Technical Whitepaper

Onboard Dell Server Configuration Profile Policies from Windows Admin Center to Azure Arc for Failover Cluster

Abstract

This white paper provides guidance to onboard Dell Server Configuration Profile (SCP) policies from Windows Admin Center to Azure Arc for failover cluster so that administrators can leverage those policies and can check the compliance against the cluster.

January 2023

Revisions

Date	Description
January 2023	Initial release

Acknowledgments

This paper was produced by the following:

Authors:

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

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

Acronyms

Acronyms	Expansion
iDRAC	Integrated Dell Remote Access Controller
OMIMSWAC	OpenManage Integration with Microsoft Windows Admin Center
MS API	Microsoft Application Programming Interface
SCP	Server Configuration Profile
XXg (ex.14g,15g)	XXth Generation of Dell Server Platforms
WS19	Windows Server 2019
WAC	Windows Admin Center

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 SCP policies to Azure Arc to monitor Hyper-V based failover clusters.

1 Introduction

Since Azure Arc is one of the primary resource management tools on cloud and hybrid platforms, it’s essential that Dell Azure Policies help administrators to maintain compliance with Dell Server Configuration Profile (SCP) throughout the lifecycle of Hyper-V based failover clusters.

OMIMSWAC helps administrators to onboard Dell SCP Policies to Azure Arc so that policies can be leveraged to monitor cluster compliance.

Prerequisites: For more information, see Prerequisites.

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

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

Onboard updated SCP Policies: For more information, see Update SCP Policies.

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

2 Prerequisites

Ensure your Failover cluster meets the following prerequisites before you onboard SCP policies to Azure Arc:

- You have an Azure subscription.
- WAC gateway is registered into Azure. For more information, see WAC Gateway Registration into Azure.
- Cluster is registered and connected to Azure Arc. For more information, see Microsoft document.
- Failover cluster nodes have the supported platform
  - 14g, 15g, and 16g
- Failover cluster nodes have the supported operating system.
  - Windows Server 2019 (WS 2019) and Windows Server 2022 (WS 2022)
- "OMIWAC Premium License" is installed on each node. For more information, see Verify License Details.

Note: If any of the prerequisite checks fail, OMIMSWAC blocks the onboarding policies to the Azure Arc. For more information, see Troubleshooting section 7.1

2.1 Register Windows Admin Center gateway with Azure

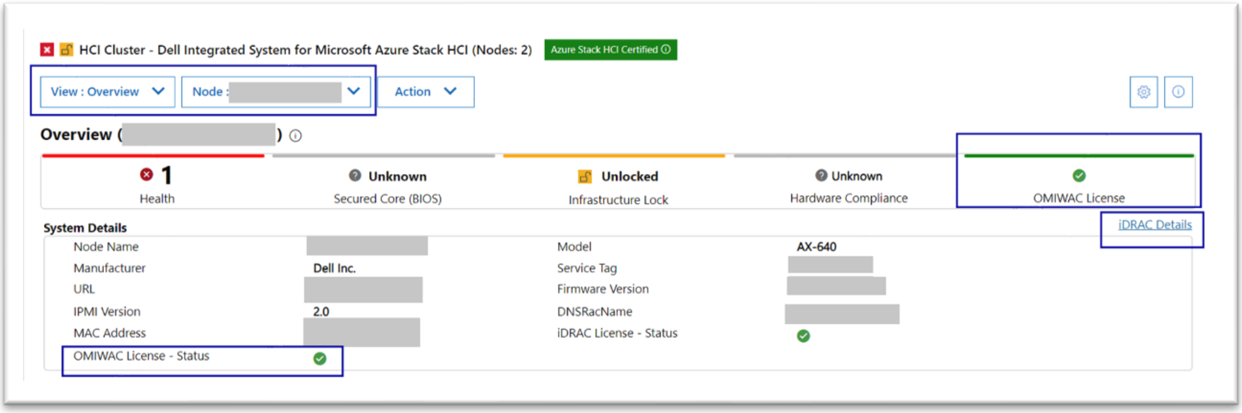
For information about registering Windows Admin Center with Azure, see Microsoft documents.

2.2 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.

Perform the following steps to check license details:

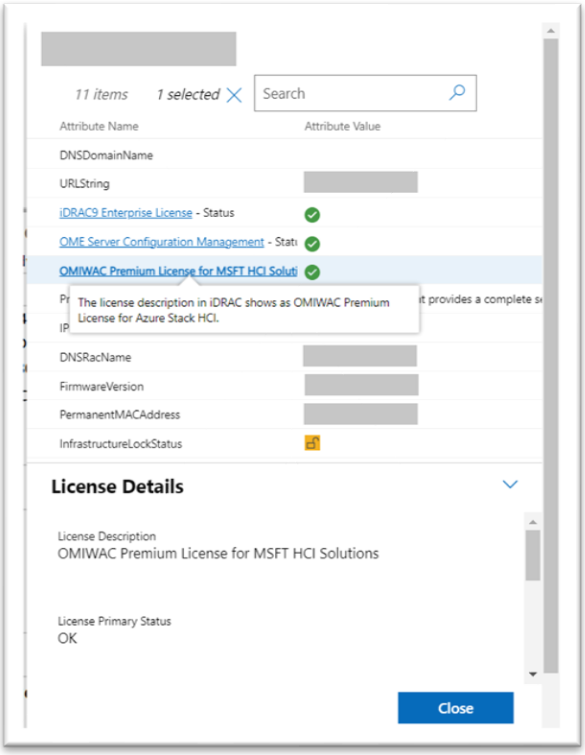
1. In the Windows Admin Center, connect to a server or cluster.
2. In the left pane of the Windows Admin Center, under **EXTENSIONS**, click **Dell OpenManage Integration**.
3. In the **View** drop-down, select **Overview,** and then select individual nodes in **Node** drop-down for cluster connections. You can see the OMIWAC license details in the **System Details** section. Also, click the **iDRAC Details** link on 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, and more.



System Details

Node Name	[redacted]	Model	AX-640
Manufacturer	Dell Inc.	Service Tag	[redacted]
URL	[redacted]	Firmware Version	[redacted]
IPMI Version	2.0	DNSRacName	[redacted]
MAC Address	[redacted]	iDRAC License - Status	✓
OMIWAC License - Status	✓		

Figure 1: Verify license details from Overview page



Attribute Name	Attribute Value
DNSDomainName	
URLString	[redacted]
iDRAC9 Enterprise License - Status	✓
OME Server Configuration Management - Statı	✓
OMIWAC Premium License for MSFT HCI Soluti	✓
Pr	t provides a complete s
IP	
DNSRacName	[redacted]
FirmwareVersion	[redacted]
PermanentMACAddress	[redacted]
InfrastructureLockStatus	🔓

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

License Details

License Description
OMIWAC Premium License for MSFT HCI Solutions

License Primary Status
OK

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 user's guide.

3 Onboard policies into Azure

In OMIMSWAC, when you click **Azure Integration** in the **View** drop-down menu, the extension checks your cluster for all the prerequisites as mentioned in the previous section. 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

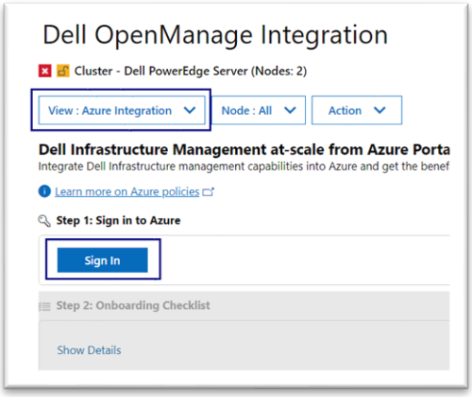
Step 2: Onboarding Checklist

Step 3: Onboard Policies

3.1 Sign-In to Azure

Perform the following steps to sign-in to Azure:

1. In the **View** drop-down, click **Azure Integration**.
2. Click **Sign In.** A Sign in pop up window appears. For more information, see Microsoft document. Once the siging is done, the status changes to **Signed In**.



