

# Deploying Dell EMC HCI Solutions for Microsoft Windows Server with OpenManage Integration for Microsoft System Center

This technical white paper describes automated solution to deploying a Microsoft Windows Server HCI cluster using Dell EMC OpenManage Integration for Microsoft System Center (OMIMSSC).

## Abstract

OMIMSSC is a Dell EMC systems management integration for Microsoft System Center products that enables complete lifecycle management of Dell EMC devices. Dell EMC HCI Solutions for Microsoft Windows Server delivers a validated and certified HCI solution that enables organizations to modernize their infrastructure for improved application uptime and performance, simplified management and operations, and lower total cost of ownership. This document provides an overview to automated remote deployment mechanism of Microsoft Windows Server HCI clusters using OMIMSSC from Microsoft System Center Virtual Machine Manager (SCVMM).

September 2021

## Revisions

Date	Description
September 2021	Deploying Dell EMC HCI Solutions for Microsoft Windows Server with OpenManage Integration for Microsoft System Center version 7.3

## Acknowledgements

This paper was authored by the following:

**Authors:** Harsha Naik and Shiva Prasad

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

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

Copyright © 2021 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [9/17/2021] [Whitepaper] [Document ID]

# Table of contents

Revisions.....	2
Acknowledgements.....	2
Table of contents .....	3
Executive summary.....	4
1 Introduction to OMIMSSC .....	5
1.1 Important links .....	5
2 Solution Prerequisites .....	6
3 Network Connectivity and Setup .....	7
4 Windows Server HCI Cluster Deployment Workflow .....	10
4.1 Discovering target nodes.....	12
4.2 Creating Logical Switch configuration profile .....	15
4.3 Preparing Operational Template .....	16
4.3.1 Create bootable WinPE image .....	17
4.3.2 Create Physical Computer Profile (PCP) .....	19
4.3.3 Create Hypervisor Profile .....	19
4.3.4 Create Operational Template .....	21
4.4 Automated Cluster Deployment.....	24
4.5 Viewing deployed Cluster .....	28
Technical support and resources.....	30
Related resources .....	30
Terms and Definitions .....	30

## Executive summary

Microsoft Storage Spaces Direct uses industry-standard servers with local-attached drives to create highly available, highly scalable software-defined storage at a fraction of the cost of traditional SAN or NAS arrays. Storage Spaces Direct is included in Windows Server 2019 Datacenter, Windows Server 2016 Datacenter, and Windows Server Insider Preview Builds. It also provides the software-defined storage layer for Azure Stack HCI. Azure Stack HCI is a hyperconverged infrastructure (HCI) cluster solution that hosts virtualized Windows and Linux workloads and their storage in a hybrid environment that combines on-premises infrastructure with cloud services.

Microsoft HCI Solutions from Dell Technologies encompass various configurations of AX nodes from Dell Technologies to power the primary compute cluster that is deployed as a hyperconverged infrastructure. Dell EMC Integrated System for Microsoft Azure Stack hyperconverged infrastructure (HCI) is an all-in-one validated HCI system that leverages an integrated foundation from Dell Technologies. Designed with full-stack lifecycle management and native Azure integration, the integrated system delivers efficient operations, flexible consumption models and high-level enterprise expertise.

HCI cluster deployment process involves various number of steps when carried out manually and requires a specialized knowledge of prerequisite and recommended configurations to be met on the solution cluster nodes. A manual operational process and insufficient knowledge can be error-prone leading to various quality hurdles and deployment challenges. Dell Technologies has partnered with Microsoft to address these challenges by providing a high degree of automation.

OpenManage Integrations for Microsoft System Center Virtual Machine Manager (OMIMSSC) is an offering from Dell EMC that provides comprehensive capabilities for deployment and lifecycle management of a Windows Server Hyperconverged (HCI) solution cluster with simplified management and operations.

It provides automated workflows that abstracts the various management complexities involved in HCI solution cluster deployment process and eliminates the need for specialized knowledge to apply configurations recommended for HCI solution. It also provides cluster management capabilities with cluster aware updates to keep your data safe while making the update process simple, safe and minimize disruptions in your datacenter.

This document provides guidance, use cases and best practices to the above-mentioned workflows, approximately reducing over 16 manual steps per node and over 15 minutes of attended time per node excluding the time put into study, assessments and guess work.

---

Note: OMIMSSC provides Microsoft HCI deployment solution (based on Microsoft Windows Server OS) using AX Nodes from Dell Technologies (also includes legacy S2D Ready Nodes) through Microsoft System Center Virtual Machine Manager (SCVMM)

---

# 1 Introduction to OMIMSSC

OpenManage Integration for Microsoft System Center (OMIMSSC) is a software-based virtual appliance that provides complete lifecycle management of Dell devices like Servers, Chassis and switches in virtual and cloud environments, when integrated with Microsoft system center configuration Manager (SCCM) and Microsoft System Center Virtual Machine Manager (SCVMM).

OMIMSSC offers capabilities of end to end deployment solution involving device discovery, hardware and firmware patching, hardware and firmware compliance reporting, operating system deployment and cluster deployment with other management automations.

SCVMM serves as a central point of management for virtualization, cloud deployments and more. This document provides guidance on how to deploy and manage a Microsoft Windows Server HCI solution cluster using OMIMSSC through SCVMM environments.

## 1.1 Important links

To download OMIMSSC, refer [Dell Support Site](#).

For information on OMIMSSC installation, refer to [Manuals](#).

For information about SCVMM, see the Microsoft documentations.

## 2 Solution Prerequisites

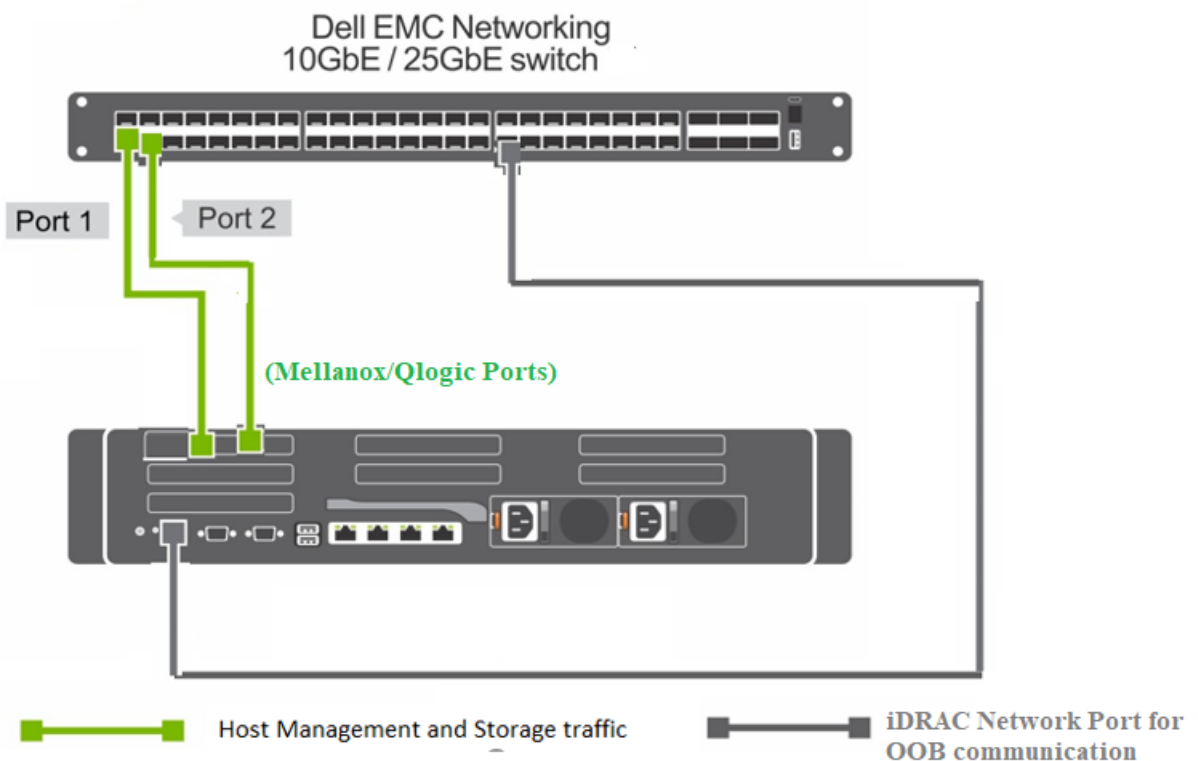
Components	Version
Management Console	Dell EMC OMIMSSC for SCCM and SCVMM Appliance version 7.3.
Microsoft Consoles (Management System)	<ul style="list-style-type: none"> <li>• SCVMM 2019</li> <li>• SCVMM 2016</li> </ul>
Managed Nodes (Dell EMC Microsoft Storage Spaces Direct Ready Nodes and AX Nodes)	<ul style="list-style-type: none"> <li>• AX6515</li> <li>• AX-740XD and RN740xd</li> <li>• AX-640 and RN640</li> <li>• RN740XD2</li> <li>• RN440</li> </ul>
Dell EMC Networking switches	For the complete list of supported switches, see <a href="#">Support Matrix for Dell EMC Solutions for Microsoft Azure Stack HCI</a> .
Supported Operating System on Managed Node	<ul style="list-style-type: none"> <li>• Microsoft Windows Server 2019</li> <li>• Microsoft Windows Server 2016</li> </ul>

Table 1 Solution Pre-requisites

### 3 Network Connectivity and Setup

OMIMSSC supports Windows Server HCI solution with “fully converged network design” supporting up to 16 nodes in a cluster which indicates that both Management and Storage network traffic will be made available on a Dual Port Mellanox/QLogic network cards present on each managed node.

