRAC | **Update Compliance** | Settings | About |

Update Compliance

1 Update Source 2 Compliance Details

Update Source ⓘ DRM Repository

CIFS share path* ⓘ \\172.18.45.9\clustercatalog\HCI_cluster_catalog.xml

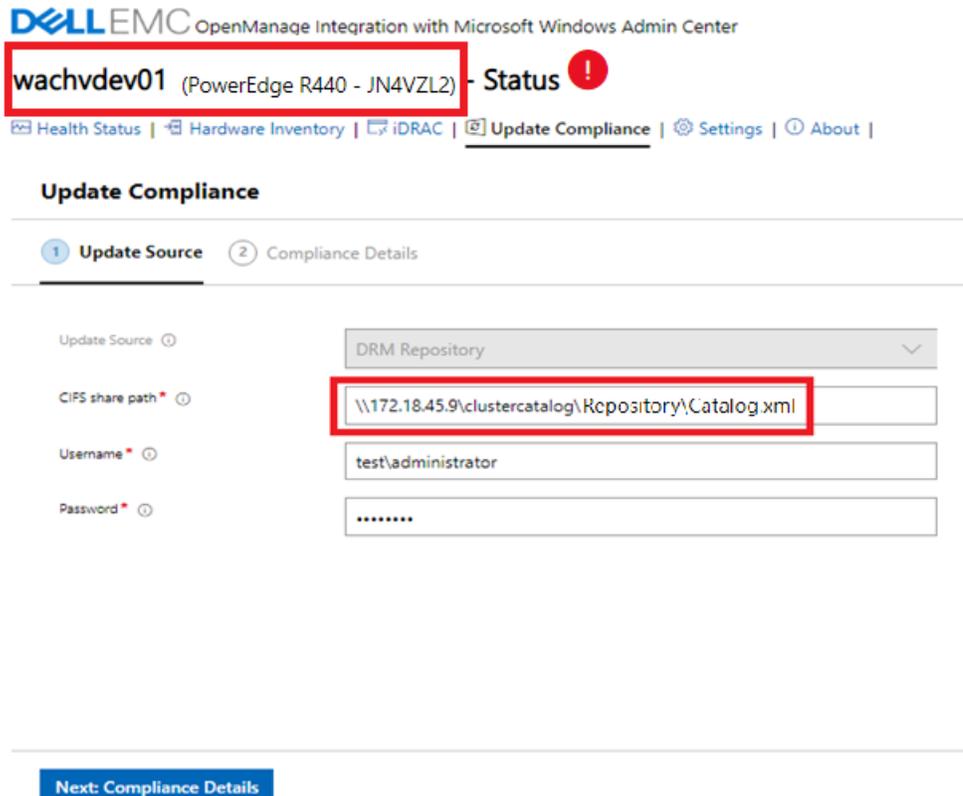
Username* ⓘ test\administrator

Password* ⓘ

Next: Compliance Details

User provides catalog details to generate comparison report for Azure Stack HCI cluster.

The following screenshot displays PowerEdge Servers supported on Microsoft Windows Server



User provides catalog details to generate comparison report for general purpose PowerEdge server.

It is recommended that you select the appropriate catalog for different types of solutions: PowerEdge servers, Hyper-V based Failover clusters, and Microsoft Azure Stack HCI clusters. For more information, see [Step 1: Creating a baseline catalog by using Dell EMC Repository Manager \(DRM\)](#).

3. To generate the update compliance, click **Next**.
The Update Compliance job runs in the background. While the job runs in the background, you can continue to use other features of OMIMSWAC.
You are notified after the update compliance report is generated.
4. To view the compliance report, click the **Update Compliance** tab.