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

View : Azure Integration | Node : All | Action

Dell Infrastructure Management at-scale from Azure Porta

Integrate Dell Infrastructure management capabilities into Azure and get the benef

Learn more on Azure policies

Step 1: Sign in to Azure

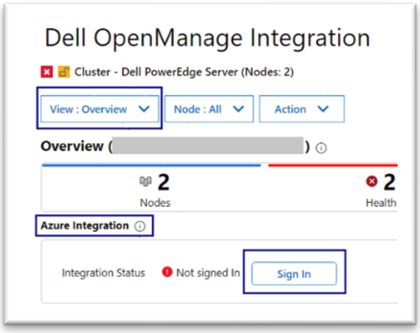
Sign In

Step 2: Onboarding Checklist

Show Details

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.



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

View : Overview | Node : All | Action

Overview ([redacted])

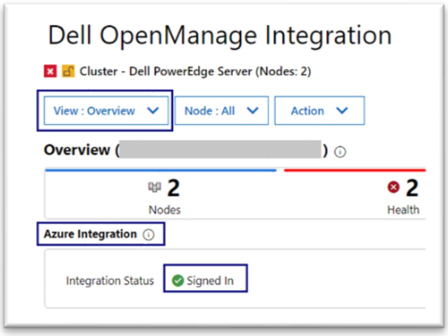
2 Nodes

2 Health

Azure Integration

Integration Status: Not signed In

Sign In



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

View : Overview | Node : All | Action

Overview ([redacted])

2 Nodes

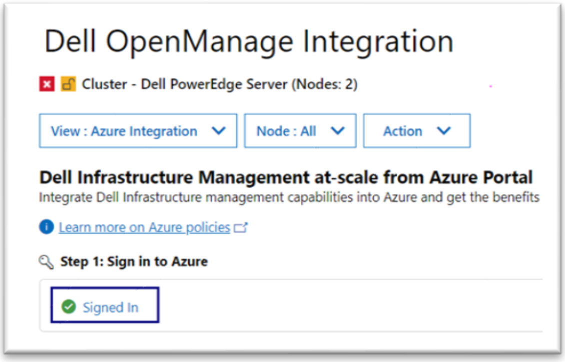
2 Health

Azure Integration

Integration Status: Signed In

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.



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

Dell Infrastructure Management at-scale from Azure Portal

Integrate Dell Infrastructure management capabilities into Azure and get the benefits

Learn more on Azure policies

Step 1: Sign in to Azure

Signed In

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:

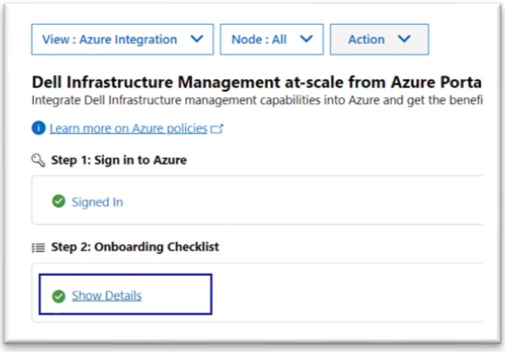
   - User must have the following list of permissions to onboard the SCP policies into Azure. Signed in user has permission to

     - 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 registered resource group must be available in the Azure.
   - Resource group and cluster have same nodes

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



Dell Infrastructure Management at-scale from Azure Porta

Integrate Dell Infrastructure management capabilities into Azure and get the benefi

Learn more on Azure policies

Step 1: Sign in to Azure

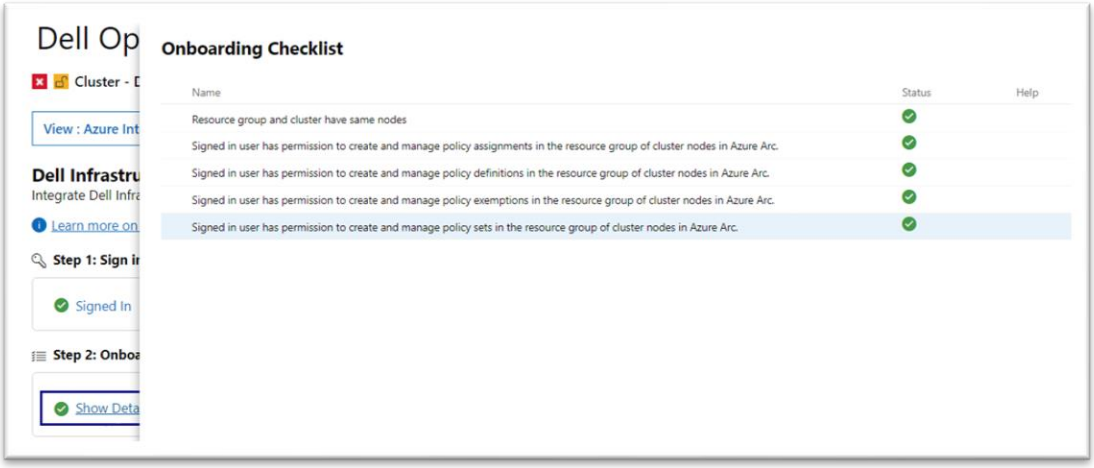
Signed In

Step 2: Onboarding Checklist

Show Details

Figure 6: Onboarding check list show details

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



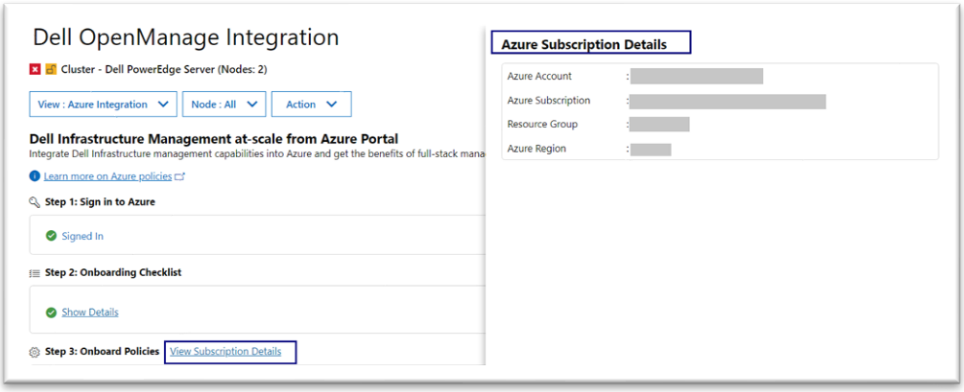
Onboarding Checklist

Name	Status	Help
Resource group and cluster have same nodes	✓	
Signed in user has permission to create and manage policy assignments in the resource group of cluster nodes in Azure Arc.	✓	
Signed in user has permission to create and manage policy definitions in the resource group of cluster nodes in Azure Arc.	✓	
Signed in user has permission to create and manage policy exemptions in the resource group of cluster nodes in Azure Arc.	✓	
Signed in user has permission to create and manage policy sets in the resource group of cluster nodes in Azure Arc.	✓	

Figure 7: Onboarding checklist pop up page

3.3 Onboard policies

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


Dell OpenManage Integration
Cluster - Dell PowerEdge Server (Nodes: 2)
View : Azure Integration
Node : All
Action
Learn more on Azure policies
Signed In
Show Details
View Subscription Details

