DELL Technologies

Technical White paper

Update cluster hardware components using Cluster-Aware Updating (CAU) in 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.

July 2023

Revisions

Date	Description
May 24, 2021	Updated Dell infrastructure using OMIMSWAC
July 24, 2023	Updated UI screenshots and workflows as per 3.1 version

Acknowledgments

Author: Gopayya Devarakonda—Software Senior Engineer, Server and Infrastructure Systems.

Support: Ajit Parhi

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.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third party content is updated by the relevant third parties, this document will be revised accordingly.

Table of contents

Executive summary

Dell OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) provides a centralized management experience for IT administrators in managing their Dell Integrated System for Azure Stack HCI, Dell 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 technical white paper are IT administrators who use OMIMSWAC to perform hardware updates for clusters using the Cluster-Aware Updating feature.

1 Introduction

Dell provides validated catalogs for PowerEdge servers, Dell Integrated System for Microsoft Azure Stack HCI, Dell HCI Solutions for Microsoft Windows Server, and Hyper-V based failover solutions. These catalogs contain essential components such as firmware, drivers, applications, and BIOS.

By using the Cluster-Aware Updating feature in OMIMSWAC, you can generate compliance report against the validated catalogs and update components of target nodes and nodes in HCI and failover clusters without affecting the workloads. You can use either an online or offline catalog to generate compliance report and update components.

To update OS and hardware on Azure Stack HCI cluster, use the Full Stack Update feature in the Dell OpenManage Integration snap-in. For more information, see the *Dell OpenManage Integration with Microsoft Windows Admin Center User's Guide* from https://www.dell.com/support/home/en-us/product-support/product/openmanage-integration-microsoft-windows-admin-center/docs.

2 Prerequisites

- Ensure that the inventory information for the target node has been retrieved and the target node is not part of any Azure Stack HCI or Windows Server HCI cluster. To update such nodes, connect to the cluster and use Cluster-Aware Updating feature.
- Ensure that WAC is not installed on the target node you want to update. If required, install WAC on another target node (non-WAC related) and complete the update.
- Ensure that the Failover Clustering feature and Failover Clustering Tools are installed on all the cluster nodes before triggering CAU. For more information, see Cluster Aware Updating requirements and best practices in Microsoft document.

Note: It is recommended to test the cluster readiness before triggering CAU. For more information, see the Tests for cluster updating readiness in.https://learn.microsoft.com/en-us/windows-server/failover-clustering/cluster-aware-updating-requirements.

- Ensure that OMIWAC premium licenses are installed on all cluster nodes to use the CAU feature. To verify licensing, go to Overview and select nodes from the Node menu in the OpenManage Integration extension to view licenses installed on each node.
- If prompted to specify the "Manage as" credentials, select **Manage as** and enter appropriate Server Administrator or Cluster Administrator accounts. The user should also be part of the local user group of gateway administrators. For more information, see the Cluster-Aware Updating requirements and best practices in Microsoft document.
- Ensure both physical, and virtual disks of cluster nodes are in healthy state before triggering CAU.
- Ensure that iDRAC lockdown mode is disabled. To disable the iDRAC system lockdown mode in cluster nodes with iDRAC firmware earlier than 4.40.00.00, see the relevant iDRAC documentation on the support site.
- For SAS-RAID_Driver, ensure the followings:
  - Set the SATA controller to RAID mode.
  - Set the NVMe PCIe SSDs to RAID mode.

Note: It is recommended that you perform only one compliance or update operation on a target node at a time. Running multiple compliance/updates simultaneously can result in failures for the existing compliance/updates.

2.1 Verify license details

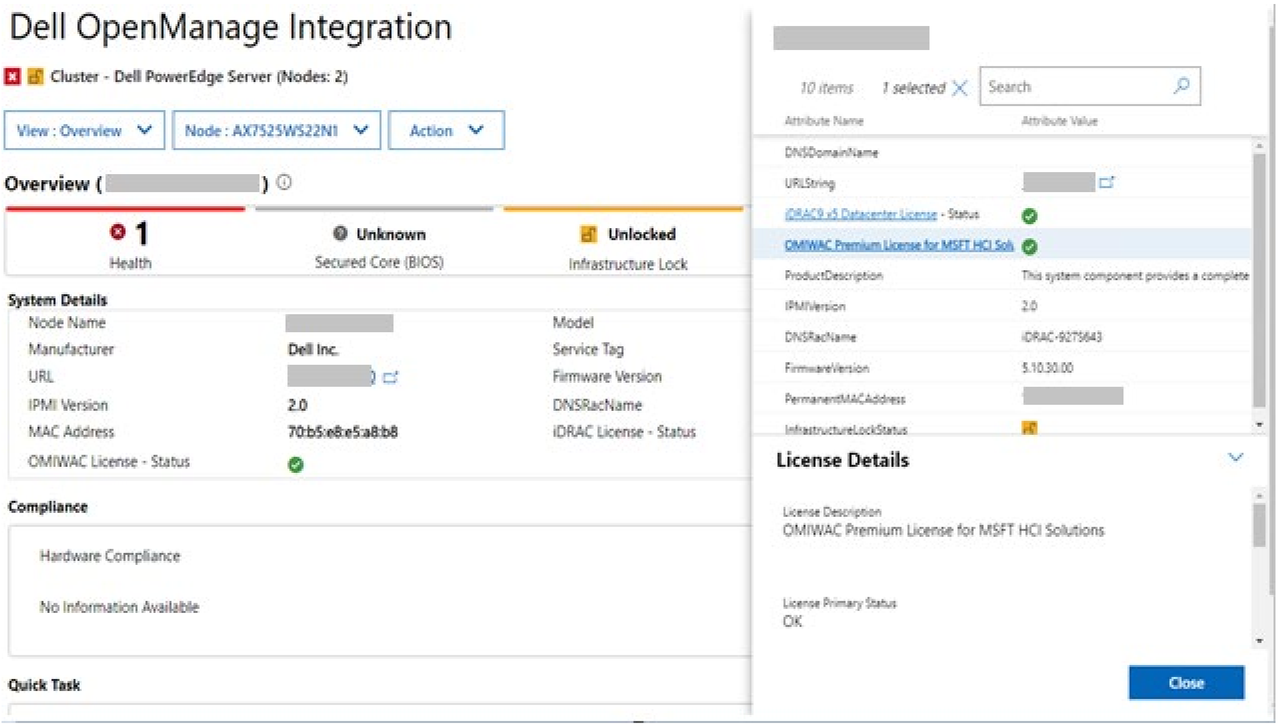
In OMIMSWAC, you can view node details and their licenses from the iDRAC inventory. The iDRAC inventory attributes are optimized to improve usability.

To verify licenses, do the following:

1. In Windows Admin Center, connect to a server or cluster.
2. In the left pane of Windows Admin Center, under EXTENSIONS, click Dell OpenManage Integration.
3. Click View **> Overview** and from the **Node** menu, select the specific node..

4. Click the **iDRAC Details** tab to view licenses installed on the node. To view license details, click a license attribute name. For example, iDRAC9 Enterprise License, OpenManage Enterprise Advanced, OMIWAC Premium License for MSFT HCI Solutions.

Note: By default, AX nodes come with the OMIWAC Premium license as part of the base solution.



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

Overview ([redacted])

1	Unknown	Unlocked
Health	Secured Core (BIOS)	Infrastructure Lock

System Details

Node Name	[redacted]	Model
Manufacturer	Dell Inc.	Service Tag
URL	[redacted]	Firmware Version
IPMI Version	2.0	DNSRacName
MAC Address	70:b5:e8:e5:a8:b8	iDRAC License - Status
OMIWAC License - Status	✓	

Compliance

Hardware Compliance

No Information Available

Quick Task

[redacted]

10 items 1 selected

Attribute Name	Attribute Value
DNSDomainName	
URLString	[redacted]
iDRAC9 x5 Datacenter License - Status	✓
OMIWAC Premium License for MSFT HCI Solı	✓
ProductDescription	This system component provides a complete
IPMIVersion	2.0
DNSRacName	iDRAC-92TS643
FirmwareVersion	5.10.30.00
PermanentMACAddress	[redacted]
InfrastructureLockStatus	

License Details

License Description
OMIWAC Premium License for MSFT HCI Solutions

License Primary Status
OK

Figure 1: Verify License Details

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, see the OMIMSWAC Guide.

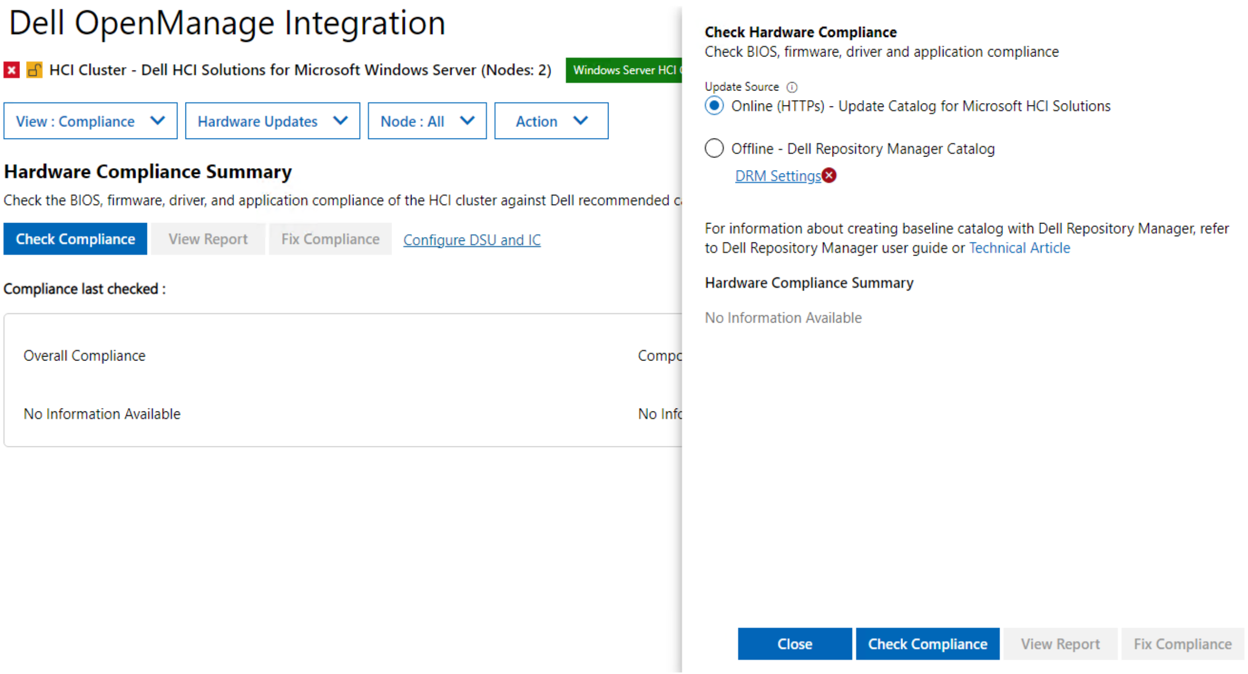
3 Update hardware using an online (HTTPS) catalog

You can choose online catalog from the update source to update hardware components. The available online catalogs are:

- Dell Enterprise Catalog: This contains the validated versions components for PowerEdge servers.
- Dell MX Solution Catalog: This contains validated versions components for PowerEdge MX Modular.
- Update Catalog for Microsoft HCI solutions: This contains validated versions components for AX nodes and Storage Spaces Direct Ready Nodes.

3.1 Generate compliance report

1. In the left pane of Windows Admin Center, under **EXTENSIONS**, click **Dell OpenManage Integration**.
2. Click **View > Compliance**. Select **Hardware Updates**. The Hardware Compliance Summary page is displayed. Alternatively, go to the Action menu, under HARDWARE COMPLIANCE AND REMEDIATION, click Check Compliance.
3. Click the **Check Compliance** button, and then under the **Update Source**, select “Online (HTTPs) – <catalog name>”. By default, Online Catalog is selected.



