A Dell EMC Technical White paper

Update firmware, BIOS, and drivers using Cluster-Aware Updating (CAU) in OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC)

Abstract

This white paper provides information about creating catalogs, generating compliance report, and updating PowerEdge servers, Microsoft Azure Stack HCI clusters, and Hyper-V based failover clusters by using OMIMSWAC.

May 2021

Revisions

Date	Description
May 24, 2021	Update Dell infrastructure using OMIMSWAC

Acknowledgements

This paper was produced by the following:

Authors:

- Gopayya Devarakonda —Software Senior Engineer, Server and Infrastructure Systems
- Karthik Sethuramalingam — Principal Engineering Technologist, Server and Infrastructure Systems

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.

Table of contents

Executive summary

Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) provides a centralized management experience for IT administrators in managing their Dell EMC Integrated System for Azure Stack HCI, Dell EMC HCI Solutions for Microsoft Windows Server, Hyper-V based failover clusters, and PowerEdge Servers as hosts. 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 PowerEdge servers as hosts, Microsoft Failover Clusters created with PowerEdge servers, Dell EMC Integrated System for Microsoft Azure Stack HCI created using AX nodes from Dell Technologies, and Hyper-Converged Infrastructure (HCI) created by using 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.

1. Introduction

Dell EMC provides validated catalogs (firmware, driver, application, and BIOS) for PowerEdge Servers, Dell EMC Integrated System for Microsoft Azure Stack HCI, Dell EMC HCI Solutions for Microsoft Windows Server, and Hyper-V based failover solutions. By using OMIMSWAC, you can view the update compliance information against these catalogs for Windows Server HCI, 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 Update Catalog for Microsoft HCI solutions files are used.

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

Step 3: Updating Nodes of Windows Server HCI, Azure Stack HCI, and Failover clusters

The following sections explain each of these steps in detail.

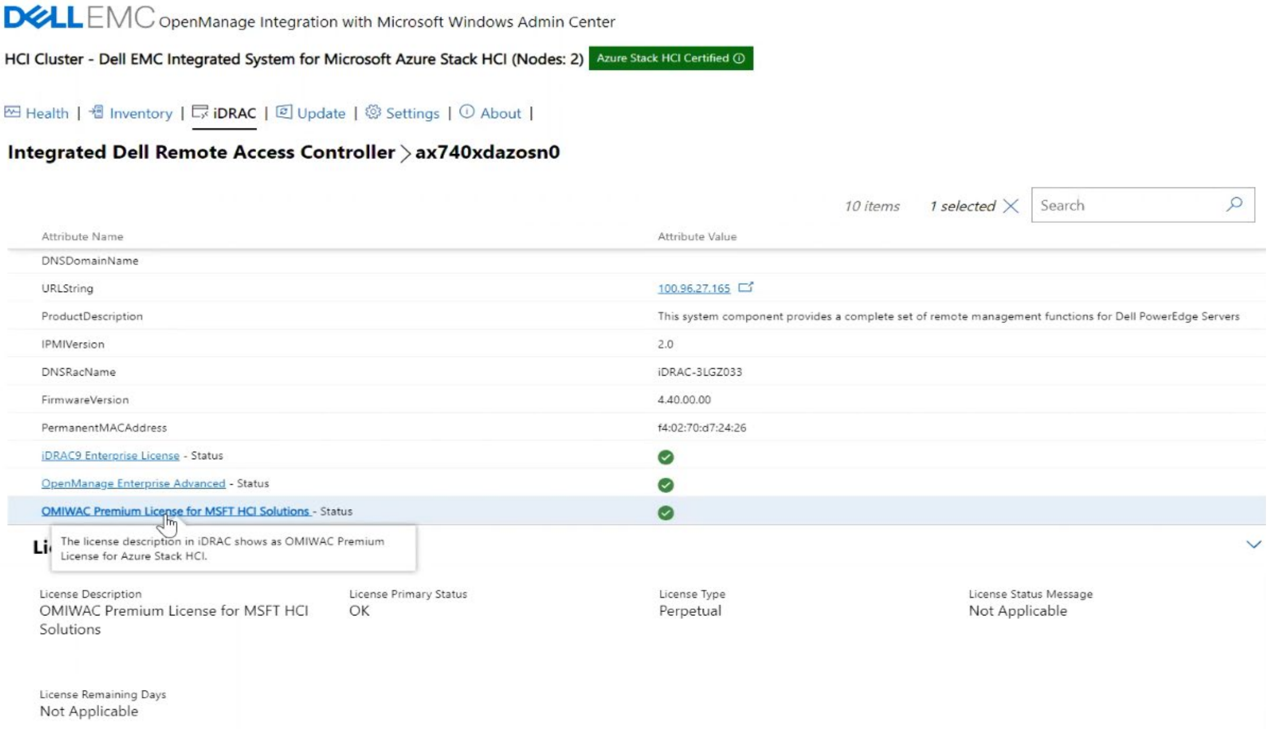
2. Verify license details

In OMIMSWAC, you can view node details and their licenses from the iDRAC inventory. The iDRAC inventory attributes are optimized to improve usability.

To verify licenses,

1. In Windows Admin Center, connect to a server or cluster.
2. In the left pane of Windows Admin Center, under **EXTENSIONS**, click Dell EMC OpenManage Integration.
3. Click the **iDRAC** tab to view licenses installed on each node.
4. To view license details, click on a license attribute name. For example, iDRAC9 Enterprise License, OpenManage Enterprise Advanced, OMIWAC Premium License for MSFT HCI Solutions, and more.

Note: AX nodes by default include OMIWAC Premium license part of the base solution.



DELL EMC OpenManage Integration with Microsoft Windows Admin Center

HCI Cluster - Dell EMC Integrated System for Microsoft Azure Stack HCI (Nodes: 2) Azure Stack HCI Certified ⓘ

Integrated Dell Remote Access Controller > ax740xdazosn0

10 items   1 selected ✕   Search

Attribute Name	Attribute Value
DNSDomainName	
URLString	100.96.27.165
ProductDescription	This system component provides a complete set of remote management functions for Dell PowerEdge Servers
IPMIVersion	2.0
DNSRacName	iDRAC-3LGZ033
FirmwareVersion	4.40.00.00
PermanentMACAddress	f4:02:70:d7:24:26
iDRAC9 Enterprise License - Status	✓
OpenManage Enterprise Advanced - Status	✓
OMIWAC Premium License for MSFT HCI Solutions - Status	✓

Li

The license description in iDRAC shows as OMIWAC Premium License for Azure Stack HCI.

License Description	License Primary Status	License Type	License Status Message
OMIWAC Premium License for MSFT HCI Solutions	OK	Perpetual	Not Applicable

License Remaining Days
Not Applicable

Figure 1: Verify License Details

Ensure that OMIWAC premium licenses are installed on all cluster nodes to use the CAU feature.

NOTE: All target nodes part of the cluster must have valid licenses, otherwise, you cannot proceed to update the cluster. For more information about OMIWAC premium licensing, refer to OMIMSWAC Installation Guide.

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

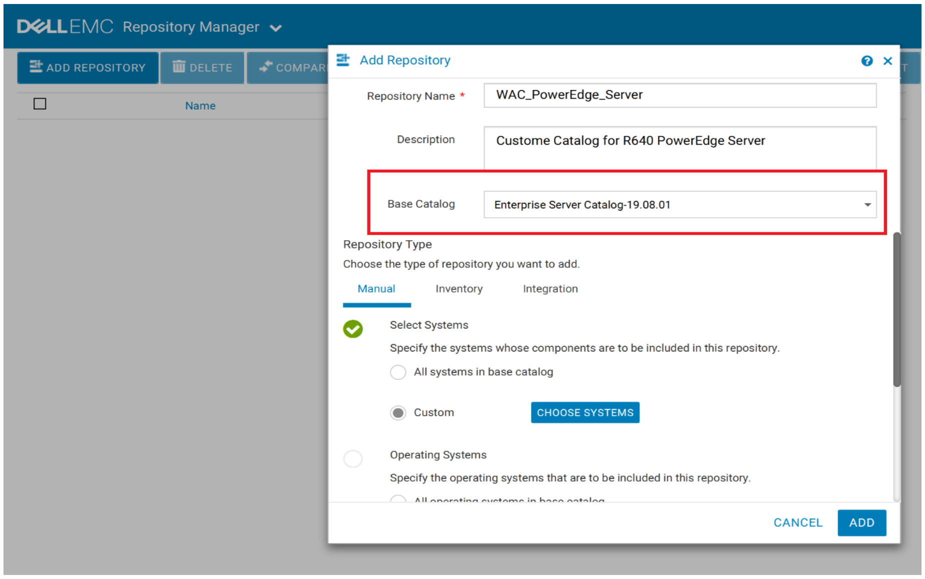
You can use Dell EMC Repository Manager (DRM) to create custom baseline catalogs for your solution (PowerEdge servers, Azure Stack HCI clusters, and Hyper-V based Failover clusters) for generating update compliance report by using OMIMSWAC.

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.



Repository Name * WAC_PowerEdge_Server

Description Custome Catalog for R640 PowerEdge Server

Base Catalog Enterprise Server Catalog-19.08.01

Repository Type

Choose the type of repository you want to add.

Manual Inventory Integration

Select Systems

Specify the systems whose components are to be included in this repository.