Dell Infrastructure Management at-scale from Azure Portal

Integrate Dell Infrastructure management capabilities into Azure and get the benefits of full-stack mana

Step 1: Sign in to Azure

Step 2: Onboarding Checklist

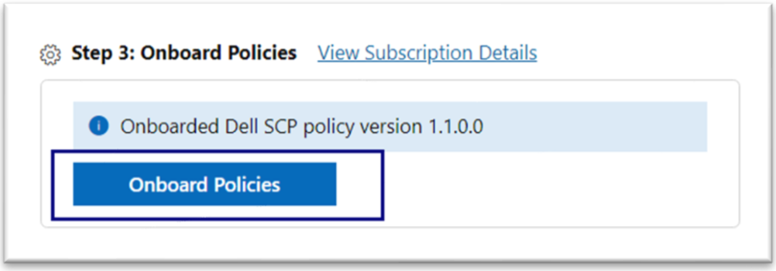
Step 3: Onboard Policies

Azure Subscription Details

Azure Account	:	[redacted]
Azure Subscription	:	[redacted]
Resource Group	:	[redacted]
Azure Region	:	[redacted]

Figure 8: View subscription details

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



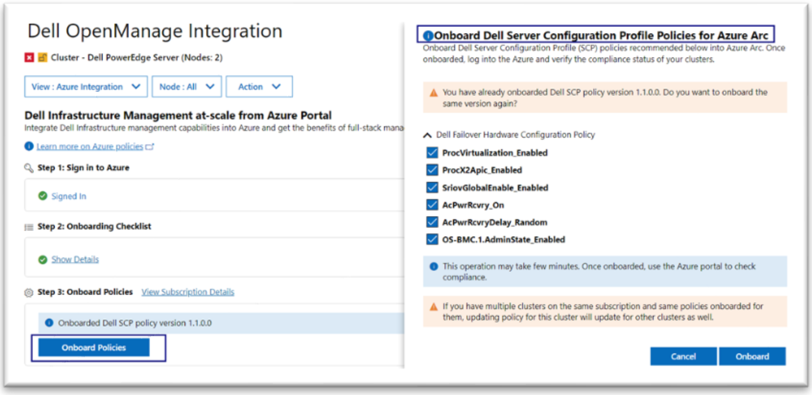
Onboarded Dell SCP policy version 1.1.0.0

Figure 9: Onboard Policies

2. Click **Onboard Policies** to view the applicable policies for upload.
   Onboard Dell Server Configuration Profile Policies for Azure Arc pane appears on the right. In this pane, the policies are grouped into categories:

   - Dell Failover Hardware Configuration Policy

   All policies are shown as selected, and you can choose the policies based on your requirements.



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

Dell Infrastructure Management at-scale from Azure Portal

Integrate Dell Infrastructure management capabilities into Azure and get the benefits of full-stack mana

Learn more on Azure policies

Step 1: Sign in to Azure

Signed In

Step 2: Onboarding Checklist

Show Details

Step 3: Onboard Policies View Subscription Details

Onboarded Dell SCP policy version 1.1.0.0

Onboard Dell Server Configuration Profile Policies for Azure Arc

Onboard Dell Server Configuration Profile (SCP) policies recommended below into Azure Arc. Once onboarded, log into the Azure and verify the compliance status of your clusters.

You have already onboarded Dell SCP policy version 1.1.0.0. Do you want to onboard the same version again?

Dell Failover Hardware Configuration Policy

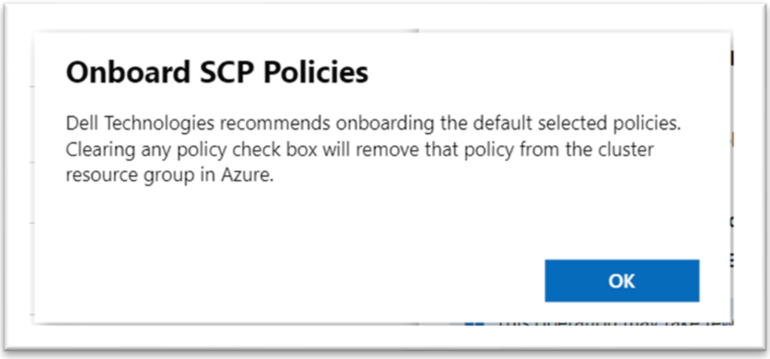
- ☑ ProcVirtualization_Enabled
- ☑ ProcX2Apic_Enabled
- ☑ SriovGlobalEnable_Enabled
- ☑ AcPwrRcvry_On
- ☑ AcPwrRcvryDelay_Random
- ☑ OS-BMC.1.AdminState_Enabled

This operation may take few minutes. Once onboarded, use the Azure portal to check compliance.

If you have multiple clusters on the same subscription and same policies onboarded for them, updating policy for this cluster will update for other clusters as well.

Figure 10: Onboard policies

If you uncheck the selected policy for the first time, you will get an alert popup as shown below.

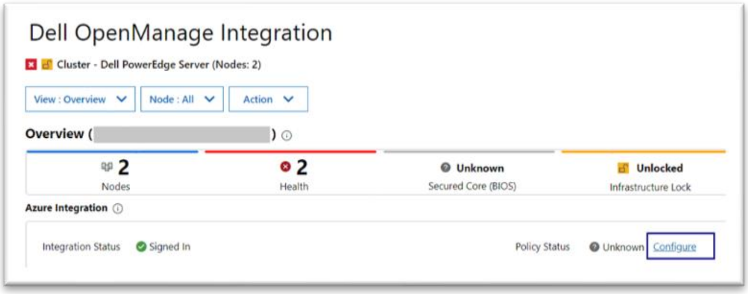


Onboard SCP Policies

Dell Technologies recommends onboarding the default selected policies. Clearing any policy check box will remove that policy from the cluster resource group in Azure.

Figure 11: Policy un-check alert popup

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



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

Overview ([redacted])

2	2	Unknown	Unlocked
Nodes	Health	Secured Core (BIOS)	Infrastructure Lock

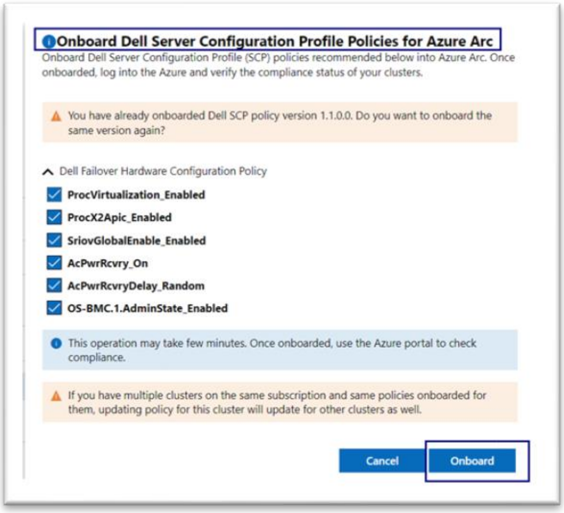
Azure Integration

Integration Status: Signed In

Policy Status: Unknown Configure

Figure 12: Configure link from Overview page

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



Onboard Dell Server Configuration Profile Policies for Azure Arc

Onboard Dell Server Configuration Profile (SCP) policies recommended below into Azure Arc. Once onboarded, log into the Azure and verify the compliance status of your clusters.

You have already onboarded Dell SCP policy version 1.1.0.0. Do you want to onboard the same version again?

