DELLEMC

Maintaining Hardware Compatibility of vSAN Clusters using Dell EMC OMIVV

Abstract

Dell EMC Open Manage Integration for VMware vCenter (OMIVV) supports driver and firmware updates of vSAN clusters. This technical white paper illustrates how OMIVV can be used to manage vSAN clusters.

November 2020

DELLEMC

Revisions

Date	Description
November 2020	Initial release

Acknowledgments

This paper was produced by the following:

Authors:

Kunal Anand – Test Engineer 2, Servers, and Infrastructure Solutions

R Chandrasekhar – Software Principal Engineer, Servers, and Infrastructure Solutions

Bhimaraju Vadde – Software Principal Engineer, Servers, and Infrastructure Solutions

Winston Fernandes – Software Principal Engineer, Servers, and Infrastructure Solutions

Support: Swapna M, Technical Content Developer 2, Information Development

Contents

Terminology

Terminology	Description
OMIVV	OpenManage Integration for VMware vCenter
iDRAC	Integrated Dell Remote Access Controller
HSM	Hardware Support Manager
HSP	Hardware Support Package
vSAN	Virtual Storage Area Network
OS	Operating System
HCL	Hardware Compatibility List
OOB	Out-of-band
CIFS	Common Internet File System
NFS	Network File System
BIOS	Basic Input/output System
FC	Fiber Channel
DRM	Dell EMC Repository Manager
RAID	Redundant Array of Independent Disks
NIC	Network Interface Controller
HCG	Hardware Compatibility Guide
OEM	Original Equipment Manufacturer

Executive summary

OpenManage Integration for VMware vCenter (OMIVV) is designed to streamline the management processes in a data center environment by allowing to use VMware vCenter server to manage full server infrastructure includes both virtual and physical.

OMIVV also enables you to set the baselines (desired state) for server configuration, firmware, and driver levels with cluster- aware updates for vSphere and vSAN clusters.

This technical white paper is intended to explain the detailed steps involved in creating custom firmware and driver repository profiles through VMware Compatibility Guide (VCG) and Dell EMC Repository Manager (DRM), attach the created firmware and driver repository to a vSAN cluster, compute the drift, and perform firmware remediation through OMIVV.

This technical white paper describes standard OMIVV workflows. For more information about how OMIVV works with vSphere Lifecycle Manager in vCenter 7.0 and later, see Dell EMC OMIVV as a Hardware Support Manager for VMware vSphere Lifecycle Manager.

1 Introduction

vSAN is an enterprise-class, storage virtualization software that allows you to manage compute and storage with a single platform when combined with vSphere. With vSAN, you can reduce the cost and complexity of traditional storage and take the easiest path to hyper-converged infrastructure and hybrid cloud.

Dell EMC vSAN Ready Nodes are jointly tested and certified solutions that takes away your effort to build the solutions. Based on trusted and proven PowerEdge servers, Dell EMC vSAN Ready Nodes offer powerful processors, high core counts, maximum memory densities, lots of fast internal storage, and innovative modular Network Interface Card (NIC) technology.

You will also get benefit from the simplicity of having a single trusted source for the entire solution—which can be installed, implemented, and supported globally by Dell EMC.

You can also build vSAN solutions using the supported components as listed in the VMware Compatibility Guide (VCG). There are wide range of options for selecting a host model, storage controller, flash devices, and magnetic disks.

It is extremely important that you follow the VCG to select these hardware components. This online tool is regularly updated to ensure that you always have the latest guidance from VMware based on hardware vendor certifications.

1.1 Importance of compliance baselines for vSAN

OMIVV provides capability of creating cluster profiles which enables you to set baselines to track against managed servers across server configuration, firmware, or driver levels to maintain corporate or support compliance levels of mentioned vSAN clusters.

Before you begin the compliance and drift detection in the vSAN clusters, ensure that you have the following in your environment:

- System profile (which determines the physical server configuration)
- Repository profile for both firmware and drivers
- Homogenous server models within the cluster
- vSAN service is enabled for the cluster
- Create a host credential profile for at least one host in the vSAN cluster where inventory is running successfully.

1.2 Hardware compatibility for vSAN clusters

VMware Compatibility Guide (VCG) is a repository maintained by VMware where specific supported benchmarks for firmware and driver support on vSphere and vSAN components are shown using certification testing and Original Equipment Manufacturer (OEM) submissions.

For instance, it makes specific recommendation for storage I/O controllers, Solid State Drives (SSDs), PCIe flash cards, NVMe storage devices, and disk drives. It also specifies which drivers have been fully tested with vSAN, and in many cases – identifies minimum levels of firmware required.

The minimum supported version is specified for BIOS, NICs, and SSDs. The exact supported version is specified for storage I/O Controllers and NVMe drives. For a vSAN cluster, ensure that the storage components

have the recommended combination of firmware and driver versions maintained for the version of vSAN on the cluster.

