DELL Technologies

Technical Whitepaper

Onboard Dell HCI Configuration Profile (HCP) policies to Azure Arc from Windows Admin Center

Abstract

This white paper provides guidance to onboard Dell HCI Configuration Profile (HCP) Policies to Azure Arc so that administrators can leverage those policies and can check the compliance against the cluster.

December 2022

Revisions

Date	Description
June 2022	Initial release
December 2022	Updated due to UI Revamp

Acknowledgments

This paper was produced by the following:

Authors:

- Pradeep Shetty —Software Senior Engineer
- Ria Susan Jacob — Software Engineer 2

Support: Ajit Parhi

Table of Contents

Acronyms

Acronyms	Expansion
iDRAC	Integrated Dell Remote Access Controller
OMIMSWAC	OpenManage Integration with Microsoft Windows Admin Center
MS API	Microsoft Application Programming Interface
HCI	Hyper-Converged Infrastructure
HCP	HCI Configuration Profile

Executive Summary

This white paper provides guidance for onboarding Dell Azure Policies to Azure Arc so that administrators can leverage those policies to monitor cluster compliance.

Intended Audience

The intended audience of this document are IT administrators who use OMIMSWAC to onboard HCP policies to Azure Arc to monitor Dell Integrated System for Microsoft Azure Stack HCI (also known as Azure Stack HCI cluster) created using AX nodes from Dell Technologies.

1 Introduction

Since Azure Arc is the one of the primary management tools for resource management on cloud and hybrid platforms, it is essential that Dell HCI Configuration Profile (HCP) policies help administrators maintain HCP compliance throughout HCI cluster/host lifecycle.

Dell HCP is the specification (collection) from Dell that captures the best practice configuration recommendation for Azure Stack HCI solutions from Dell. Therefore, Dell Technologies recommends that administrators strictly adhere to the HCP recommendations to improve the performance and resilience of their HCI solutions.

OMIMSWAC helps administrators to onboard Dell HCP Policies to Azure Arc so that they can leverage those policies to monitor cluster compliance.

Prerequisites: For more information, see Prerequisite.

Onboarding policies into Azure: For more information, see Onboarding policies into Azure.

Onboarded Policies Report: For more information, see Export the Onboarded Policies Report.

Update HCP Policies: For more information, see Update HCP Policies.

Remediate HCP Policies: For more information, see Remediate HCP Policies.

2 Prerequisites

Ensure your Azure Stack HCI cluster meets the following prerequisites before you onboard HCP policies to Azure Arc:

- Users must have an Azure subscription.
- WAC gateway must be registered into Azure. For more information, see WAC Gateway Registration into Azure.
- Azure Stack HCI Cluster nodes must have Dell supported model & OS and all node models & OS must be same across the cluster. For more information, see Model and OS check.
- “OMIWAC Premium License” is required for each of the nodes. For more information, see Verify License Details.

If any of the prerequisite checks fail, OMIMSWAC blocks the onboarding policies to the Azure Arc.

2.1 Register WAC Gateway with Azure

For information about registering Windows Admin Center with Azure, see Microsoft documents.

2.2 Model and OS Check

In OMIMSWAC, when you click the **Azure Integration** option from the view dropdown menu, the extension checks the cluster’s model and OS. Ensure your cluster meets the following prerequisites for model and OS.

- Azure Stack HCI Cluster nodes must have Dell supported models & OS and all node models & OS must be the same across the cluster.

OMIMSWAC 3.0 and higher versions supports YX4X and YX5X PowerEdge servers for onboarding HCP policies to Azure. For more information about the supported models, see the compatibility matrix in the user's guide.

Use the latest version of the extension and refer to the updated compatibility matrix. You can also refer the "About" page in the extension for updated documentation.

Note: If any of the cluster nodes fail the model or OS check, an error banner message will appear and block further steps. For more information, see Troubleshooting section 7.1

2.3 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.

Perform the following steps to check license details:

1. In the Windows Admin Center, connect to a server or cluster.
2. In the left pane of the Windows Admin Center, under **EXTENSIONS**, click **Dell OpenManage Integration**.
3. Select **Overview** in view menu drop down and select individual node name in node drop down for cluster connections. You can see the OMIWAC license details in **System Details** section. Also, you can click **iDRAC Details** link in the right-side corner of System Details section to view more about the license details.

4. To view the license details, click on a license attribute name. For example, iDRAC9 Enterprise License, OME Server Configuration Management, OMIWAC Premium License for MSFT HCI Solutions, and more.

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

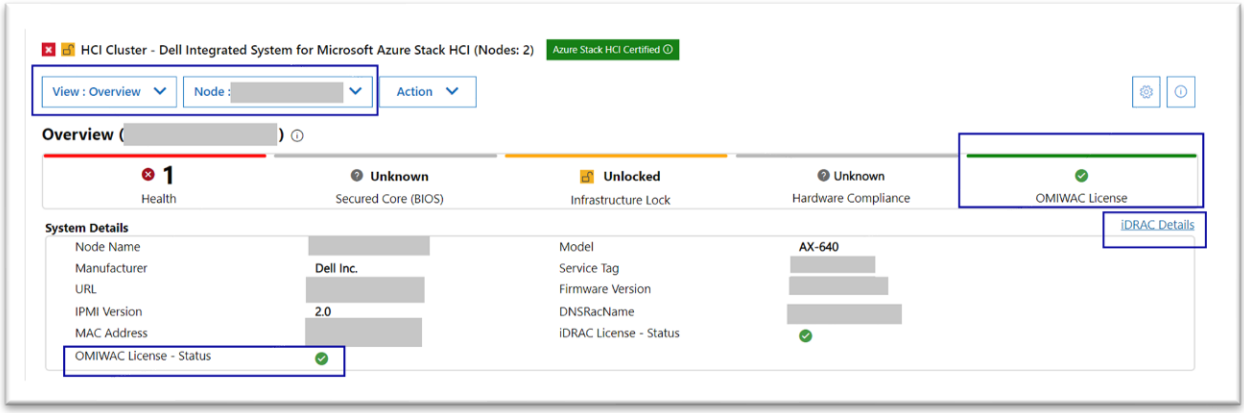

Figure 1: Verify License Details from Overview page

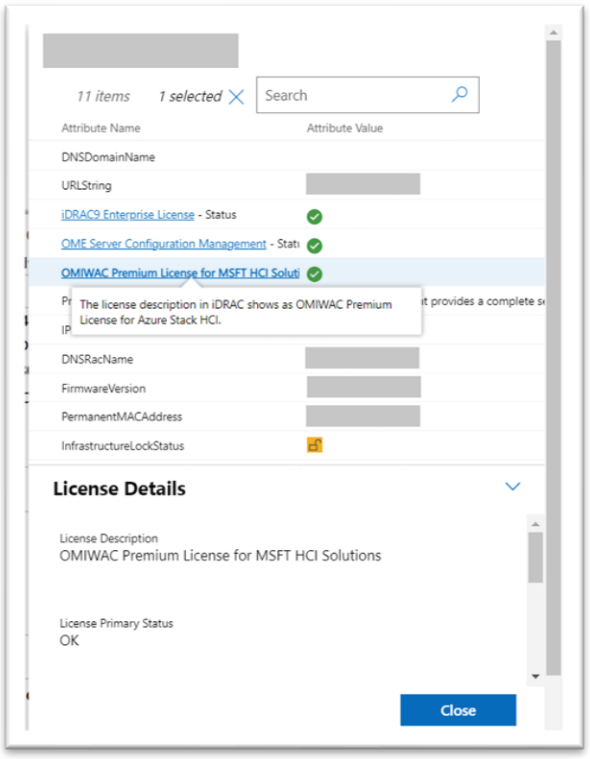

Figure 2: iDRAC Details pop-up page

Note: Ensure that OMIWAC premium licenses are installed on all cluster nodes to use the Azure feature. For more information about OMIWAC premium licensing, see OMIMSWAC Installation Guide.