Dell Failover Hardware Configuration Policy

- ☑ ProcVirtualization_Enabled
- ☑ ProcX2Apic_Enabled
- ☑ SriovGlobalEnable_Enabled
- ☑ AcPwrRcvry_On
- ☑ AcPwrRcvryDelay_Random
- ☑ OS-BMC.1.AdminState_Enabled

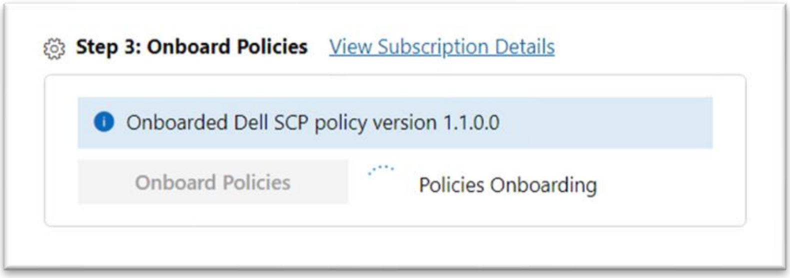
This operation may take few minutes. Once onboarded, use the Azure portal to check compliance.

If you have multiple clusters on the same subscription and same policies onboarded for them, updating policy for this cluster will update for other clusters as well.

Figure 13: Onboard Dell Server Configuration Profile Policies for Azure Arc

Note: Policies are onboarded/updated at the subscription level. Hence, if the policies are assigned to different resources (e.g, specific to the cluster), then updating policies will reflect in all the resources.

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.



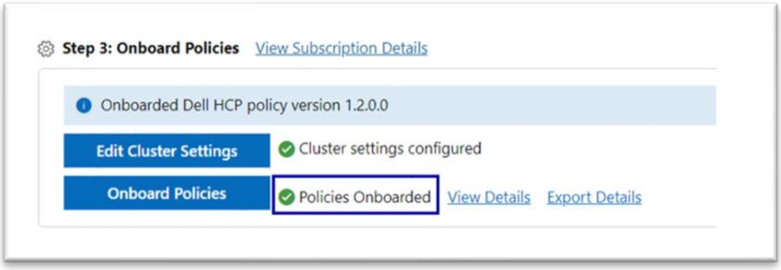
Step 3: Onboard Policies View Subscription Details

Onboarded Dell SCP policy version 1.1.0.0

Policies Onboarding

Figure 14: Onboarding Policies

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



Step 3: Onboard Policies View Subscription Details

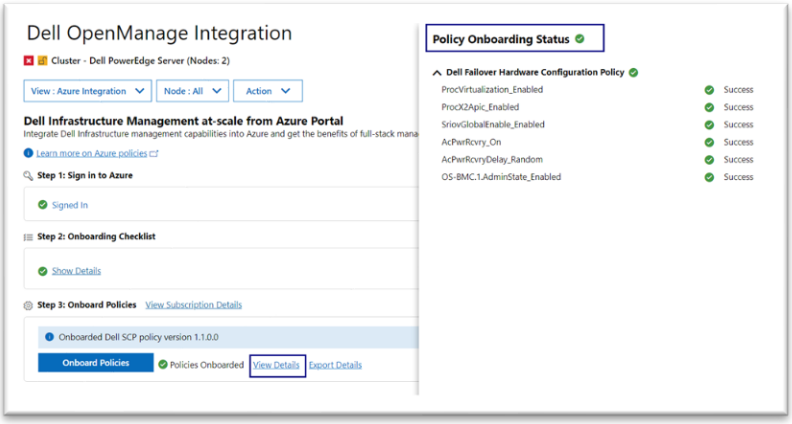
Onboarded Dell HCP policy version 1.2.0.0

Cluster settings configured

Policies Onboarded View Details Export Details

Figure 15: Policies Onboarded- status

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



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

View : Azure Integration | Node : All | Action

Dell Infrastructure Management at-scale from Azure Portal

Integrate Dell Infrastructure management capabilities into Azure and get the benefits of full-stack mana

Learn more on Azure policies

Step 1: Sign in to Azure

✓ Signed In

Step 2: Onboarding Checklist

✓ Show Details

Step 3: Onboard Policies View Subscription Details

Onboarded Dell SCP policy version 1.1.0.0

Onboard Policies ✓ Policies Onboarded View Details Export Details

Policy Onboarding Status ✓

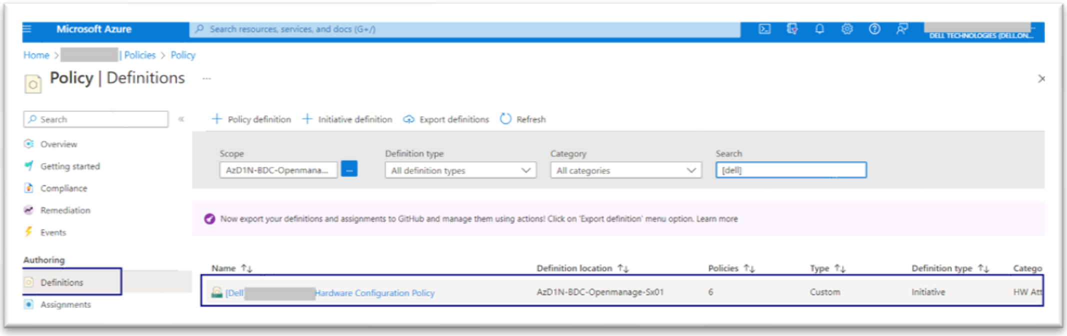
Dell Failover Hardware Configuration Policy ✓

ProcVirtualization_Enabled	✓ Success
ProcX2Apic_Enabled	✓ Success
SriovGlobalEnable_Enabled	✓ Success
AcPwrRcvry_On	✓ Success
AcPwrRcvryDelay_Random	✓ Success
OS-BMC.1.AdminState_Enabled	✓ Success

Figure 16: 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.

6. Once the policies are successfully onboarded to Azure, you can view the onboarded policies in the Azure portal. For more information, see Microsoft document.



Microsoft Azure
Search resources, services, and docs (G+/)
[redacted] DELL TECHNOLOGIES (DELLON...
Home > [redacted] | Policies > Policy

Policy | Definitions

Scope: AzD1N-BDC-Openmana...

Definition type: All definition types

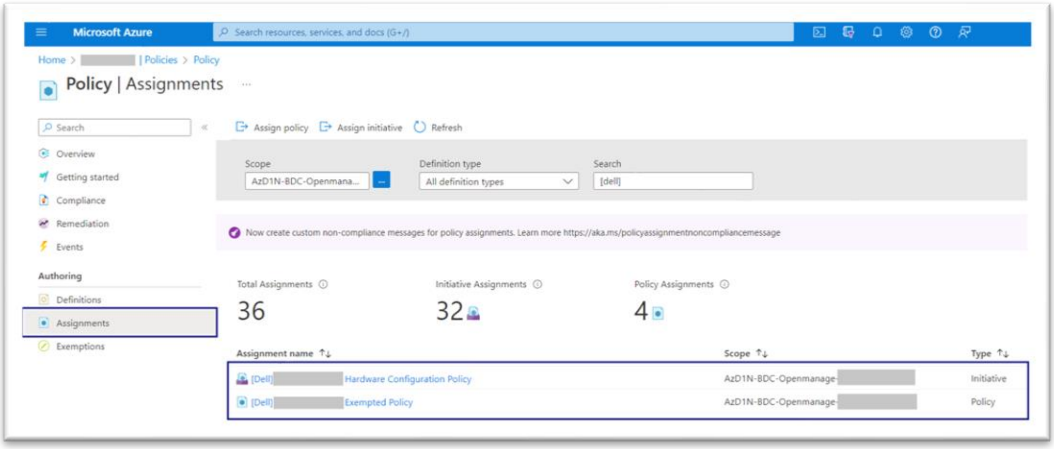
Category: All categories

Search: [dell]

Now export your definitions and assignments to GitHub and manage them using actions! Click on 'Export definition' menu option. Learn more

Name ↑↓	Definition location ↑↓	Policies ↑↓	Type ↑↓	Definition type ↑↓	Catego
[Dell [redacted] Hardware Configuration Policy	AzD1N-BDC-Openmanage-Sx01	6	Custom	Initiative	HW Att

Figure 17: SCP policy details in Azure portal



Microsoft Azure
Search resources, services, and docs (G+/)
Home > [redacted] | Policies > Policy

Policy | Assignments

Scope: AzD1N-BDC-Openmana...