OMIVV can help you to update and maintain vSAN solution up to date with VMware recommended firmware and driver.

To use OMIVV as a solution for vSAN firmware and driver update, you should know how to create firmware and driver repository that is compatible with VCG.

2 Custom repositories

2.1 Create custom firmware repository using Dell EMC Repository Manager (DRM)

Ensure that you have installed following in your environment:

- Dell EMC Repository Manager (DRM). For more information, see [Dell EMC Repository Manager](#).
- OMIVV is installed and configured. For more information, see [OMIVV 5.2 Install Guide](#).

1. Launch [VMware Compatibility Guide](#).
2. In the **Supported Releases** section, select an ESXi version as installed in your vSAN solution,
3. In the **Brand Name** section, select brand name as **DELL**.
4. In the **Device Type** section, select device type for the component.
5. Click **Update and View Results**.

The result is displayed as shown in the screenshot below.

6. Click the component for which you want to download firmware or drivers. For example, the PERC H730P Mini Adapter is selected in the following screenshot.
    After selecting the component, you will be redirected to the page (as shown in screenshot) where you can see the list of driver and firmware version which are compatible with each other.

7. Once you have the firmware and driver compatible version, download the firmware from Dell support web site and drivers from VMware Web site.
8. To download firmware, go to **https://www.dell.com/support/**, in the **Search Support** section, search for PowerEdge servers. You can use Service Tag or server model name. You can also use the **Browse all products** option to navigate to the server page.
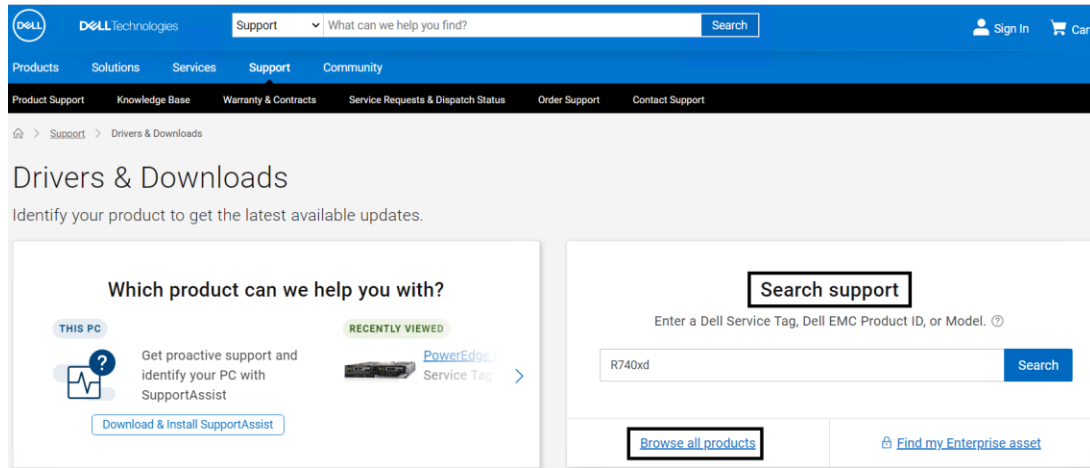
9. Search for the component as shown in the following screenshot. If you do not see the firmware as latest, click the older version to see the list of all firmware.

After you have downloaded the firmware, integrate firmware to your existing catalog or repository share. To get the firmware components that are not present in VCG, use the latest online catalog (http://downloads.dell.com/catalog/Catalog.gz).