3 Onboard policies into Azure

In OMIMSWAC, when you click **Azure Integration** in **View** dropdown menu , the extension checks your cluster for all the prerequisites as mentioned in the previous sections. Once the prerequisites are met, proceed to onboard the policies.

To onboard policies into Azure, perform the following steps:

Step 1: Sign-In to Azure

Step 2: Onboarding Checklist

Step 3: Onboard HCP Policies

3.1 Sign-In to Azure

Perform the following steps to sign-in to Azure:

1. Click **Sign In.** A Sign in pop up window appears. For more information, see Microsoft document.

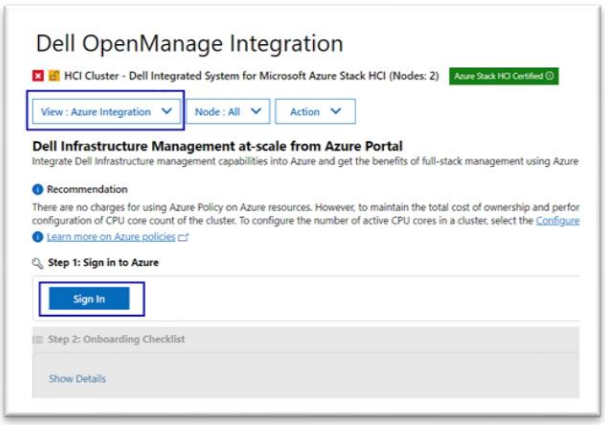

Figure 3: Sign-in

Note: Alternatively, you can also sign in to Azure from the **Overview** page. In **Azure Integration** section, click **Sign-in** to go to the Azure integration page. Sign-in pop up window will appear for you to sign In to the Azure.

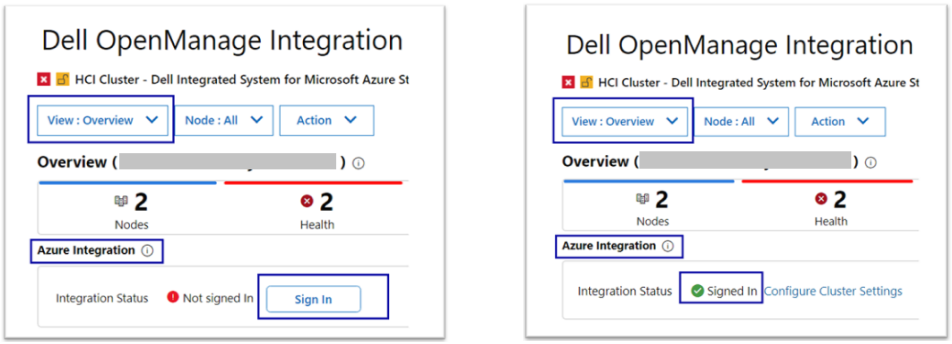

Figure 4: Sign-In from Overview page (before and after Sign-In status)

Once you have signed-In, **step 2: Onboarding Checklist** section is enabled.

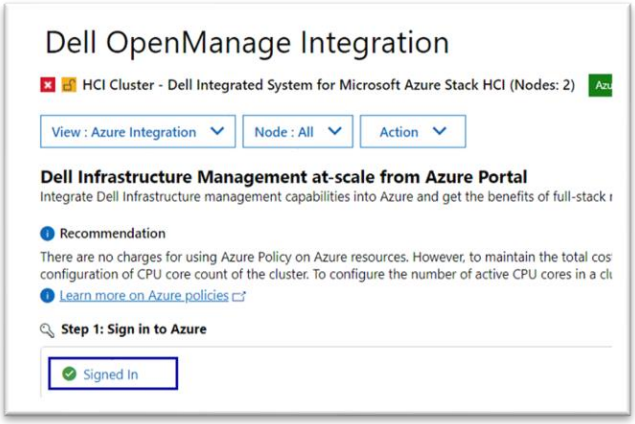

Figure 5: Sign-in status

Note: Sign-in to Azure is handled by Microsoft Windows Admin Center APIs and Dell extension does not have any control over it.

3.2 Onboarding Checklist

1. After the **step 2: Onboarding Checklist** is enabled, OMIMSWAC will check the following list to ensure that the user and the cluster meet all the onboarding checklists:

   - User must have the following list of permissions to onboard the HCP policies into Azure. Signed in user has permission to

     - create and manage policy assignments
     - create and manage policy definitions
     - create and manage policy exemptions
     - create and manage policy sets

     For more information about roles, see Microsoft document.

   - Cluster is registered and connected to Azure Arc. For more information, see Microsoft document.
   - Cluster registered resource group must be available in the Azure.

2. After all the onboarding checklists are met, the next **step 3: Onboard Policies** is enabled.

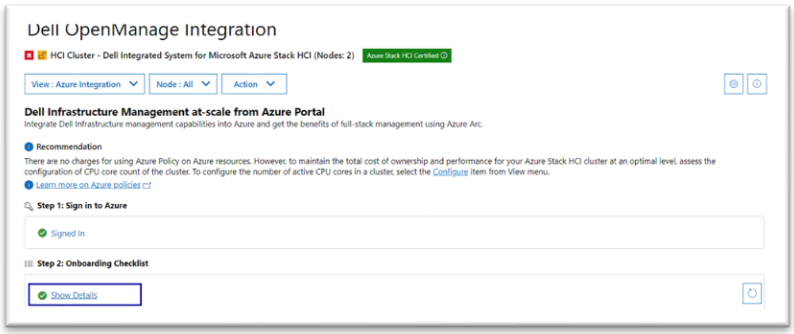

Figure 6: Onboarding chek list show details

3. Click **Show Details** to see the list of checklists and their status.

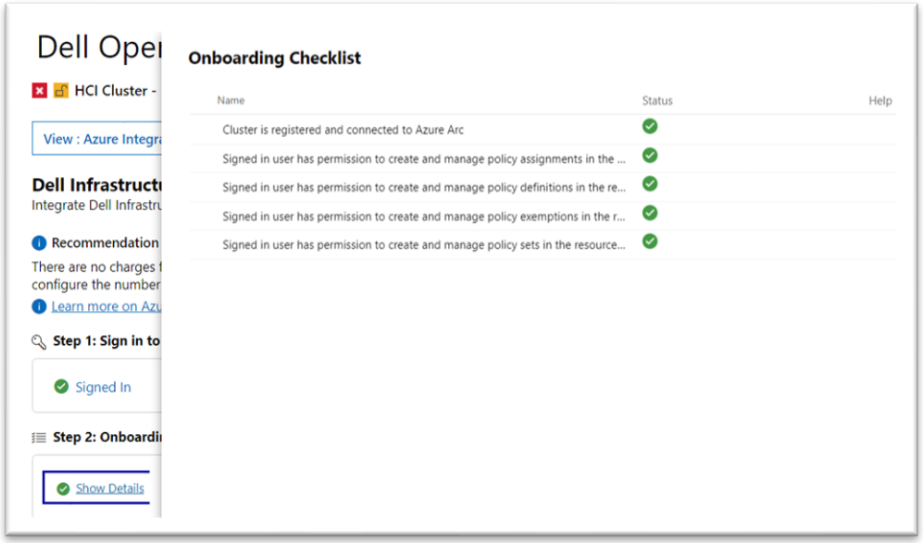

Figure 7: Onboarding checklist pop up page

3.3 Onboard HCP Policies

1. After the **Step 3: Onboard Policies** is enabled, click **View Subscription Details** to view the subscription and resource group info.