Dell OpenManage Integration

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

Hardware Compliance Summary

Check the BIOS, firmware, driver, and application compliance of the HCI cluster against Dell recommended c

Compliance last checked :

Overall Compliance

No Information Available

Check Hardware Compliance

Check BIOS, firmware, driver and application compliance

Update Source

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

○ Offline - Dell Repository Manager Catalog

DRM Settings

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

Hardware Compliance Summary

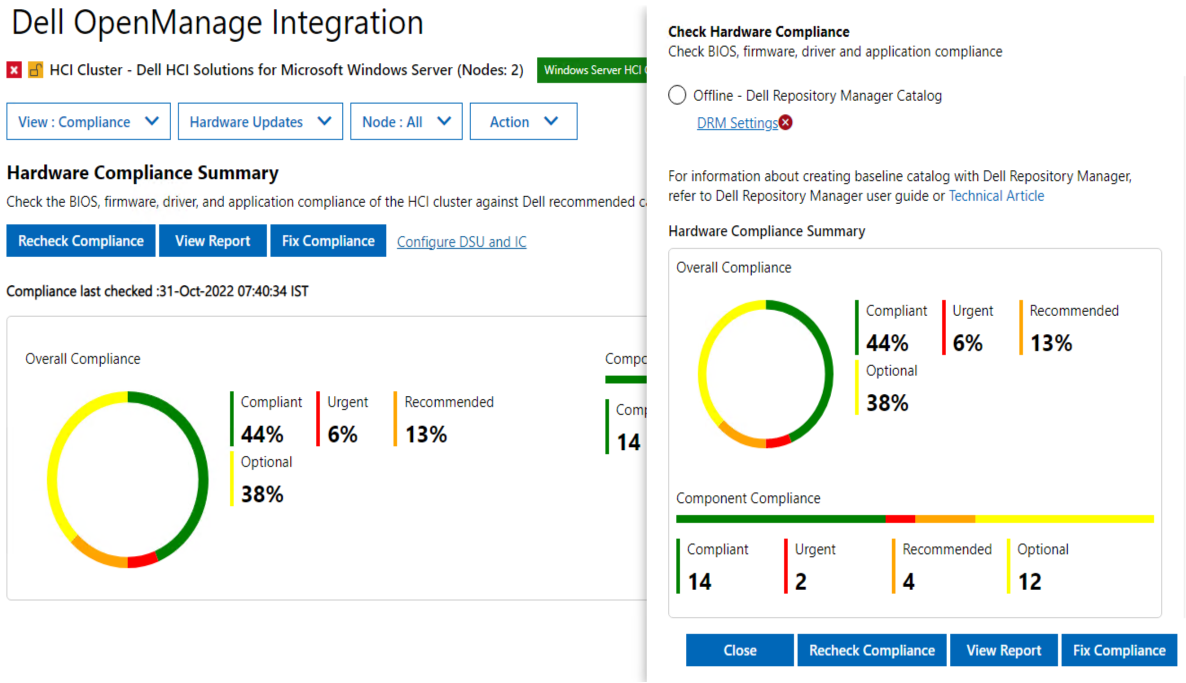
No Information Available

Figure 2: Select update source in OMIMSWAC

4. Click Check **Compliance** to generate the compliance report.
5. OpenManage Integration compares the cluster hardware component versions with the components present in the catalog before generating a compliance report.
6. While the update compliance 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.

7. To view the compliance report, click **View > Compliance**. Another menu appears, select **Hardware Updates**. Hardware Compliance Summary page appears. Alternatively, go to the **Action** menu, under **HARDWARE COMPLIANCE AND REMEDIATION**, click **Check Compliance**.



Dell OpenManage Integration

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

Hardware Compliance Summary

Check the BIOS, firmware, driver, and application compliance of the HCI cluster against Dell recommended c

Compliance last checked :31-Oct-2022 07:40:34 IST

Check Hardware Compliance

Check BIOS, firmware, driver and application compliance

○ Offline - Dell Repository Manager Catalog

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

Figure 3: Compliance report

8. The doughnut chart displays the overall compliance summary using different color codes. The bar chart displays the number of components in compliant, urgent/critical, recommended, and optional states using different color codes.
    - To view compliance information for each component, click **View Report**. A window appears on the right side that displays node level component compliance status. You can expand or collapse node, and its component level information.
    - 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.
    - Along with compliance information, the license status (OMIWAC Premium License) for each node is also displayed.
9. To generate the compliance report later, click **Recheck Compliance**. The timestamp of the latest compliance report is displayed below the Recheck compliance.

3.2 Update hardware components

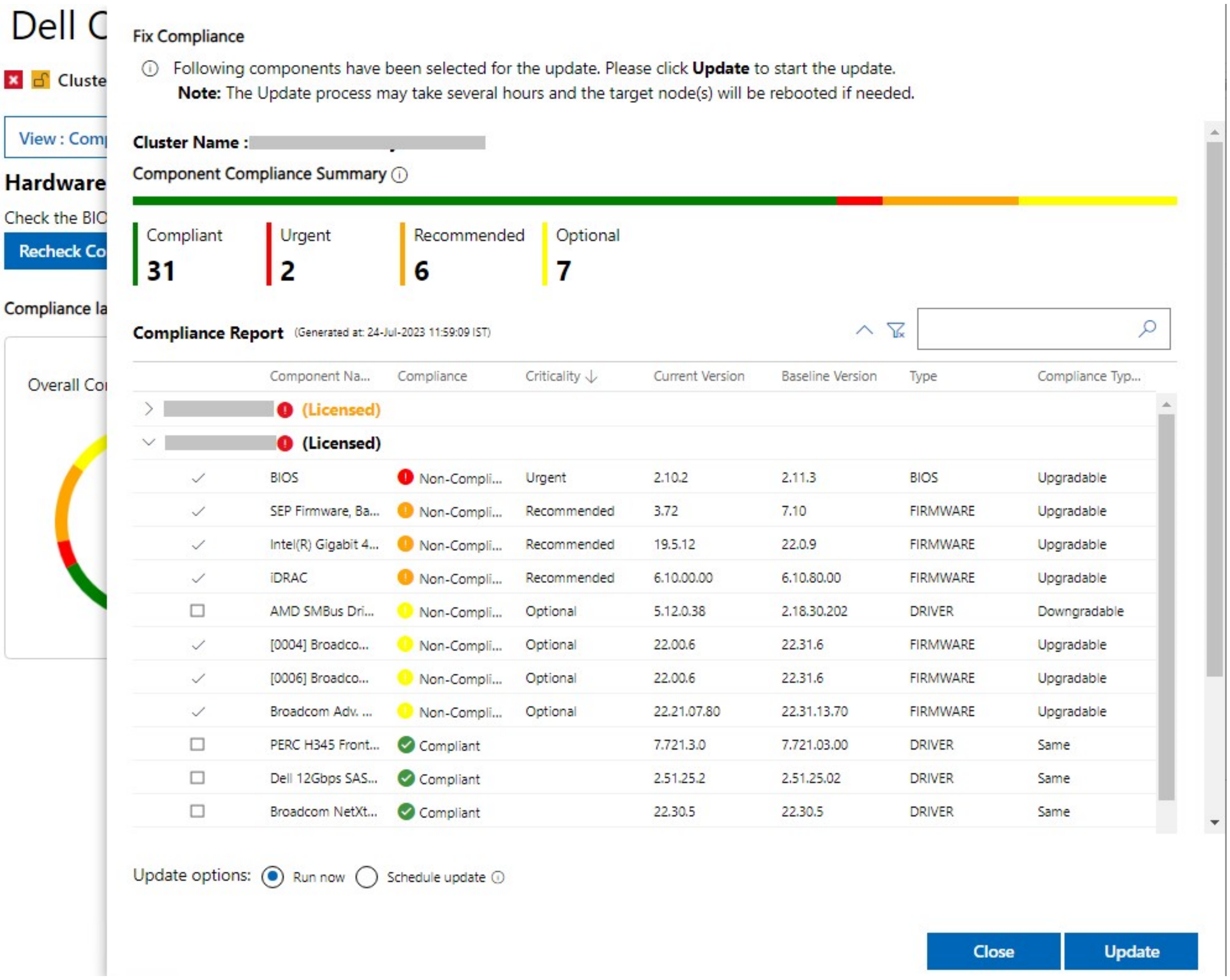
In the compliance report, the 'upgradable' components that are 'non-compliant' are selected by default for update.

1. You may clear 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.

2. To generate the compliance report later, click **Recheck Compliance**. The timestamp of the latest compliance report is displayed below the Recheck compliance.
3. To select non-compliant components for update, Click **Fix Compliance.**

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



Fix Compliance

ⓘ Following components have been selected for the update. Please click **Update** to start the update.
Note: The Update process may take several hours and the target node(s) will be rebooted if needed.

Cluster Name : [redacted]

Component Compliance Summary ⓘ

Compliant	Urgent	Recommended	Optional
31	2	6	7

Compliance Report (Generated at: 24-Jul-2023 11:59:09 IST)

	Component Na...	Compliance	Criticality ↓	Current Version	Baseline Version	Type	Compliance Typ...
>	[redacted] ● (Licensed)						
∨	[redacted] ● (Licensed)						
✓	BIOS	● Non-Compli...	Urgent	2.10.2	2.11.3	BIOS	Upgradable
✓	SEP Firmware, Ba...	● Non-Compli...	Recommended	3.72	7.10	FIRMWARE	Upgradable
✓	Intel(R) Gigabit 4...	● Non-Compli...	Recommended	19.5.12	22.0.9	FIRMWARE	Upgradable
✓	iDRAC	● Non-Compli...	Recommended	6.10.00.00	6.10.80.00	FIRMWARE	Upgradable
□	AMD SMBus Dri...	● Non-Compli...	Optional	5.12.0.38	2.18.30.202	DRIVER	Downgradable
✓	[0004] Broadco...	● Non-Compli...	Optional	22.00.6	22.31.6	FIRMWARE	Upgradable
✓	[0006] Broadco...	● Non-Compli...	Optional	22.00.6	22.31.6	FIRMWARE	Upgradable
✓	Broadcom Adv. ...	● Non-Compli...	Optional	22.21.07.80	22.31.13.70	FIRMWARE	Upgradable
□	PERC H345 Front...	✓ Compliant		7.721.3.0	7.721.03.00	DRIVER	Same
□	Dell 12Gbps SAS...	✓ Compliant		2.51.25.2	2.51.25.02	DRIVER	Same
□	Broadcom NetXt...	✓ Compliant		22.30.5	22.30.5	DRIVER	Same

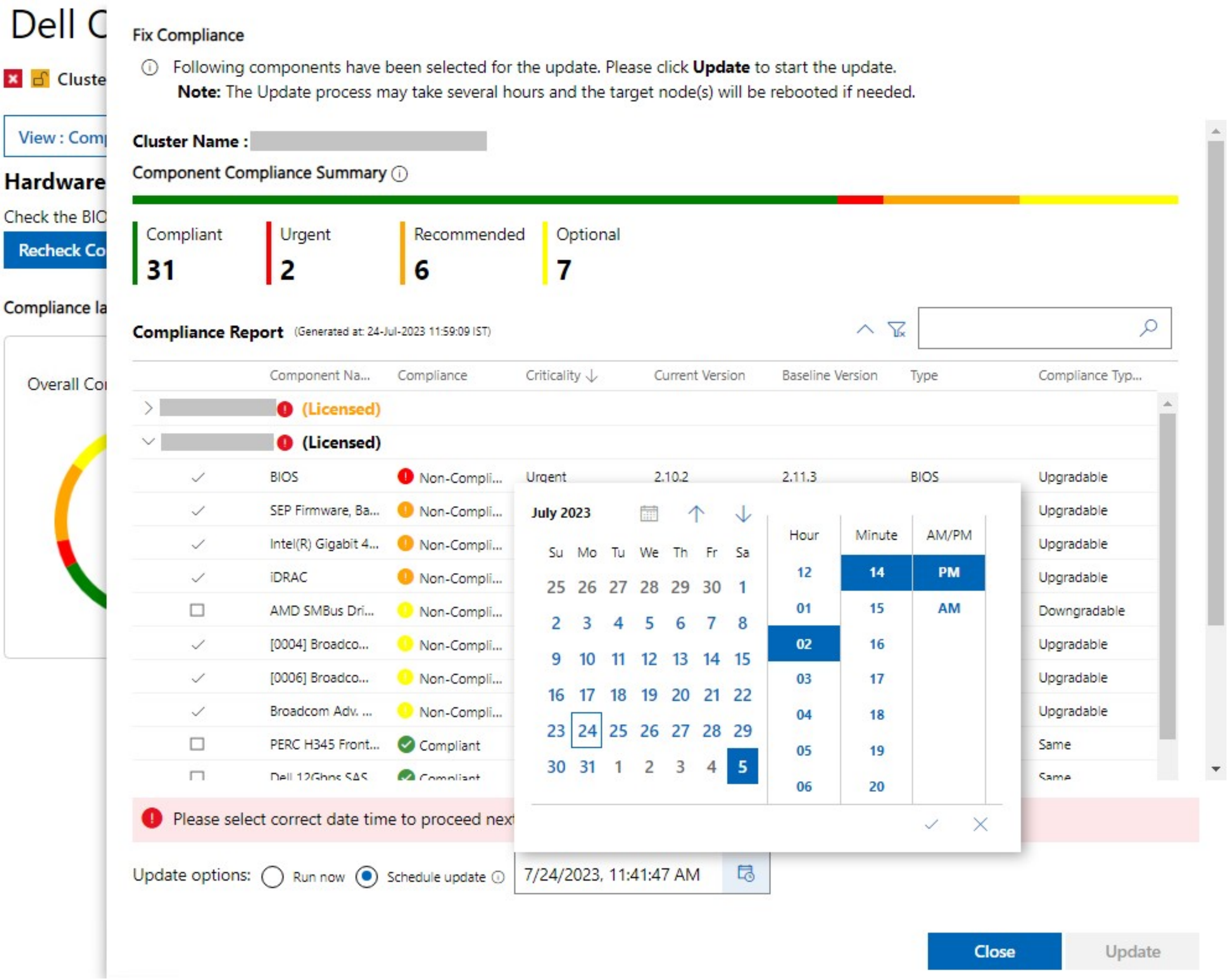
Update options: ● Run now ○ Schedule update ⓘ

Figure 4: Summary for update

4. On the **Summary** page, review the components that should be updated. You have two options:

   a. If you select **Run now**, the cluster update starts right away. If necessary, nodes may be rebooted during this process.

   b. If you select **Schedule Update,** select a future date and time for the cluster update. This will download and copy the necessary files, preparing the cluster for the update at the specified time.