Definition type: All definition types

Search: [dell]

Now create custom non-compliance messages for policy assignments. Learn more https://aka.ms/policyassignmentnoncompliancemessage

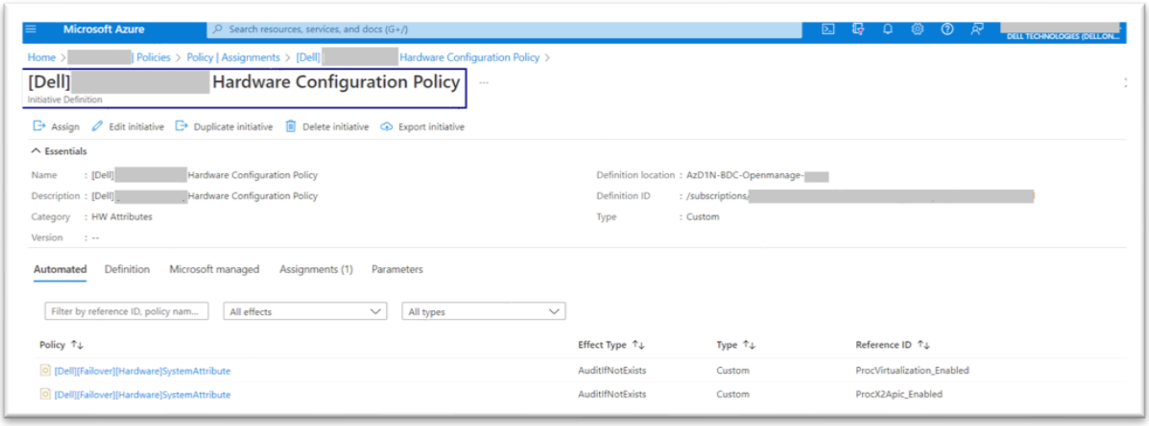
Total Assignments 36

Initiative Assignments 32

Policy Assignments 4

Assignment name ↑↓	Scope ↑↓	Type ↑↓
[Dell] [redacted] Hardware Configuration Policy	AzD1N-BDC-Openmanage- [redacted]	Initiative
[Dell] [redacted] Exempted Policy	AzD1N-BDC-Openmanage- [redacted]	Policy

Figure 18: Policy assignment in Azure Portal



Microsoft Azure | Search resources, services, and docs (G+/) | [redacted] DELL TECHNOLOGIES (DELLON...

Home > [redacted] | Policies > Policy | Assignments > [Dell] [redacted] Hardware Configuration Policy >

[Dell] [redacted] Hardware Configuration Policy ...

Initiative Definition

Assign | Edit initiative | Duplicate initiative | Delete initiative | Export initiative

Essentials

Name : [Dell] [redacted] Hardware Configuration Policy

Description : [Dell] [redacted] Hardware Configuration Policy

Category : HW Attributes

Version : --

Definition location : AzD1N-BDC-Openmanage-[redacted]

Definition ID : /subscriptions/[redacted]

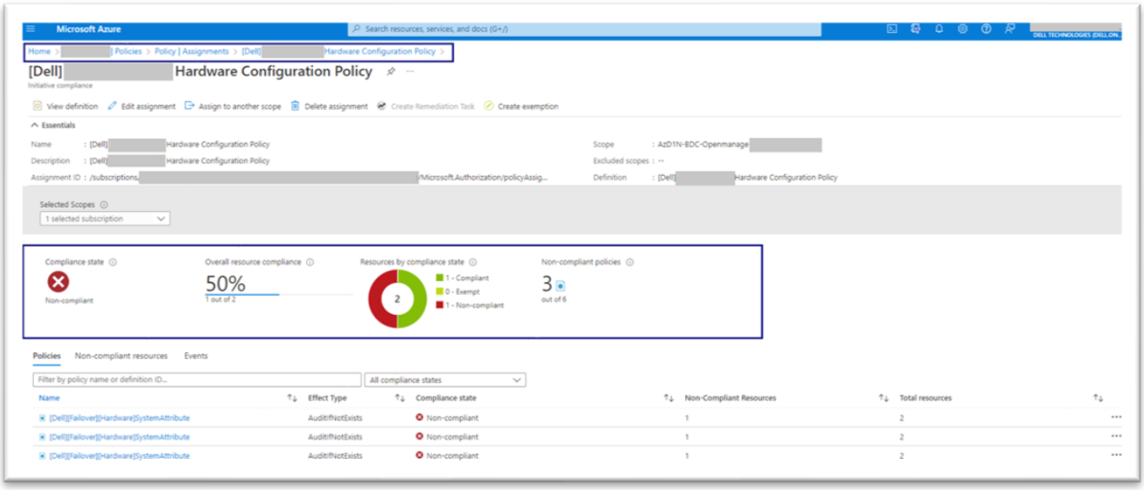
Type : Custom

Automated | Definition | Microsoft managed | Assignments (1) | Parameters

Filter by reference ID, policy nam... | All effects | All types

Policy ↑↓	Effect Type ↑↓	Type ↑↓	Reference ID ↑↓
[Dell][Failover][Hardware]SystemAttribute	AuditIfNotExists	Custom	ProcVirtualization_Enabled
[Dell][Failover][Hardware]SystemAttribute	AuditIfNotExists	Custom	ProcX2Apic_Enabled

Figure 19: Policy definition in Azure portal



Microsoft Azure | Search resources, services, and docs (G+/) | [redacted] DELL TECHNOLOGIES (DELLON...

Home > [redacted] | Policies > Policy | Assignments > [Dell] [redacted] Hardware Configuration Policy >

[Dell] [redacted] Hardware Configuration Policy ...

Initiative compliance

View definition | Edit assignment | Assign to another scope | Delete assignment | Create Remediation Task | Create exemption

Essentials

Name : [Dell] [redacted] Hardware Configuration Policy

Description : [Dell] [redacted] Hardware Configuration Policy

Assignment ID : /subscriptions/[redacted]/Microsoft.Authorization/policyAssig...

Scope : AzD1N-BDC-Openmanage[redacted]

Excluded scopes : --

Definition : [Dell] [redacted] Hardware Configuration Policy

Selected Scopes: 1 selected subscription

Compliance state: Non-compliant

Overall resource compliance: 50% (1 out of 2)

Resources by compliance state: 2

Non-compliant policies: 3 out of 6

Policies | Non-compliant resources | Events

Filter by policy name or definition ID... | All compliance states

Name ↑↓	Effect Type ↑↓	Compliance state ↑↓	Non-Compliant Resources ↑↓	Total resources ↑↓
[Dell][Failover][Hardware]SystemAttribute	AuditIfNotExists	Non-compliant	1	2
[Dell][Failover][Hardware]SystemAttribute	AuditIfNotExists	Non-compliant	1	2
[Dell][Failover][Hardware]SystemAttribute	AuditIfNotExists	Non-compliant	1	2

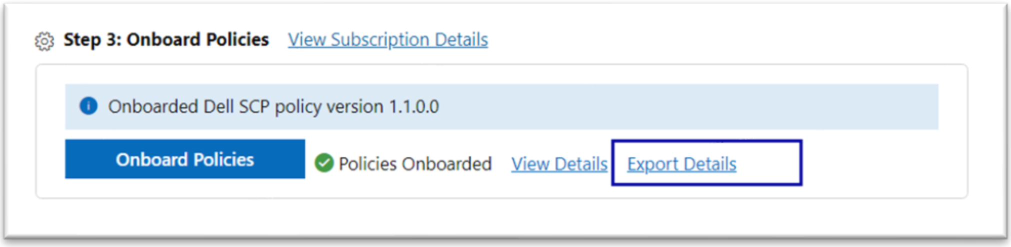
Figure 20: Policy compliance in Azure portal

Note: The policy compliance report is available on Azure Arc as well as in the OMIMSWAC Cluster Recommendation 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), you can export the onboarded policies details in an excel (.xls) file.