Figure below is an illustration of a simple connected topology of an AX Node with top of rack (TOR) network switch. For more information on AX Node connectivity and Network Switch configurations see [Storage Spaces Direct Network configuration guide](#).



Simple Topology of single node connected with TOR switch

---

NOTE: In case redundant switch connection is chosen and nodes are connected over two separate network switches then both switches will require access to all the subnets so that fail over can occur. Also, ensure that the iDRAC network (i.e. Management Network) is reachable from OMIMSSC and SCVMM.

---

OMIMSSC facilitates the software settings on network adapter ports of each Managed Node to enable management and storage network traffic. User will require to provide inputs to cluster node like IP range,

subnet details, VLAN, DNS and gateway details matching the physical network environment where Managed Nodes are connected to.

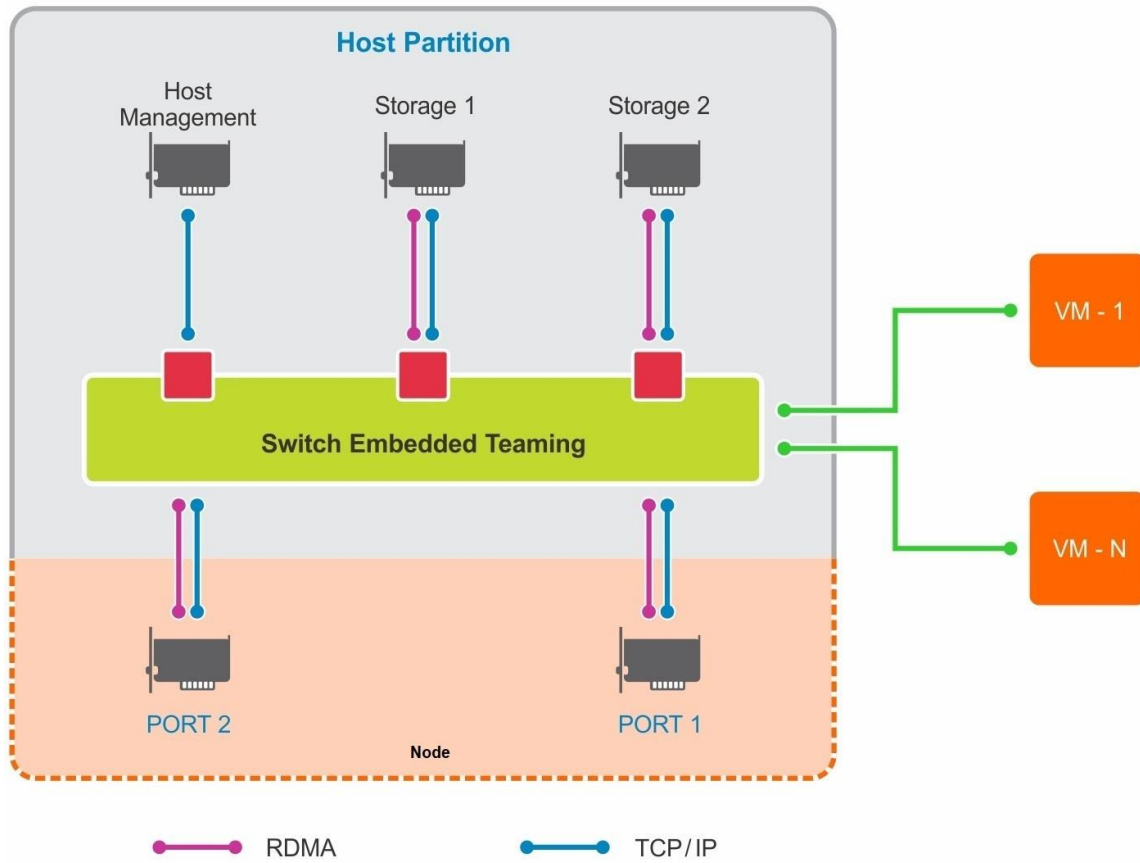
Below table represents the network traffic to be configured.

Traffic Class	Purpose	VLAN Tagging
Management	For management of cluster, cluster nodes and VM traffic	Untagged
Storage 1 (Fault Domain 1)	SMB traffic for storage data transmission	Tagged
Storage 2 (Fault Domain 2)	SMB Traffic for storage data transmission	Tagged

Table 2 Configured Network Traffic settings by OMIMSSC on each Managed Node

Figure below is as illustration of how solution will configure the network traffic internally on each Managed Node.





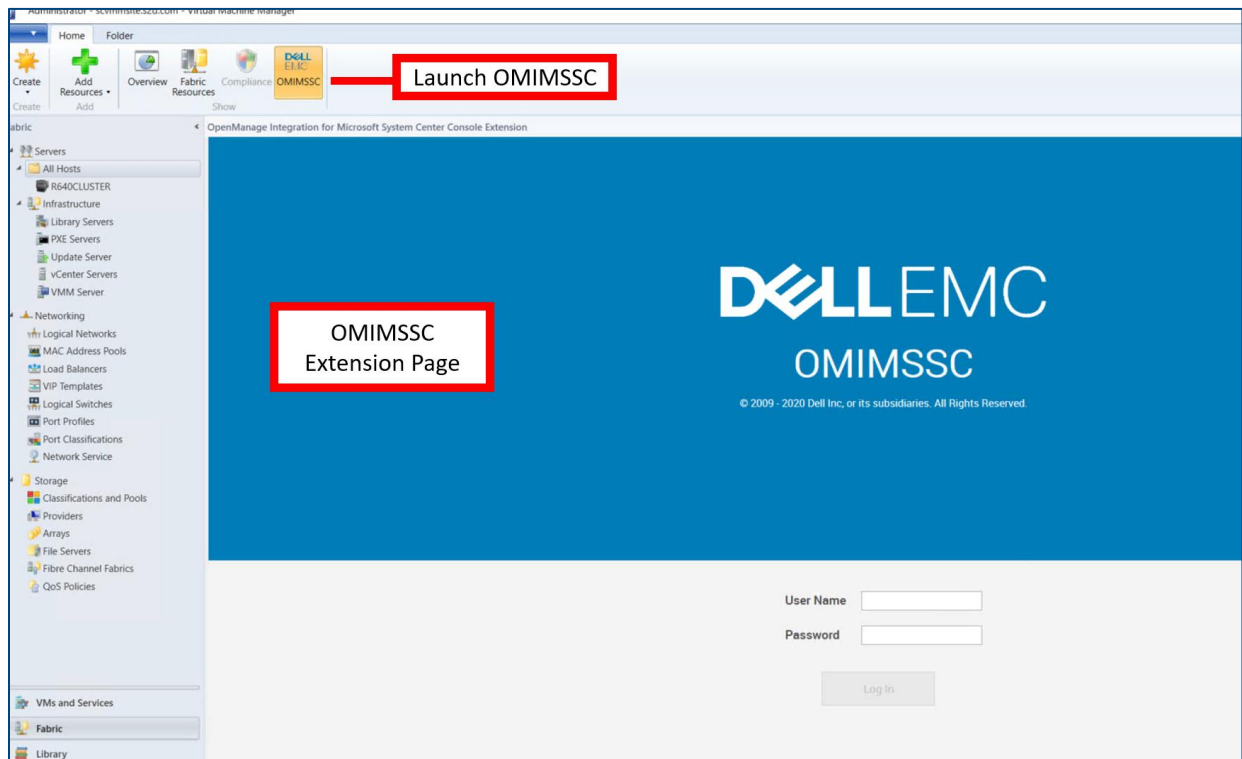
Configured Network-Traffic on each node

Details on configuration steps is discussed in the “Logical Switch Configuration” section.

## 4 Windows Server HCI Cluster Deployment Workflow

Let us start off with HCI cluster deployment workflow by launching OMIMSSC extension page that is embedded into SCVMM console.