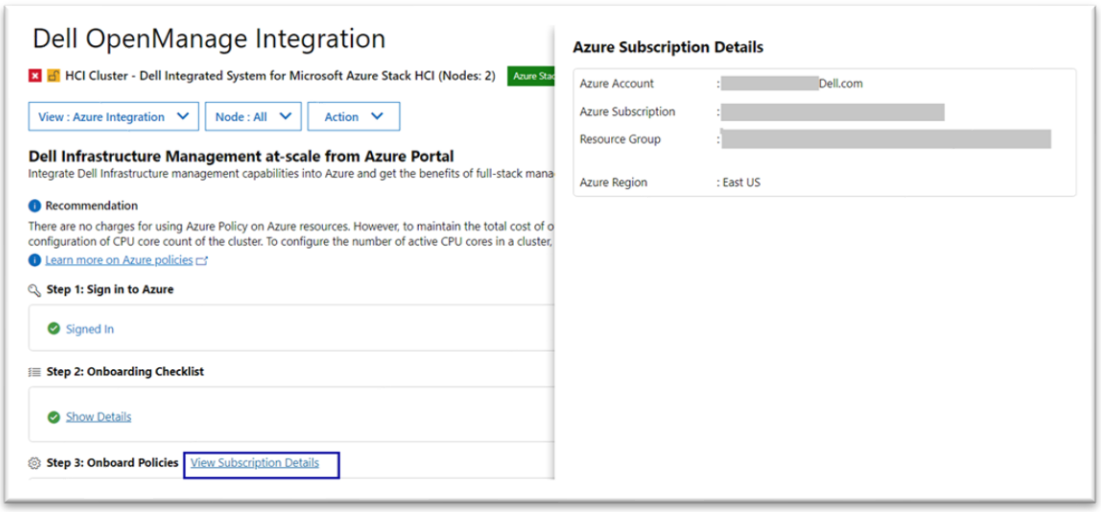

Figure 8: View subscription details

2. Click **Configure Cluster Settings** to configure the network topology and deployment model. **Cluster Settings** page appears.

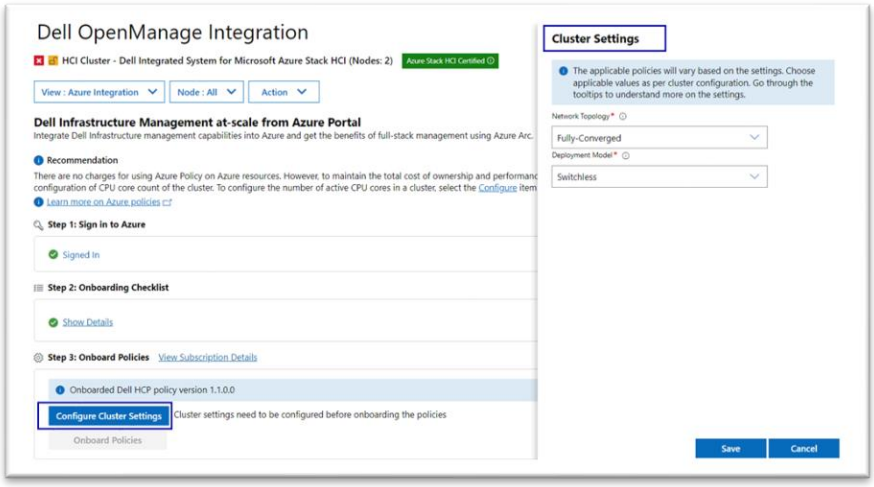

Figure 8: Cluster settings popup page

a. Select the Network Topology and Deployment model. For more information, see Appendix section 8.1
b. Click **Save.** All applicable policies for the cluster based on the selection and cluster node model are fetched.

Note: Alternatively, you can also click the **Configure Cluster Settings** link from the **Overview** page which will redirect to the "**Cluster Settings**" popup page.

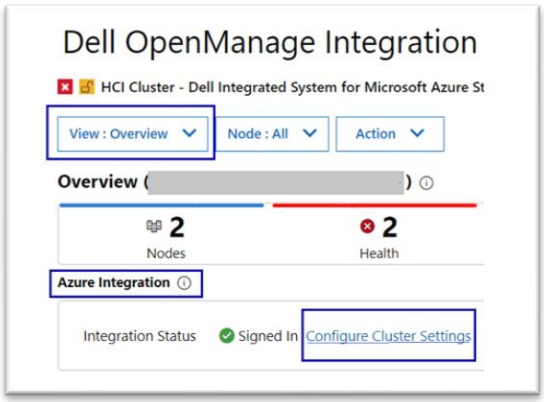

Figure 10: Configure cluster settings from overview page

3. If you want to change the network topology and deployment selection, click **Edit Cluster Settings** and repeat the above steps.

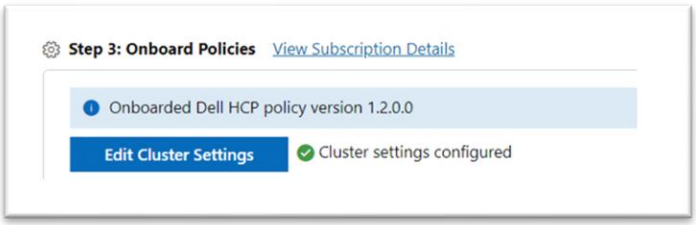

Figure 11: Edit Settings pop up page

After the policies are fetched, **Onboard Policies** button is enabled.

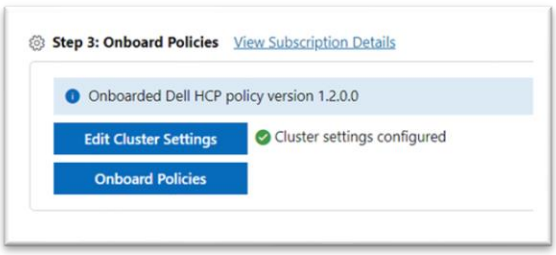

Figure 12: Onboard Policies

4. Click **Onboard Policies** to view the applicable policies for upload.
   Onboard Dell HCP policies for Azure Arc page appears on the right. In this page, the policies are grouped into three categories:

   - Dell HCI Hardware configuration policy
   - Dell HCI OS configuration policy
   - Dell HCI Cluster configuration policy

   Each group has a toggle button to collapse and expand the selections. All policies are shown as selected, and the user can de-select only non-mandatory policies.