○ All systems in base catalog

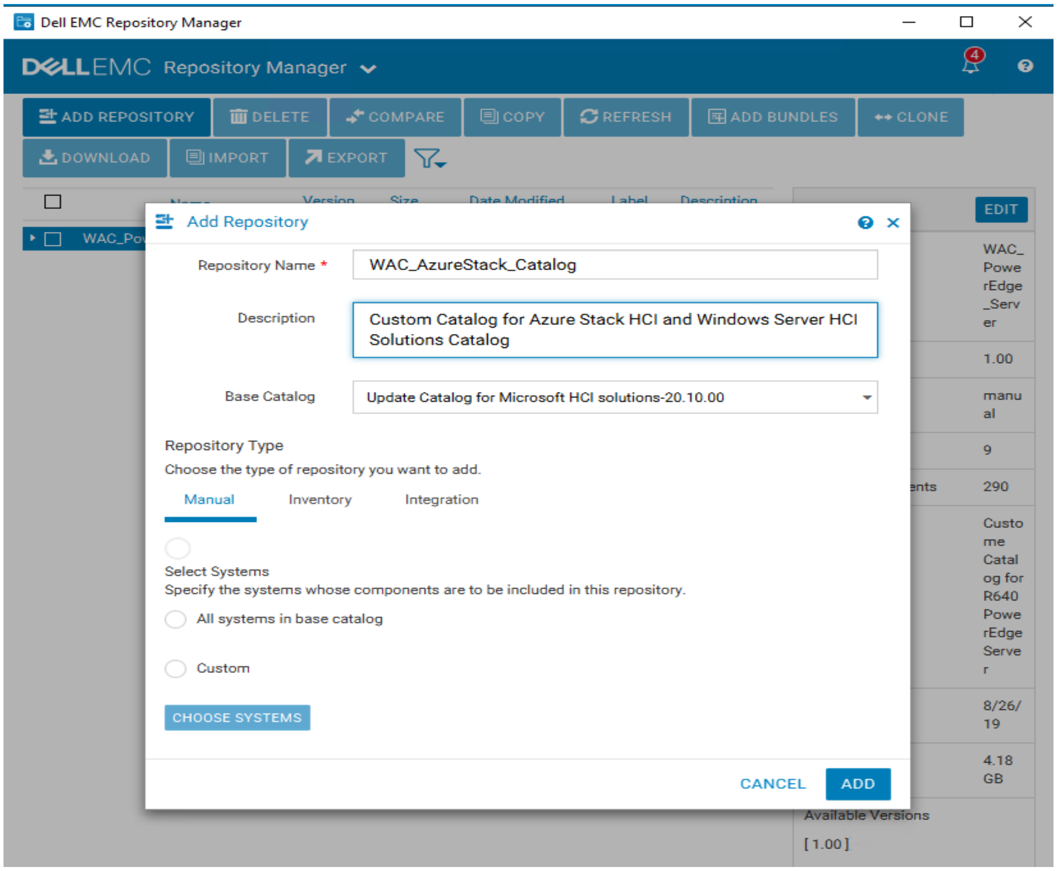
● Custom

Operating Systems

Specify the operating systems that are to be included in this repository.

Figure 2: Add repository in DRM

   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 a validated ASHCI catalog, select **Index Catalog** from the **Base Catalog** drop-down list.



Add Repository

Repository Name * WAC_AzureStack_Catalog

Description: Custom Catalog for Azure Stack HCI and Windows Server HCI Solutions Catalog

Base Catalog: Update Catalog for Microsoft HCI solutions-20.10.00

Repository Type

Choose the type of repository you want to add.

Manual | Inventory | Integration

Select Systems

Specify the systems whose components are to be included in this repository.

○ All systems in base catalog

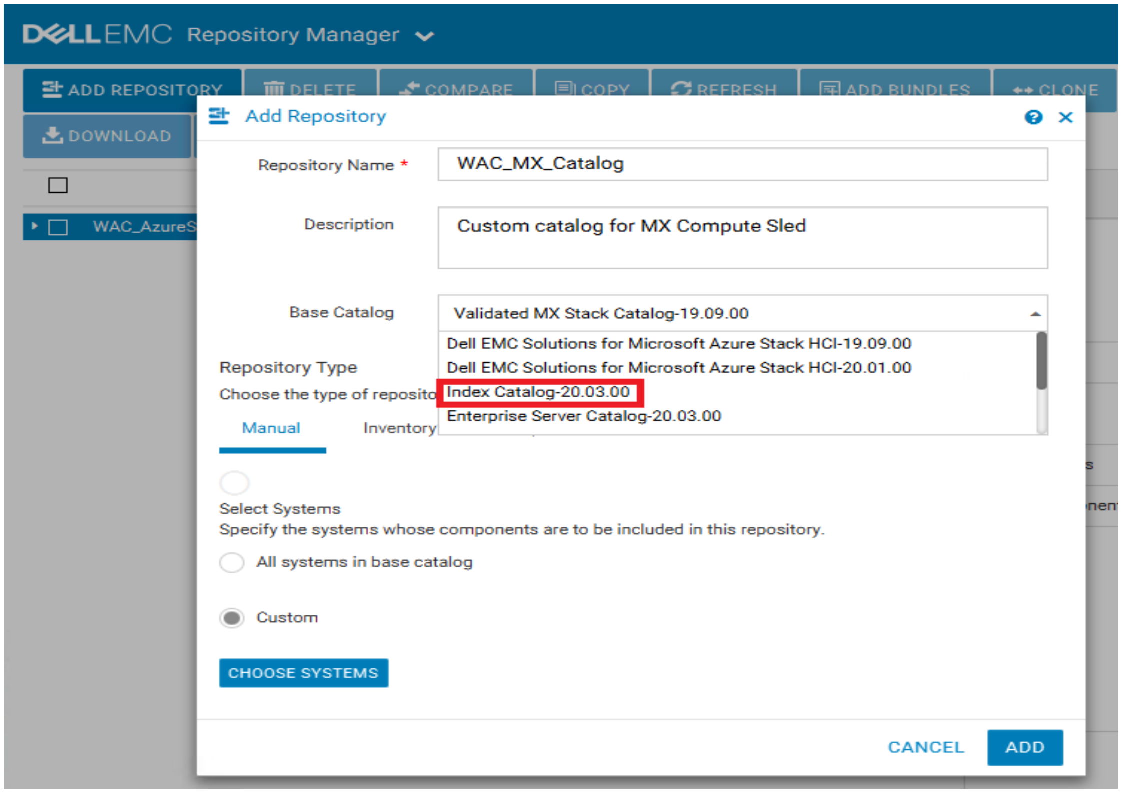
○ Custom

Figure 3: Add repository in DRM

i Select **Catalog Groups** as **Update catalog for Microsoft HCI solutions**.

ii 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.



Add Repository

Repository Name * WAC_MX_Catalog

Description: Custom catalog for MX Compute Sled

Base Catalog: Validated MX Stack Catalog-19.09.00

- Dell EMC Solutions for Microsoft Azure Stack HCI-19.09.00
- Dell EMC Solutions for Microsoft Azure Stack HCI-20.01.00
- Index Catalog-20.03.00
- Enterprise Server Catalog-20.03.00

Repository Type

Choose the type of reposito

Manual | Inventory

Select Systems

Specify the systems whose components are to be included in this repository.

○ All systems in base catalog

● Custom

CHOOSE SYSTEMS

CANCEL ADD

Figure 4: Add repository in DRM

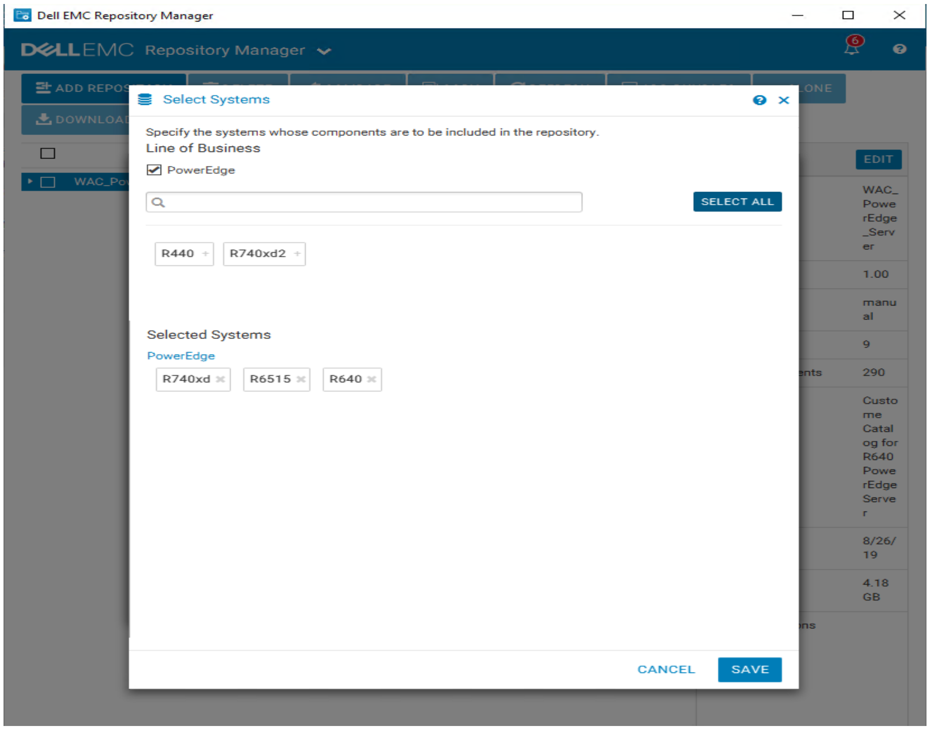
i Select **Catalog Groups** as **Validated MX Stack Catalog**.

ii 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 or below pane.



Select Systems

Specify the systems whose components are to be included in the repository.