10. To integrate the firmware to existing catalog or repository share, import the firmware in DRM and create a new repository using the export option.
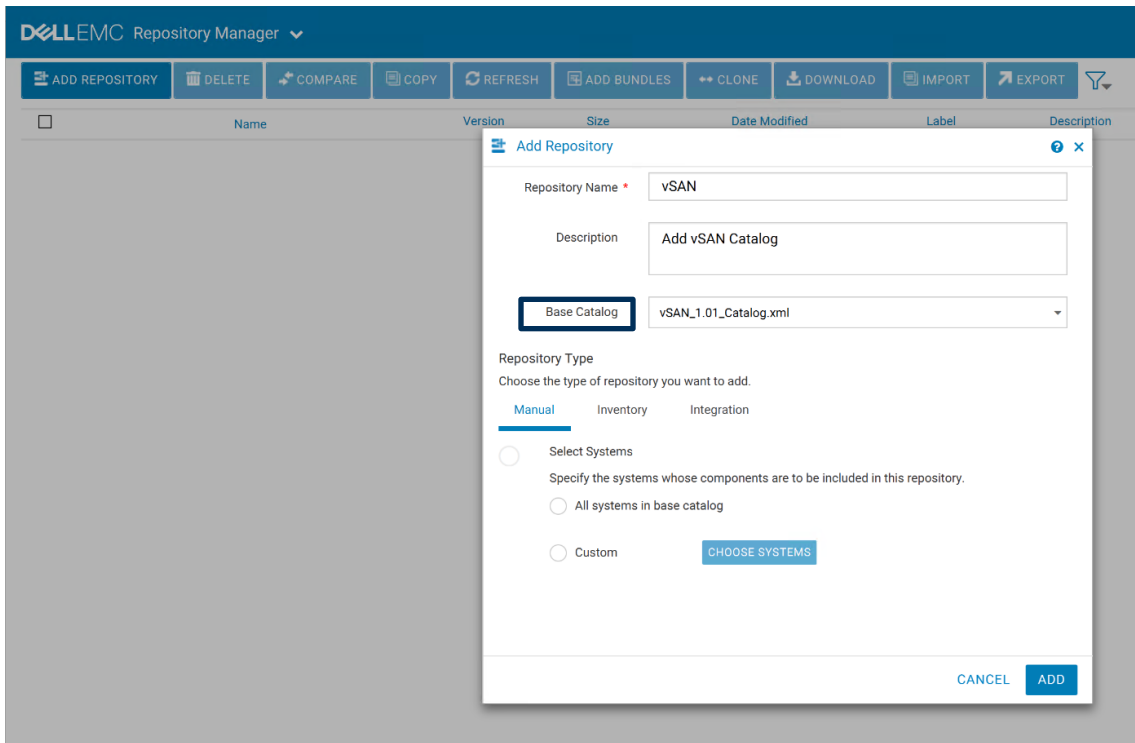
For example, if you already have a repository share for vSAN solution as shown in the following screenshot, integrate the downloaded firmware to it.
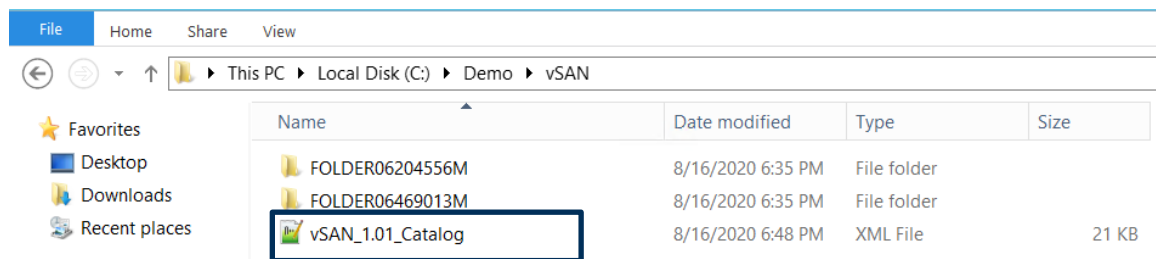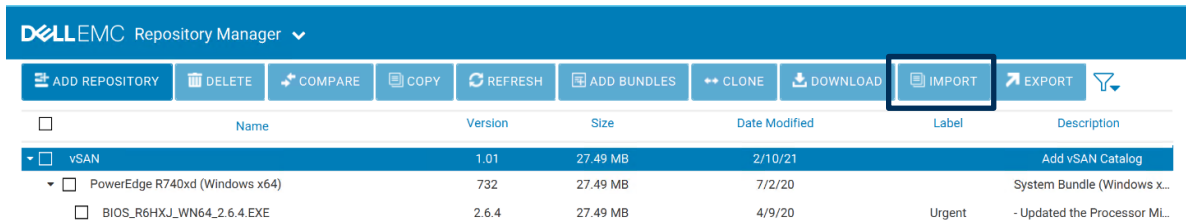

a) Launch Dell EMC Repository Manager (DRM).
b) To import above catalog to DRM, click **Add Repository**.
c) From the **Base Catalog** drop-down menu, select **Choose File**, and then select the catalog.
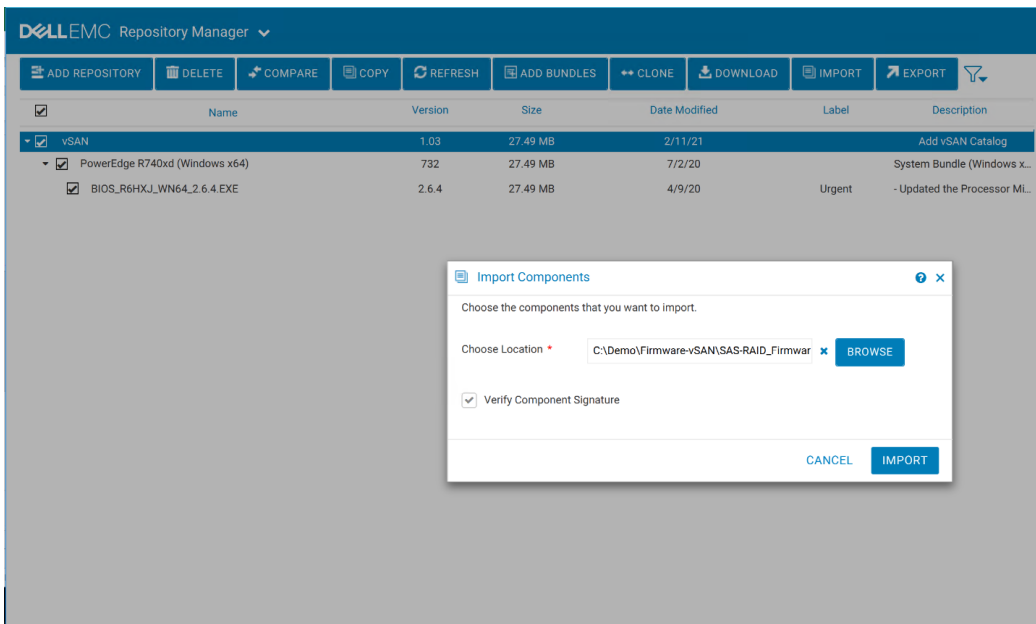
After the catalog is successfully imported, you will see the imported catalog as shown in the following screenshot.