Step 3: Generating update compliance in OMIMSWAC by using the catalog generated by DRM

Update Compliance

Update Source | Compliance Details

Cluster Summary



Component Compliance Summary



Re-run Compliance

Compliance Report

(Generated at: 2019-11-12 05:38:16 PM)

Component Name	Compliance	Criticality ↓	Current Version	Baseline Version	Type
Intel(R) Chipset INF	Compliant		10.1.17861.8101	10.1.17861.8101	Driver
Integrated Remote Access Controller	Non-Compliant	Recommended	3.34.34.34	3.36.36.36	Firmware
BIOS	Compliant		2.3.10	2.3.10	BIOS
Disk 0 of BOSS-S1 Adapter	Compliant		DL43	DL43	Firmware
System CPLD	Compliant		1.0.6	1.0.6	Firmware
Disk 2 in Backplane 1 of Dell HBA330 ...	Compliant		NT32	NT32	Firmware
Driver for Marvell Unify Configuration	Compliant		1.2.0.1048	1.2.0.1048	Driver
Dell HBA330 Mini Driver	Compliant		2.51.25.2	2.51.25.02	Driver
Disk 0 in Backplane 1 of Dell HBA330 ...	Compliant		AS0E	AS0E	Firmware
Dell HBA330 Mini Controller 0 Firmw...	Compliant		16.17.00.05	16.17.00.05	Firmware
BOSS-S1	Compliant		2.5.13.3022	2.5.13.3022	Firmware
Mellanox ConnectX-4 LX Dual Port 25...	Compliant		14.25.10.20	14.25.10.20	Firmware
Disk 0 in Backplane 1 of Dell HBA330 ...	Compliant		AS0E	AS0E	Firmware
Driver for Marvell Unify Configuration	Compliant		1.2.0.1048	1.2.0.1048	Driver
Dell HBA330 Mini Driver	Compliant		2.51.25.2	2.51.25.02	Driver
Dell HBA330 Mini Controller 0 Firmw...	Compliant		16.17.00.05	16.17.00.05	Firmware
Integrated Remote Access Controller	Non-Compliant	Recommended	3.34.34.34	3.36.36.36	Firmware

Exit

To filter the compliance based on the criticality, click the respective sections on the doughnut chart. The compliance report will also be filtered to display only the selected critical components. To clear the filter, click the **Clear Filter** icon next to the search box.

To generate the compliance report later, click **Re-run Compliance**. The timestamp of the latest compliance report is displayed below the title of the compliance report.

Note: The Update Compliance feature of OMIMSWAC is supported on host with Microsoft Windows Server 2012 R2 and later.

After the update compliance is generated, OMIMSWAC saves the information of the baseline catalog used for each solution. If there are updates to the DRM catalogs from the previous version, you are automatically notified in the OMIMSWAC extension.

Step 3: Generating update compliance in OMIMSWAC by using the catalog generated by DRM

The screenshot displays the Dell EMC OpenManage Integration with Microsoft Windows Admin Center interface. The main section shows the 'Health Status' for a cluster of 2 Dell EMC S2D Ready Nodes. The overall health status is 'Critical', indicated by a red circle with the number '2' inside. Below this, there are three donut charts: 'Nodes' (2 Critical, 0 Warning, 0 Unknown, 0 Healthy), 'CPUs' (4 Healthy, 0 Warning, 0 Critical), and 'Memory' (24 Healthy, 0 Warning, 0 Critical). A 'Notification details' panel on the right shows a message: 'A new catalog file is available. Run Update Compliance again by providing the new catalog path to get the latest report.'

Dell EMC OpenManage Integration with Microsoft Windows Admin Center
Cluster - Dell EMC S2D Ready Node (Nodes: 2)

Health Status | Hardware Inventory | iDRAC | Update Compliance | Settings | About

Health Status

Overall Health Status 1

Nodes: 2 (Critical), 0 (Warning), 0 (Unknown), 0 (Healthy)

CPUs: 4 (Healthy), 0 (Warning), 0 (Critical)

Memory: 24 (Healthy), 0 (Warning), 0 (Critical)

Notification details:
Update Compliance_Update Source
6:10:07 AM
Source: [Go to Dell EMC OpenManage Integration.](#)
Type: Information
Message: A new catalog file is available. Run Update Compliance again by providing the new catalog path to get the latest report.

The generated update compliance report assists the IT administrators to understand the update requirements and plan their update cycles effectively. IT administrators can use the iDRAC or Dell Server Update (DSU) utility to update their data center environments with the latest updates and keep their environment secure.

Note: With Microsoft System Center Virtual Machine Manager, once the Update Compliance report is obtained from OMIMSWAC, administrators can use the Dell EMC OpenManage Integration for Microsoft System Center (OMIMSSC) for System Center Virtual Machine Manager to remediate their Clusters and PowerEdge Servers including Cluster Aware Firmware Update for their distributed data center environments.