Line of Business

☑ PowerEdge

R440 + R740xd2 +

Selected Systems

PowerEdge

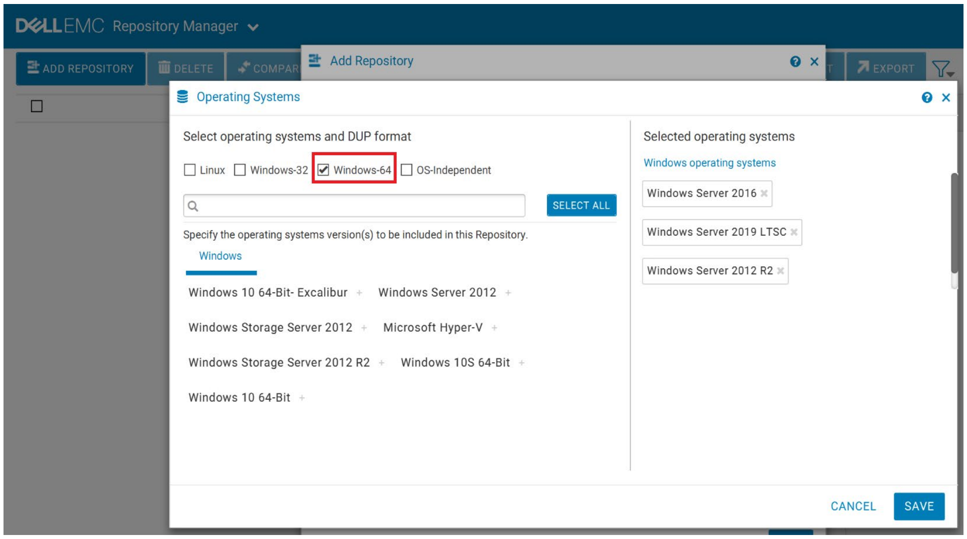
R740xd × R6515 × R640 ×

Figure 5: Choose system in DRM

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.



Operating Systems

Select operating systems and DUP format

☐ Linux ☐ Windows-32 ☑ Windows-64 ☐ OS-Independent

Specify the operating systems version(s) to be included in this Repository.

Windows 10 64-Bit- Excalibur + Windows Server 2012 +
Windows Storage Server 2012 + Microsoft Hyper-V +
Windows Storage Server 2012 R2 + Windows 10S 64-Bit +
Windows 10 64-Bit +

Selected operating systems

Windows operating systems

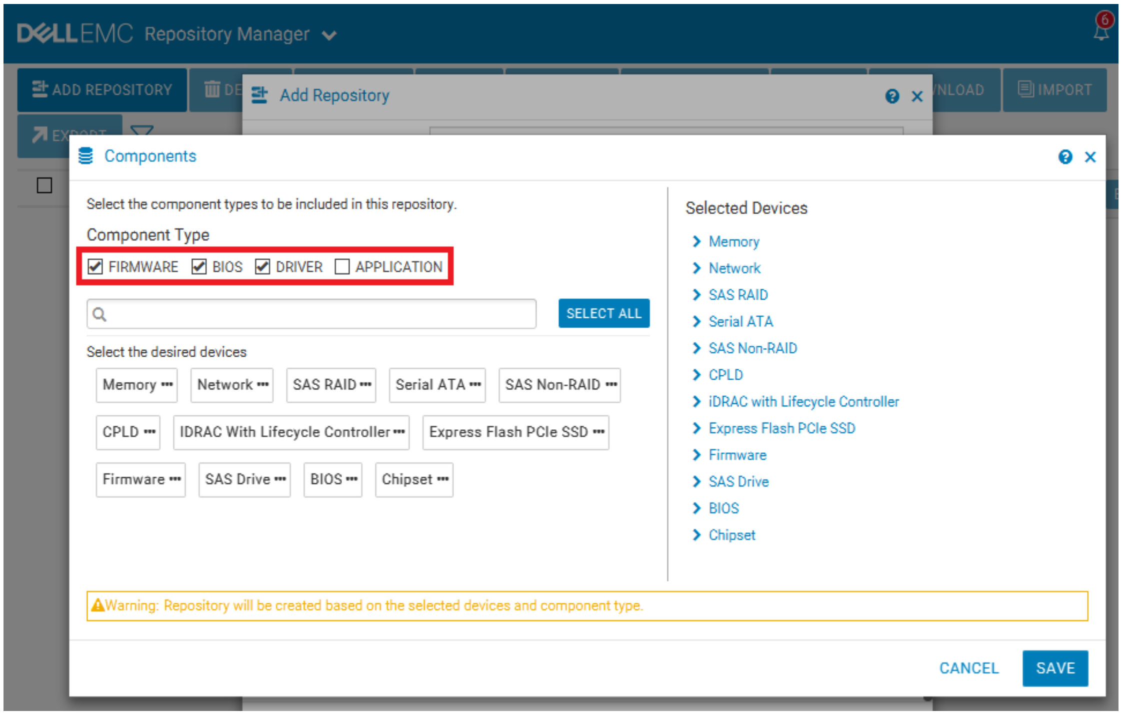
Windows Server 2016 ×
Windows Server 2019 LTSC ×
Windows Server 2012 R2 ×

Figure 6: Choose operating system in DRM

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.



Select the component types to be included in this repository.

Component Type

☑ FIRMWARE ☑ BIOS ☑ DRIVER ☐ APPLICATION

Selected Devices

- Memory
- Network
- SAS RAID
- Serial ATA
- SAS Non-RAID
- CPLD
- iDRAC with Lifecycle Controller
- Express Flash PCIe SSD
- Firmware
- SAS Drive
- BIOS
- Chipset

⚠Warning: Repository will be created based on the selected devices and component type.

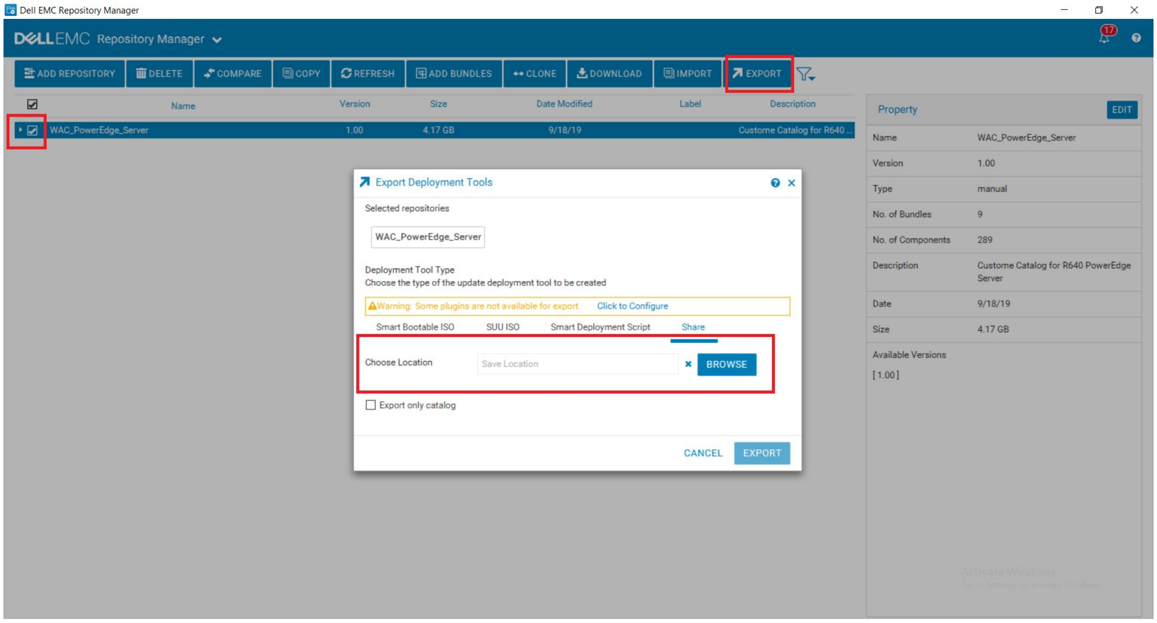
Figure 7: Choose components in DRM

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 Repository** option and click **Export**.



☑	Name	Version	Size	Date Modified	Label	Description
☑	WAC_PowerEdge_Server	1.00	4.17 GB	9/18/19		Custome Catalog for R640 ...

Export Deployment Tools

Selected repositories

WAC_PowerEdge_Server

Deployment Tool Type
Choose the type of the update deployment tool to be created

Warning: Some plugins are not available for export. Click to Configure

Smart Bootable ISO SUU ISO Smart Deployment Script Share

Choose Location: Save Location

☐ Export only catalog

Property	
Name	WAC_PowerEdge_Server
Version	1.00
Type	manual
No. of Bundles	9
No. of Components	289
Description	Custome Catalog for R640 PowerEdge Server
Date	9/18/19
Size	4.17 GB
Available Versions [1.00]	

Figure 8: Export in DRM

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

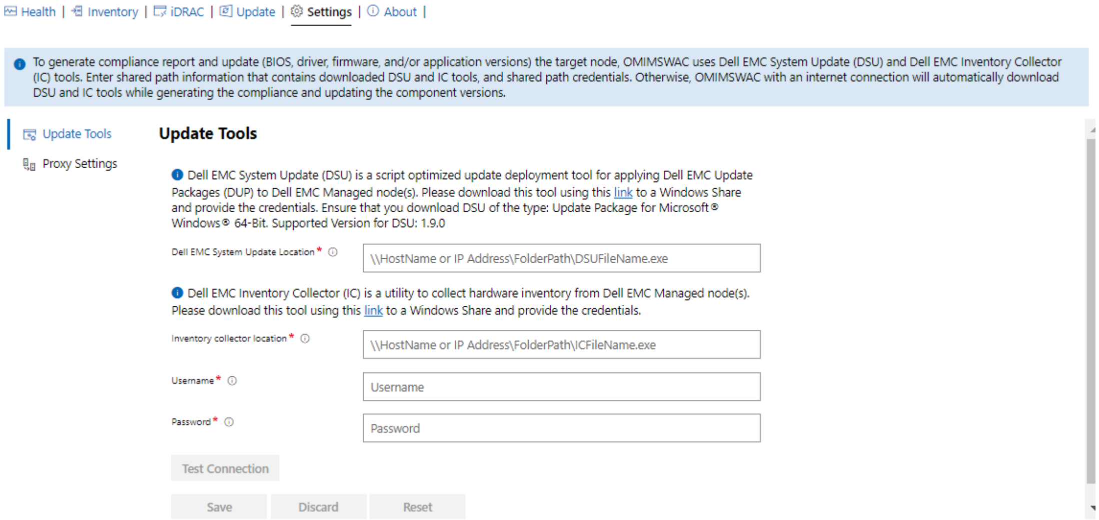
Recommendation: Based on your data center environment, you might require multiple baseline catalogs to compute the compliance. Therefore, it is recommended to name each catalog with an appropriate name to identify the catalogs at a later time.