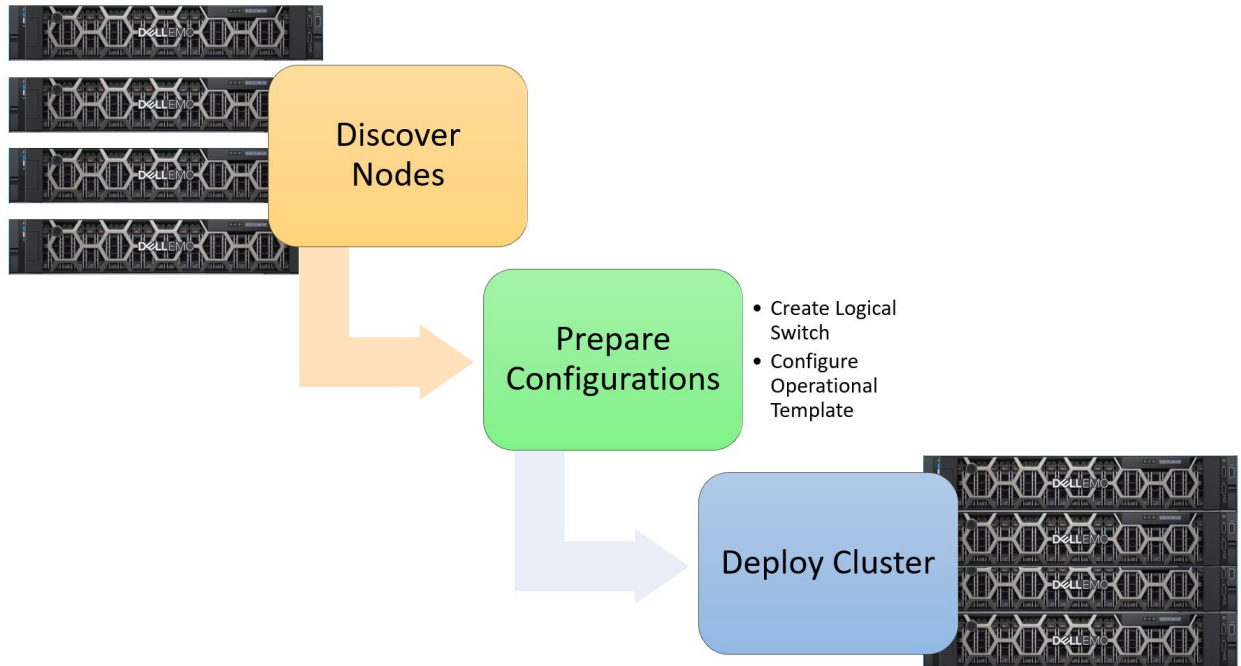
Once you are in Microsoft SCVMM Console, click on Hosts or Hosts group to find “Dell EMC OMIMSSC” under “Home” ribbon. This is the launch point of Dell EMC OMIMSSC extension.



### Dell EMC OMIMSSC Extension Console

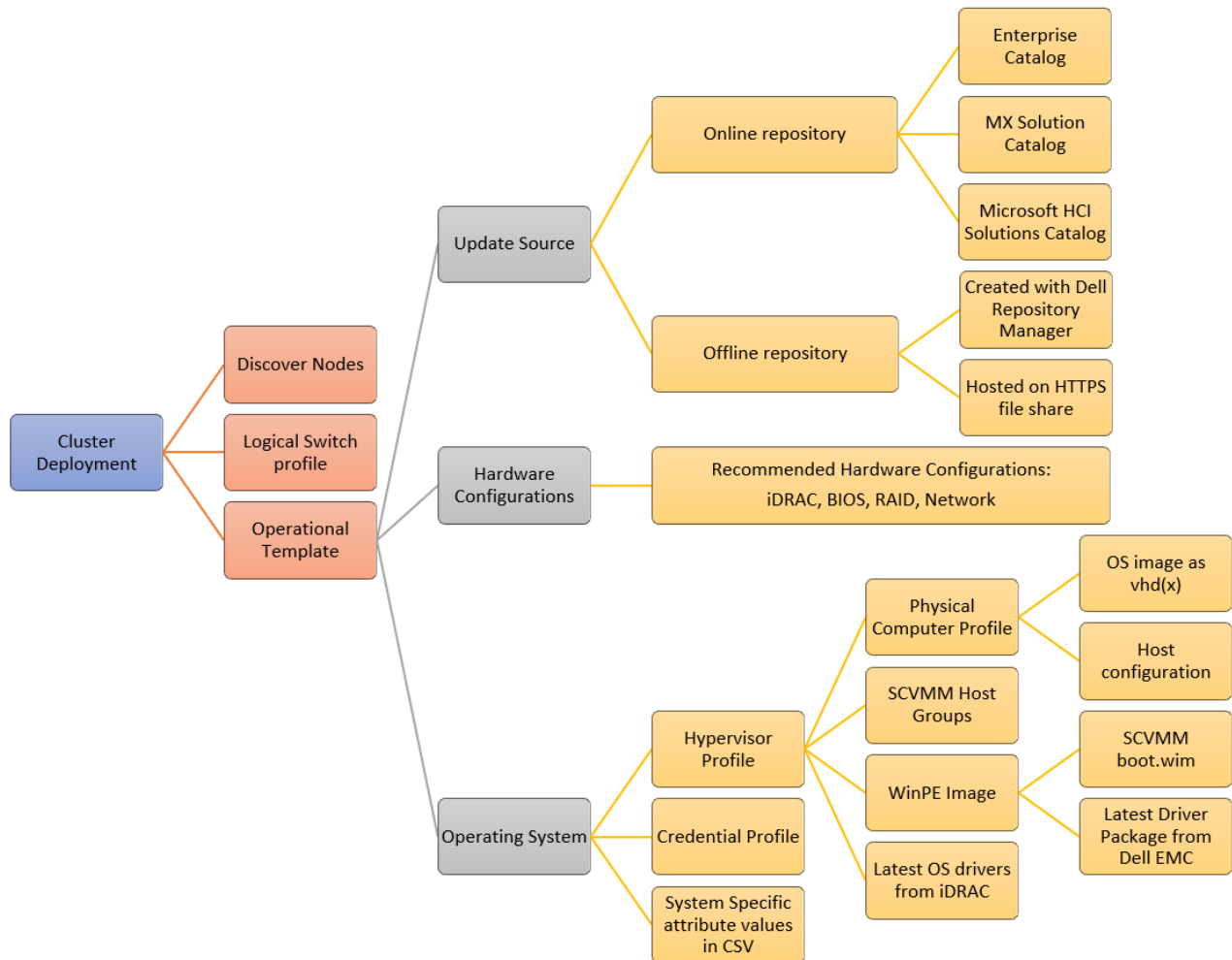
On a high level, creating a Windows Server HCI cluster using OMIMSSC, consists steps that are fully automated by OMIMSSC bringing in seamless cluster creation that is repeatable eliminating guesswork and the risk of manual error(s)

1. Discover the nodes to be provisioned for cluster using iDRAC IP.
2. Prepare the configurations to be deployed:
  - a. Create Logical Switch profile with Management, Storage and Cluster networking configurations.
  - b. Configure Operational Template with Operating System specific details.  
Note: Operational Template already contains validated update repository and recommended hardware configurations from Dell Technologies.
3. Deploy Cluster.



Cluster deployment steps overview

To understand different artifacts used for deployment, refer to the below image. Steps and purpose of each of these artifacts are detailed in further sections.