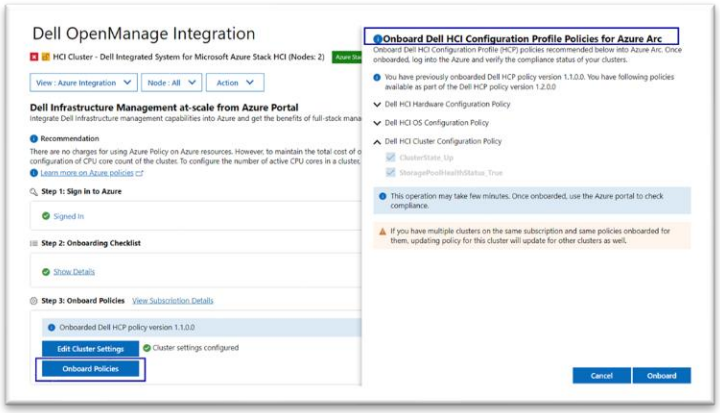

Figure 13: Onboard Policies

Note: Alternatively, you can also click the **Configure** link from the **Overview** page which will redirect to "**Onboard Dell HCI Configuration Profile Policies for Azure Arc**" popup window in Azure page.

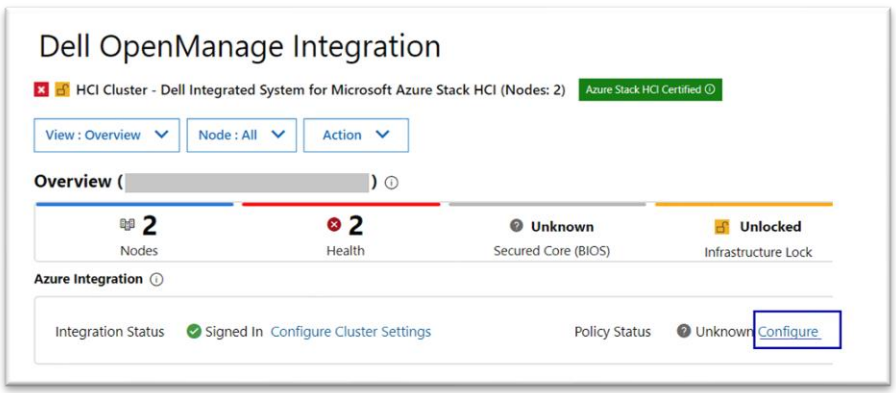

Figure 14: Configure link from Overview page

5. Click **Onboard** to onboard the policies into Azure.

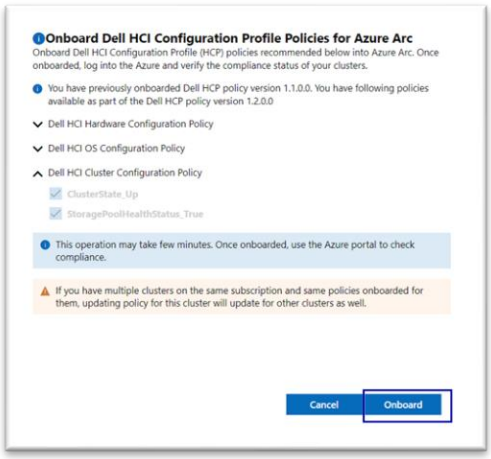

Figure 15: Onboard Dell HCI Configuration Profile Policies for Azure Arc

After you click **Onboard**, the popup closes and the onboarding of the policies to Azure begins. Policies are created in Azure and respective policy definitions along with policy assignments.

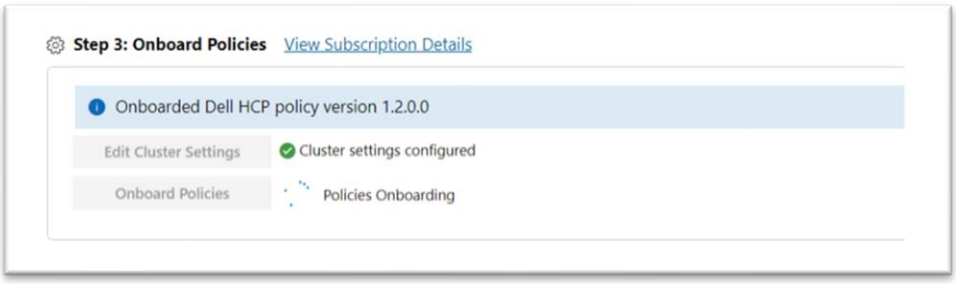

Figure 16: Onboarding Policies

6. After Onboarding is complete, **View Details** and **Export Details** links are available.
   For both Success/ Failure, corresponding notifications are shown with additional context.

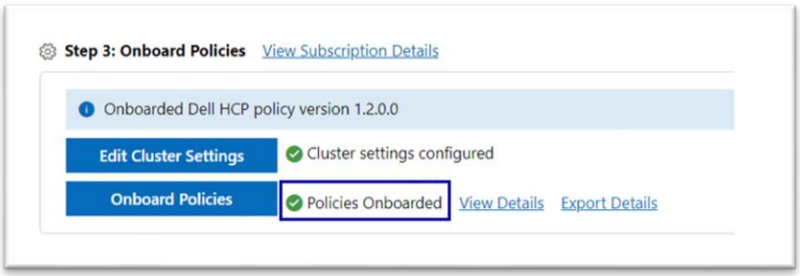

Figure 17: Policies Onboarded- status

7. Click **View Details** to view the details of each policy creation and assignments status.

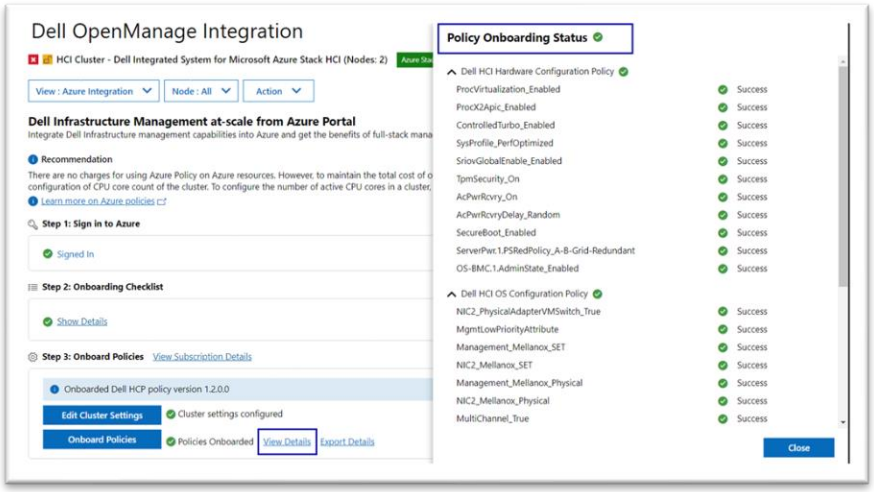

Figure 18: View Details – Onboarded Policies Status

Note: By using this feature, you can use the same policies across multiple clusters to manage multiple clusters at scale in Azure Arc.

8. Once the policies are successfully onboarded to Azure, users can view the onboarded policies in the Azure portal. For more information, see [Microsoft document].