4. 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.

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**.



To generate compliance report and update (BIOS, driver, firmware, and/or application versions) the target node, OMIMSWAC uses Dell EMC System Update (DSU) and Dell EMC Inventory Collector (IC) tools. Enter shared path information that contains downloaded DSU and IC tools, and shared path credentials. Otherwise, OMIMSWAC with an internet connection will automatically download DSU and IC tools while generating the compliance and updating the component versions.

Update Tools

Dell EMC System Update (DSU) is a script optimized update deployment tool for applying Dell EMC Update Packages (DUP) to Dell EMC Managed node(s). 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: 1.9.0

Dell EMC System Update Location * : \\HostName or IP Address\FolderPath\DSUFileName.exe

Dell EMC Inventory Collector (IC) is a utility to collect hardware inventory from Dell EMC Managed node(s). Please download this tool using this link to a Windows Share and provide the credentials.

Inventory collector location * : \\HostName or IP Address\FolderPath\ICFileName.exe

Username * : Username

Password * : Password

Figure 9: Update Tools to specify DSU and IC in OMIMSWAC

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.

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.

5. Step 3: Updating Nodes of Windows Server HCI, Azure Stack HCI, and Failover clusters

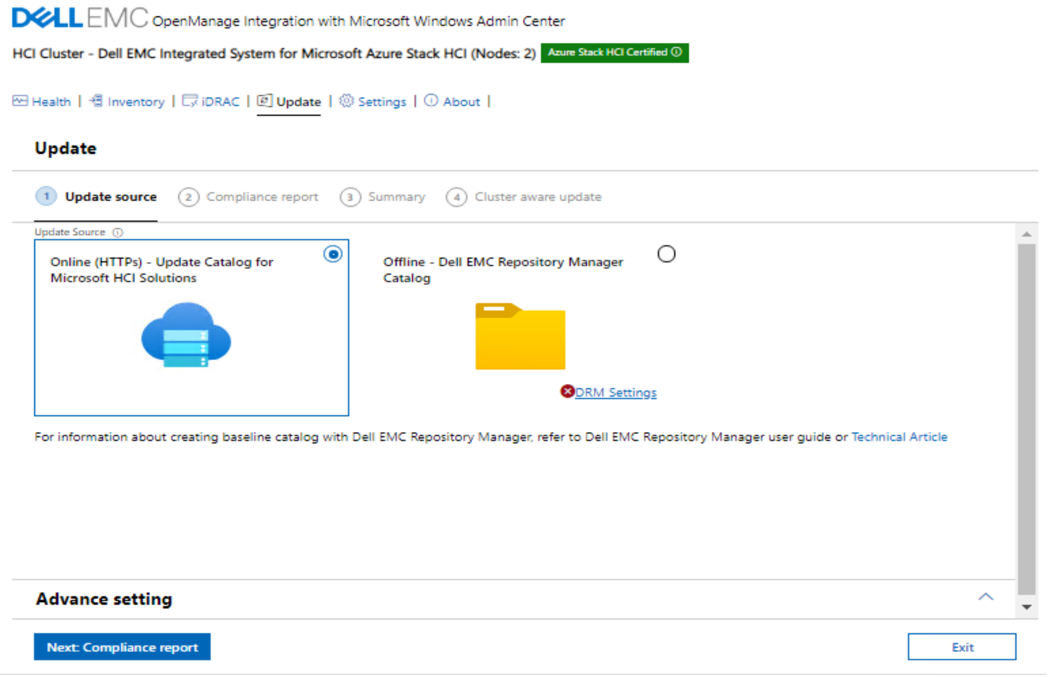
OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) allows you to generate compliance details and update components, such as BIOS, driver, firmware, and/or system management applications of target nodes and nodes in an HCI and failover clusters. You can use either an online or offline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

Additionally, for Azure Stack HCI, hyperconverged infrastructure (HCI) operating system , if you want to do a full stack update which includes OS patches, Security updates, Drivers, Firmware, BIOS you can use the Full stack update by invoking the OpenManage Integration snap-in for more info see the Dell EMC OpenManage Integration with Microsoft Windows Admin Center User's Guide from here.

5.1 Update using online (HTTPs) catalog

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

1. In the left pane of Windows Admin Center, under **EXTENSIONS**, click **Dell EMC OpenManage Integration**.
2. Click the **Update** tab, and then under **Update Source**, select "Online (HTTPs) – <catalog name>". By default, Online Catalog is selected.



OpenManage Integration with Microsoft Windows Admin Center

HCI Cluster - Dell EMC Integrated System for Microsoft Azure Stack HCI (Nodes: 2)

Update Source

● Online (HTTPs) - Update Catalog for Microsoft HCI Solutions

○ Offline - Dell EMC Repository Manager Catalog

For information about creating baseline catalog with Dell EMC Repository Manager, refer to Dell EMC Repository Manager user guide or Technical Article

Figure 10: Select update source in OMIMSWAC

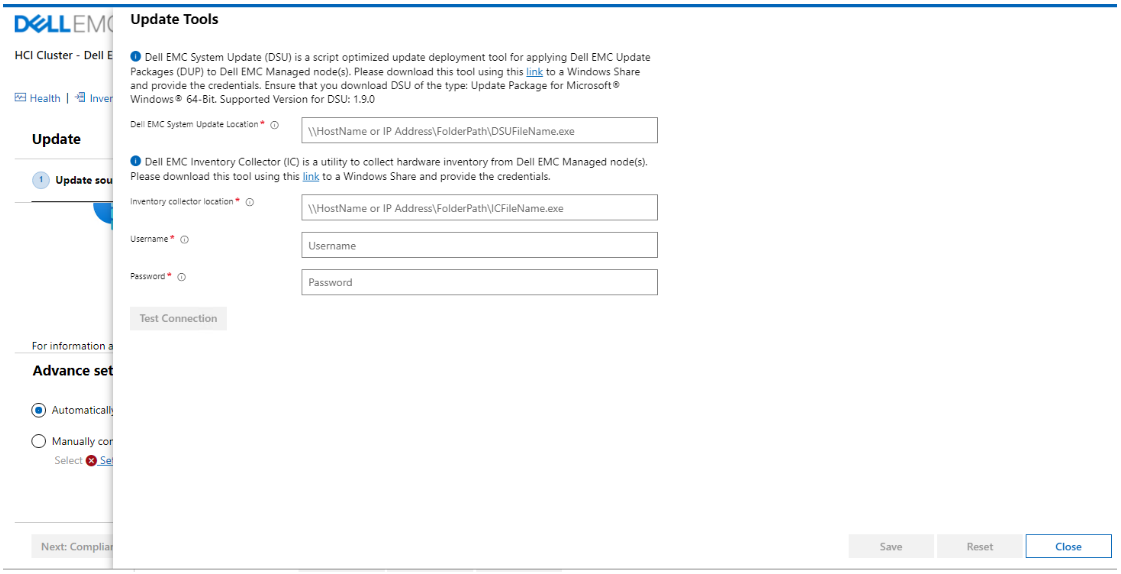
DSU and IC settings, configured using Update Tool settings in OpenManage Integration extension will also be available under **Advance setting**.

a) To use the Dell EMC System Update (DSU) and Inventory Collector (IC) tools, in **Advance setting,** select one of the followings:

- **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.

  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.

- **Manually configure DSU and IC** 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. For more information, see Step 2: Downloading Dell EMC System Update and Dell EMC Inventory Collector tools.



Update Tools

Dell EMC System Update (DSU) is a script optimized update deployment tool for applying Dell EMC Update Packages (DUP) to Dell EMC Managed node(s). 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: 1.9.0

Dell EMC System Update Location * \\HostName or IP Address\FolderPath\DSUFileName.exe

Dell EMC Inventory Collector (IC) is a utility to collect hardware inventory from Dell EMC Managed node(s). Please download this tool using this link to a Windows Share and provide the credentials.

Inventory collector location * \\HostName or IP Address\FolderPath\ICFileName.exe

Username * Username

Password * Password

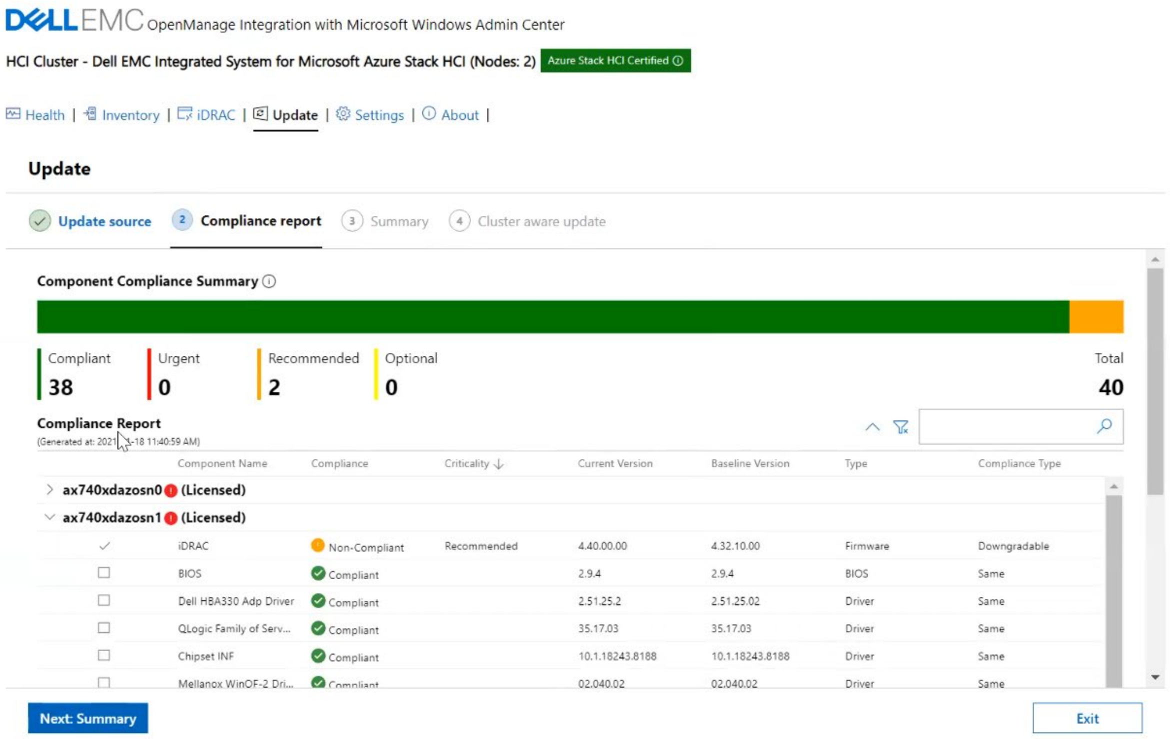
Figure 11: Update Tools via Advance settings to specify DSU and IC in OMIMSWAC

3. To generate the update compliance, click **Next Compliance Report**.

   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 will be notified after the update compliance report is generated.