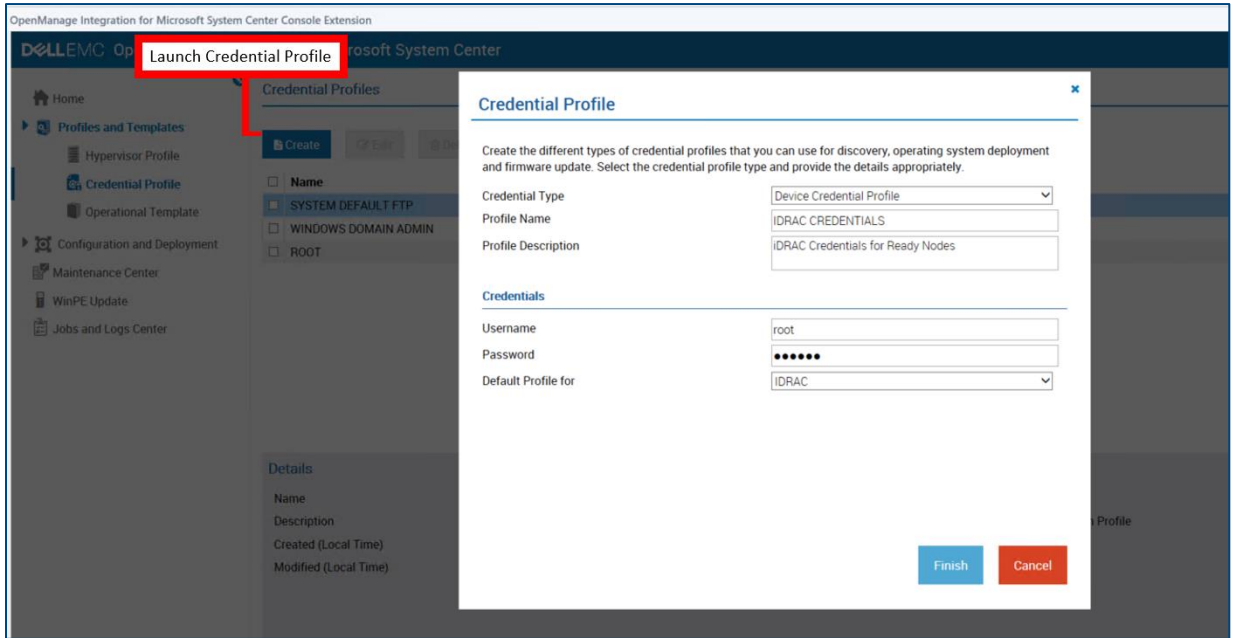


Cluster Deployment Pre-requisites and artifacts roll up

## 4.1 Discovering target nodes

**PRE- REQUISITE:** Create a **Credential Profile** of type device that carries iDRAC credentials to discover the nodes. To create a **Credential Profile**, navigate Dell EMC OMIMSSC extension, click **Profiles and Templates**, and then click **Credential Profile** and click **Create**.

**IMPORTANT:** iDRAC credentials provided in **Credential Profile** must have administrator privilege on iDRAC.

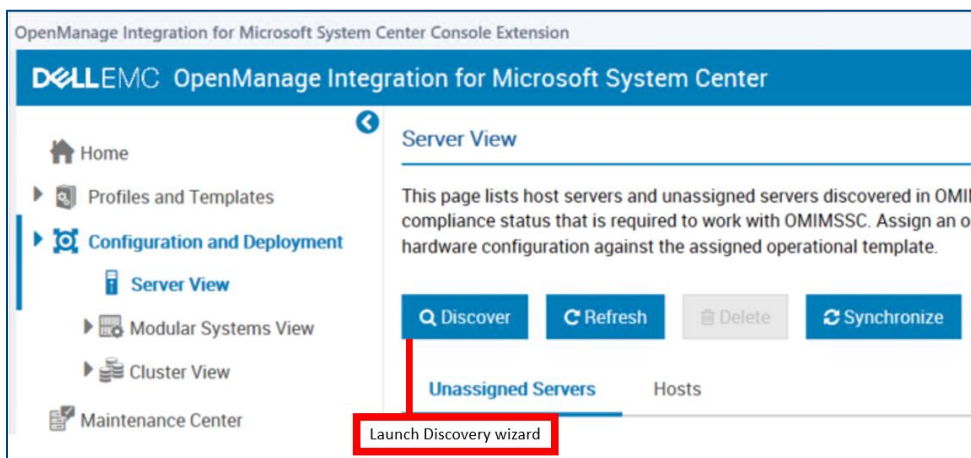


### Create Credential Profile

Have the iDRAC IP and Service Tags of all Managed Nodes participating in HCI cluster deployment handy. It would help us select nodes for cluster deployment.

We will discover the nodes with its iDRAC IP and credentials in OMIMSSC with below steps within Dell EMC OMIMSSC extension:

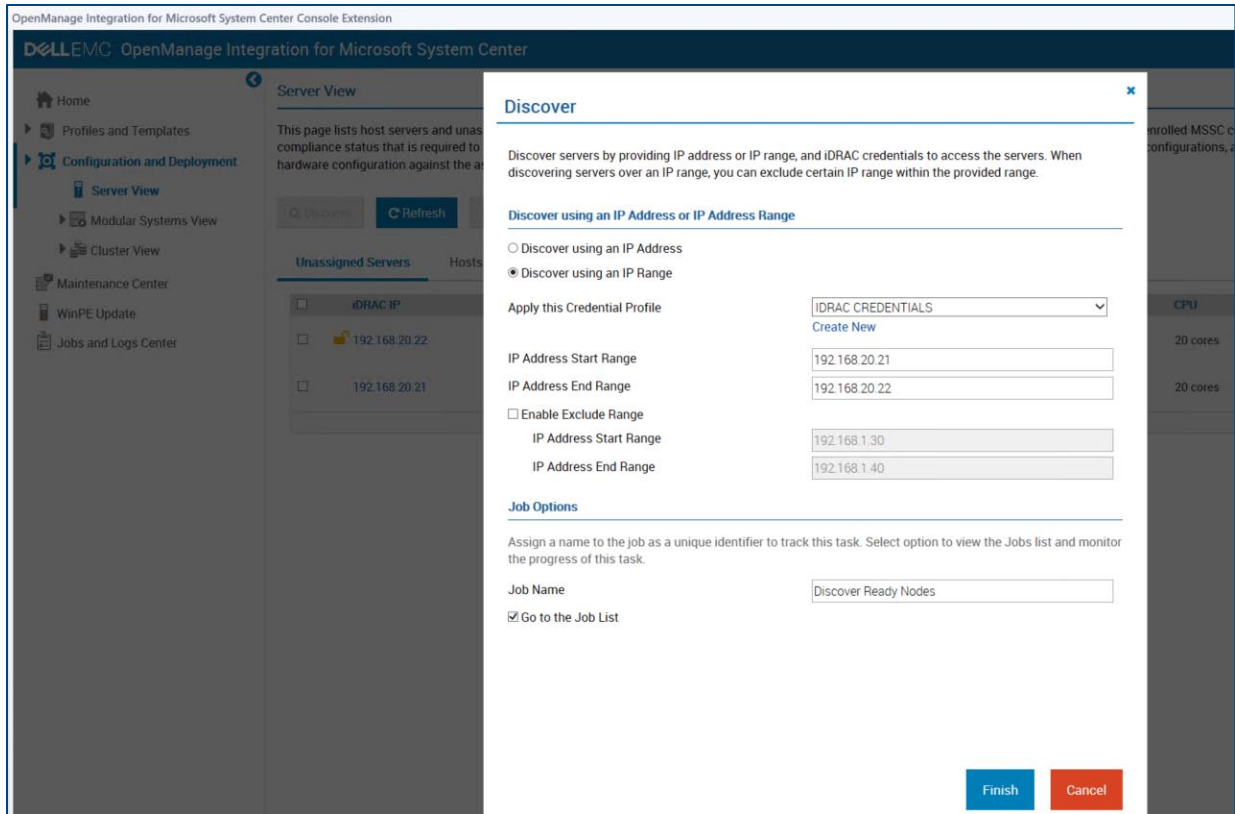
1. In the **Configuration and Deployment** page, in the left pane navigate to **Server View** and click **Discover**.



### Launch Discovery Wizard

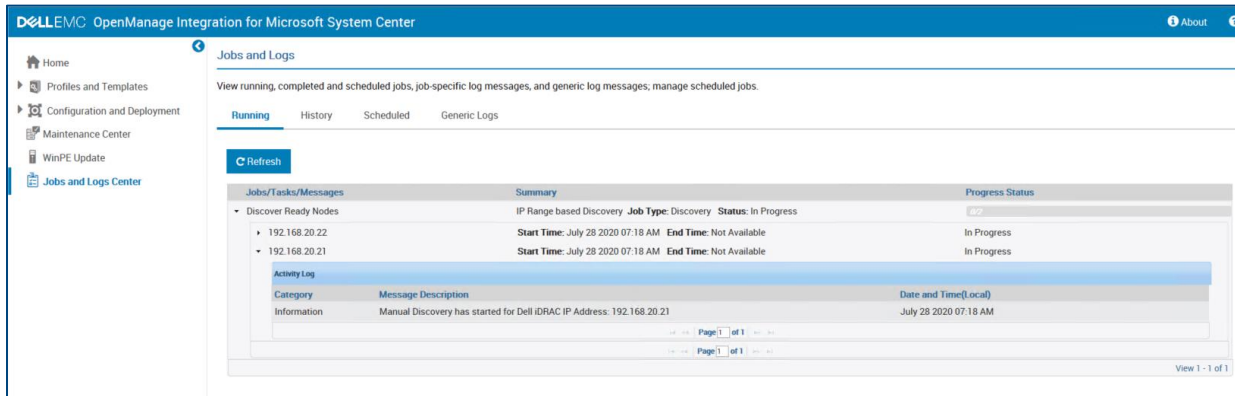
2. Provide the iDRAC IP range, Credential Profile with iDRAC credentials and job details.

3. Submit the job to discover these Managed Nodes in few minutes.



Enter iDRAC IP details and discover.

**NOTE:** Track the progress of the discovery at **Jobs and Logs Center**. Identify the job using the provided name.



Jobs and Logs Center for tracking job progress.

## 4.2 Creating Logical Switch configuration profile

Windows Server HCI solution requires necessary network settings to be configured to enable network traffic on each cluster node.