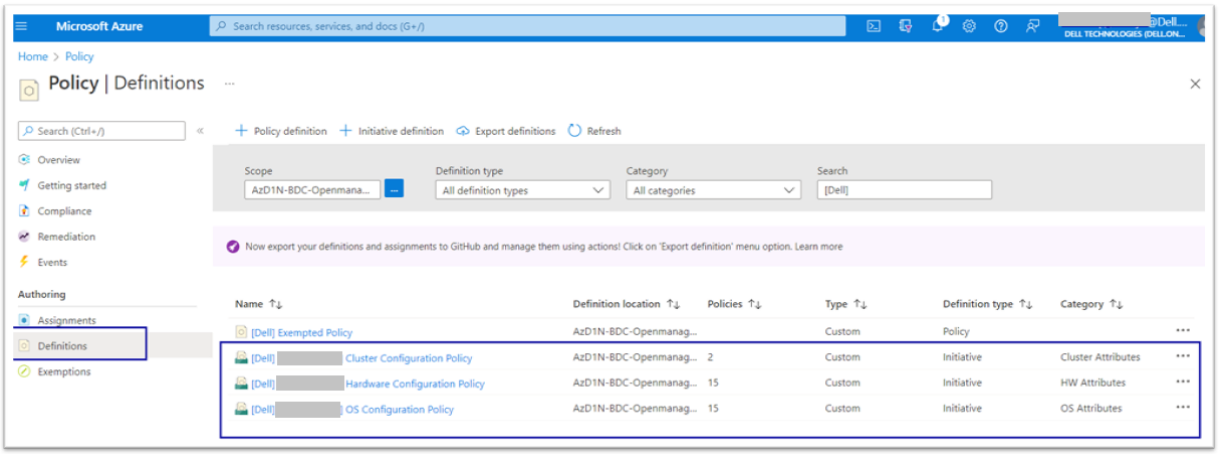

Figure 19: HCP Policy Details in Azure Portal

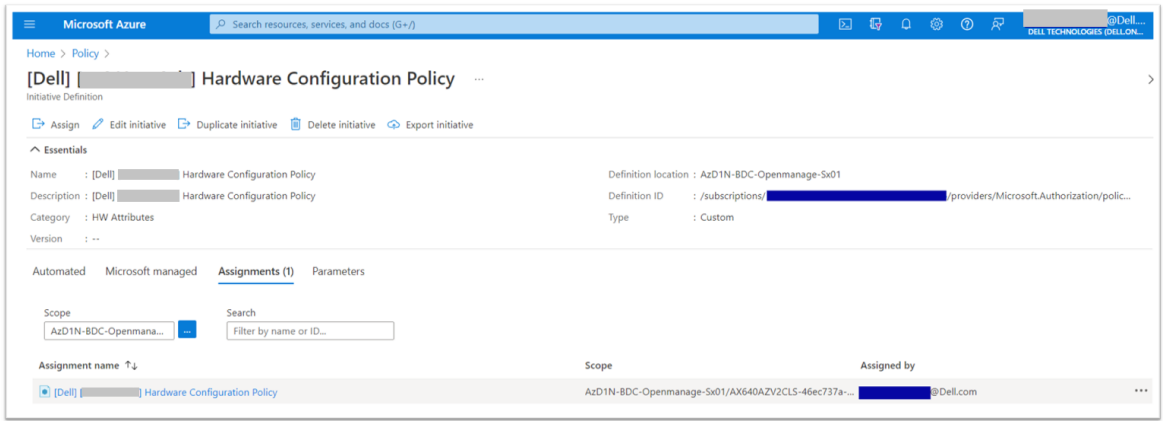

Figure 20: Policy Assignment in Azure Portal

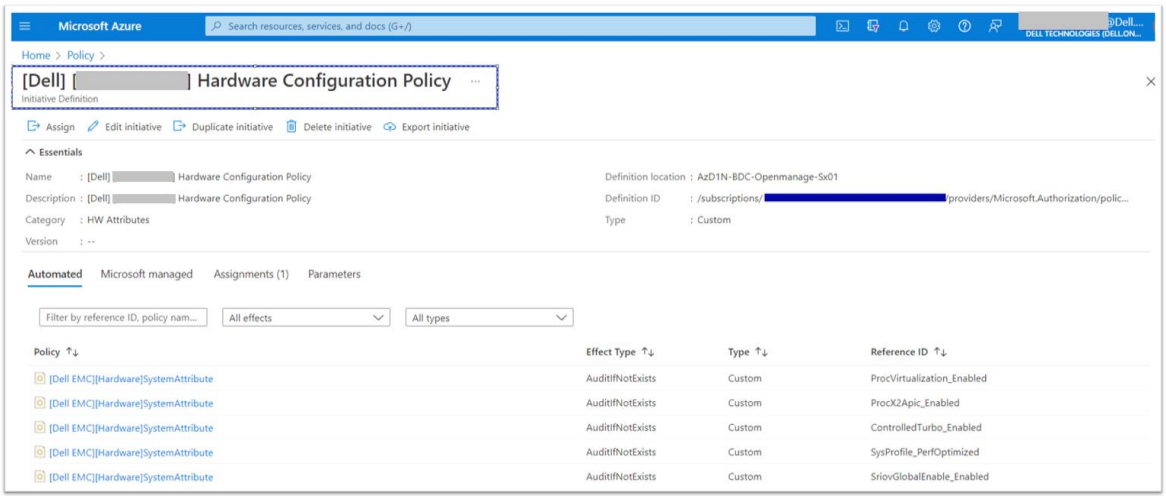

Figure 21: Policy Definition in Azure Portal

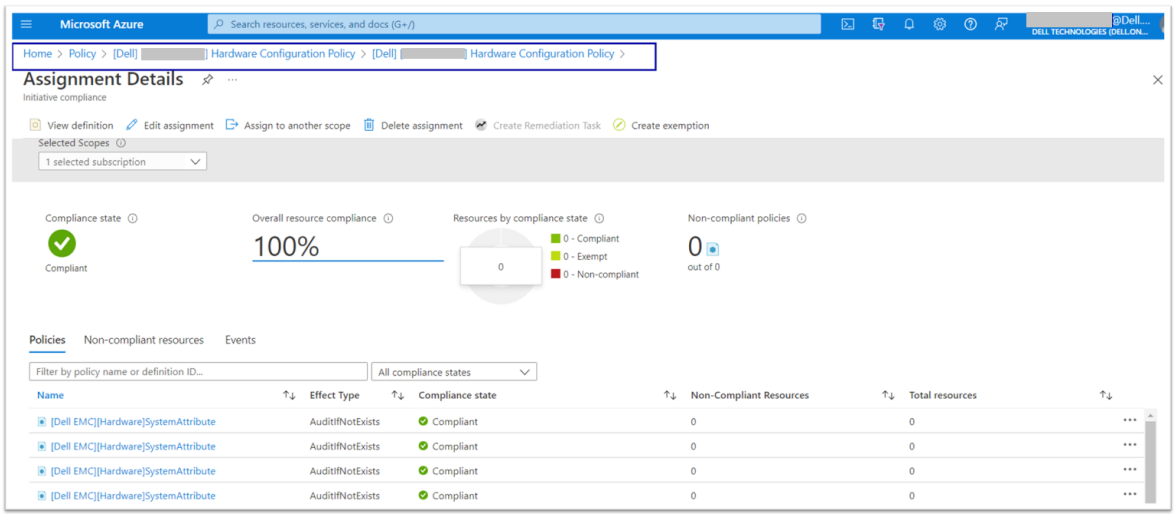

Figure 22: Policy Compliance in Azure Portal

Note: The policy compliance report is available on Azure Arc as well as in the OMIMSWAC HCP Compliance page, providing a consistent management experience.

4 Export the Onboarded Policies Report

Once the policies are successfully onboarded to Azure Arc (section 3.1-3.3), users can export the onboarded policies details in an excel (.xls) file.