Fix Compliance

ⓘ Following components have been selected for the update. Please click **Update** to start the update.
Note: The Update process may take several hours and the target node(s) will be rebooted if needed.

Cluster Name : [redacted]

Component Compliance Summary ⓘ

Compliant	Urgent	Recommended	Optional
31	2	6	7

Compliance Report (Generated at: 24-Jul-2023 11:59:09 IST)

	Component Na...	Compliance	Criticality ↓	Current Version	Baseline Version	Type	Compliance Typ...
> [redacted] ● (Licensed)							
∨ [redacted] ● (Licensed)							
✓	BIOS	● Non-Compli...	Urgent	2.10.2	2.11.3	BIOS	Upgradable
✓	SEP Firmware, Ba...	● Non-Compli...					Upgradable
✓	Intel(R) Gigabit 4...	● Non-Compli...					Upgradable
✓	iDRAC	● Non-Compli...					Upgradable
□	AMD SMBus Dri...	● Non-Compli...					Downgradable
✓	[0004] Broadco...	● Non-Compli...					Upgradable
✓	[0006] Broadco...	● Non-Compli...					Upgradable
✓	Broadcom Adv. ...	● Non-Compli...					Upgradable
□	PERC H345 Front...	✓ Compliant					Same
□	Dell 12Gbps SAS	✓ Compliant					Same

July 2023 ↑ ↓

Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	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

Hour	Minute	AM/PM
12	14	PM
01	15	AM
02	16	
03	17	
04	18	
05	19	
06	20	

✓ ✕

! Please select correct date time to proceed next

Update options: ○ Run now ● Schedule update ⓘ 7/24/2023, 11:41:47 AM

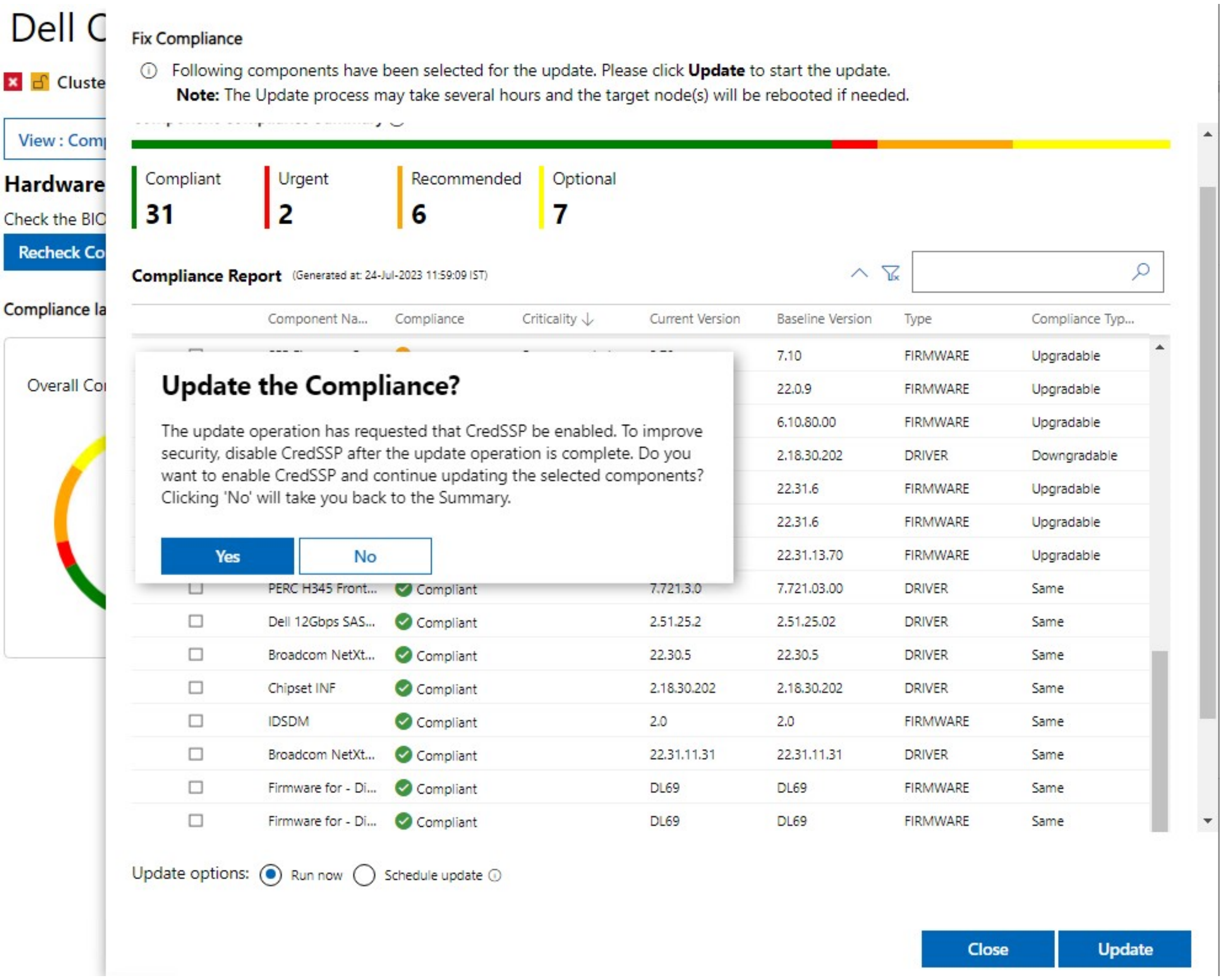
Close Update

Figure 5: Schedule update

At any given time, only one CAU job can be scheduled for a cluster. If a new CAU job is initiated (Run now or Schedule later), it replaces the existing scheduled job.

Note: When components are selected and confirmed, if the 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 on the support site.

5. Click **Update**.



Fix Compliance

ⓘ Following components have been selected for the update. Please click **Update** to start the update.
Note: The Update process may take several hours and the target node(s) will be rebooted if needed.

Compliant	Urgent	Recommended	Optional
31	2	6	7

Compliance Report (Generated at: 24-Jul-2023 11:59:09 IST)

	Component Na...	Compliance	Criticality ↓	Current Version	Baseline Version	Type	Compliance Typ...
					7.10	FIRMWARE	Upgradable
					22.0.9	FIRMWARE	Upgradable
					6.10.80.00	FIRMWARE	Upgradable
					2.18.30.202	DRIVER	Downgradable
					22.31.6	FIRMWARE	Upgradable
					22.31.6	FIRMWARE	Upgradable
					22.31.13.70	FIRMWARE	Upgradable
□	PERC H345 Front...	✓ Compliant		7.721.3.0	7.721.03.00	DRIVER	Same
□	Dell 12Gbps SAS...	✓ Compliant		2.51.25.2	2.51.25.02	DRIVER	Same
□	Broadcom NetXt...	✓ Compliant		22.30.5	22.30.5	DRIVER	Same
□	Chipset INF	✓ Compliant		2.18.30.202	2.18.30.202	DRIVER	Same
□	IDSDM	✓ Compliant		2.0	2.0	FIRMWARE	Same
□	Broadcom NetXt...	✓ Compliant		22.31.11.31	22.31.11.31	DRIVER	Same
□	Firmware for - Di...	✓ Compliant		DL69	DL69	FIRMWARE	Same
□	Firmware for - Di...	✓ Compliant		DL69	DL69	FIRMWARE	Same

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.

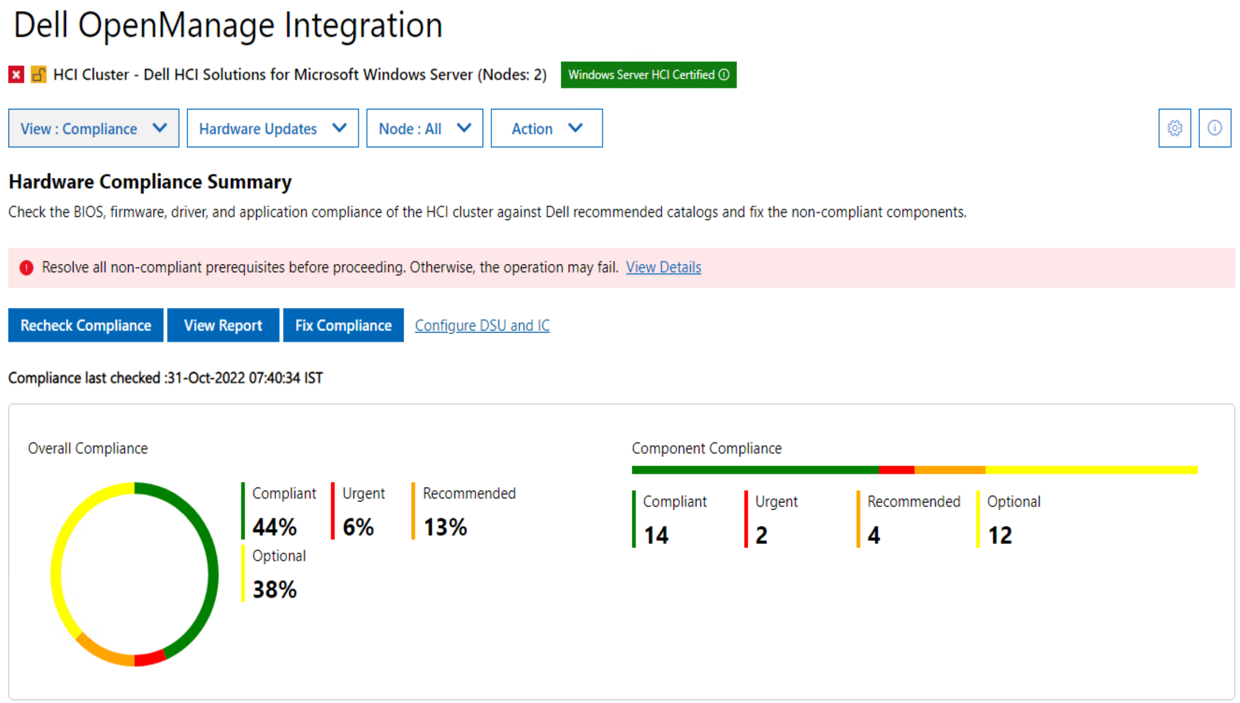
Yes No

Update options: ● Run now ○ Schedule update ⓘ

Close Update

Figure 6: Enable CredSSP

6. A message is prompted to enable CredSSP. Click '**Yes'** to enable the CredSSP and continue updating the selected components. To improve the security, disable the CredSSP after the update is complete. For more information, see [CredSSP Security Configuration guide.](#)
7. OpenManage Integration extension checks the prerequisites required to complete the update job. If all prerequisites are met, the extension proceeds to update the components.



Dell OpenManage Integration

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

Hardware Compliance Summary

Check the BIOS, firmware, driver, and application compliance of the HCI cluster against Dell recommended catalogs and fix the non-compliant components.