As part of the automated cluster deployment workflow, OMIMSSC applies these network configurations using a Logical Switch template created from OMIMSSC, leveraged from SCVMM.

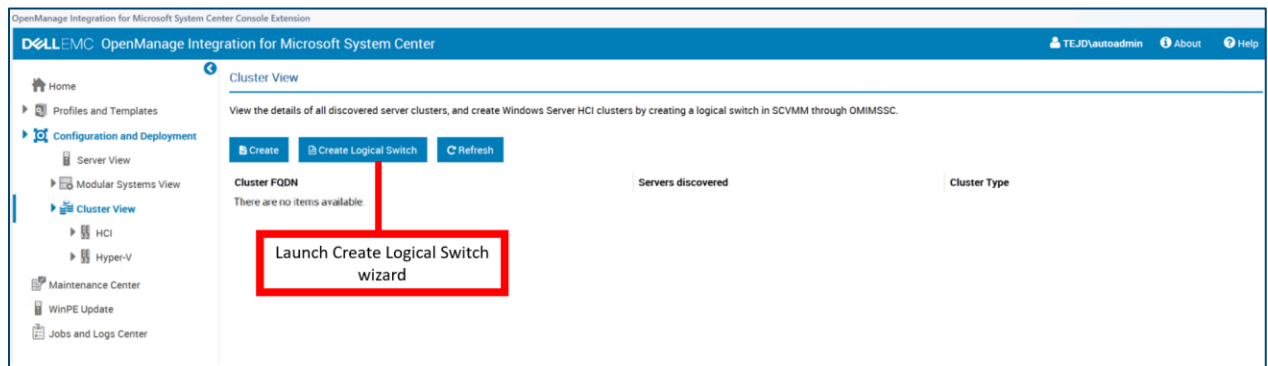
---

**BEST PRACTICE:** Release any unused or unallocated IP addresses used within IP pools created in SCVMM console and ensure to use new IP addresses before creating logical switch profile

---

To create this Logical Switch profile within Dell EMC OMIMSSC extension:

1. In the **Configuration and Deployment** page, in the left pane navigate to **Cluster View** and click **Create Logical Switch**.



Creating Logical Switch for Cluster Network traffic

2. Provide the required parameters for management and storage network traffic, matching the network environment of your lab.

## Create Logical Switch ✕

Create a logical switch, for a group of host servers in SCVMM console by providing management and storage network details.

Logical Switch Name

SCVMM Host Group Destination

---

### Configuration for Management

Start IP	<input style="width: 100%;" type="text" value="192.168.10.2"/>	DNS Server	<input style="width: 100%;" type="text" value="192.168.0.1"/>
End IP	<input style="width: 100%;" type="text" value="192.168.10.6"/>	DNS Suffix	<input style="width: 100%;" type="text" value="hcidomain.com"/>
Subnet	<input style="width: 100%;" type="text" value="192.168.10.1/24"/>	Gateway	<input style="width: 100%;" type="text" value="192.168.10.1"/>

---

<h4>Configuration for Storage 1</h4> <p>VLAN ID <input style="width: 100%;" type="text" value="2"/></p> <p>Start IP <input style="width: 100%;" type="text" value="192.168.12.2"/></p> <p>End IP <input style="width: 100%;" type="text" value="192.168.12.6"/></p> <p>Subnet <input style="width: 100%;" type="text" value="192.168.12.1/24"/></p>	<h4>Configuration for Storage 2</h4> <p>VLAN ID <input style="width: 100%;" type="text" value="3"/></p> <p>Start IP <input style="width: 100%;" type="text" value="192.168.13.2"/></p> <p>End IP <input style="width: 100%;" type="text" value="192.168.13.6"/></p> <p>Subnet <input style="width: 100%;" type="text" value="192.168.13.1/24"/></p>
---	---

---

### Job Options

Assign a name to the job as a unique identifier to track this task. Select option to view the Jobs list and monitor the progress of this task.

Configure Management and Storage Network traffic details

3. Navigate to SCVMM to confirm the created Logical Switch Profile and dependencies with specified cluster and network details.

---

RECOMMENDATION: Logical Switch and other dependency profiles that are created by OMIMSSC in SCVMM will be created with Dell EMC recommended network adapter vendor configurations and internal naming conventions, modifying it may cause failure during cluster creation operation.

---

## 4.3 Preparing Operational Template

To perform Day 0 Cluster deployment, OMIMSSC facilitates with a single template containing Firmware, Hardware and Operating System details known as the **Operational Template**.



---

NOTE: OMIMSSC has pre-built Operational Templates carrying Dell EMC validated and recommended hardware configurations for your chosen AX nodes (or legacy S2D Ready Nodes) with supported Network Adapter vendor choices.

NOTE: OMIMSSC carries validated update catalog maintained online containing qualified set of firmware and drivers recommended for HCI cluster solutions. This is named as the “**Update Catalog for Microsoft HCI Solutions**”

---

OMIMSSC leverages SCVMM's Physical Computer Profile (PCP) and WinPE image for OS deployment purpose. We will first look at the steps to create bootable WinPE image and PCP, and then move on to configuring them as a single template i.e. Operational Template in later sections.

### 4.3.1 Create bootable WinPE image

This section details the steps to create a bootable WinPE image.

#### Generate SCVMM WinPE image

OMIMSSC for OS deployment uses WinPE (Windows Preinstallation Environment) boot image to perform pre-OS configurations. To generate this boot.wim file, enable Windows Deployment Services (WDS) role on the server where SCVMM is installed and add PXE server to SCVMM. This will create a boot.wim file at <WDS directory>\RemoteInstall\DCMgr\Boot\Windows\Images location.

For information about the WDS role on a server, and adding a PXE server to SCVMM, see [Provisioning a Hyper-V host or cluster from bare-metal computers section](#) of Microsoft documentation.

We will further inject latest boot critical drivers (i.e. Network and Storage) to this image using OMIMSSC in subsequent steps. As a preparation for this injection step, copy this boot.wim to CIFS share accessible to OMIMSSC appliance.

---

NOTE: Consider keeping the CIFS share in SCVMM machine to unify network traffic.

---

#### Download and extract latest boot critical drivers

OMIMSSC is enabled with a provision to inject latest boot critical drivers using Dell EMC OpenManage Server Driver Pack DVD. It is a publicly released package from Dell EMC which packages OS drivers for all the Server platforms.

To download OpenManage driver pack, launch <https://www.dell.com/support/> -> Search for the keyword Dell EMC OpenManage server Driver Pack DVD and download the corresponding OpenManage server driver pack based on the supported platforms.

Following are the steps to extract drivers from OpenManage server driver pack.

1. Mount the ISO as a drive in any local Windows machine.
2. Use command prompt and navigate to the <Mounted Drive>:\server\_assistant\driver\_tool\bin.
3. Run command `make_driver_dir.exe -i -d -o --extract`

Let us take an example where the OM Server Driver Pack is mounted drive at F and extracted output path is C:\lom\_server\_diver\_pack. Command to be executed would look like:

```
make_driver_dir.exe -i F:\ - d c:\lom_server_driver_pack -o WINPE10 --extract
```

---

NOTE: The existing files in the extracted output path will be deleted after extraction, hence it is recommended to create a new empty folder for extraction of drivers.

NOTE: Extraction of drivers will take up to 30 minutes. During the process of extraction of drivers, the OMIMSSC console extension may logout automatically as it will be idle for about 30 minutes. Hence save your work before exiting the console extension to perform other operations.