   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. To view the compliance report, click the **Update** tab.


DELLEMC OpenManage Integration with Microsoft Windows Admin Center
Health | Inventory | iDRAC | Update | Settings | About |
Update source
2 Compliance report
3 Summary
4 Cluster aware update
Next: Summary
Exit

HCI Cluster - Dell EMC Integrated System for Microsoft Azure Stack HCI (Nodes: 2) Azure Stack HCI Certified

Update

Component Compliance Summary

Compliant	Urgent	Recommended	Optional	Total
38	0	2	0	40

Compliance Report
(Generated at: 2021[illegible]-18 11:40:59 AM)

	Component Name	Compliance	Criticality ↓	Current Version	Baseline Version	Type	Compliance Type
› ax740xdazosn0 ● (Licensed)							
⌄ ax740xdazosn1 ● (Licensed)							
✓	iDRAC	● Non-Compliant	Recommended	4.40.00.00	4.32.10.00	Firmware	Downgradable
☐	BIOS	✓ Compliant		2.9.4	2.9.4	BIOS	Same
☐	Dell HBA330 Adp Driver	✓ Compliant		2.51.25.2	2.51.25.02	Driver	Same
☐	QLogic Family of Serv...	✓ Compliant		35.17.03	35.17.03	Driver	Same
☐	Chipset INF	✓ Compliant		10.1.18243.8188	10.1.18243.8188	Driver	Same
☐	Mellanox WinOF-2 Dri...	✓ Compliant		02.040.02	02.040.02	Driver	Same

Figure 12: 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.

Note: To perform Cluster Aware Updates (CAU), all nodes in the cluster must have valid OMIWAC premium licenses. For more information about licensing, see OMIMSWAC Installation Guide.

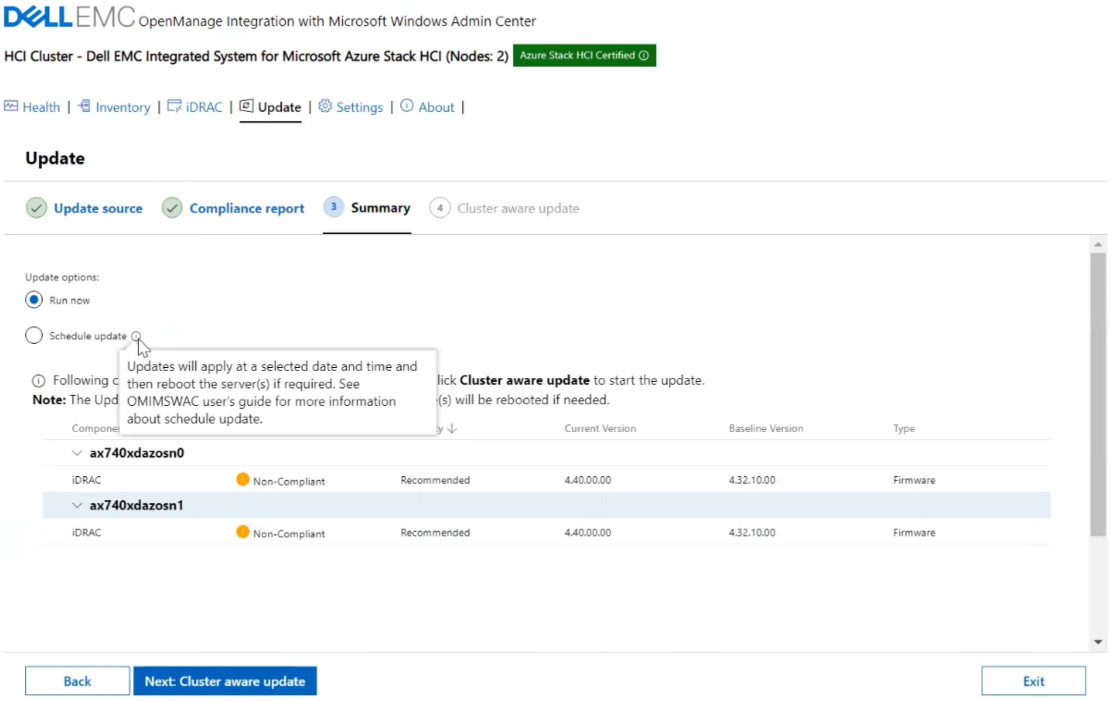
5. To filter the compliance based on the criticality, click the respective color on the bar chart or use the search box to filter out the required components. The compliance report will also be filtered to display only the selected critical components. To clear the filter, click the **Clear Filter** icon next to the search box.

6. 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.

7. Click **Next: Summary.**

   Selected components against each node for update are displayed in the summary page.

Note: 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**.


DELL EMC OpenManage Integration with Microsoft Windows Admin Center
Azure Stack HCI Certified ⓘ
Health | Inventory | iDRAC | Update | Settings | About |
Update source
Compliance report
3 Summary
4 Cluster aware update
Back
Next: Cluster aware update
Exit

HCI Cluster - Dell EMC Integrated System for Microsoft Azure Stack HCI (Nodes: 2)

Update

Update options:

● Run now

○ Schedule update ⓘ

Updates will apply at a selected date and time and then reboot the server(s) if required. See OMIMSWAC user's guide for more information about schedule update.

ⓘ Following c lick **Cluster aware update** to start the update.

Note: The Upd (s) will be rebooted if needed.

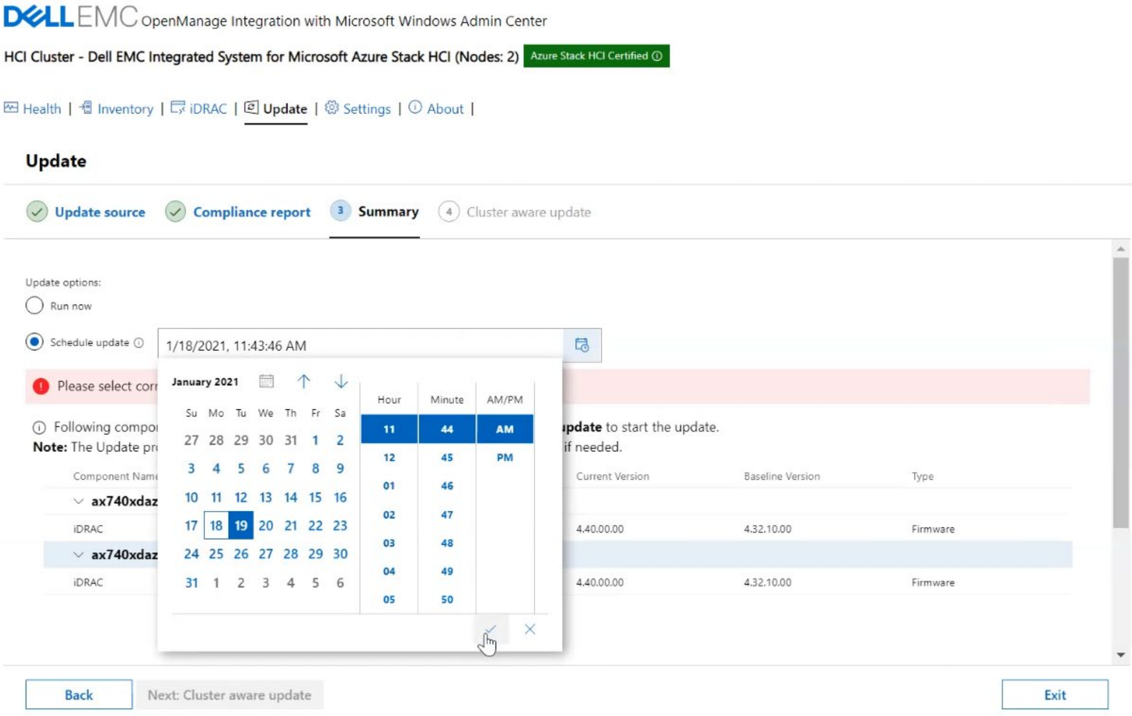
Componen		y ↓	Current Version	Baseline Version	Type
ax740xdazosn0					
iDRAC	● Non-Compliant	Recommended	4.40.00.00	4.32.10.00	Firmware
ax740xdazosn1					
iDRAC	● Non-Compliant	Recommended	4.40.00.00	4.32.10.00	Firmware

Figure 13: Summary for update

8. On the **Summary** tab, review the components to be updated and choose to run the cluster update now or schedule the cluster update for later:

    a. If you select **Run now**, this will trigger the cluster-aware update immediately and reboot nodes if required.

       If you select **Schedule Update,** then select a future date and time when the cluster-aware update will be performed. This will download and copy the required files and keep the cluster ready for update at the specified time.