Resolve all non-compliant prerequisites before proceeding. Otherwise, the operation may fail. View Details

Compliance last checked :31-Oct-2022 07:40:34 IST

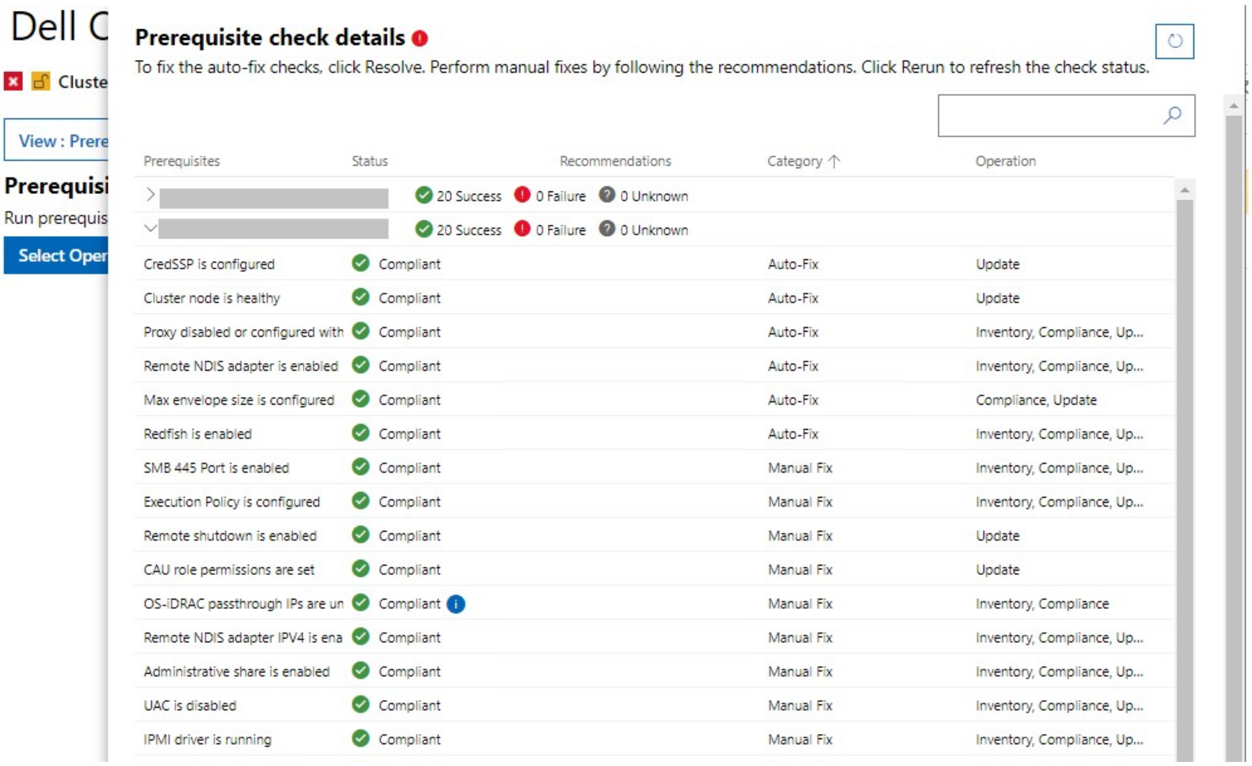
Overall Compliance

Compliant	Urgent	Recommended	Optional
44%	6%	13%	38%

Component Compliance

Compliant	Urgent	Recommended	Optional
14	2	4	12

Figure 7: Hardware compliance report



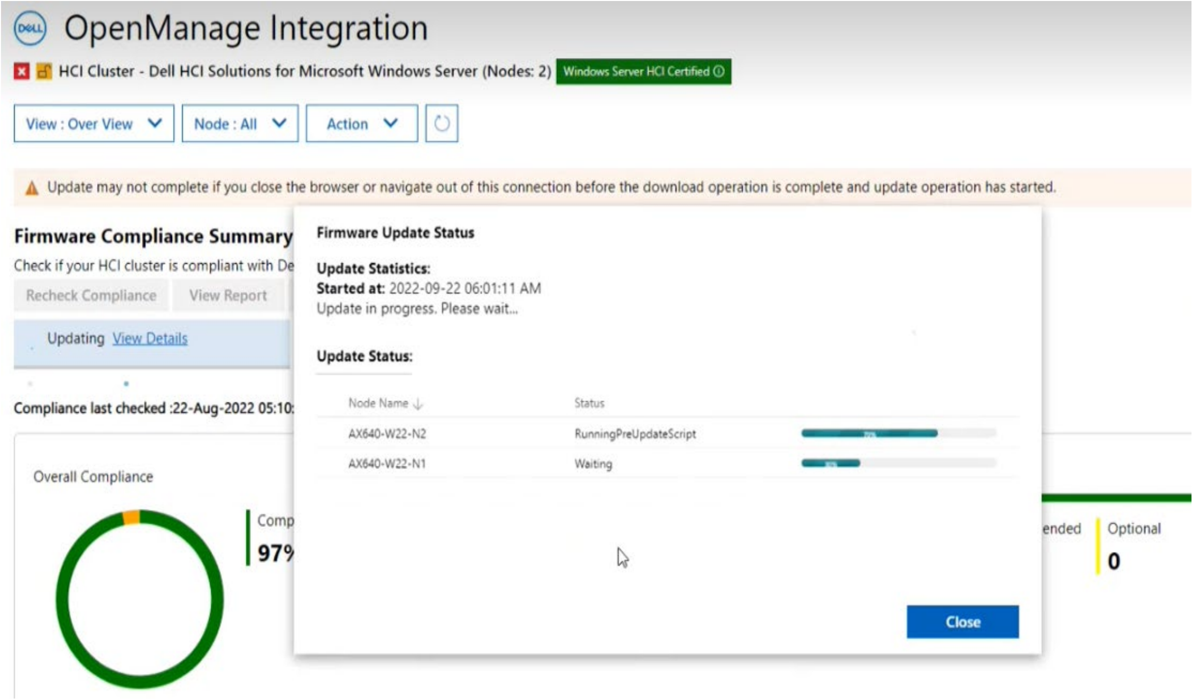
Prerequisite check details

To fix the auto-fix checks, click Resolve. Perform manual fixes by following the recommendations. Click Rerun to refresh the check status.

Prerequisites	Status	Recommendations	Category	Operation
[redacted]	20 Success 0 Failure 0 Unknown			
[redacted]	20 Success 0 Failure 0 Unknown			
CredSSP is configured	Compliant		Auto-Fix	Update
Cluster node is healthy	Compliant		Auto-Fix	Update
Proxy disabled or configured with	Compliant		Auto-Fix	Inventory, Compliance, Up...
Remote NDIS adapter is enabled	Compliant		Auto-Fix	Inventory, Compliance, Up...
Max envelope size is configured	Compliant		Auto-Fix	Compliance, Update
Redfish is enabled	Compliant		Auto-Fix	Inventory, Compliance, Up...
SMB 445 Port is enabled	Compliant		Manual Fix	Inventory, Compliance, Up...
Execution Policy is configured	Compliant		Manual Fix	Inventory, Compliance, Up...
Remote shutdown is enabled	Compliant		Manual Fix	Update
CAU role permissions are set	Compliant		Manual Fix	Update
OS-IDRAC passthrough IPs are un	Compliant		Manual Fix	Inventory, Compliance
Remote NDIS adapter IPV4 is ena	Compliant		Manual Fix	Inventory, Compliance, Up...
Administrative share is enabled	Compliant		Manual Fix	Inventory, Compliance, Up...
UAC is disabled	Compliant		Manual Fix	Inventory, Compliance, Up...
IPMI driver is running	Compliant		Manual Fix	Inventory, Compliance, Up...

Figure 8: Pre-requisites check page

8. If any of the prerequisites fails, a banner message is displaced. Click **View Details** to see the non-compliant prerequisites and ways you can resolve them. Resolve the non-compliant prerequisites and try the operation again. Navigate to the Prerequisites check from the **View** or **Actions** menu.


OpenManage Integration
HCI Cluster - Dell HCI Solutions for Microsoft Windows Server (Nodes: 2)
Windows Server HCI Certified
View : Over View
Node : All
Action
Recheck Compliance
View Report
Close

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.

Firmware Compliance Summary

Check if your HCI cluster is compliant with De

Updating View Details

Compliance last checked :22-Aug-2022 05:10:

Overall Compliance

Comp 97%

ended

Optional 0

Firmware Update Status

Update Statistics:
Started at: 2022-09-22 06:01:11 AM
Update in progress. Please wait...

Update Status:

Node Name	Status
AX640-W22-N2	RunningPreUpdateScript
AX640-W22-N1	Waiting

Figure 9: CAU update status for Windows Server HCI

The 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.

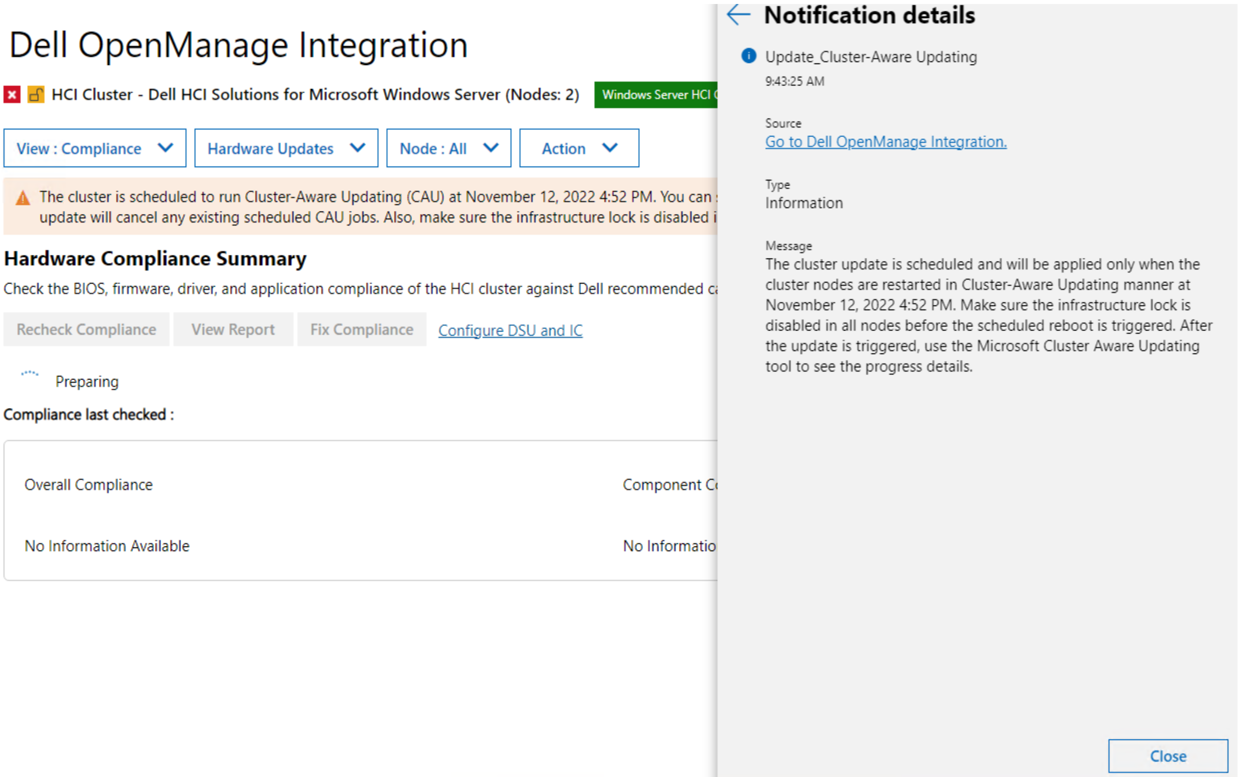
Note: While the update is in progress on the **Cluster aware update** tab, it is recommended not to exit or close the browser. If you close or exit the browser, node updates may fail, and the update status may not be shown. You can check the status by using the Microsoft Cluster Aware Updating tool, which is a part of Microsoft Failover Clustering tools and features. For more information, see the Cluster Aware Updating requirements and best practices in Microsoft document.

9. 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 report is generated, OMIMSWAC saves the information of the baseline catalog that is used for each solution.

Note: The Update feature of OMIMSWAC is supported on the host with Microsoft Windows Server 2016 and later, also Azure Stack HCI OS 21H2 and later.

Note: If BitLocker is enabled, it is "Suspended" while the hardware update is in progress. In Azure Stack HCI cluster version 22H2, BitLocker is again reenabled automatically after the update is complete.