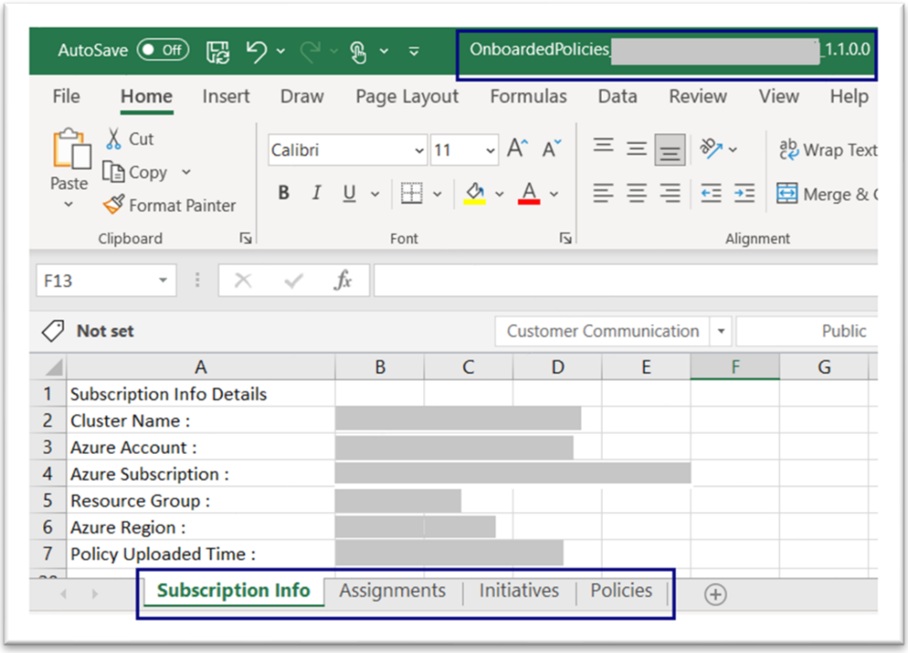
Click **Export Details** to download the details



Onboarded Dell SCP policy version 1.1.0.0

Policies Onboarded

Figure 21: Export details



OnboardedPolicies[redacted]1.1.0.0

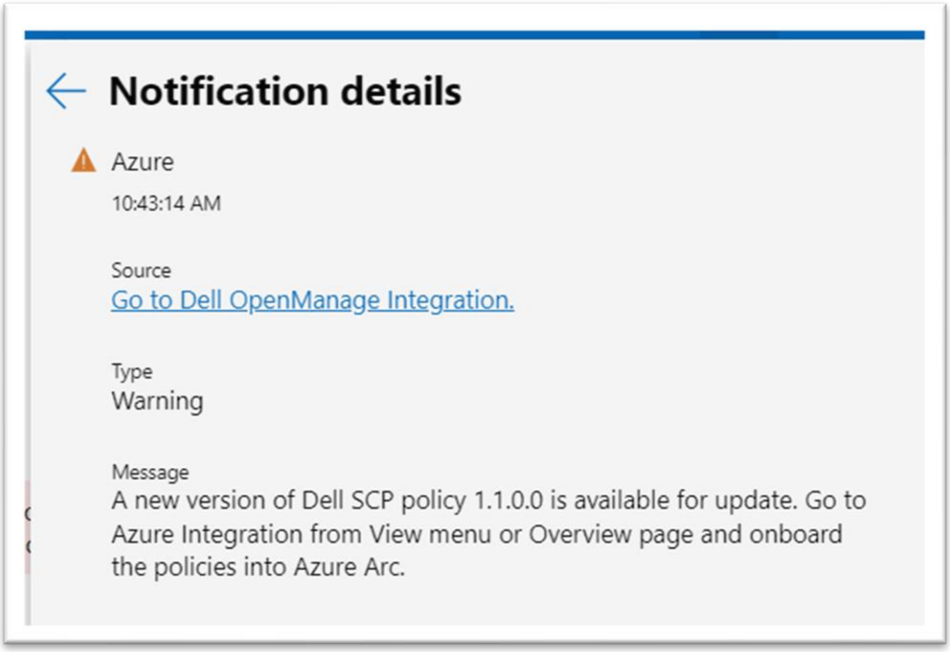
	A	B
1	Subscription Info Details	
2	Cluster Name :	[redacted]
3	Azure Account :	[redacted]
4	Azure Subscription :	[redacted]
5	Resource Group :	[redacted]
6	Azure Region :	[redacted]
7	Policy Uploaded Time :	[redacted]

Figure 22: Export details – Excel file

5 Onboard updated SCP policies

After policies are onboarded in Azure Arc, it's essential to keep the policies up-to-date. You will get a notification in OMIMSWAC, when a new version of the policy is available. Use the "**Onboard Policies**" button to reload the policy.

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



Notification details

Azure

10:43:14 AM

Source

Go to Dell OpenManage Integration.

Type

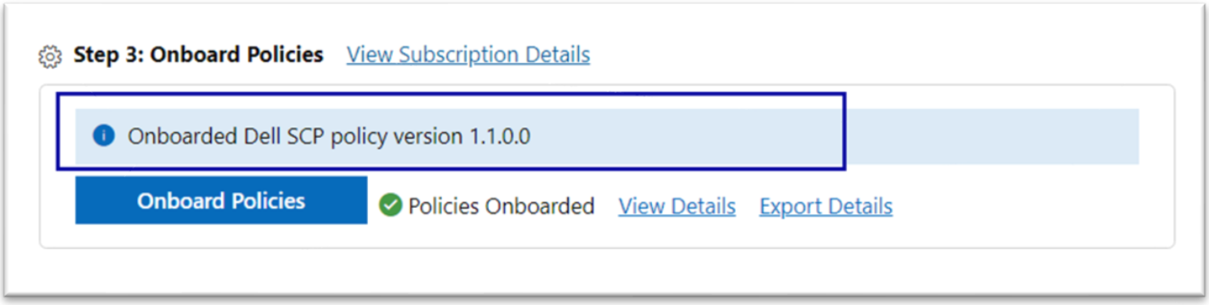
Warning

Message

A new version of Dell SCP policy 1.1.0.0 is available for update. Go to Azure Integration from View menu or Overview page and onboard the policies into Azure Arc.

Figure 23: Notification for new SCP policy version

1 When a new version of the onboarded policy is available, a notification appears. Follow the steps mentioned in section 3 and click **Onboard Policies**. The version of the policy, which is currently present in Azure, is displayed in **Step 3: Onboarded Policies** section.