Click **Export Details** to download the details

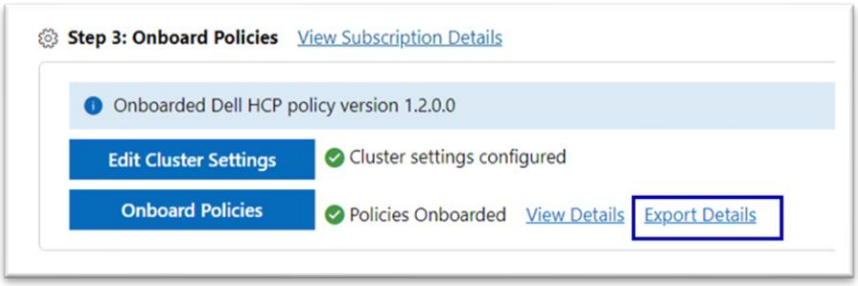

Figure 23: Export Details

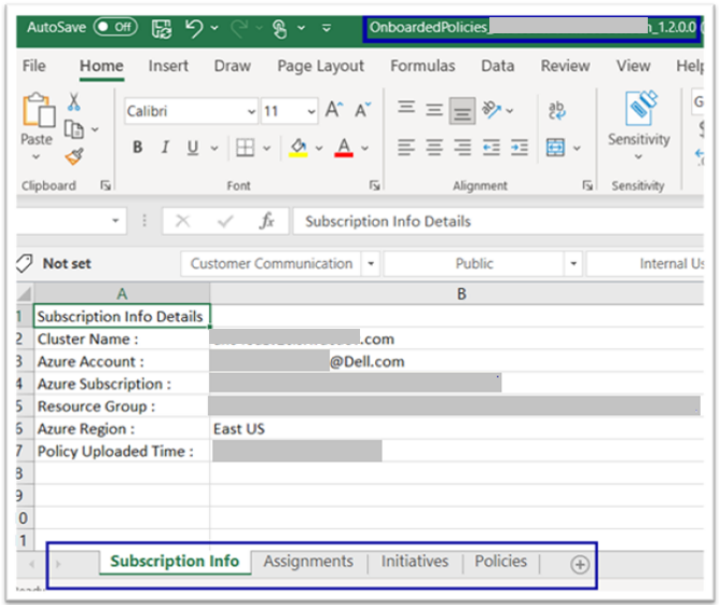

Figure 24: Export Details – Excel file

5 Onboard updated HCP Policies to Azure

When onboarded policies in Azure Arc are changed (section 3.1 – 3.3), you can use the "Onboard Policies" button to reload the policy.

Note: If a new version of Dell HCP policy is available, you will get a notification with following message "A new version of Dell HCP policy <version number> is available for update. Go to Azure Integration from View menu or Overview page and onboard the policies into Azure Arc."

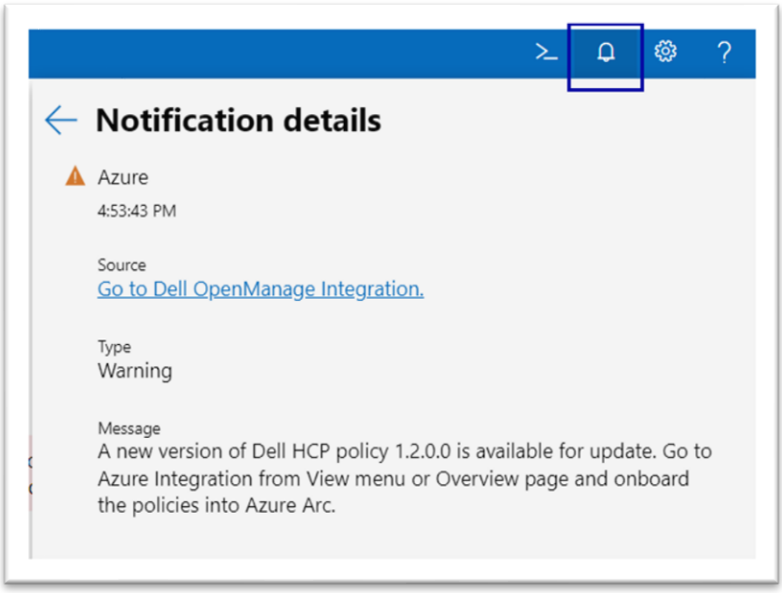

Figure 25: HCP Policy New Version Notification

1 If there are any changes in the policy, to update the previously uploaded policies, click **Onboard Policies**. The version of the policy, which is currently present in Azure, is displayed.

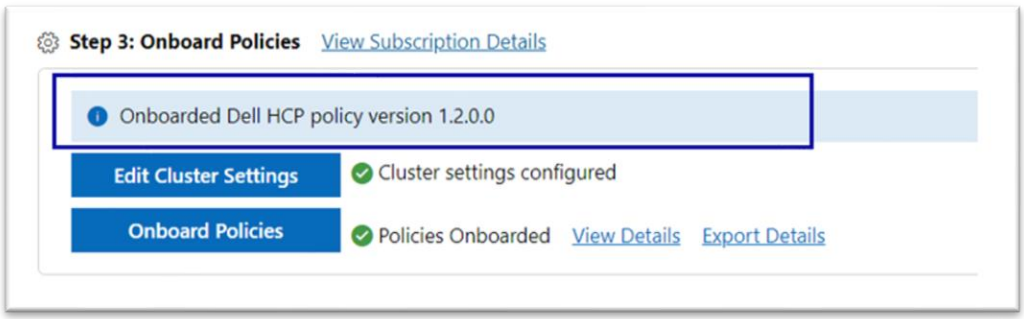

Figure 26: HCP Policy Version

2 **Onboard Dell HCI Configuration Profile Policies for Azure Arc** page appears on the right. You can see the version details of the policy being uploaded in the pop up.

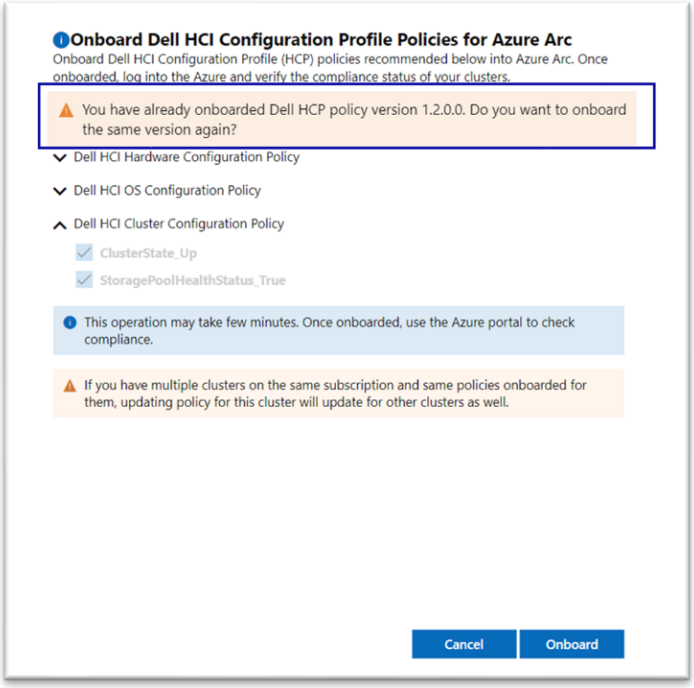

Figure 27: HCP Policy Version in pop up

6 Remediate HCP Policies

After you onboard the policies into Azure Arc (see Onboard policies into Azure), you can use OpenManage Integration in Windows Admin Center to manage Dell HCP policy compliance. This includes remediating Dell HCP policy to fix any non-compliant policies in an automated fashion using Cluster-Aware Update framework.