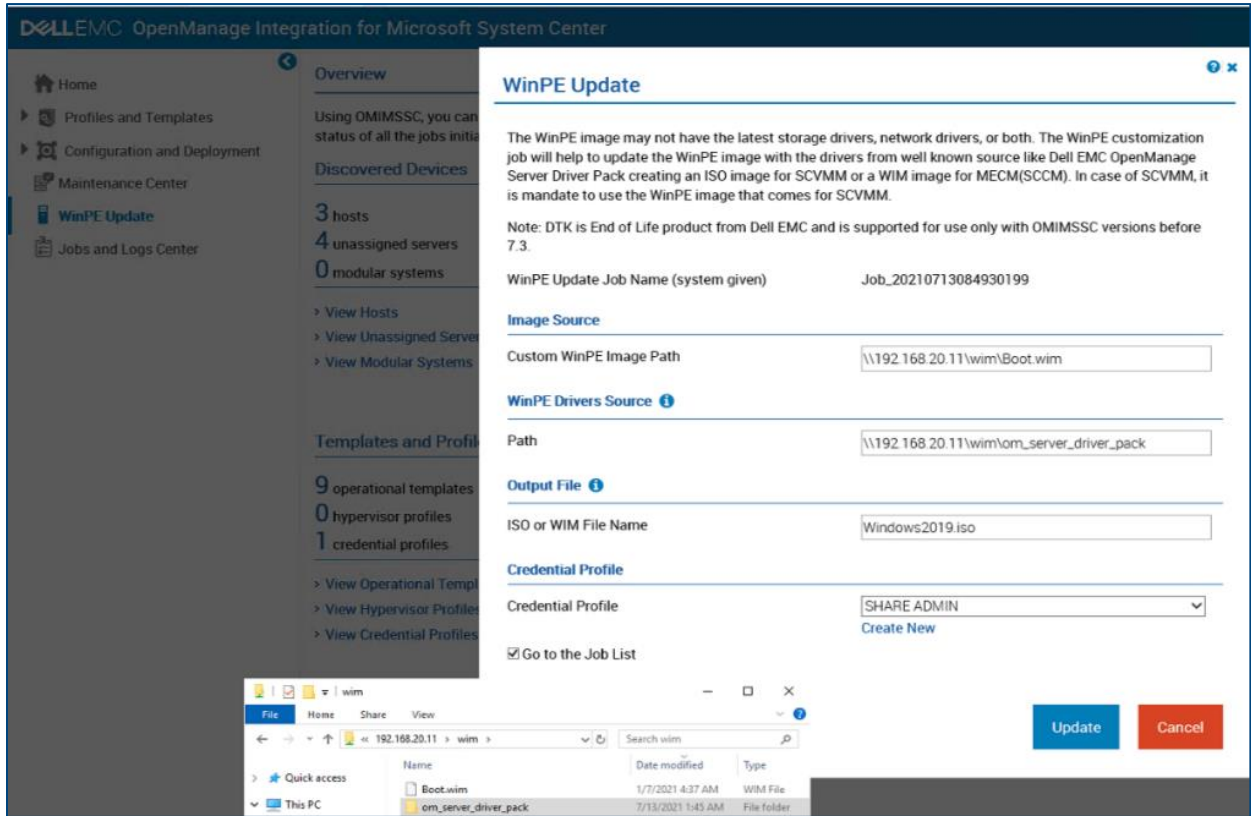
---

4. Now copy the extracted driver pack to a CIFS share folder accessible by OMIMSSC appliance.

## Inject latest boot critical drivers to create a bootable WinPE image

Following are the steps below to create a bootable WinPE image.

1. Navigate to **WinPE Update** on the left pane to launch WinPE Update wizard.
2. Input **Image Source**, CIFS share path to the boot.wim from *Generate SCVMM WinPE image* step.
3. Input **Driver Path**, CIFS share path to the extracted driver pack obtained from Download and extract boot critical drivers' step.  
RECOMMENDATION: Provide the boot.wim and extracted drivers through same CIFS share.
4. Provide the **Output File**, <file\_name.iso>. This will be the boot image generated based on boot.wim from SCVMM injected with latest drivers from driver pack. Mentioned ISO file will be generated in the same share as the above CIFS share.
5. Select the **Credential Profile**, created with Windows Credential Profile type containing domain user credentials having remote access to specified CIFS share.
6. Click **Update**, to submit the WinPE image update with latest drivers. You can track the progress of this activity in Jobs and Logs Center using the system given Job Name (specified in WinPE Update wizard screen)



WinPE Update screen and Windows network share contents

### 4.3.2 Create Physical Computer Profile (PCP)

Physical Computer Profile in SCVMM defines settings used to provision servers. This profile typically contains OS image (vhd or vhdx), domain, host Administrator account, license key and other configurations related to OS deployment.

OMIMSSC leverages this profile and provides value add of combining all these configurations into a single, ready to deploy Operational Template.

For information on creating PCP, see Create a physical computer profile section in Pre-requisites of Microsoft documentation on [Provisioning a Hyper-V host or cluster from bare-metal computers](#).

---

BEST PRACTICE: Latest security updates are applied to the vhd to be deployed and on SCVMM machine.

---

### 4.3.3 Create Hypervisor Profile

Hypervisor Profile is a profile maintained in OMIMSSC to contain all the OS artifacts we discussed above. Consider this profile to be container of pointers to specific Host Group, Physical Computer Profile, WinPE image and source of post OS drivers.

To create a Hypervisor Profile in OMIMSSC,

1. Click **Profiles and Templates**, in the left pane.
2. Click **Hypervisor Profile**.
3. Click **Create**, to launch a guided wizard to create Hypervisor Profile.
4. In **Name and Description** screen, provided unique name for Hypervisor Profile.

---

**BEST PRACTICE:** Provide a name to identify the OS flavour or Host Type information contained in the Hypervisor Profile.

---

5. In **SCVMM Information** screen, select the SCVMM Host Group where the deployed host must be categorized and select the Physical Computer Profile created in above step.

The screenshot shows the 'Hypervisor Profile Wizard' window. The left sidebar contains a list of steps: 'Welcome', 'Name and Description', 'SCVMM Information' (highlighted in blue), 'WinPE Boot Image Source', 'Drivers Source', and 'Summary'. The main area is titled 'SCVMM Information' and contains the following text: 'In SCVMM, select the host group and host profile or physical computer profile that you have assigned for OMIMSSC.' Below this text are two dropdown menus: 'SCVMM Host Group Destination' with 'All Hosts' selected, and 'SCVMM Host Profile/Physical Computer Profile' with 'windows server 2019' selected.

SCVMM Information screen

6. In **WinPE Boot Image Source** screen, input the bootable WinPE iso generated in CIFS share from the above step and select the Credential Profile containing domain user with remote access privilege to the WinPE ISO CIFS path.

The screenshot shows the 'Hypervisor Profile Wizard' window. The left sidebar contains a list of steps: 'Welcome', 'Name and Description', 'SCVMM Information', 'WinPE Boot Image Source' (highlighted in blue), 'Drivers Source', and 'Summary'. The main area is titled 'WinPE Boot Image Source' and contains the following text: 'Provide path and name of the Windows Preinstallation Environment (WinPE) ISO image that will be used for deployment, and the credentials to access the share folders.' Below this text are two input fields: 'Network WinPE ISO Path' with the value '\\192.168.20.11\wim\Windows2019.iso' and 'Credential Profile' with 'SHARE ADMIN' selected. There is also a 'Create New' link below the credential profile dropdown.

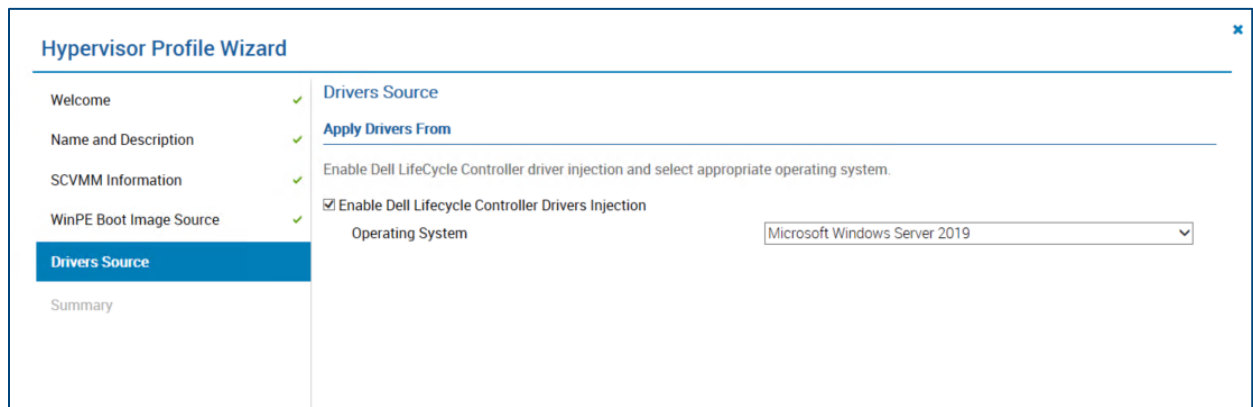
WinPE Boot Image Source

7. In **Drivers Source** screen, select to **Enable Dell Lifecycle Controller Drivers Injection** option with selected Operating System for deployment in Physical Computer Profile. Enabling this option will fetch the latest OS drivers from iDRAC for the specified OS and install them automatically during deployment.

---

**INFORMATION:** If this step is enabled, during deployment you may see a Library Share being created in SCVMM containing the latest OS drivers extracted from iDRAC and Physical Computer Profile cloned into multiple devices (one per selected device for deployment) tagged with these drivers.

---



Drivers Source screen

### 4.3.4 Create Operational Template

OMIMSSC provides pre-configured templates which serves as a single deployment template that carries out all the recommended and mandatory configurations required on a HCI cluster. Different templates are available to suite the different Server models and Network Adapter vendors. When these templates are chosen for deployment, only matching nodes will be listed and allowed for deployment.

---

**RECOMMENDATION:** Configure pre-configured and available Operational Template in OMIMSSC that matches the server model and network adapter manufacturer of your target nodes.