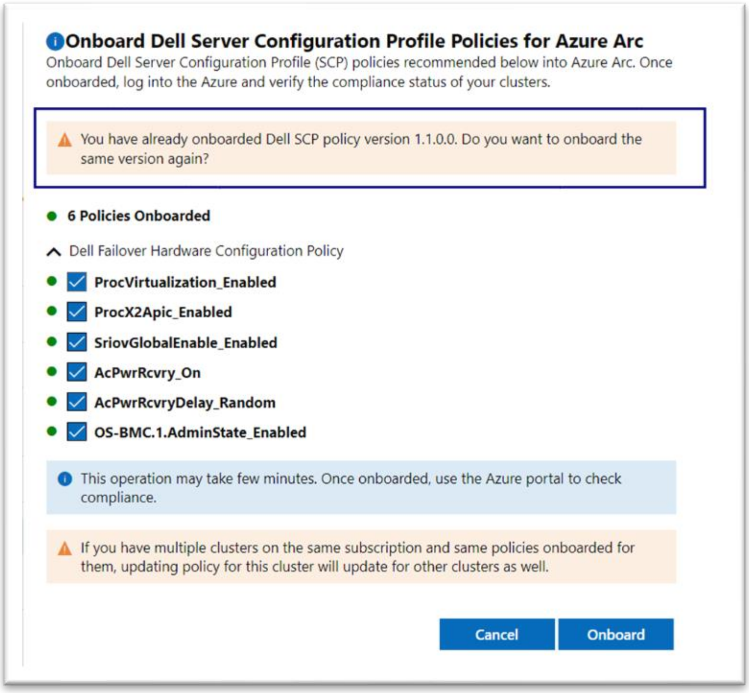


Step 3: Onboard Policies View Subscription Details

Onboarded Dell SCP policy version 1.1.0.0

Figure 24: SCP Policy Version

2 **Onboard Dell Server Configuration Profile Policies for Azure Arc** pane appears on the right. View the version details of the policy being uploaded.



Onboard Dell Server Configuration Profile Policies for Azure Arc

Onboard Dell Server Configuration Profile (SCP) policies recommended below into Azure Arc. Once onboarded, log into the Azure and verify the compliance status of your clusters.

You have already onboarded Dell SCP policy version 1.1.0.0. Do you want to onboard the same version again?

● **6 Policies Onboarded**

Dell Failover Hardware Configuration Policy

- ● ☑ **ProcVirtualization_Enabled**
- ● ☑ **ProcX2Apic_Enabled**
- ● ☑ **SriovGlobalEnable_Enabled**
- ● ☑ **AcPwrRcvry_On**
- ● ☑ **AcPwrRcvryDelay_Random**
- ● ☑ **OS-BMC.1.AdminState_Enabled**

This operation may take few minutes. Once onboarded, use the Azure portal to check compliance.

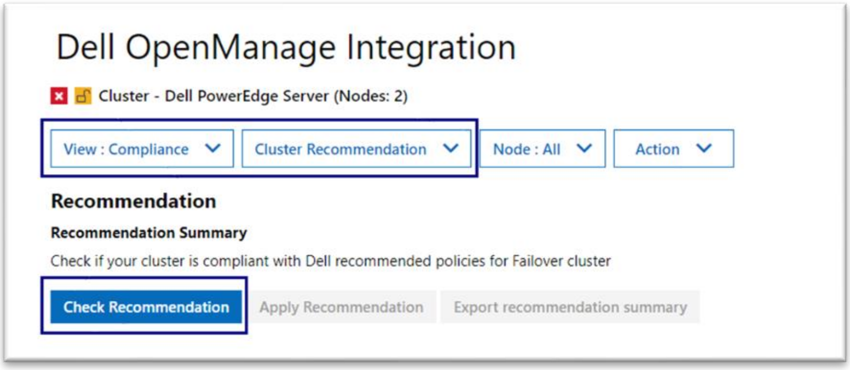
If you have multiple clusters on the same subscription and same policies onboarded for them, updating policy for this cluster will update for other clusters as well.

Figure 25: SCP policy version pane

Note: For Dell SCP policies, which are already onboarded in Azure, a "green**"** circular icon will be shown next to the checkbox in the "**Onboard Dell Server Configuration Profile Policies for Azure Arc**" pane.

6 Remediate SCP 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 SCP policy compliance. This includes remediating Dell SCP policy to fix any non-compliant policies in an automated fashion using Cluster-Aware Update framework.



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

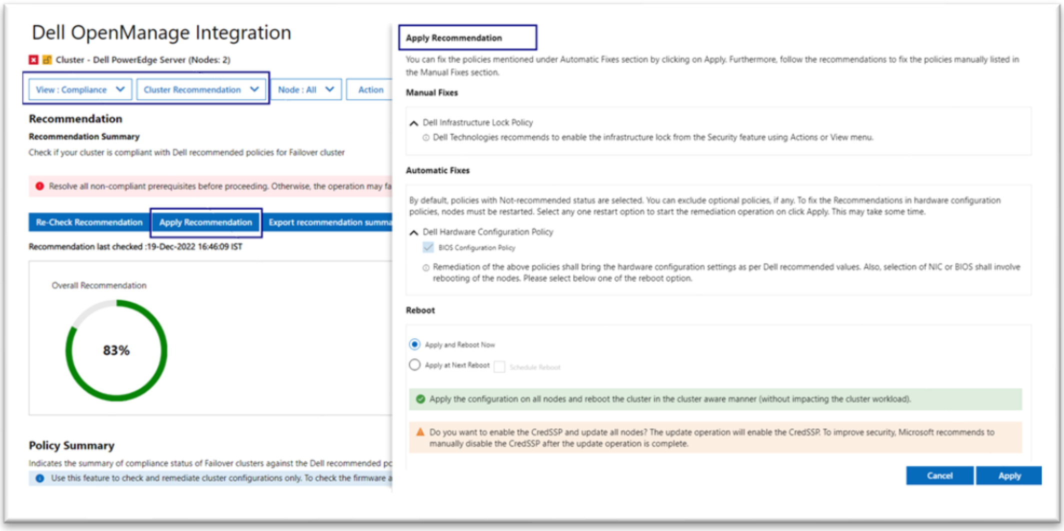
Recommendation

Recommendation Summary

Check if your cluster is compliant with Dell recommended policies for Failover cluster

Figure 26: Check Recommendation in Cluster Recommendation

From the **View** drop-down, click **Compliance** and then from the next drop-down menu, click **Cluster Recommendation**. Next, click **Check Recommendation** to automatically compare the recommended rules packaged together in the Dell SCP policy definitions with the cluster configurations. These rules include configurations addressing the hardware, high level compatibility, and security.



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

Recommendation

Recommendation Summary

Check if your cluster is compliant with Dell recommended policies for Failover cluster

Resolve all non-compliant prerequisites before proceeding. Otherwise, the operation may fa

Recommendation last checked :19-Dec-2022 16:46:09 IST

Policy Summary

Indicates the summary of compliance status of Failover clusters against the Dell recommended pc

Use this feature to check and remediate cluster configurations only. To check the firmware a

Apply Recommendation

You can fix the policies mentioned under Automatic Fixes section by clicking on Apply. Furthermore, follow the recommendations to fix the policies manually listed in the Manual Fixes section.

Manual Fixes

Dell Infrastructure Lock Policy

Dell Technologies recommends to enable the infrastructure lock from the Security feature using Actions or View menu.

Automatic Fixes

By default, policies with Not-recommended status are selected. You can exclude optional policies, if any. To fix the Recommendations in hardware configuration policies, nodes must be restarted. Select any one restart option to start the remediation operation on click Apply. This may take some time.

Dell Hardware Configuration Policy

☑ BIOS Configuration Policy

Remediation of the above policies shall bring the hardware configuration settings as per Dell recommended values. Also, selection of NIC or BIOS shall involve rebooting of the nodes. Please select below one of the reboot option.

Reboot

● Apply and Reboot Now

○ Apply at Next Reboot □ Schedule Reboot

Apply the configuration on all nodes and reboot the cluster in the cluster aware manner (without impacting the cluster workload).