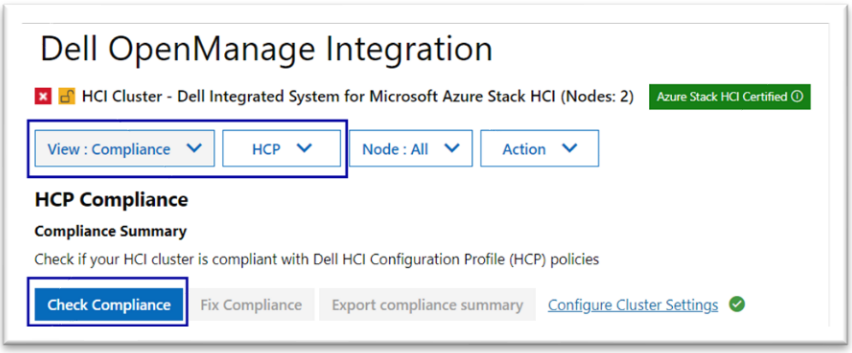

Figure 28: Check Compliance in HCP Compliance

Click **Check Compliance** to automatically compare the recommended rules packaged together in the Dell HCP policy definitions with the cluster settings. These rules include configurations addressing the hardware, cluster symmetry, cluster operations, and security.

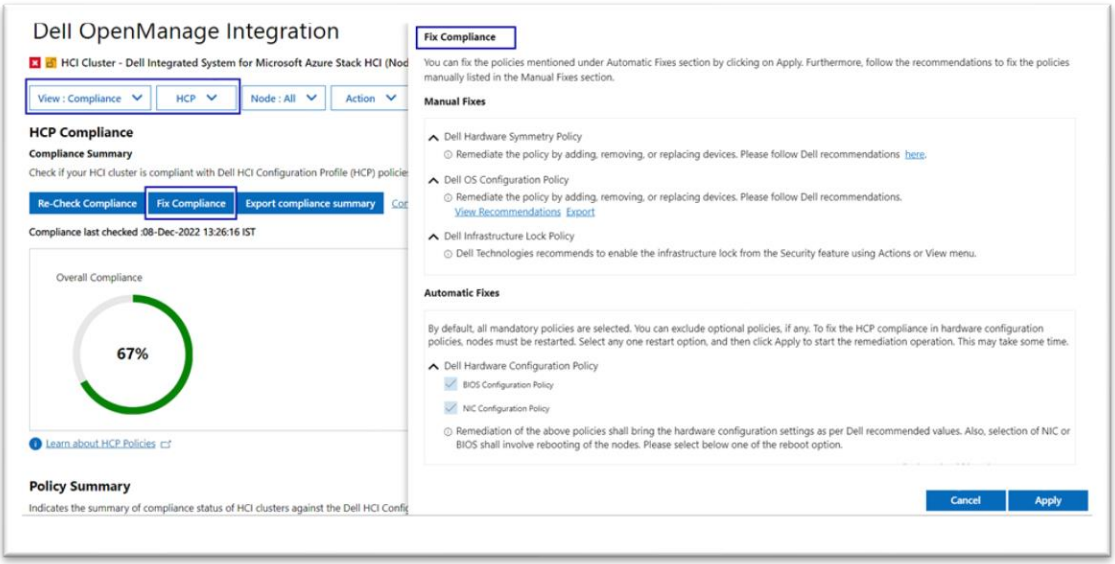

Figure 29: Fix Compliance

Once the compliance report is generated and if any non-compliant policies are identified by Dell HCP Policies, then you can proceed to fix them using **Fix Compliance**. On the **Fix Compliance** window, follow the recommendations to fix the compliance issues. Some fixes may require manual intervention and others can be corrected in a fully automated manner.

Any automated fixes that require a reboot of the Azure Stack HCI cluster nodes will be performed in a cluster-aware fashion, which results in no interruption to running workloads. For more information about remediating using HCP policies, see Validate and Remediate Azure Stack HCI clusters in the user's guide.

7 Troubleshooting

7.1 Model and OS Check Failure

If any of the cluster nodes fail the model or OS check, an error banner message will appear and block further steps.

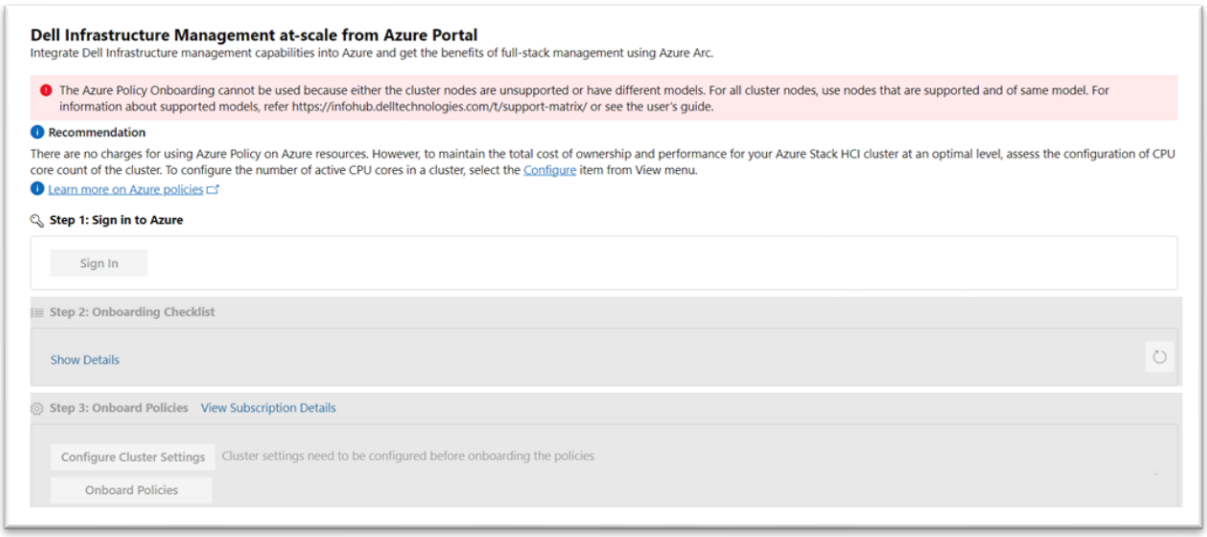

Figure 30: Error Banner for Model Check Failure

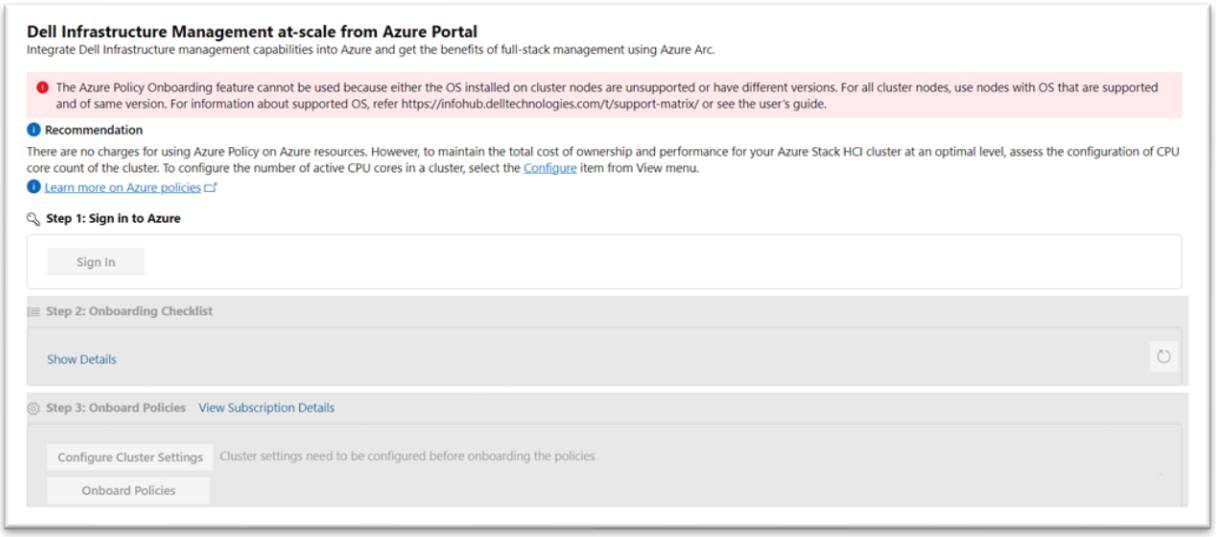

Figure 31: Error Banner for OS Check Failure

For more information about the supported models, see the compatibility matrix in the user's guide.