DELL EMC OpenManage Integration with Microsoft Windows Admin Center

HCI Cluster - Dell EMC Integrated System for Microsoft Azure Stack HCI (Nodes: 2) Azure Stack HCI Certified

Update

Update options:

○ Run now

● Schedule update 1/18/2021, 11:43:46 AM

Please select corr

Following compo ... pdate to start the update.
Note: The Update pr ... if needed.

Component Name	Current Version	Baseline Version	Type
ax740xdaz			
iDRAC	4.40.00.00	4.32.10.00	Firmware
ax740xdaz			
iDRAC	4.40.00.00	4.32.10.00	Firmware

January 2021

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

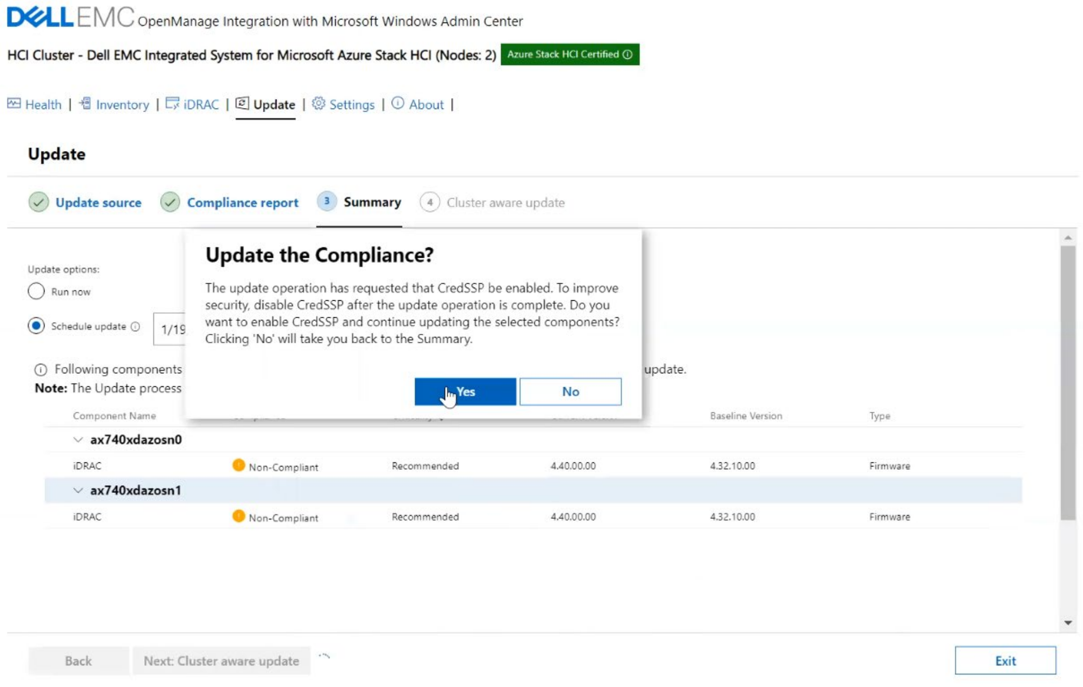
Hour	Minute	AM/PM
11	44	AM
12	45	PM
01	46	
02	47	
03	48	
04	49	
05	50	

Figure 14: Schedule update

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.

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.

9. Click **Next: Cluster aware Update**.


DELL EMC OpenManage Integration with Microsoft Windows Admin Center
HCI Cluster - Dell EMC Integrated System for Microsoft Azure Stack HCI (Nodes: 2)
Azure Stack HCI Certified
Health | Inventory | iDRAC | Update | Settings | About |
Update
Update source
Compliance report
3 Summary
4 Cluster aware update
Update options:
○ Run now
● Schedule update
1/19
Yes
No
Back
Next: Cluster aware update
Exit

Update the Compliance?

The update operation has requested that CredSSP be enabled. To improve security, disable CredSSP after the update operation is complete. Do you want to enable CredSSP and continue updating the selected components? Clicking 'No' will take you back to the Summary.

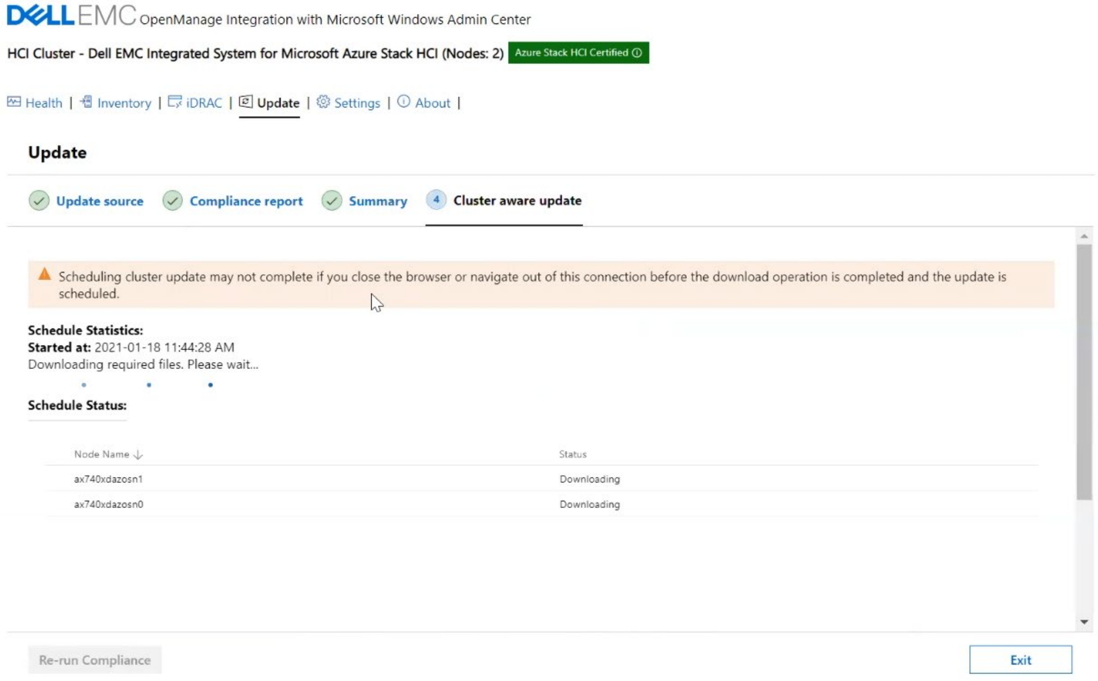
Following components … update.

Note: The Update process …

Component Name				Baseline Version	Type
ax740xdazosn0					
iDRAC	● Non-Compliant	Recommended	4.40.00.00	4.32.10.00	Firmware
ax740xdazosn1					
iDRAC	● Non-Compliant	Recommended	4.40.00.00	4.32.10.00	Firmware

Figure 15: Enable CredSSP

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. For more information see CredSSP Security Configuration guide.


DELL EMC OpenManage Integration with Microsoft Windows Admin Center
HCI Cluster - Dell EMC Integrated System for Microsoft Azure Stack HCI (Nodes: 2)
Azure Stack HCI Certified
Health | Inventory | iDRAC | Update | Settings | About |
Update
Update source
Compliance report
Summary
4 Cluster aware update
Re-run Compliance
Exit

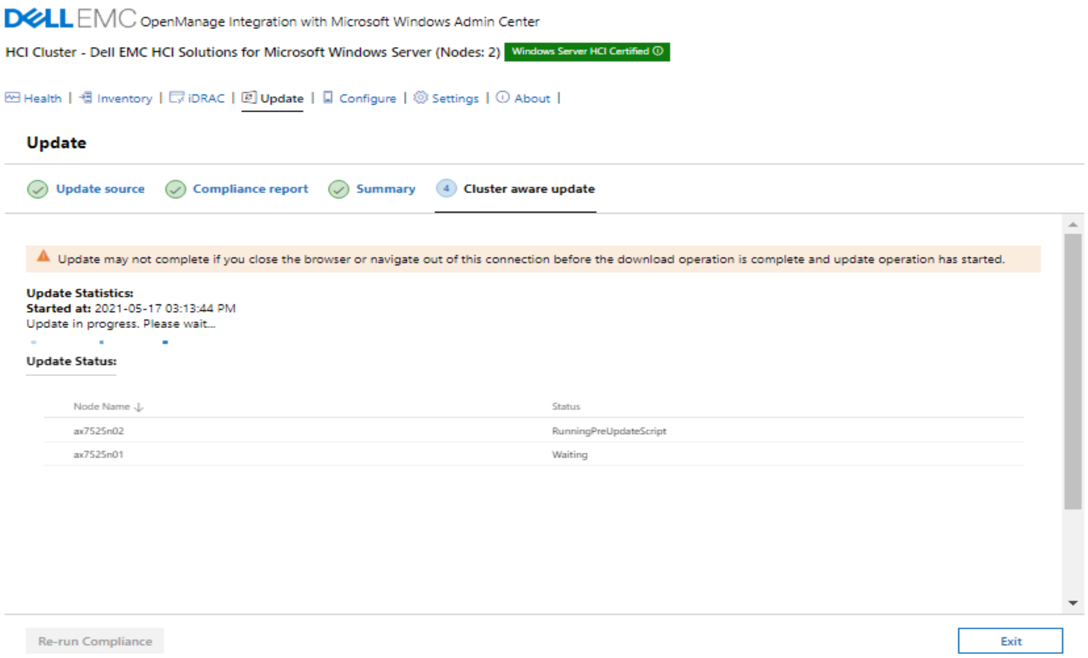
Scheduling cluster update may not complete if you close the browser or navigate out of this connection before the download operation is completed and the update is scheduled.

Schedule Statistics:
Started at: 2021-01-18 11:44:28 AM
Downloading required files. Please wait...