10. If you want to run an update on the scheduled cluster, then a warning message is displayed at the top. You can still proceed with ‘**Recheck 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 OpenManage Integration

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

The cluster is scheduled to run Cluster-Aware Updating (CAU) at November 12, 2022 4:52 PM. You can s
update will cancel any existing scheduled CAU jobs. Also, make sure the infrastructure lock is disabled i

Hardware Compliance Summary

Check the BIOS, firmware, driver, and application compliance of the HCI cluster against Dell recommended ca

Preparing

Compliance last checked :

Overall Compliance: No Information Available

Component C: No Informatio

Notification details

Update_Cluster-Aware Updating

9:43:25 AM

Source

Go to Dell OpenManage Integration.

Type

Information

Message

The cluster update is scheduled and will be applied only when the cluster nodes are restarted in Cluster-Aware Updating manner at November 12, 2022 4:52 PM. Make sure the infrastructure lock is disabled in all nodes before the scheduled reboot is triggered. After the update is triggered, use the Microsoft Cluster Aware Updating tool to see the progress details.

Figure 10: Warning message when cluster update scheduled

The generated update compliance report helps 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.

4 Update hardware using the catalog generated by DRM (Offline)

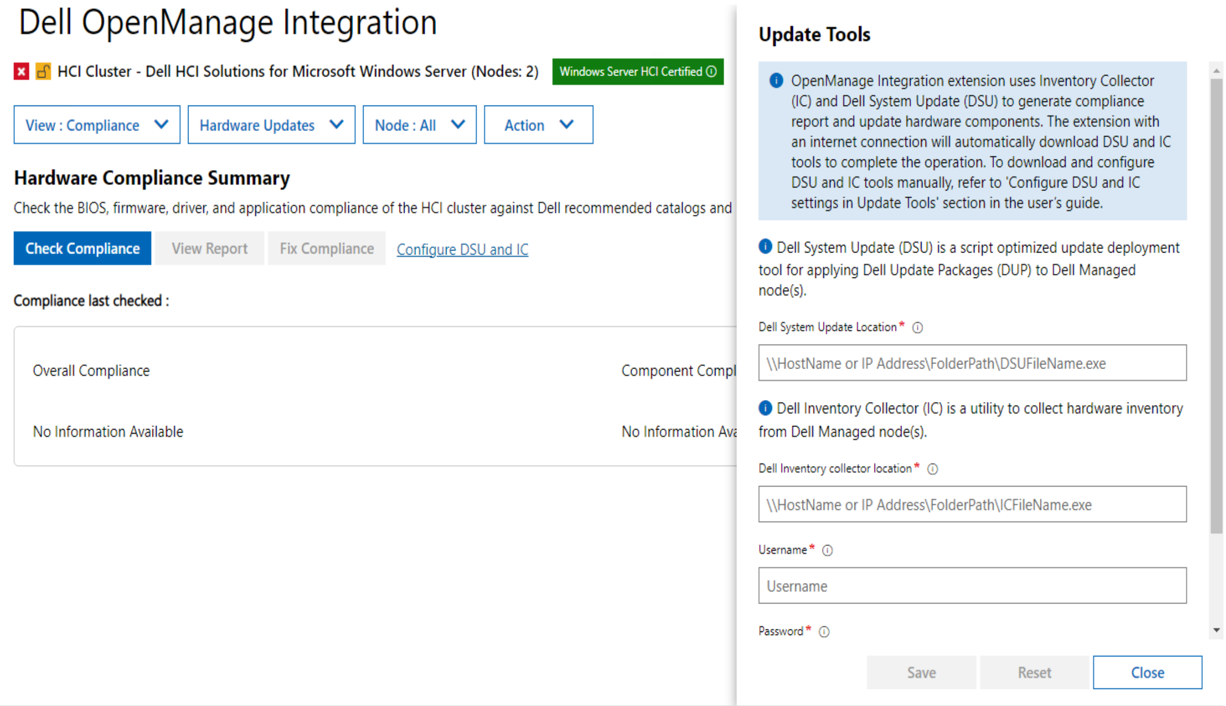
You can choose offline-Dell Repository Manager Catalog from the update source to perform hardware updates. Before you use the DRM catalog, ensure to create a DRM catalog first and place it in a shared drive where the extension can access. You can use the DRM catalog when you do not have an active Internet connection, or you want to use a customized catalog to generate compliance reports and update hardware components.

4.1 Configure Dell System Update and Dell Inventory Collector tools

OMIMSWAC uses the standard and supported Dell Server Update tools such as, Dell System Update (DSU) and Dell Inventory Collector (IC), to generate compliance report. The extension downloads the catalog and retrieves the DSU and IC tools, which are configured from a CIFS share, and generates a compliance report. If DSU and IC tools are not configured manually, then the extension downloads them from downloads.dell.com to generate a compliance report.

To generate a compliance report using the offline method, you must configure the DSU and IC.

1. Install the latest version of the OMIMSWAC extension. For installation instructions, see *OMIMSWAC User's Guide.*
2. In the left pane of Windows Admin Center, select **Dell OpenManage Integration**. Click **View** > **Compliance**. Select **Hardware Updates**. Alternatively, click the **Hardware Updates** from the **Action** menu. A window is displayed on the right side, select **Update Tools** from dropdown.



Hardware Compliance Summary

Check the BIOS, firmware, driver, and application compliance of the HCI cluster against Dell recommended catalogs and

Compliance last checked :

Overall Compliance: No Information Available

Component Compl: No Information Ava

OpenManage Integration extension uses Inventory Collector (IC) and Dell System Update (DSU) to generate compliance report and update hardware components. The extension with an internet connection will automatically download DSU and IC tools to complete the operation. To download and configure DSU and IC tools manually, refer to 'Configure DSU and IC settings in Update Tools' section in the user's guide.

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

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

Dell Inventory Collector (IC) is a utility to collect hardware inventory from Dell Managed node(s).

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

Username * : Username

Password *

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

3. In the **Configure DSU and IC** tab, to download DSU and IC tools, check the **Configure DSU and IC settings manually** section from OMIMSWAC user's guide 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. These settings are retained for subsequent sessions and will only be deleted when WAC is uninstalled, and not when the OMIMSWAC extension is uninstalled.

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

You can also use proxy settings to download catalog, DSU, and IC utilities from the Internet to generate compliance reports only. For more information about proxy settings, see Configure proxy settings. To update hardware components using Proxy, configure the proxy in WAC settings.

4.2 Create a baseline catalog by using Dell Repository Manager (DRM)

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

Before you update hardware components using the offline method, you must create a catalog using DRM.

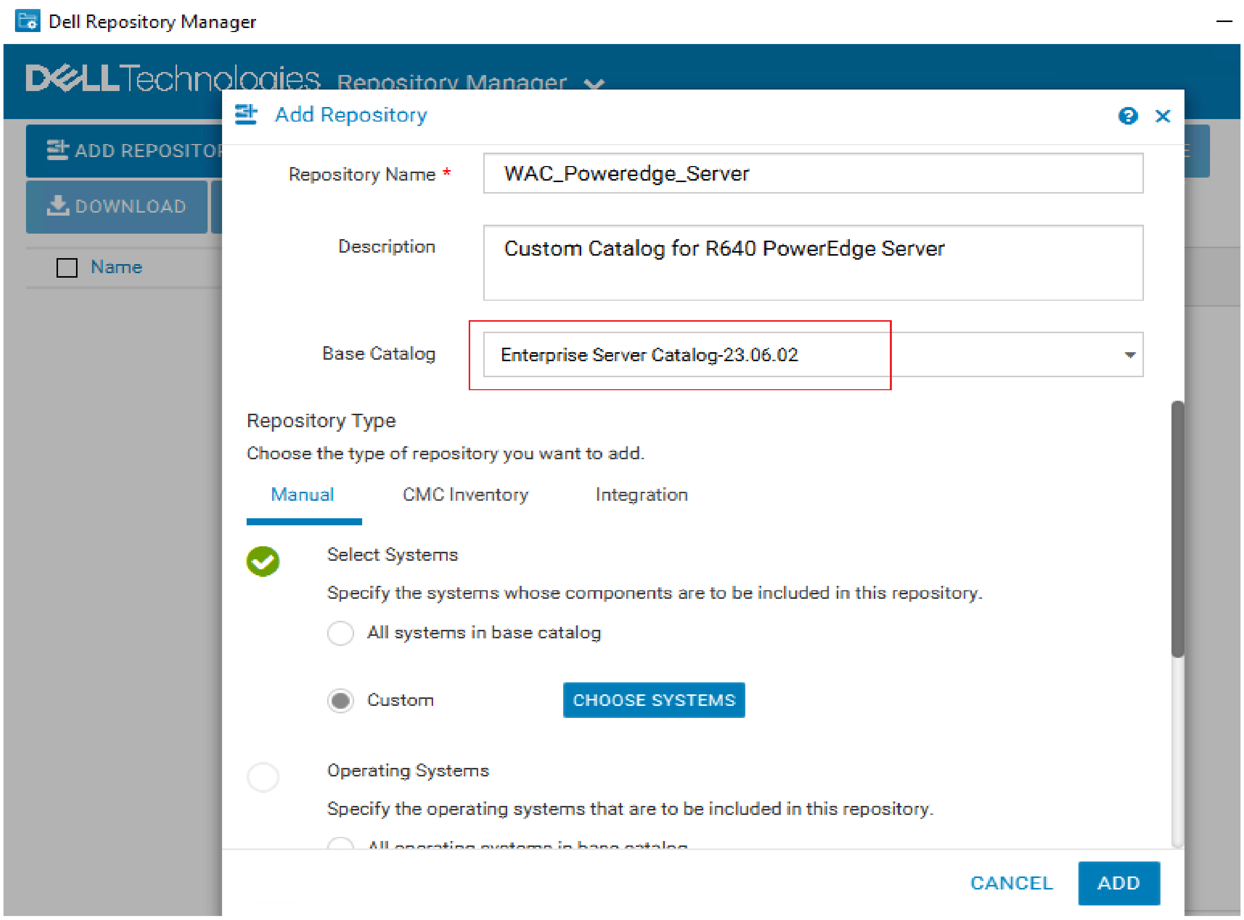
To create a baseline catalog:

1. Download and install the DRM utility from here. For more information about downloading and using DRM, see the Dell Repository Manager User’s Guide.

Note: Ensure that the system used for downloading DRM has an active Internet connection.

2. From the Start menu, select Dell Repository Manager.
3. To create a 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. This catalog contains recommended firmware and drivers for general-purpose PowerEdge servers.



Repository Name * WAC_Poweredge_Server

Description Custom Catalog for R640 PowerEdge Server

Base Catalog Enterprise Server Catalog-23.06.02

Repository Type

Choose the type of repository you want to add.