d. To select the downloaded firmware, click **IMPORT**.

e. Once you have selected the firmware, to import the firmware in existing catalog, click **OPEN**, and then click **IMPORT** (as shown in the following screenshots).
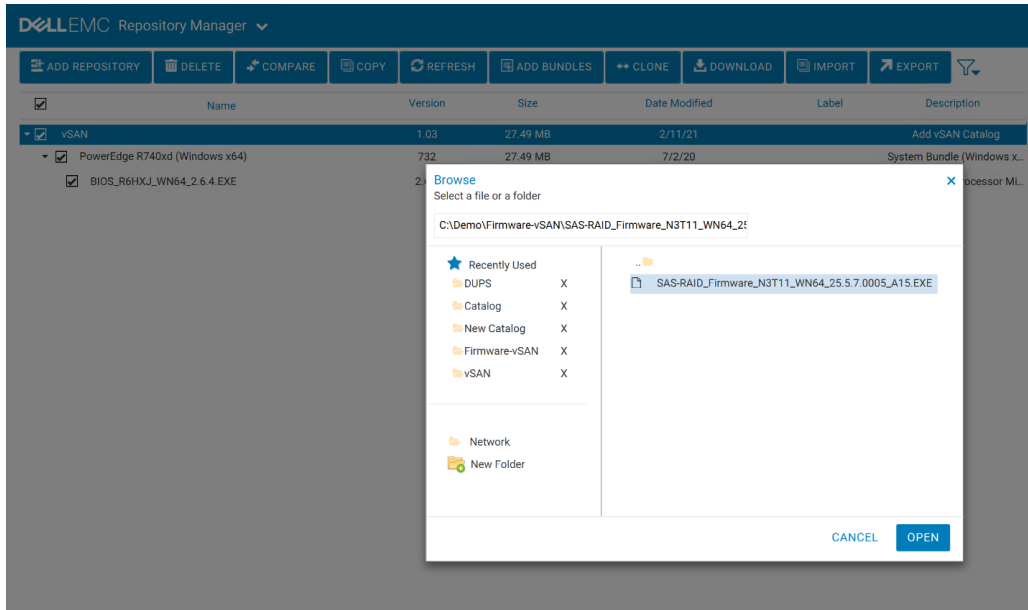
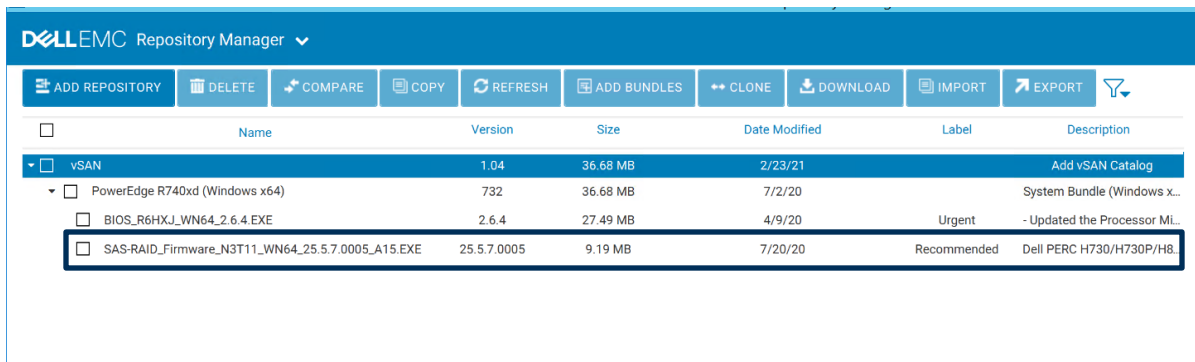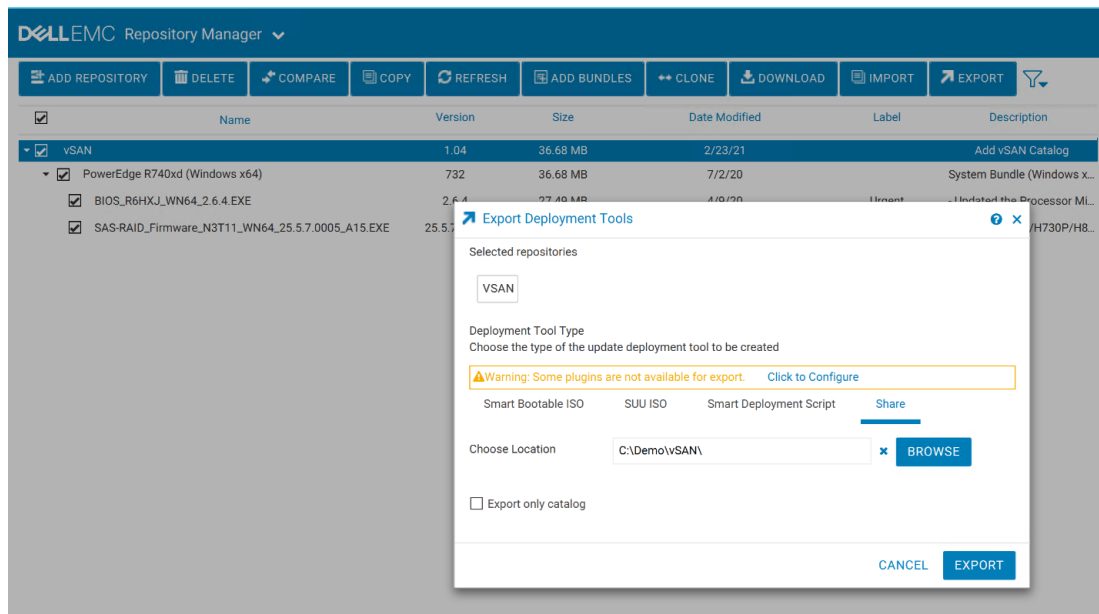After the firmware is successfully imported, you can see the imported firmware in the list as shown in the following screenshot.