Schedule Status:

Node Name ↓	Status
ax740xdazosn1	Downloading
ax740xdazosn0	Downloading

Figure 16: CAU update status for Azure Stack HCI



DELL EMC OpenManage Integration with Microsoft Windows Admin Center

HCI Cluster - Dell EMC HCI Solutions for Microsoft Windows Server (Nodes: 2) Windows Server HCI Certified

Health | Inventory | iDRAC | Update | Configure | Settings | About |

Update

Update source
Compliance report
Summary
4 Cluster aware update

Update may not complete if you close the browser or navigate out of this connection before the download operation is complete and update operation has started.

Update Statistics:
Started at: 2021-05-17 03:13:44 PM
Update in progress. Please wait...

Update Status:

Node Name ↓	Status
ax7525n02	RunningPreUpdateScript
ax7525n01	Waiting

Figure 17: CAU update status for Windows Server HCI

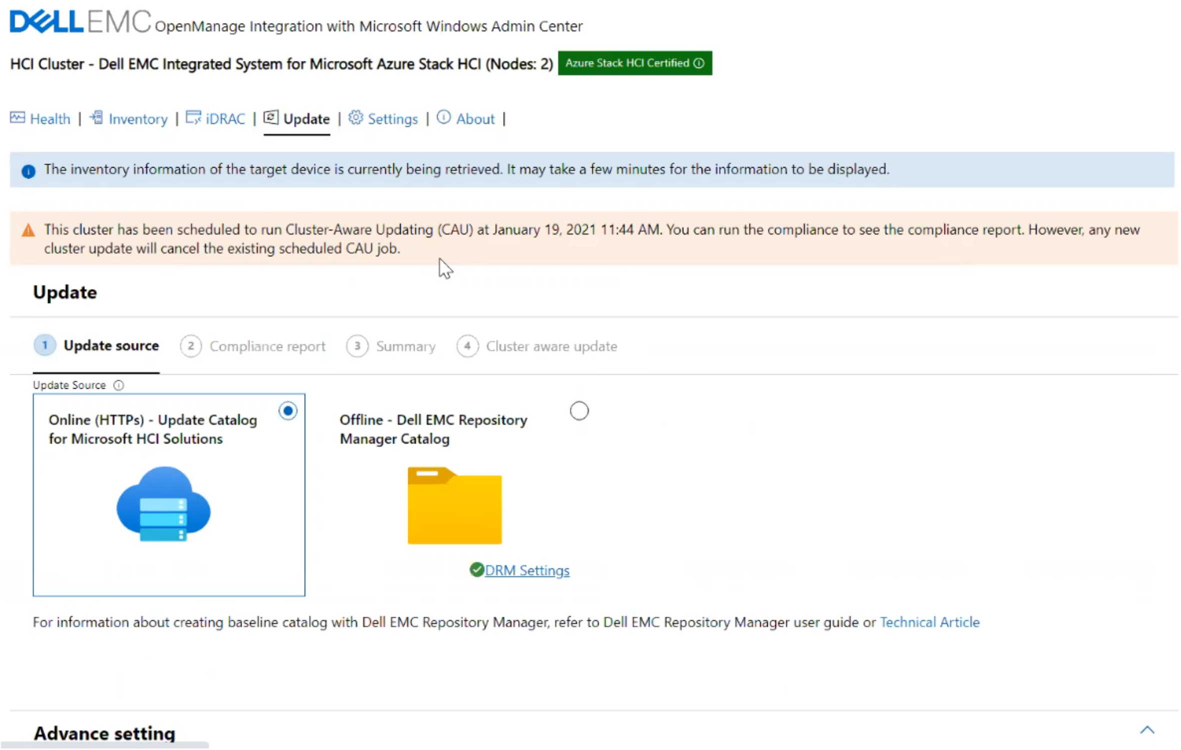
Status column indicates the current state of the node that is Downloading/Successful/Failed/Scheduled. To improve security, disable the CredSSP after the update operation is complete.

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. You can check the status by using Microsoft Cluster Aware Updating tool. Cluster Aware Updating tool coming as Microsoft Failover Clustering tool and feature's. For more information, see Cluster-Aware Updating requirements and best practices in Microsoft document.

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 the update compliance repot is generated, OMIMSWAC saves the information of the baseline catalog used for each solution.

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

10. If you want to run update on scheduled cluster then warning message appears at top. You can still proceed with '**Re-run compliance'**, but 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.


DELL EMC OpenManage Integration with Microsoft Windows Admin Center
Azure Stack HCI Certified
Health | Inventory | iDRAC | Update | Settings | About |
Update
1 Update source
2 Compliance report
3 Summary
4 Cluster aware update
Update Source
DRM Settings
Advance setting

HCI Cluster - Dell EMC Integrated System for Microsoft Azure Stack HCI (Nodes: 2)

The inventory information of the target device is currently being retrieved. It may take a few minutes for the information to be displayed.

This cluster has been scheduled to run Cluster-Aware Updating (CAU) at January 19, 2021 11:44 AM. You can run the compliance to see the compliance report. However, any new cluster update will cancel the existing scheduled CAU job.

● Online (HTTPs) - Update Catalog for Microsoft HCI Solutions

○ Offline - Dell EMC Repository Manager Catalog

For information about creating baseline catalog with Dell EMC Repository Manager, refer to Dell EMC Repository Manager user guide or Technical Article

Figure 18: Warning message when cluster update scheduled

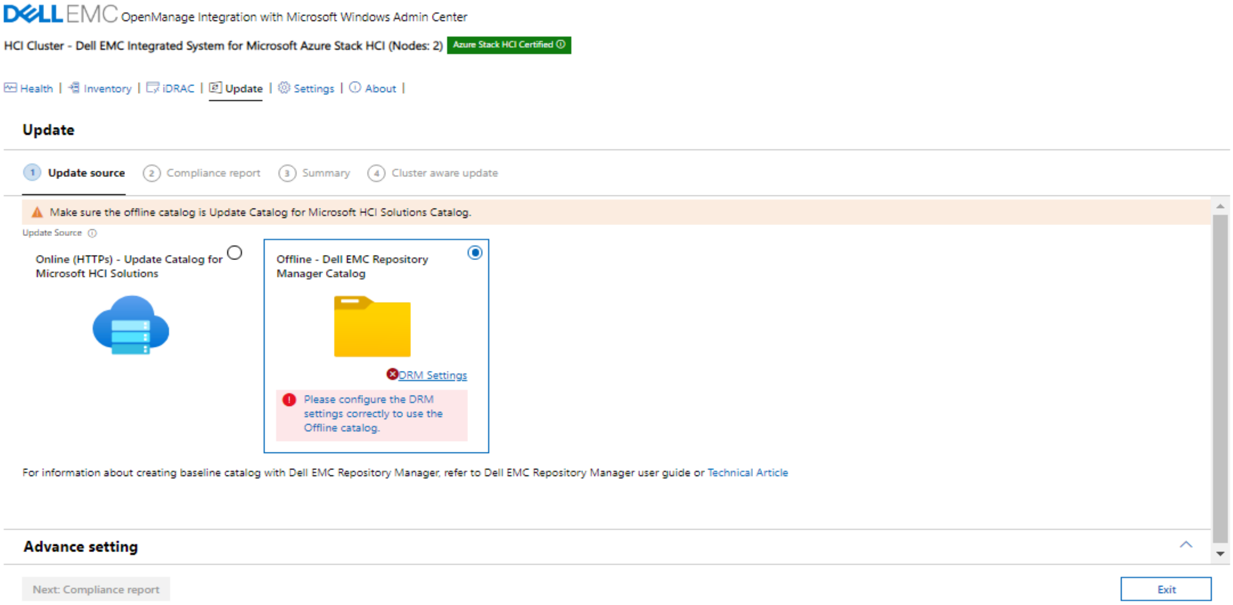
The generated update compliance report helps the IT administrators to understand the update requirements and plan their update cycles effectively. IT administrators can use the iDRAC or Dell Server Update (DSU) utility to update their data center environments with the latest updates and keep their environments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

5.2 Update using the catalog generated by DRM (Offline)

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

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

2. Click the **Update** tab, and then under **Update Source,** select "Offline - Dell EMC Repository Manager Catalog" to use the DRM catalog configured in a CIFS location.



HCI Cluster - Dell EMC Integrated System for Microsoft Azure Stack HCI (Nodes: 2)

Make sure the offline catalog is Update Catalog for Microsoft HCI Solutions Catalog.

Update Source

○ Online (HTTPs) - Update Catalog for Microsoft HCI Solutions

● Offline - Dell EMC Repository Manager Catalog

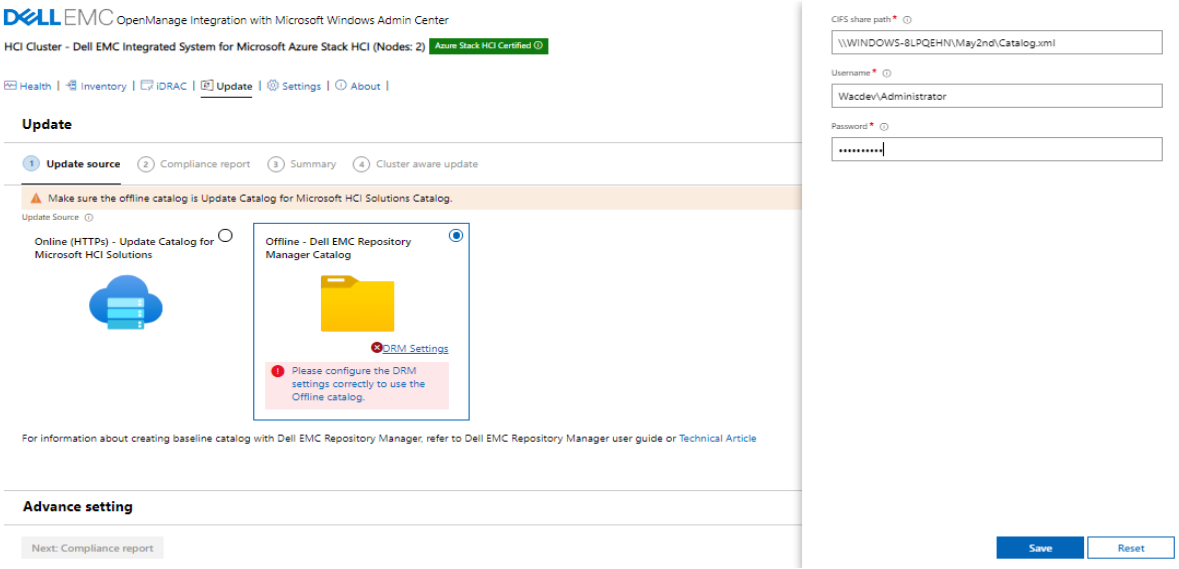
Please configure the DRM settings correctly to use the Offline catalog.