Select Systems

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

○ All systems in base catalog

● Custom

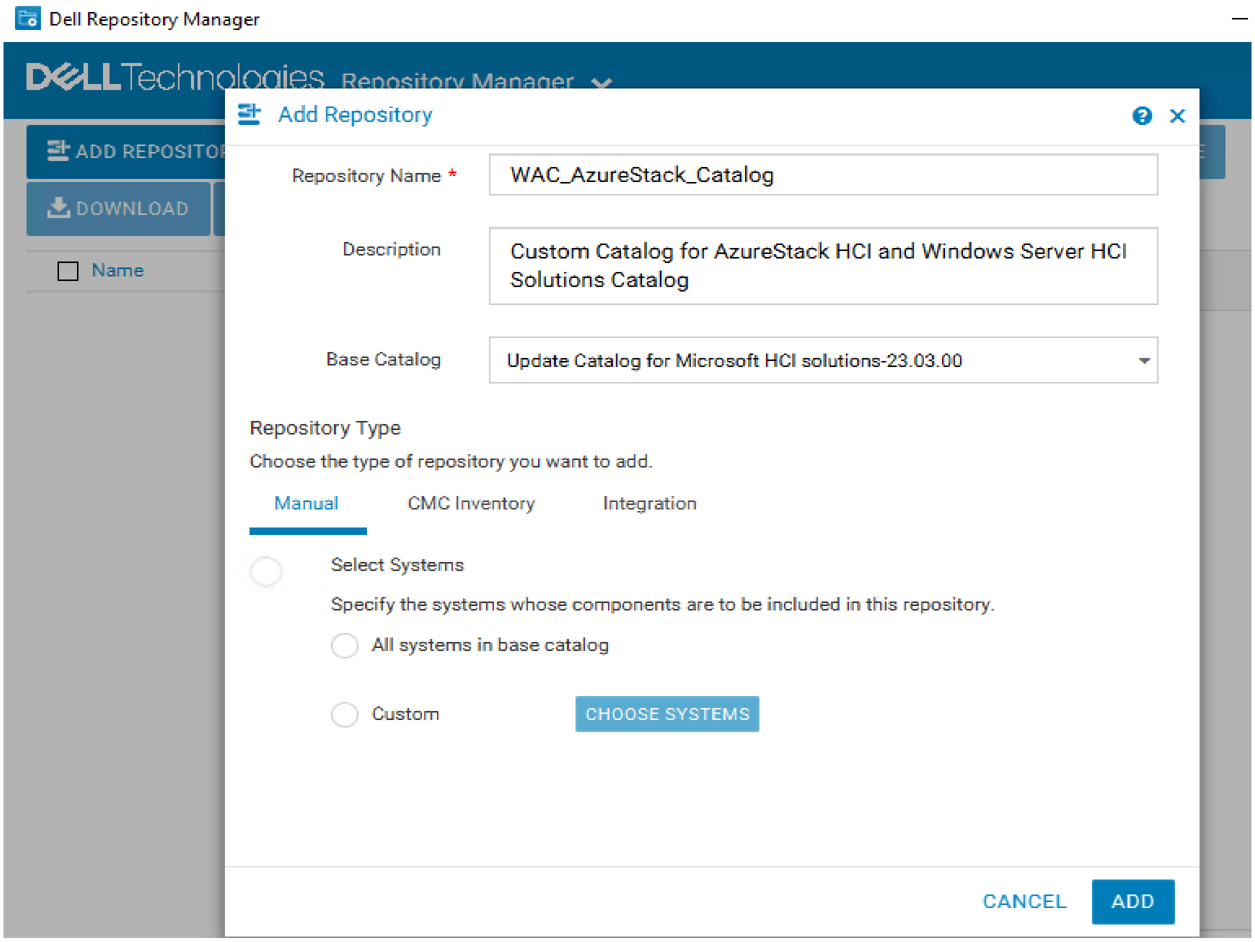
Operating Systems

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

○ All operating systems in base catalog

Figure 12: Add repository in DRM

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



Repository Name * WAC_AzureStack_Catalog

Description: Custom Catalog for AzureStack HCI and Windows Server HCI Solutions Catalog

Base Catalog: Update Catalog for Microsoft HCI solutions-23.03.00

Repository Type

Choose the type of repository you want to add.

Manual | CMC Inventory | Integration

○ Select Systems

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

○ All systems in base catalog

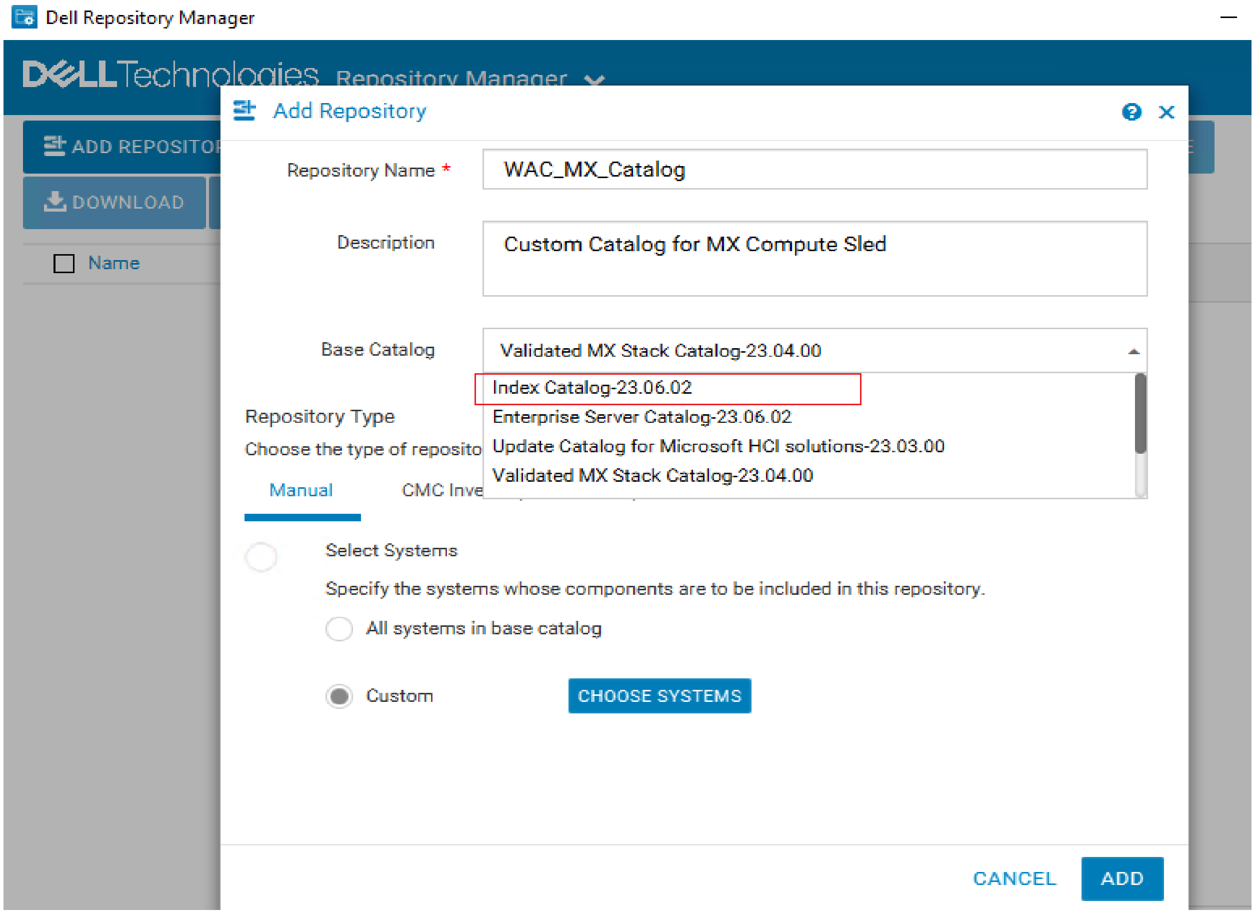
○ Custom

Figure 13: 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 provides validated firmware for MX Compute Sleds. To create a validated MX catalog, select **Index Catalog** from the **Base Catalog** dropdown list.



Repository Name * WAC_MX_Catalog

Description Custom Catalog for MX Compute Sled

Base Catalog Validated MX Stack Catalog-23.04.00

- Index Catalog-23.06.02
- Enterprise Server Catalog-23.06.02
- Update Catalog for Microsoft HCI solutions-23.03.00
- Validated MX Stack Catalog-23.04.00

Repository Type

Choose the type of reposito

○ Select Systems

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

○ All systems in base catalog

● Custom

Figure 14: Add repository in DRM

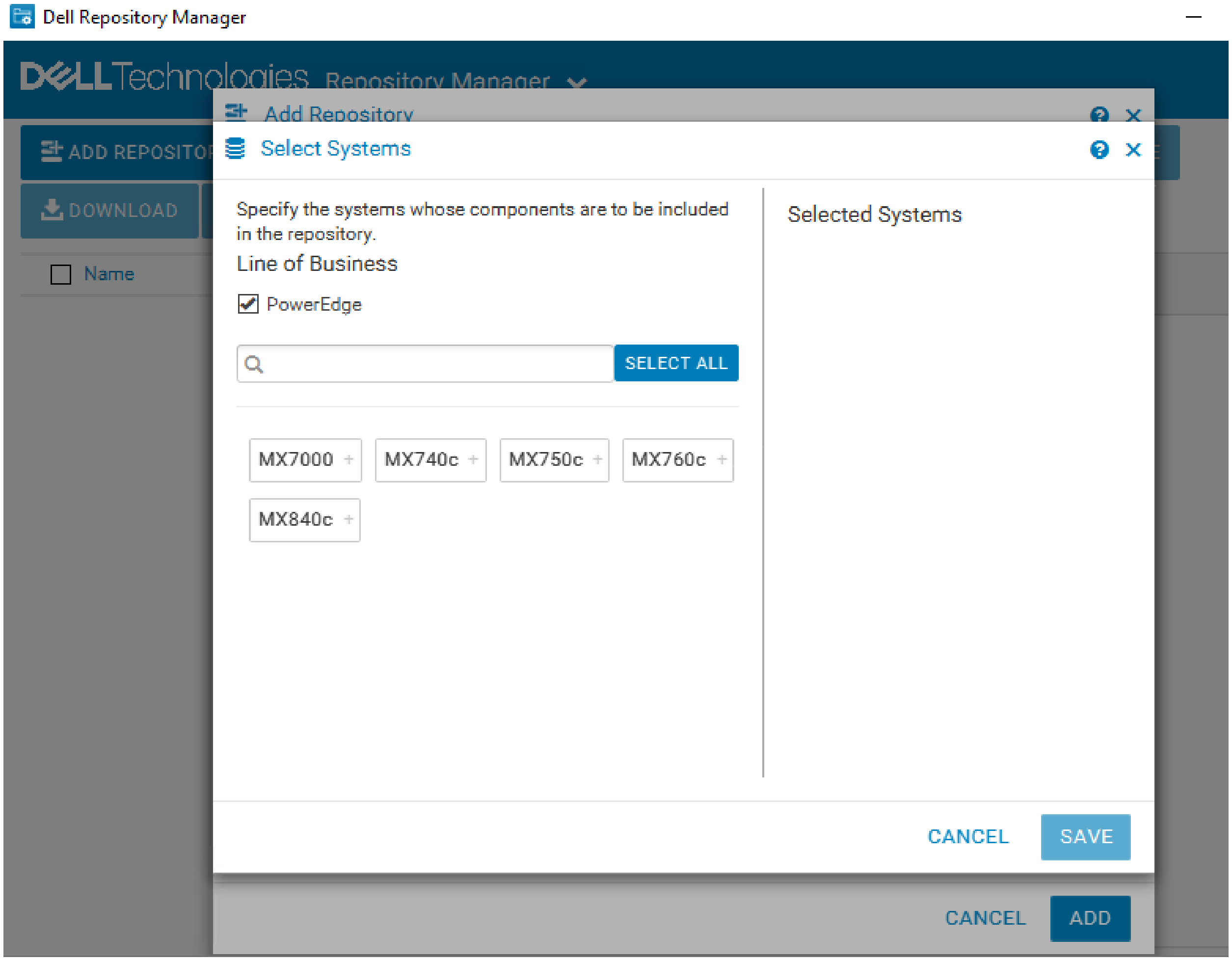
i Select **Catalog Groups** as **Validated MX Stack Catalog**.

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 the pane.



Dell Repository Manager

Select Systems

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

Line of Business

☑ PowerEdge

Figure 15: 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.