f. Select the repository to export the new catalog along with firmware to the same location or new location.
g. Click **EXPORT**, and then click **BROWSE** to select the location.

h. After the job is successfully completed, the new catalog created at same location (if you have used the existing location) along with the firmware as below.
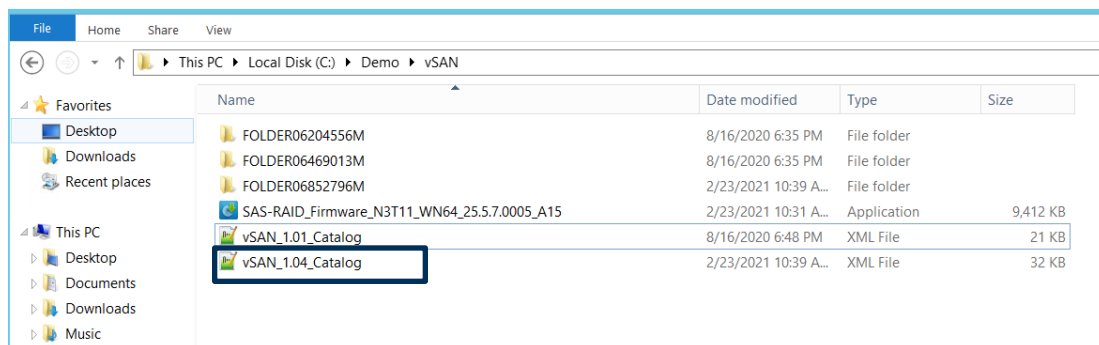
After the new repository is created you need to create firmware repository profile in OMIVV. OMIVV supports CIFS, NFS, and HTTPS share as firmware repository. For more information about creating the firmware repository, see create repository profile.

2.2　Create custom driver repository

1. Launch VMware Compatibility Guide.

2. To search the compatible driver and firmware, complete the steps 1–8 listed in the Create custom firmware repository using Dell Repository Manager (DRM) section.

3. After the list of compatible drivers and firmware is listed, expand the + button and it will have the link to that driver.

4. To go to the driver download page, click the link.
5. To download the driver, click **DOWNLOAD NOW**.

6. Once the driver is downloaded, you need to extract the zip file.
7. Copy the zip file which is the offline bundle to any share.

Once you have the offline bundle in share you need to create a repository profile of type driver in OMIVV. OMIVV supports CIFS and NFS share as driver repository. For more information about creating driver repository, see create repository profile.