---

On a high level, Operational templates takes care of the following activities during deployment:

1. Updating the firmware and drivers on managed nodes to the HCI recommended baseline. Choose between offline and Dell EMC maintained and validated online repositories
  - Offline: Repository accessible through a CIFS share created using Dell EMC Repository Manager tool.
  - Online: Dell EMC validated, published, and maintained Azure Stack HCI repository available online provided as a simple drop-down option as Update Source under Firmware component in Operational Template.

---

**NOTE:** OMIMSSC supports HCI solution clusters that are based on Microsoft Windows Server 2016/2019 OS

---

2. Hardware configuration non-compliance remediation.
  - Operational Templates carry HCI recommended hardware configurations for your Cluster Nodes. You can view and modify available hardware configurations in Operational Template. Selected configurations will be applied during deployment.

---

**IMPORTANT:** Recommended settings are preconfigured and non-editable.

---

3. Operating System Configurations.
  - o Choose the Hypervisor Profile and IP configuration in OS component.

Follow the below steps to view, edit and prepare the Operational Template for deployment.

1. Click **Profiles and Templates**, on the left pane.
2. Select **Operational Templates**, to view these pre-defined templates.

---

**IMPORTANT:** Ensure you pick the relevant Operational Template for your Cluster deployment.

---

Below are the available Pre-defined Operational Templates:

Template names are self-explanatory to denote the purpose of the template that is supported AX/Storage Spaces Direct Ready Node server model and the Network Adapter vendor combination.

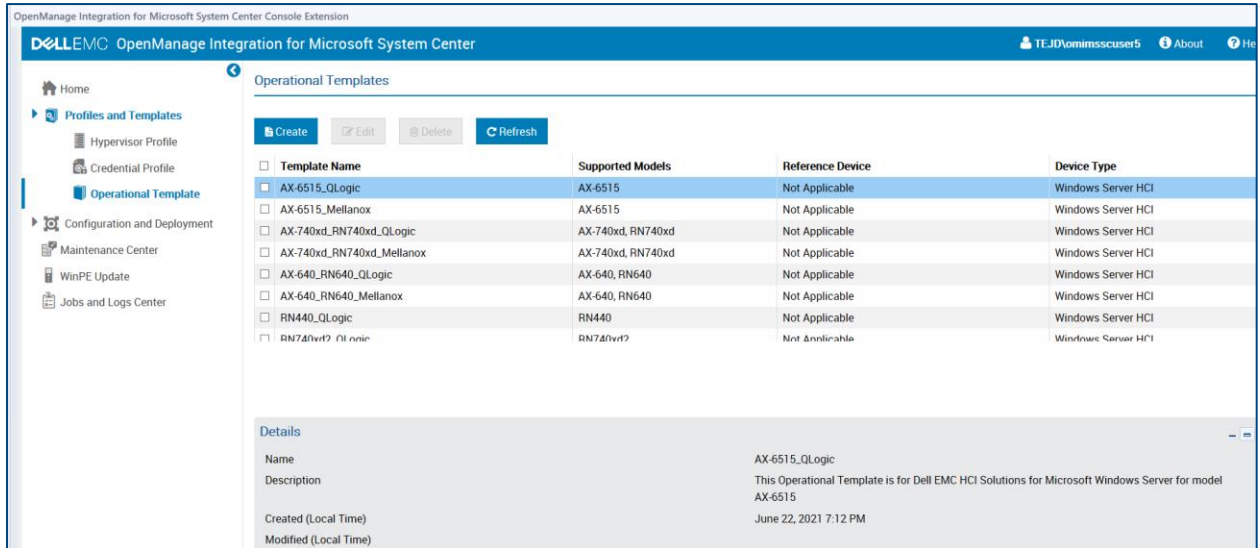
Operational Template Name	Description
AX-6515_QLogic	For server models AX-6515 with RDMA enabled QLogic Network Adapter
AX-6515_Mellanox	For server models AX-6515 with RDMA enabled Mellanox Network Adapter
AX-740xd_RN740xd_QLogic	For server models AX-740xd and RN740xd with RDMA enabled QLogic Network Adapter
AX-740xd_RN740xd_Mellanox	For server models AX-740xd and RN740xd with RDMA enabled Mellanox Network Adapter
AX-640_RN640_Mellanox	For server models AX-640 and RN640 with RDMA enabled Mellanox Network Adapter
AX-640_RN640_QLogic	For server models AX-640 and RN640 with RDMA enabled Mellanox Network Adapter
RN440_QLogic	For server models AX-6515 with RDMA enabled Qlogic Network Adapter
RN740xd2_Mellanox	For server models RN740xd2 with RDMA enabled Mellanox Network Adapter
RN740xd2_QLogic	For server models RN740xd2 with RDMA enabled Qlogic Network Adapter

---

**RECOMMENDATION:** Do not delete these pre-defined Windows Server HCI Operational Templates.

---

3. From the pre-configured templates listed, choose the template to prepare based on server model and network card vendor.
4. Select the template and click **Edit**. This will display a guided wizard for providing configurable attributes across firmware, hardware, and OS components of deployments.



View and Edit pre-configured Operational Templates for HCI cluster deployment

NOTE: You may see a fixed Network card slot number in network component of Operational Template which may not be the slot number of the actual Network card in the node. However irrespective of network card slot number on the ready nodes, solution will take care of dynamically applying the network component configurations on the cluster nodes.

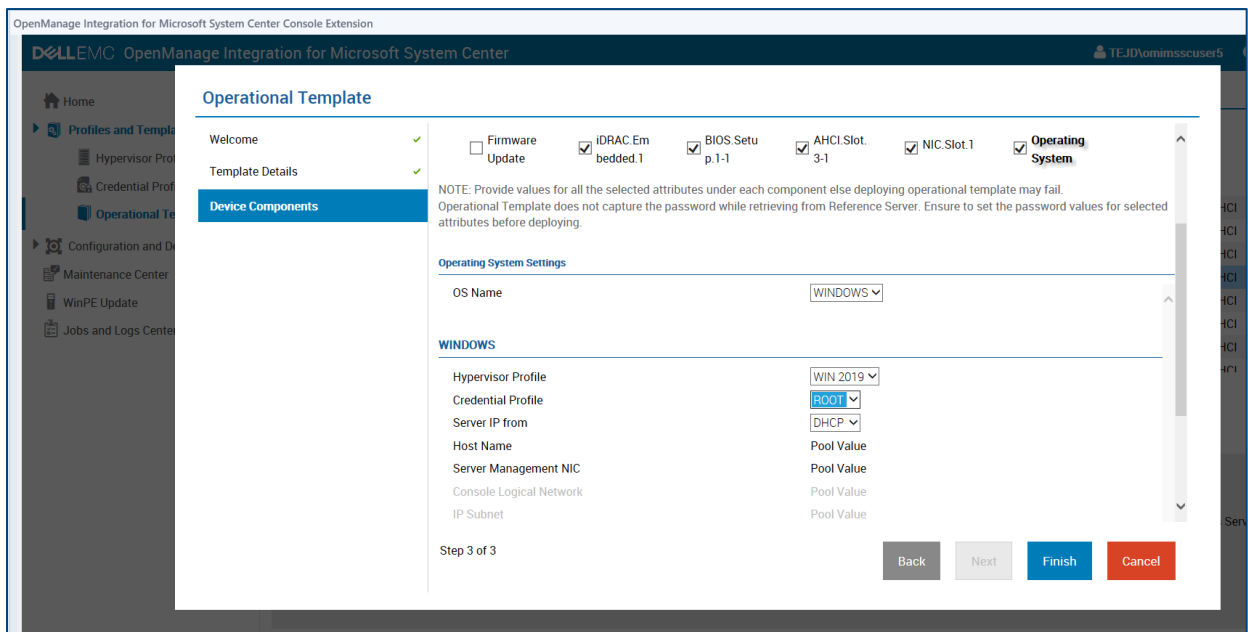
5. For **Firmware Update** component of Operational Template, select **Update Source** dropdown menu to view the pre-built and configured baseline repositories.
  - For appliance VM network configured with access to internet (with or without proxy), make use of validated, maintained and quarterly updated baseline repository. You may identify this repository with the name **“UPDATE CATALOG FOR MICROSOFT HCI SOLUTIONS”**.
  - For appliance VM network configured with no access to internet, and if you require any customization on how the baseline repository must be created and maintained, choose Dell Repository Manager (DRM) software. Create repository with custom models and components targeted for specific OSES with DRM and expose the catalog XML with repository files through CIFS share folder to OMIMSSC.

BEST PRACTICE: Perform Test Connection of Update Source selected in Operational Template at Maintenance Center by editing the update source under Maintenance Settings.

BEST PRACTICE: Ensure the bell icon in Maintenance Center on the top right corner is green, indicating that the catalog in the Update Sources are latest. If it is yellow, click the bell icon to retrieve the latest catalog.