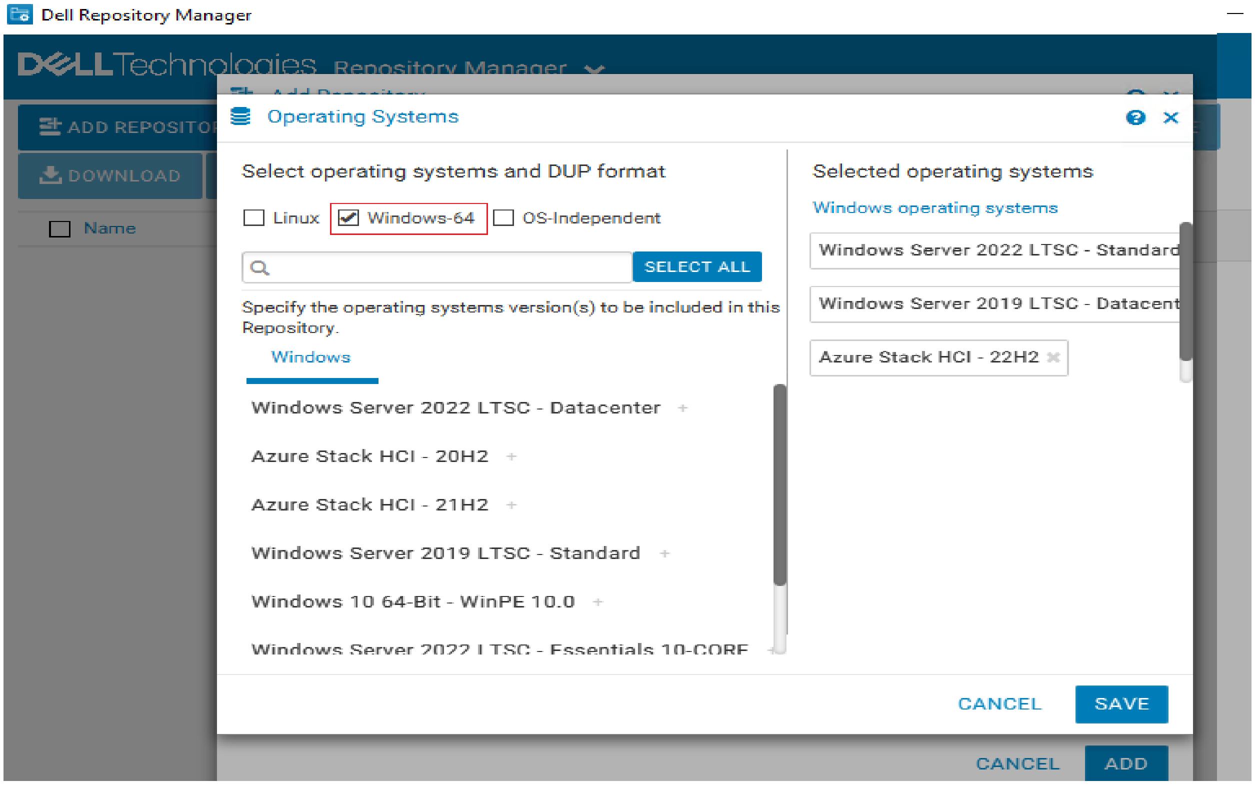
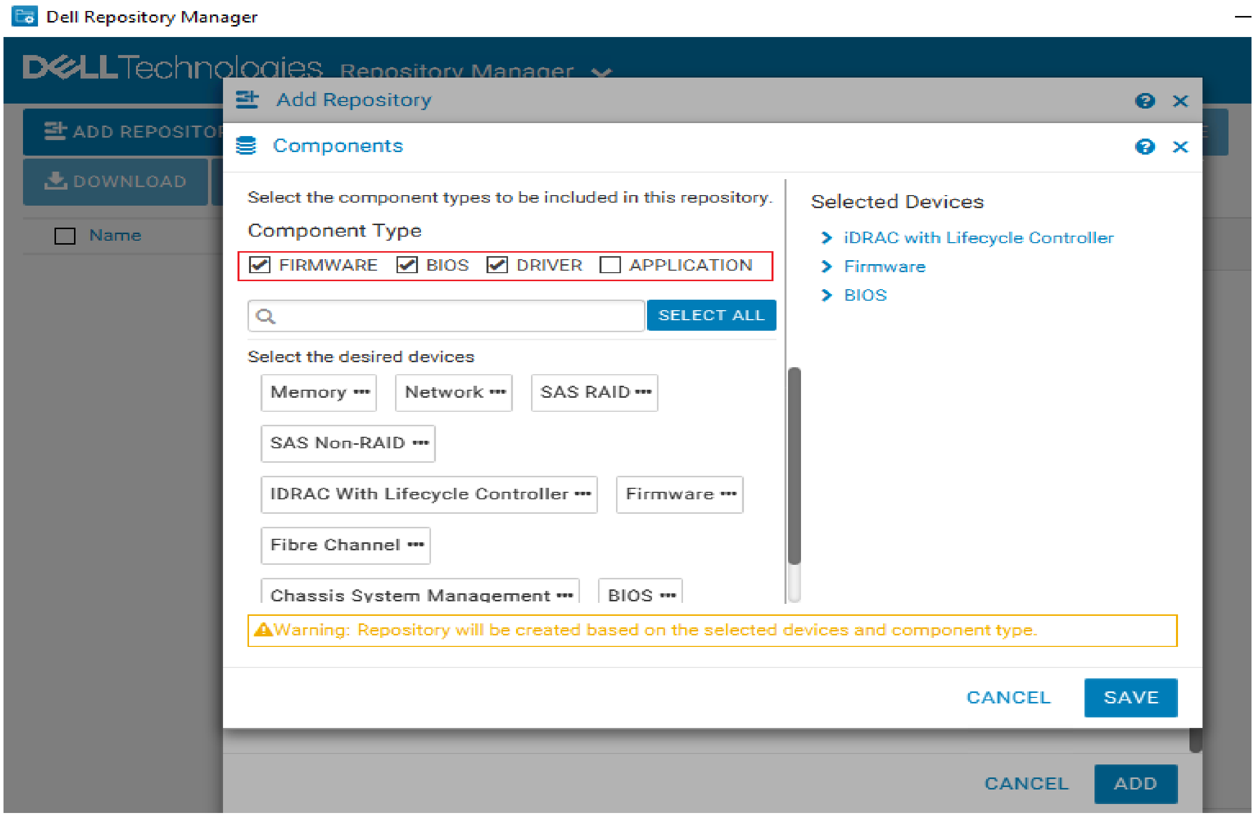

Dell Repository Manager
DELL Technologies Repository Manager
ADD REPOSITORY
DOWNLOAD
Name
Operating Systems
Select operating systems and DUP format
□ Linux
☑ Windows-64
□ OS-Independent
SELECT ALL
Specify the operating systems version(s) to be included in this Repository.
Windows
Windows Server 2022 LTSC - Datacenter +
Azure Stack HCI - 20H2 +
Azure Stack HCI - 21H2 +
Windows Server 2019 LTSC - Standard +
Windows 10 64-Bit - WinPE 10.0 +
Windows Server 2022 LTSC - Essentials 10-CORE +
Selected operating systems
Windows operating systems
Windows Server 2022 LTSC - Standard
Windows Server 2019 LTSC - Datacent
Azure Stack HCI - 22H2
CANCEL
SAVE
CANCEL
ADD

Figure 16: 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

Select the desired devices

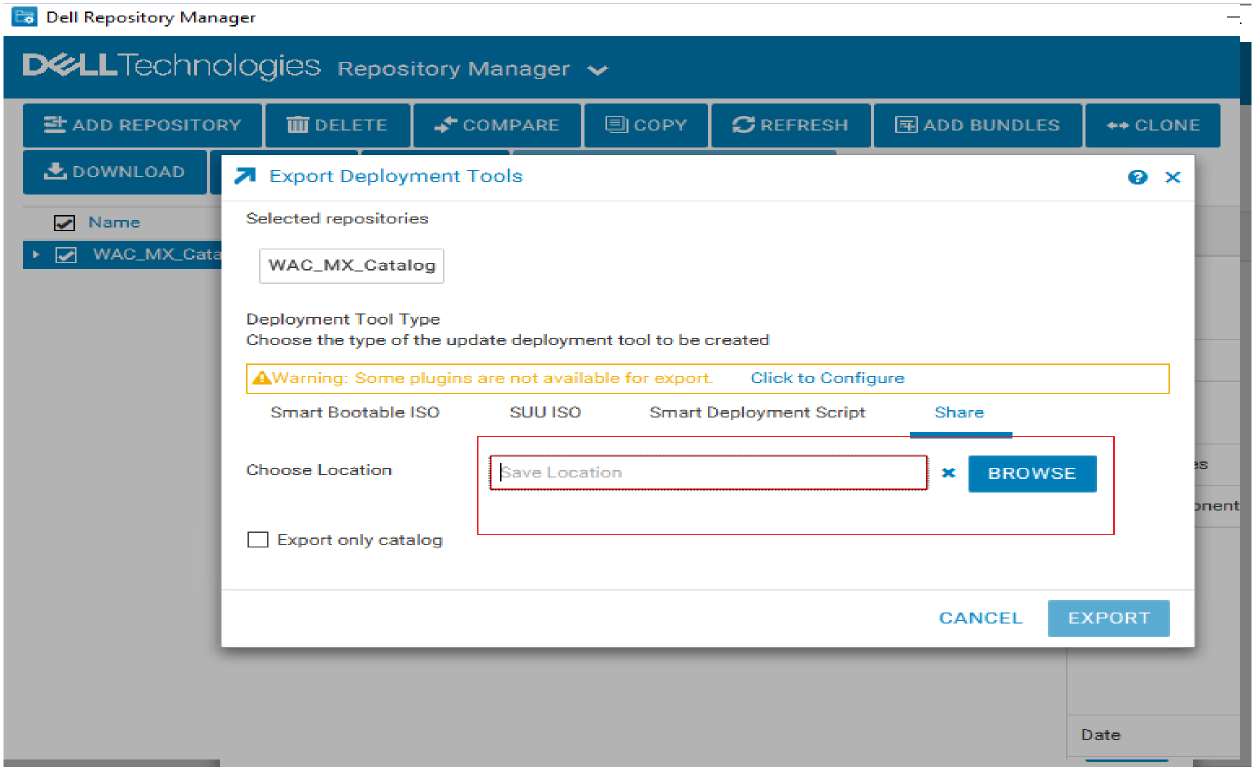
Selected Devices

- iDRAC with Lifecycle Controller
- Firmware
- BIOS

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

Figure 17: 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**.



Export Deployment Tools

Selected repositories

WAC_MX_Catalog

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 ✖ BROWSE

□ Export only catalog

CANCEL EXPORT

Figure 18: Export in DRM

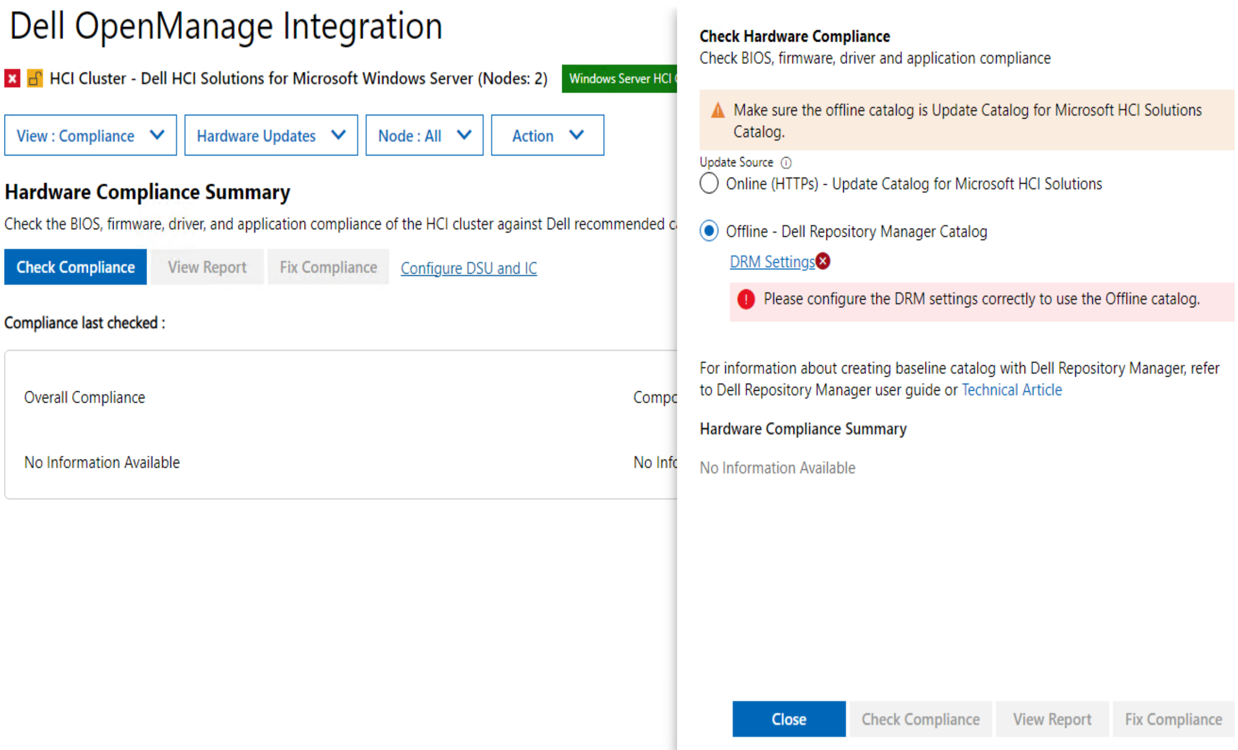
Note: The gateway administrator of the Microsoft Windows Admin Center must have access to the selected network file share.

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 later.

4.3 Generate compliance report

To generate compliance reports for firmware, BIOS, drivers, and application components in OMIMSWAC using the offline catalog, follow these steps:

1. In the left pane of Windows Admin Center, under **EXTENSIONS**, click **Dell OpenManage Integration**.
2. Click **View > Compliance**. Another menu appears, select **Hardware Updates**. Hardware Compliance Summary page appears.
   Alternatively, go to the Action menu, under HARDWARE COMPLIANCE AND REMEDIATION, and click Check Compliance.
3. Click the **Check Compliance** button, and then under **Update Source**, select “Offline - Dell Repository Manager Catalog”. This option allows you to use the DRM catalog configured in a CIFS location in OMIMSWAC, with or without Internet access. You may opt for this when Internet access is unavailable or when using a customized DRM catalog.