3   Manage firmware and driver repositories using repository profile

3.1   Repository Profile

A repository profile enables you to create and manage driver or firmware repositories. The driver profile is used to update the drivers and the firmware profile is used to update firmware for the vSAN cluster.

These profiles can also be associated to Cluster Profile and the profile created is used to baseline the vSAN Cluster. While creating firmware and driver repository profiles, there is a step to provide driver and firmware share. The firmware and driver shares created in the earlier sections will be provided during firmware and driver profile creation.

The default OMIVV firmware catalogs are Dell EMC Default Catalog and Validated MX Stack Catalog. These cannot be used to update or baseline vSAN clusters.

3.1.1   Create repository profile

1. On the OMIVV home page, click **Compliance & Deployment** > **Profiles** > **Repository Profile**.
2. Click **CREATE NEW PROFILE** or **EDIT**.
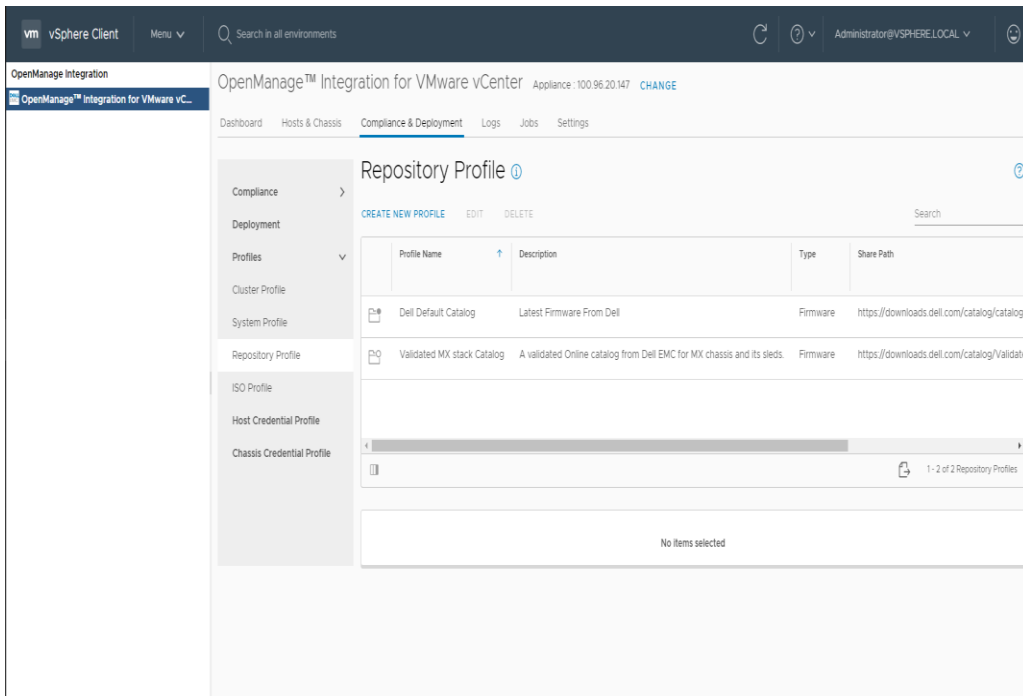
3. On the **Repository Profile** page, read the instructions, and then click **GET STARTED**.
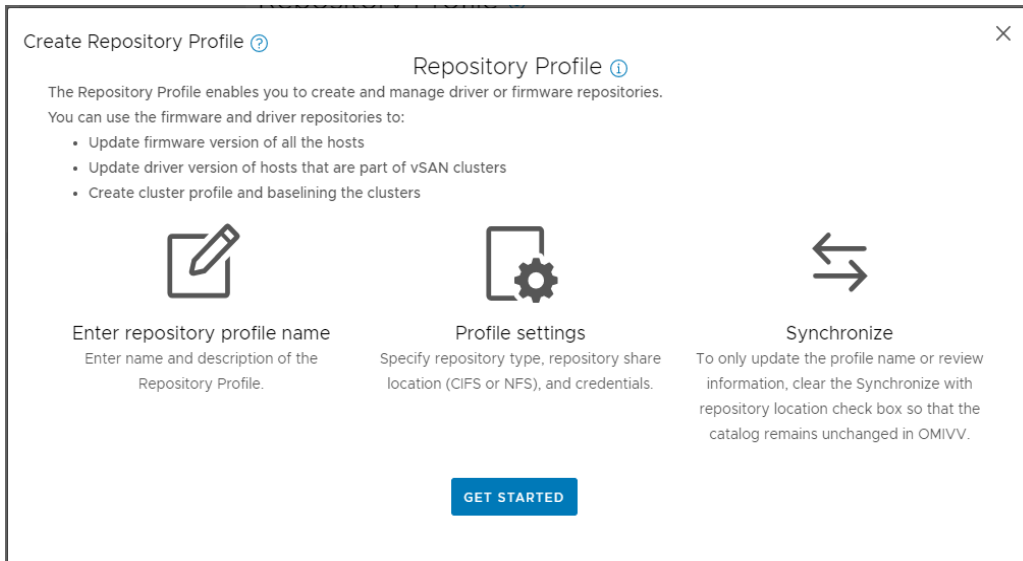
4. On the **Profile Name and Description** page, enter profile name and description. The description field is optional and limited to 255 characters.
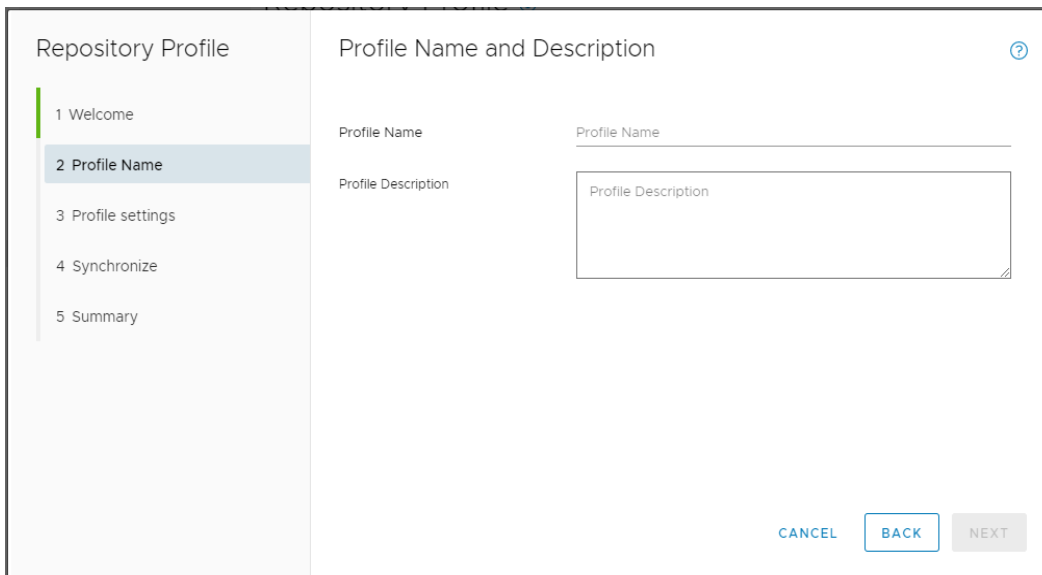
5. Click **NEXT**.