6. For Hardware configuration, select the specific components. View, select and edit applicable attributes with desired configurations.
7. For **Operating System** component,
  - Select **OS Name** as WINDOWS.

- Select the **Hypervisor Profile** created in previous section.
- Select **Credential Profile** with iDRAC user details. If the credentials used to discover the nodes has not changed, select the same Credential Profile.
- Select **Server IP from**, this is the source of IP (Static/DHCP) for deployed OS before Logical Switch is applied to communicate with SCVMM.



#### Operating System component configuration

**IMPORTANT:** System specific values specified in Operational Template would be configured in final cluster deployment step. Some of the examples to system specific values are Host Name, Static IP, AssetTag .

**BEST PRACTICE:** Assign the configured Operational Template to servers considered for cluster deployment to check hardware configuration compliance of these servers against the configured template.

## 4.4 Automated Cluster Deployment

We now are in the final step to deploy the Cluster. From the above sections, you need two artifacts:

1. Logical Switch
2. Operational Template

Additionally, have the below information handy to be provided during deployment

1. Cluster Name.
2. Cluster IP.



---

NOTE: Cluster IP must be from the same subnet as the Management IP provided in the Logical Switch profile.

---

One last step before you trigger an unattended automated deployment of Cluster is to configure the system specific attributes that are selected in Operational template. Let's do this as part of Cluster deployment step.

To start the Cluster deployment step, follow the below steps

1. In the **Configuration and Deployment** page, in the left pane navigate to **Cluster View** and click **Create**.
2. Select **Operational Template** that was configured in previous sections. Based on the Model and Network vendor type of the selected Operational Template, all RDMA enabled nodes will be listed below with Service Tag, iDRAC IP and Model as a selection of cluster nodes for deployment.
3. Configure system specific hardware attributes for the listed servers against the attributes in selected Operational Template. Click **Export Attribute Value Pool** which exports these system specific attributes replicated for all listed Service Tags as CSV file. Some of the OS component related attributes are listed below image.

## Create Cluster ✕

---

Using this page, you can update firmware, configure hardware, and deploy or redeploy operating system using predefined operational templates. Deploying the template creates clusters with the required network configurations to enable Windows Server HCI feature on that cluster.

Cluster Name

IP Address

Logical Switch

Operational Template

Export Attribute Value Pool

<input checked="" type="checkbox"/> Server Identifier	iDRAC IP	Model
<input checked="" type="checkbox"/> 28MR9P2	192.168.20.10	AX-640
<input checked="" type="checkbox"/> 28M0BP2	192.168.20.21	AX-640

Attribute Value Pool  ✕ Browse

---

### Job Options

Assign a name to the job as a unique identifier to track this task. Select option to view the Jobs list and monitor the progress of this task.

Job Name

Go to the Job List

Create
Cancel

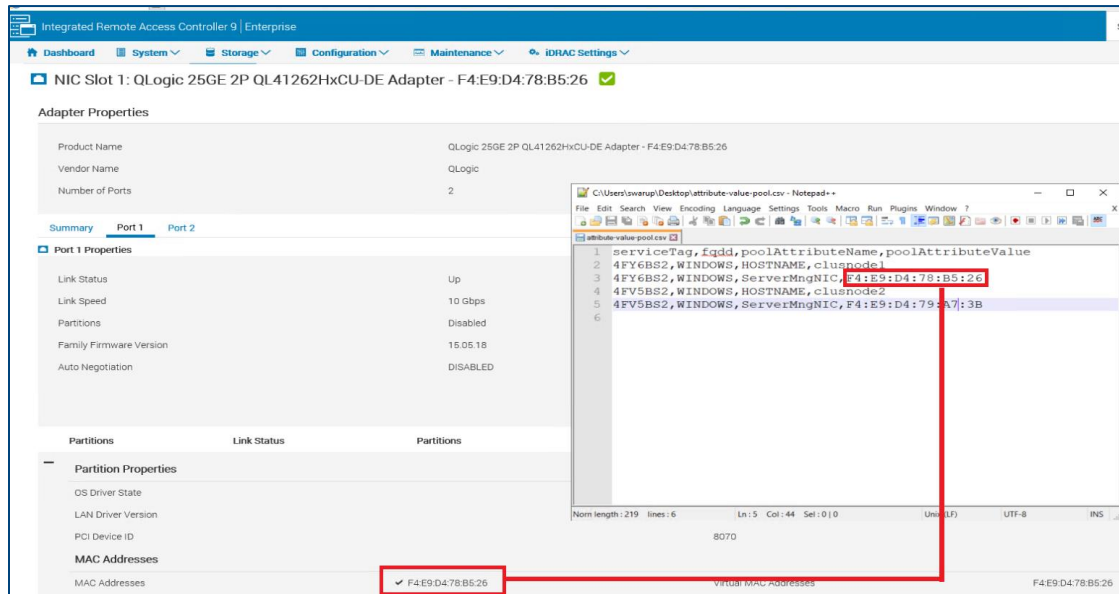
Export Attribute Value Pool

---

**NOTE:** Ensure the CSV file download is not blocked by “Do not save encrypted pages to disk” in the Internet Explorer security settings.

---

- HOSTNAME: This will be the Windows hostname of deployed node of the specific **serviceTag**.
- ServerMngNIC: Populate the MAC ID of the network port which is physical configured with network switch that can communicate with SCVMM.



#### Populate Attribute Value Pool csv file

4. Click **Browse** against **Attribute Value Pool** and Import the created CSV file with system specific values.
5. Configure **Cluster Name** and **Cluster IP Address**.
6. Provide a **Job Name** to track the progress of deployment task.
7. Click **Create** to submit the deployment task.

## Create Cluster ✕

---

Using this page, you can update firmware, configure hardware, and deploy or redeploy operating system using predefined operational templates. Deploying the template creates clusters with the required network configurations to enable Windows Server HCI feature on that cluster.

Cluster Name

IP Address

Logical Switch

Operational Template

Export Attribute Value Pool

<input checked="" type="checkbox"/> Server Identifier	iDRAC IP	Model
<input checked="" type="checkbox"/> 28MR9P2	192.168.20.10	AX-640
<input checked="" type="checkbox"/> 28M0BP2	192.168.20.21	AX-640

Attribute Value Pool

Browse

---

### Job Options

Assign a name to the job as a unique identifier to track this task. Select option to view the Jobs list and monitor the progress of this task.

Job Name

Go to the Job List

Create
Cancel

Input Attribute Value Pool csv file and Create Cluster

## 4.5 Viewing deployed Cluster

To view the deployed Cluster:

1. In the **Configuration and Deployment** page, in the left pane navigate to **Cluster View**
2. View the clusters list under classification by Cluster Name.
3. Select Cluster Name to view the cluster node details.
  - You could also extend the management of these cluster nodes by launching iDRAC from the **iDRAC IP** column.

The screenshot shows the Dell EMC OpenManage console interface. The top navigation bar includes the Dell EMC logo and the text "OpenManage Integration for Microsoft System Center". The left sidebar contains a navigation menu with the following items: Home, Profiles and Templates, Configuration and Deployment (expanded), Server View, Modular Systems View, Cluster View (highlighted with a red arrow), HCI, Hyper-V, Maintenance Center, WinPE Update, and Jobs and Logs Center. The main content area is titled "Cluster View" and contains the instruction: "View the details of all discovered server clusters, and create Windows Server HCI clusters by creating a logical switch in SCVMM through OMIMSSC." Below this instruction are three buttons: "Create", "Create Logical Switch", and "Refresh". A table displays the discovered clusters with the following data:

Cluster FQDN	Servers discovered	Cluster Type
ax-640cluster.hcidomain.com	3	Windows Server HCI

Below the table, it indicates "1 Item(s) Found. Displaying 1-1".

Deployed cluster in Cluster View

## Technical support and resources

[Dell.com/support](https://dell.com/support) is focused on meeting customer needs with proven services and support.

## Related resources

[Dell EMC OpenManage Integration Version 7.3 for Microsoft Endpoint Configuration Manager \(MECM\) and Microsoft System Center Virtual Machine Manager \(SCVMM\) Downloads page](#)

[Dell EMC OpenManage Integration Version 7.3 for Microsoft Endpoint Configuration Manager \(MECM\) and Microsoft System Center Virtual Machine Manager \(SCVMM\) User Manuals](#)

[Dell EMC Solutions for Microsoft Azure Stack HCI documentation](#)

## Terms and Definitions

Terms	Definitions
OMIMSSC	Dell EMC OpenManage Integration for Microsoft System Center Appliance
SCVMM	Microsoft System Center Virtual Machine Manager
RN	Ready Node
iDRAC	Integrated Dell remote access controller
OOB	Out of Band
OSD	Operating System Deployment
OT	Operational Template
Update Source	Referring to Online/Offline update repositories
Windows Server HCI	HCI Solution from Dell EMC supporting Windows Server 2016/2019 Operating System