Use the latest version of the extension and refer to the updated compatibility matrix. You can also refer the "About" page in the extension for updated documentation.

7.2 Onboarding Checklist Failure

If any of the checklist items fail, see the recommendations on the Onboarding Checklist page to fix them and then click **Refresh** to get the latest status.

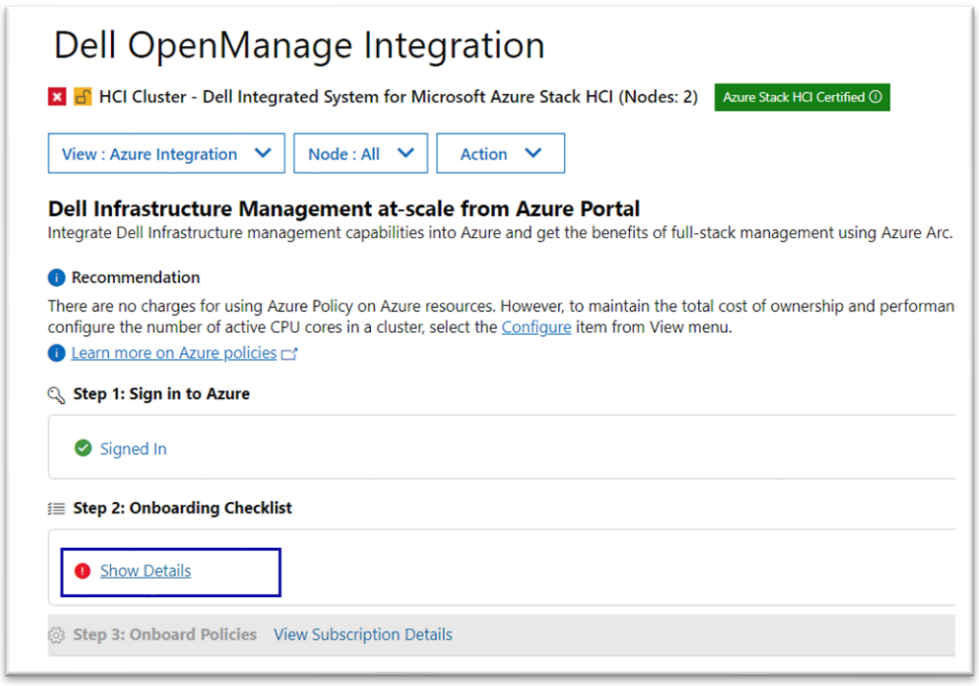

Figure 32: Onboarding Checklist Failure Status

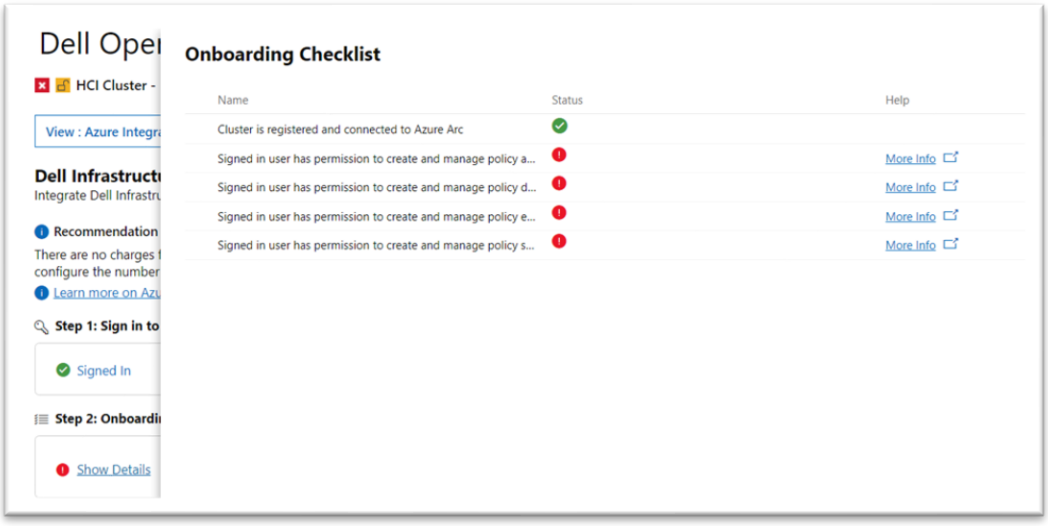

Figure 33: Onboarding Checklist popup page – Failure Status

8 Appendix

8.1 Network Topology and Deployment Model

i. Network Topology:

- Fully converged: All storage ports from the server are connected to the same network fabric. Within the host operating system, the NIC ports are used for both storage and management/VM traffic.
- Non-Converged: The storage traffic is separated from the management/VM traffic using dedicated storage network adapters.
  - Non-Converged-Physical: Storage traffic is on the physical storage network adapter ports and management/VM traffic through a SET created using network ports of the server rNDC.
  - Non-Converged-SET: Storage traffic uses virtual adapters in the host operating system connected to a SET.

For more information, see Reference Guide—Network Integration and Host Network Configuration Options.

ii. Deployment Model:

- Scalable: Ability of the infrastructure to handle increased load. The Dell Solutions for Azure Stack HCI scalable architectures support from 2 to 16 nodes in a cluster.
- Switchless: This Microsoft HCI Solutions from Dell Technologies infrastructure type offers two to four nodes in a switchless configuration for storage traffic. This infrastructure can be implemented using any of the validated and supported AX nodes. However, the number of nodes in a cluster varies between the AX node models and the number of network adapters that each model supports.
- Stretch: A stretched cluster with Azure Stack HCI consists of servers residing at two different locations or sites, with each site having two or more servers, replicating volumes either in synchronous or asynchronous mode.

For more information, see Reference Guide—Network Integration and Host Network Configuration Options.

9 Conclusion

Using this white paper, one can easily use OMIMSWAC to onboard Dell policies on Azure Arc for monitoring Azure Stack HCI clusters using Azure.

A Technical Support and Resources

For more information about the user documentation, see the OpenManage Integration with Microsoft Windows Admin Center product support page at https://www.dell.com/support.

A.1 Related Resources

- OMIMSWAC's User's Guide, Release Notes, and Security Configuration Guide, see link.
- Microsoft Windows Admin Center Overview, see link.
- Connect and manage Azure Stack HCI registration, see link.
- Azure built-in roles, see link.
- Create and manage policies to enforce compliance, see link.
- Register Windows Admin Center with Azure, see link.