The **Profile Settings** page is displayed.

6. On the **Profile Settings** page, select **Firmware** or **Driver**.

   The following are applicable for driver repository profile:

   - Driver repository profile can have a maximum of 10 drivers. If more than 10 drivers are present, OMIVV randomly selects 10 drivers while creating driver repository profile.
   - Only offline driver bundles (.zip files) are used.
   - Download and extract the offline driver bundles (.zip files) and save to the shared location by providing the full path of the shared location. OMIVV automatically creates the catalog inside the OMIVV appliance. Driver bundles are available at https://my.vmware.com/web/vmware/downloads.
   - OMIVV requires write access to the CIFS or NFS.
   - Files within the subfolders are ignored.
   - Files exceeding 10-MB sizes are ignored.
   - Driver repository is applicable only for vSAN clusters.

7. In the **Repository Share Location** area, perform the following tasks:

   a. Enter the repository share location (NFS or CIFS).
   b. For CIFS, enter the credentials.

   OMIVV supports only Server Message Block (SMB) version 1.0 and SMB version 2.0 based CIFS shares.

NOTE: For SMB 1.0 share used for driver repository, add the file separator at the end of the directory path.

To validate the catalog path and credentials, click **BEGIN TEST**.

To continue creating a repository profile, you must complete this validation process.

The test connection results are displayed.

8. Click **NEXT**.

   The **Synchronize with repository location** page is displayed.