Do you want to enable the CredSSP and update all nodes? The update operation will enable the CredSSP. To improve security, Microsoft recommends to manually disable the CredSSP after the update operation is complete.

Figure 27: Apply Recommendation

View the compliance report generated. If any non-compliant policies are identified by Dell SCP Policies, then you can proceed to fix them using **Apply Recommendation**. On the **Apply Recommendation** pane, follow the recommendations to fix the compliance issues. Some fixes may require manual intervention and others can be corrected in a fully automated manner. Click **Apply** to resolve issues listed below **Automatic Fixes** categories.

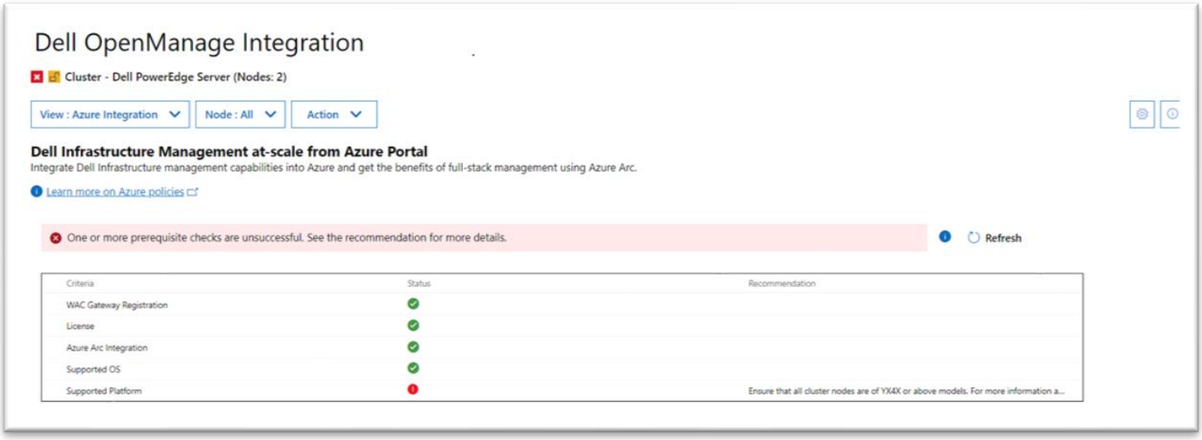
Any automated fixes that require a reboot of the Failover cluster nodes will be performed in a cluster-aware fashion, which results in no interruption to running workloads. For more information about remediating using SCP policies, see Validate and Remediate failover clusters in the user's guide.

7 Troubleshooting

7.1 Prerequisite check failure

If any prerequisite checks fail, you will be redirected to the **Prerequisite** page instead of the Azure Integration main page.

An error banner message will appear and show the prerequisite check table with status and recommendations. Follow the recommendations to resolve the prerequisite issues.



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

Dell Infrastructure Management at-scale from Azure Portal

Integrate Dell Infrastructure management capabilities into Azure and get the benefits of full-stack management using Azure Arc.

Learn more on Azure policies

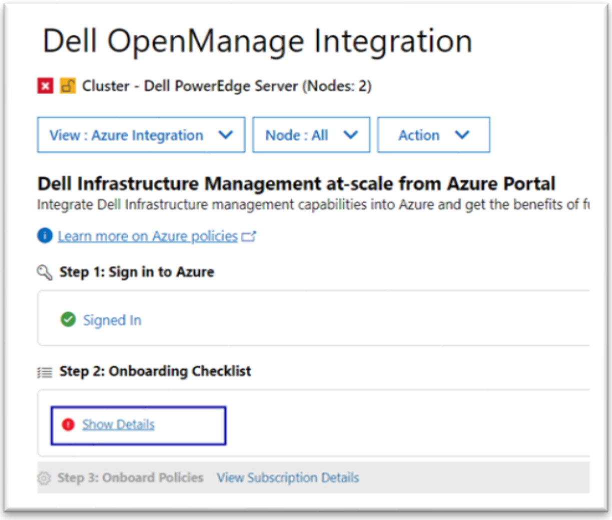
One or more prerequisite checks are unsuccessful. See the recommendation for more details.

Criteria	Status	Recommendation
WAC Gateway Registration	✓	
License	✓	
Azure Arc Integration	✓	
Supported OS	✓	
Supported Platform	●	Ensure that all cluster nodes are of YX4X or above models. For more information a...

Figure 28: Prerequisite check failure

7.2 Onboarding checklist failure

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



Dell OpenManage Integration

Cluster - Dell PowerEdge Server (Nodes: 2)

Dell Infrastructure Management at-scale from Azure Portal

Integrate Dell Infrastructure management capabilities into Azure and get the benefits of fı

Learn more on Azure policies

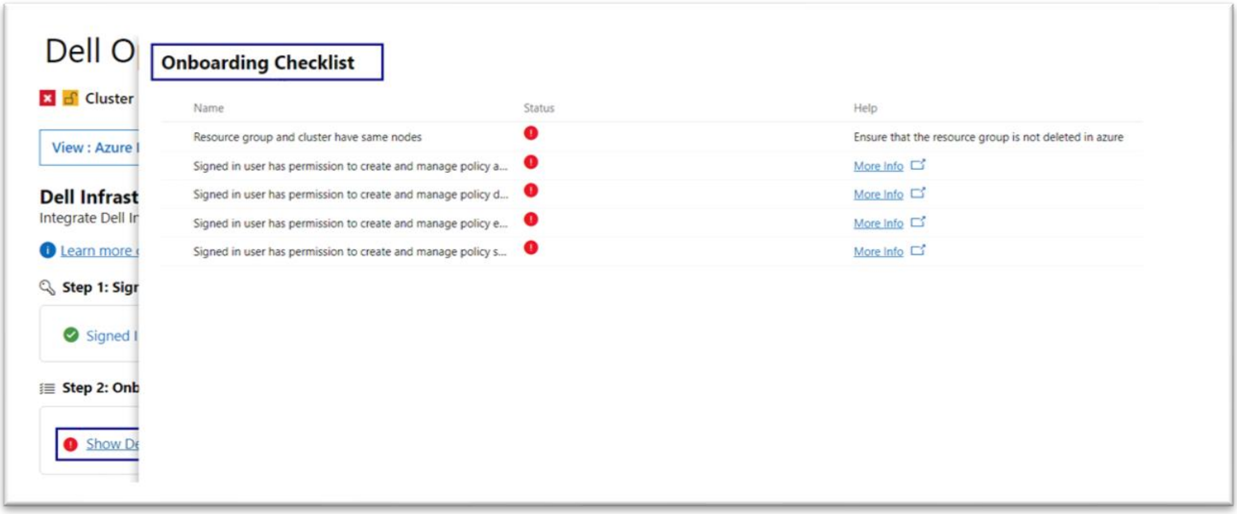
Step 1: Sign in to Azure

Signed In

Step 2: Onboarding Checklist

Step 3: Onboard Policies View Subscription Details

Figure 29: Onboarding checklist failure status



Onboarding Checklist

Name	Status	Help
Resource group and cluster have same nodes	●	Ensure that the resource group is not deleted in azure
Signed in user has permission to create and manage policy a...	●	More Info
Signed in user has permission to create and manage policy d...	●	More Info
Signed in user has permission to create and manage policy e...	●	More Info
Signed in user has permission to create and manage policy s...	●	More Info

Figure 30: Onboarding checklist popup page – Failure Status

8 Conclusion

Using this white paper, one can easily use OMIMSWAC to onboard Dell SCP policies on Azure Arc for monitoring Hyper-V based failover 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 hybrid machines to Azure from Windows Admin Center, see link.
- Connect hybrid machines to Azure using a deployment script, 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.