For information about creating baseline catalog with Dell EMC Repository Manager, refer to Dell EMC Repository Manager user guide or Technical Article

Figure 19: Select Update Source in OMIMSWAC

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.

3. 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 here. Enter the catalog file share location (suffixed with the catalog file name) and credentials to access the file share location as given below.


DELL EMC OpenManage Integration with Microsoft Windows Admin Center
Azure Stack HCI Certified
Health | Inventory | iDRAC | Update | Settings | About |
1 Update source
2 Compliance report
3 Summary
4 Cluster aware update
DRM Settings
Advance setting
Next: Compliance report
Save
Reset

HCI Cluster - Dell EMC Integrated System for Microsoft Azure Stack HCI (Nodes: 2)

Update

Make sure the offline catalog is Update Catalog for Microsoft HCI Solutions Catalog.

Update Source

○ Online (HTTPs) - Update Catalog for Microsoft HCI Solutions

● Offline - Dell EMC Repository Manager Catalog

Please configure the DRM settings correctly to use the Offline catalog.

For information about creating baseline catalog with Dell EMC Repository Manager, refer to Dell EMC Repository Manager user guide or Technical Article

CIFS share path *: \\WINDOWS-8LPQEHN\May2nd\Catalog.xml

Username *: Wacdev\Administrator

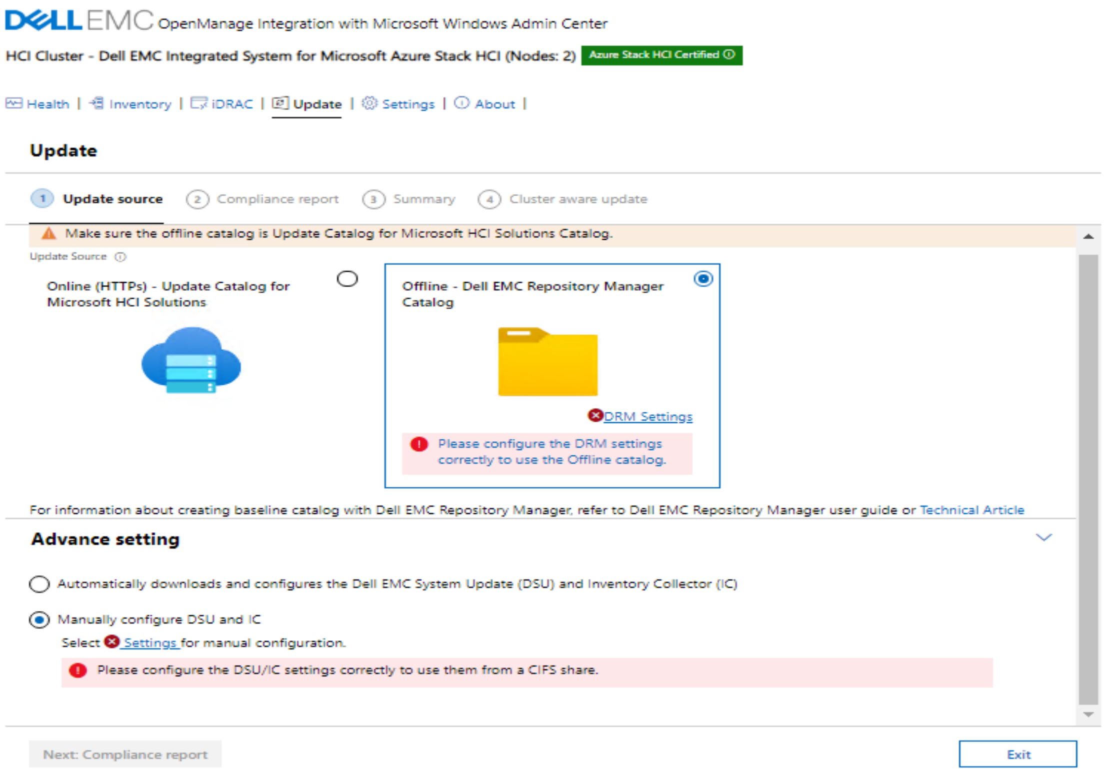
Password *: ••••••••••

Figure 20: User provides catalog details to generate a comparison report for Azure Stack HCI servers.

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)*.

Note: We recommend to use 'Update Catalog for Microsoft HCI solutions' catalog for Azure Stack HCI and Windows Server HCI.

Note: You must provide individual catalog files with the user credentials for server manager, and cluster manager respectively.



DELL EMC OpenManage Integration with Microsoft Windows Admin Center

HCI Cluster - Dell EMC Integrated System for Microsoft Azure Stack HCI (Nodes: 2) Azure Stack HCI Certified

Update

⚠ Make sure the offline catalog is Update Catalog for Microsoft HCI Solutions Catalog.

Update Source

○ Online (HTTPs) - Update Catalog for Microsoft HCI Solutions

● Offline - Dell EMC Repository Manager Catalog

DRM Settings

Please configure the DRM settings correctly to use the Offline catalog.

For information about creating baseline catalog with Dell EMC Repository Manager, refer to Dell EMC Repository Manager user guide or Technical Article

Advance setting

○ Automatically downloads and configures the Dell EMC System Update (DSU) and Inventory Collector (IC)

● Manually configure DSU and IC

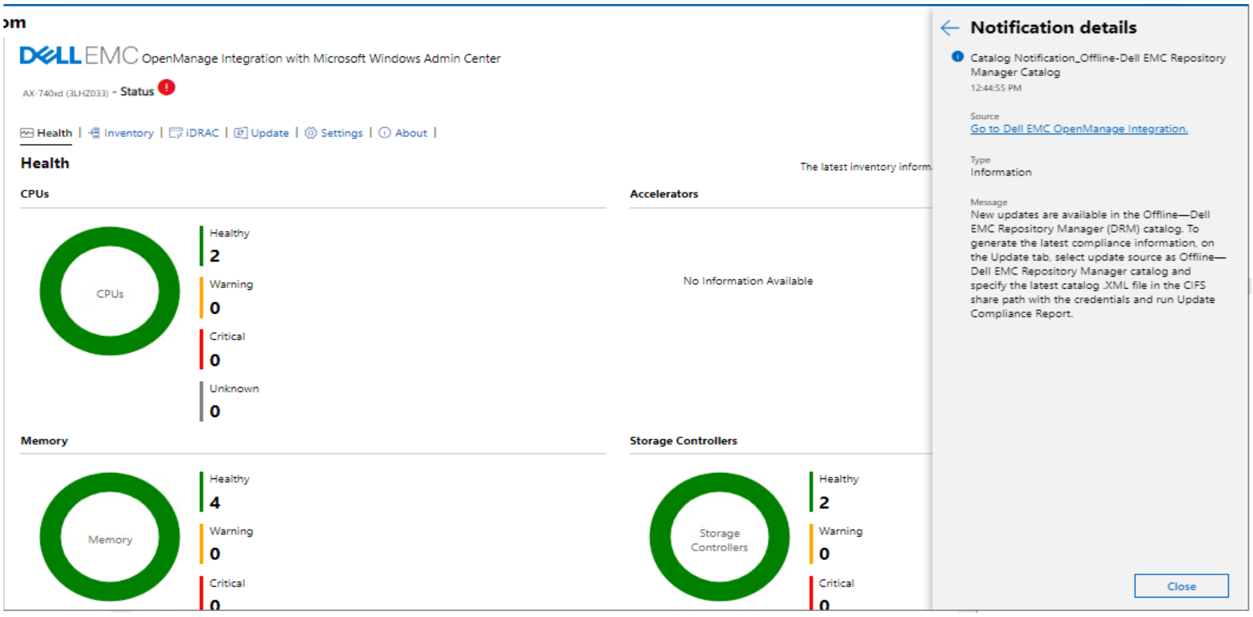
Select Settings for manual configuration.

Please configure the DSU/IC settings correctly to use them from a CIFS share.

Figure 21: Update Tools via Advance settings for specifying DSU and IC in OMIMSWAC

4. To use the Dell EMC System Update (DSU) and Inventory Collector (IC) tools, select **Advance setting**, and then follow [Update using online catalog](#) from **step 2. a** onwards.

   After the update compliance repot 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.



DELL EMC OpenManage Integration with Microsoft Windows Admin Center

AX-740xd (3LHZ033) - Status

Health

The latest inventory inform

CPUs	
Healthy	2
Warning	0
Critical	0
Unknown	0

Accelerators: No Information Available

Memory	
Healthy	4
Warning	0
Critical	0

Storage Controllers	
Healthy	2
Warning	0
Critical	0

Notification details

Catalog Notification_Offline-Dell EMC Repository Manager Catalog
12:44:55 PM

Source
Go to Dell EMC OpenManage Integration.

Type
Information

Message
New updates are available in the Offline—Dell EMC Repository Manager (DRM) catalog. To generate the latest compliance information, on the Update tab, select update source as Offline—Dell EMC Repository Manager catalog and specify the latest catalog .XML file in the CIFS share path with the credentials and run Update Compliance Report.

Figure 22: Node health status and new offline catalog notification

The generated update compliance report helps 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 environments secure.

5.3 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, proxy configurations do not allow updating target nodes or clusters using online catalogs. In this case, compliance and updates using the offline catalog are supported.

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:

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 in the below format, and click Save.

   <port number> (https) or <port number> (http)

For example: 443 (https) or 80 (http)