9. Click **NEXT**.

   The **Summary** page is displayed that provides the information about the repository profile.
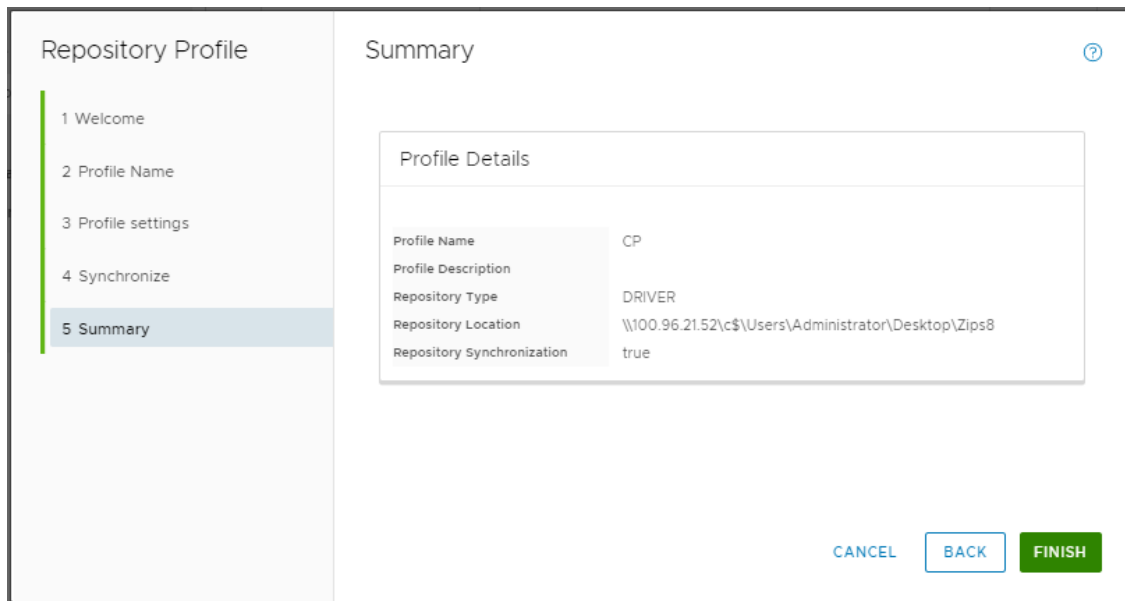
10. Click **FINISH**.

    After creating the catalog, it downloads, parses, and the status is displayed on the home page of the repository profile.

    Successfully parsed repository profiles are available during the cluster profile creation and during the firmware update.

4 Create Cluster Profile

OMIVV allows you to maintain single image that comprises of firmware and driver repositories. You can maintain the same firmware and driver versions across the cluster.

This can be achieved by creating cluster profile in OMIVV and associating the cluster profile with firmware repository and/or driver repository.

The cluster profile will not refresh itself when the source repository changes. To identify the updated profiles that are associated with cluster profile, go to the Cluster Profiles page. Yellow warning icon will be displayed next to the updated cluster profile.

To update the cluster profile with the latest available driver or firmware, select the impacted cluster profile, click **Update Profiles** on the **Cluster Profile** page. For more information, see OMIVV 5.2 User's guide.

5 Drift view for the cluster

When Cluster profile is created and associated to specific cluster, OMIVV shows the deviation of each hosts in that cluster to the firmware and driver repository versions present in the cluster profile. In this way, you can view the holistic view of hosts and get the drift of both firmware and driver versions of host compared to the versions present in cluster profile.

When a new host is added to a cluster after the cluster profile is created (and added to host credential profile in OMIVV), the host automatically gets added to the list of hosts for the drift detection process during the next scheduled run of the drift detection job. For more information, see OMIVV 5.2 User's guide.

6 Remediation of cluster (firmware and/or drivers)

Remediation of firmware and driver drifts can be achieved by using the firmware update functionality which is available as cluster action.

Right-click cluster and select **OMIVV firmware update action**. While updating the cluster, you must choose the suitable firmware or driver repositories that are created for the selected cluster (which is selected by you for an update action).

Once the cluster-aware update is triggered, if the host requires reboot, OMIVV puts hosts in maintenance mode. For more information about vSAN cluster firmware update, see OMIVV 5.2 User's Guide.

7 Common issues when using OMIVV to create repository profiles

Issue: The creation of Driver Profile fails with an error message

Category	Date and Time	Description
⊘ Error	08/16/2020 03:53:04 PM (GMT+05:30)	Unable to create the driver catalog for repository profile CP with id 1008. Provide a repository path that has valid offline driver bundle(s) (or) components.
⊘ Error	08/16/2020 03:53:04 PM (GMT+05:30)	Unable to parse the driver file(s) for repository profile CP with id 1008. Provide a repository path that has valid offline driver bundle(s) (or) components.
ⓘ Info	08/16/2020 03:53:04 PM (GMT+05:30)	Successfully downloaded 2 file(s) for repository profile CP with id 1008.
ⓘ Info	08/16/2020 03:53:01 PM (GMT+05:30)	Repository profile CP with id 1008 is created or updated successfully.

Resolution: Check the offline bundle in the location. For more information, see [Create repository profile](#).

The zip folder obtained from the VCG needs to be extracted to get the offline bundle.

8 Conclusion

It is very important for the components of the vSAN cluster to be compliant with VMware Compatibility Guide (VCG) for vSAN. OMIVV has been offering an ability to baseline clusters in the vCenter against drivers, firmware and configuration drift, and provides an ability to report the drift with periodical checks and allows you to remediate the firmware drift against the baseline. Using these functionalities, the you can make sure the components are compliant with VCG for vSAN by performing cluster-aware update.

9 Technical Support and Resources

Dell.com/support

OMIVV product page

OMIVV Documentation page