Hardware Compliance Summary

Check the BIOS, firmware, driver, and application compliance of the HCI cluster against Dell recommended c

Compliance last checked :

Overall Compliance — No Information Available

Compo — No Info

Check Hardware Compliance

Check BIOS, firmware, driver and application compliance

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 Repository Manager Catalog

DRM Settings

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

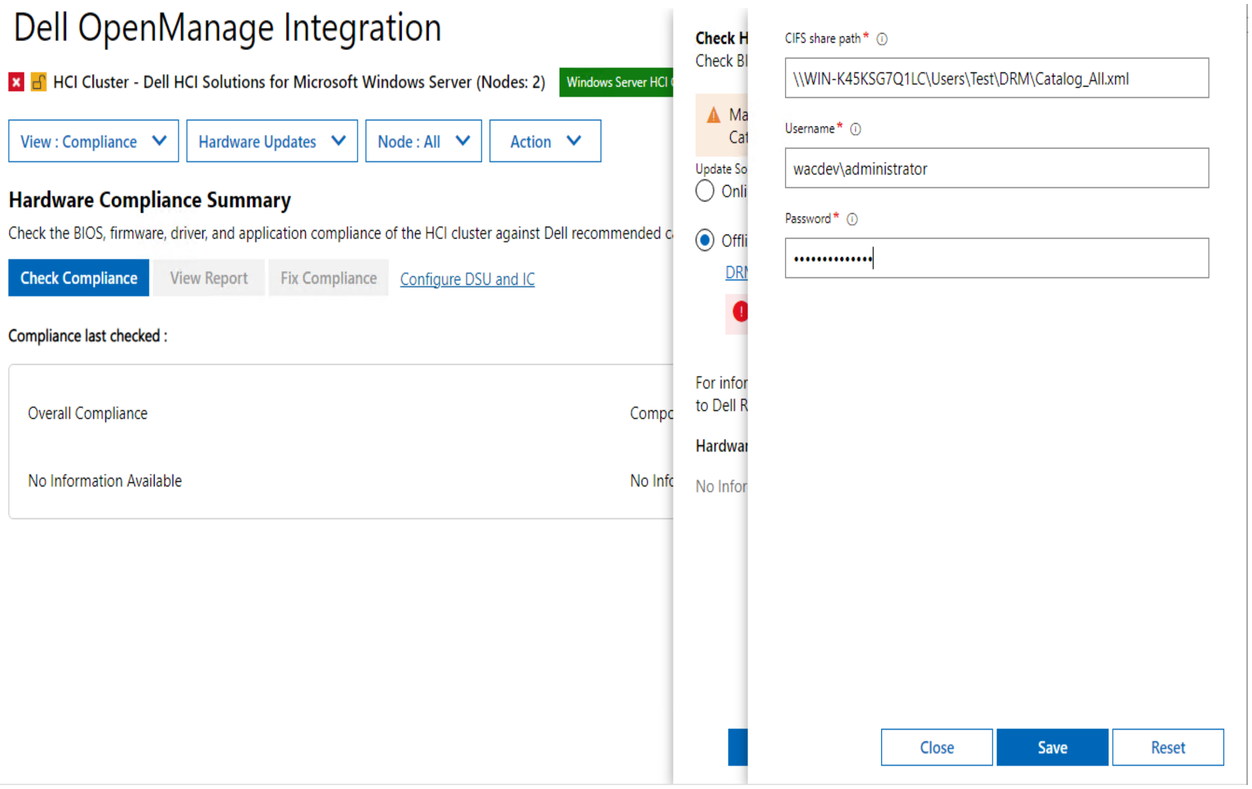
For information about creating baseline catalog with Dell Repository Manager, refer to Dell Repository Manager user guide or Technical Article

Hardware Compliance Summary

No Information Available

Figure 19: Select Update Source in OMIMSWAC

4. To use the offline catalog, select **DRM Settings** to ensure the CIFS share path is configured with the DRM catalog. The supported version of the DRM application can be downloaded from https://www.dell.com/support/kbdoc/en-in/000177083/support-for-dell-emc-repository-manager-drm.
5. Enter the catalog file share location (suffixed with the catalog file name) and credentials to access the file share location as given below.



CIFS share path *: \\WIN-K45KSG7Q1LC\Users\Test\DRM\Catalog_All.xml

Username *: wacdev\administrator

Password *: ••••••••••••••

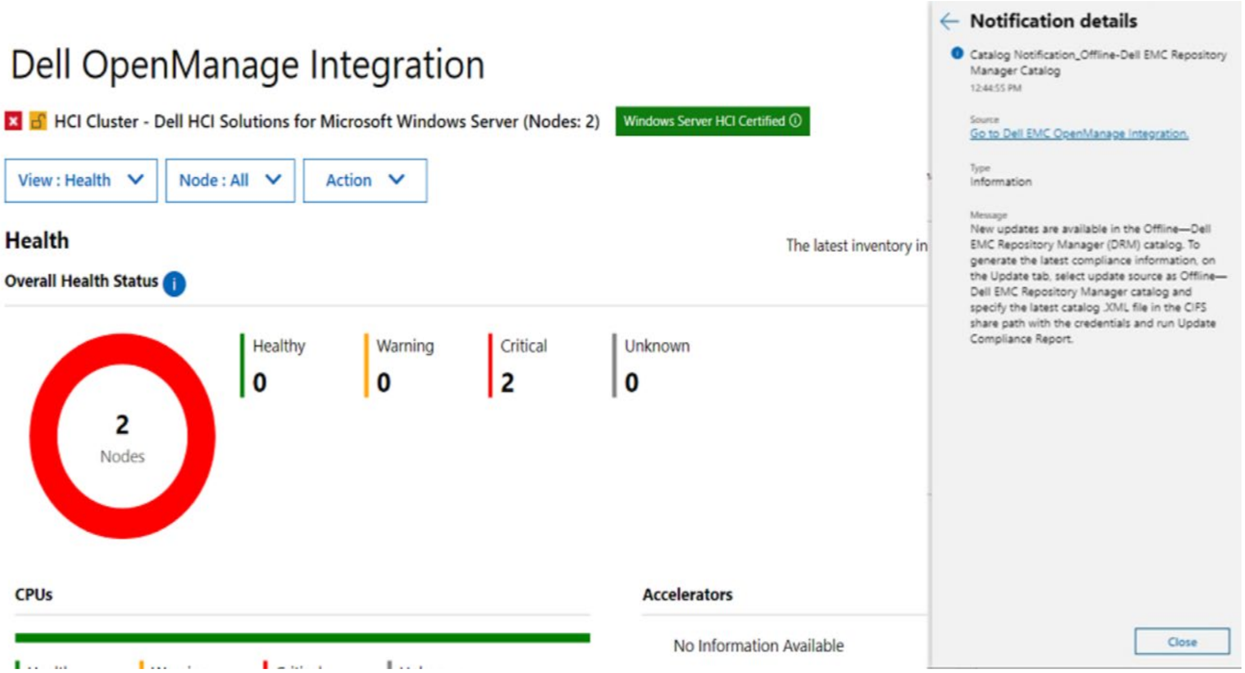
Figure 20: User provides catalog details to generate a comparison report for Azure Stack HCI servers.

It is recommended to select the appropriate catalog for different types of solutions such as, PowerEdge servers, Hyper-V based Failover clusters, and Microsoft Azure Stack HCI clusters. For more information, see *Creating a baseline catalog by using Dell Repository Manager (DRM).*

Note: It is recommended to use the “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 the server manager, and cluster manager respectively.

6. To use the Dell System Update (DSU) and Inventory Collector (IC) tools, see configuring Dell System Update and Dell Inventory Collector tools
7. Click **Save** to store the DRM catalog configuration details, and then click **Check Compliance** to generate the update the compliance report.
8. After the update compliance report 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 will receive notification automatically from the OMIMSWAC extension.



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 21: Node health status and new offline catalog notification

The generated compliance report helps 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.

4.4 Update hardware components

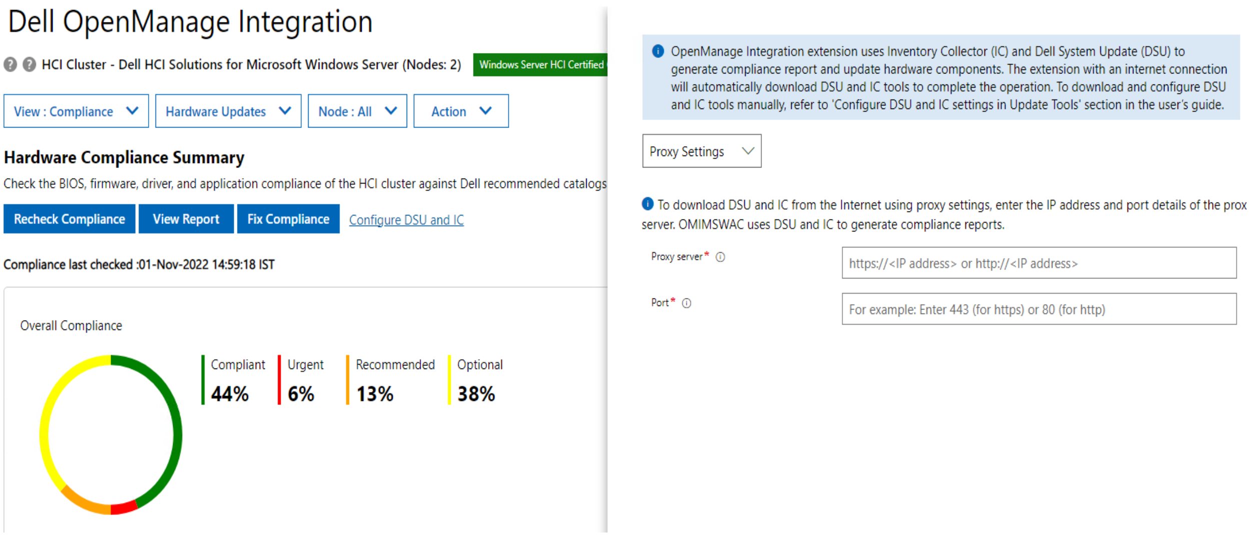
See Update hardware components in section 3.2.

5 Configure proxy settings

The OpenManage Integration extension provides an option to download catalog, DSU, and IC utilities from the Internet using proxy settings to generate compliance reports. However, proxy configurations do not allow updating target nodes or clusters using online catalogs. In such cases, compliance and updates can be accomplished using the offline catalog.

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 checks the Internet connectivity using the proxy settings.

Note: Proxy settings are not supported in the OpenManage Integration snap-in.



Dell OpenManage Integration

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

Hardware Compliance Summary

Check the BIOS, firmware, driver, and application compliance of the HCI cluster against Dell recommended catalogs

Compliance last checked :01-Nov-2022 14:59:18 IST

Overall Compliance: Compliant 44%, Urgent 6%, Recommended 13%, Optional 38%

OpenManage Integration extension uses Inventory Collector (IC) and Dell System Update (DSU) to generate compliance report and update hardware components. The extension with an internet connection will automatically download DSU and IC tools to complete the operation. To download and configure DSU and IC tools manually, refer to 'Configure DSU and IC settings in Update Tools' section in the user's guide.

Proxy Settings

To download DSU and IC from the Internet using proxy settings, enter the IP address and port details of the prox server. OMIMSWAC uses DSU and IC to generate compliance reports.

Proxy server* https://<IP address> or http://<IP address>

Port* For example: Enter 443 (for https) or 80 (for http)

Figure 22: Proxy Configuration.

To connect to a proxy server:

1. In the OpenManage Integration extension, click the **Settings** icon. A window is displayed the right side, select **Proxy Settings** from the dropdown.
2. Enter the IP address of the proxy server in the following format: https://<IP address> or http://<IP address>
3. Enter the Port number of the proxy server in the following format and click **Save**. <port number> (https) or <port number> (http)

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

6 Troubleshooting

If the update operation fails, check the log files that is stored at the following path for more details.

- Gateway system: *<WindowsDirectory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs*
- Windows 10 gateway system: *<WindowsDirectory>\Users\<user_name>\AppData\Local\Temp\generated\logs*
- After the scheduled cluster update is over, logs for individual nodes can be found in *<WindowsDirectory>\Temp\OMIMSWAC* folder on the respective nodes.
- Logs for pre-update script running on HCI clusters to put storage into maintenance mode are available at <*Windows Directory*>*\Temp\precau.log* on each node.
- Logs for post update script running on HCI clusters to restore storage from maintenance mode are available at <*Windows Directory*>*\Temp\postcau.log* on each node.