# OpenManage Integration for VMware vCenter Version 5.2.1

Release Notes

January 2021
Rev. A01

## Notes, cautions, and warnings

**NOTE:** A NOTE indicates important information that helps you make better use of your product.

**CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

**WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

# Contents

**Chapter 1: Release summary....4**
Priority and recommendations....4

**Chapter 2: Compatibility....5**
Supported devices and platforms....5
Supported operating system....5
Supported web browsers....5
Supported software....5

**Chapter 3: New and enhanced features....6**

**Chapter 4: Fixes....7**

**Chapter 5: Important notes....8**

**Chapter 6: Known issues....9**

**Chapter 7: Features and fixes in previous releases....16**

**Chapter 8: Limitations....18**

**Chapter 9: Instructions for installing....19**
Downloading the software package....19
Installation prerequisites....19
Installation process....19
Upgrade prerequisites....19
Upgrade process....19

**Chapter 10: Contacting Dell EMC....20**

# 1

# Release summary

The OMIVV 5.2.1 is a defect fix Release. For more information, see Fixes on page 7.

**NOTE:** The OpenManage Integration for VMware vCenter (OMIVV) 5.2.1 is an RPM only release.

## Version

5.2.1

## Release date

January 2021

# Priority and recommendations

Urgent: Dell EMC highly recommends updating your OMIVV instance to version 5.3.1 available at https://www.dell.com/support. This update contains enhancements to keep OMIVV compatible with the latest system software like BIOS, firmware, and drivers for different system modules.

**NOTE:** If you have installed OMIVV 5.2 or earlier versions, it is recommended that you update OMIVV to 5.2.1 or 5.3, and then perform update to the latest version.

To update OMIVV 5.2 or earlier versions to 5.2.1, use the https://linux.dell.com/repo/hardware/vcenter-plugin-x64/5.2/5.2.1.2352/ repository path.

# 2

# Compatibility

## Supported devices and platforms

For more information about supported devices and platforms, see the **Hardware Requirements** section in the *OpenManage Integration for VMware vCenter Version 5.2 Installation Guide*.

## Supported operating system

### ESXi version support

- v6.0 U3
- v6.5, v6.5 U1, v6.5 U2, v6.5 U3
- v6.7, 6.7 U1, v6.7 U2, v6.7 U3
- v7.0, v7.0 U1

### vCenter version support

- v6.5 U2, v6.5 U3
- v6.7, v6.7 U1, v6.7 U2, v6.7 U3
- v7.0, v7.0 U1

**NOTE:** Use the latest patch build 13638625 or later for vCenter 6.5 U2.

## Supported web browsers

- Google Chrome
- Mozilla Firefox

## Supported software

For more information about supported software, see the **Software Requirements** section in *OpenManage Integration for VMware vCenter Version 5.2 Installation Guide*.

# 3

# New and enhanced features

The OMIVV 5.2.1 is a defect fix Release. For more information, see Fixes on page 7.

# 4

# Fixes

This release provides fixes for the following issues:

- 185589 and 186588—OMIVV displays 200002 error indicating the SSL certificate is not valid or InaccessibleWSDLException when:
  - The other client plugins (such as Stormagic, Emulex, HCX plugins) are installed at vCenter
  - The vROPS client plugin is removed from vCenter
- 186218— The Subject Alternate Name (SAN) mentioned while generating the Certificate Signing Request (CSR) is not displayed in the generated CSR.

# 5

# Important notes

1. The following are the important items to note before upgrading to OMIVV 5.2.1:
   a. From OMIVV 5.0 onwards, only VMware vSphere Client (HTML5) is supported and the vSphere Web Client (FLEX) is not supported.
   b. 11G servers are not supported. Only the 12G and later generations servers are retained after restore.
   c. Hardware profiles and deployment templates are not supported. System profiles now have two types, where Basic is intended to replace the same settings that were captured in the Hardware Profile. For deployment, the deployment process asks what system profiles (configuration) and ISO repository (hypervisor image) you want to use for the deployment.
2. For using the DNS server, the recommended practices are:
   a. OMIVV supports only IPv4 IP addresses. Although both static IP assignment and DHCP assignment are supported, Dell recommends you to assign a static IP address. Assign a static IP address and hostname when you deploy an OMIVV appliance with a valid DNS registration. A static IP address ensures that during the system restart, the IP address of the OMIVV appliance remains same.
   b. Ensure that OMIVV hostname entries are present in both forward and reverse lookup zones in your DNS server.
3. For the OMIVV appliance mode, ensure that you deploy OMIVV in the appropriate mode based on your virtualization environment. For more information, see the **System requirements for deployment modes** topic in *OpenManage Integration for VMware vCenter Version 5.2 Installation Guide*.
4. Configure your network to match the port requirements. For more information, see the **Port information** topic in *OpenManage Integration for VMware vCenter Version 5.2 Installation Guide*.
5. When restoring the OMIVV data, ensure that you end all the vCenter sessions.

# 6

# Known issues

- **Issue 1**: iDRAC might not send an event when your system reboots.

  Description: Sometimes, the iDRAC might not send an event when your system reboots. In this case, OMIVV sends latest health update notification by polling mechanism and you receive the latest health update within an hour.

  Version affected: 4.0 and later

- **Issue 2**: iDRAC license type and description are displayed incorrectly for non-compliant vSphere hosts.

  Description: If a host is noncomplaint when CSIOR is disabled or has not been run, the iDRAC license information is displayed incorrectly although valid iDRAC license is available. Hence, you can view the host in vSphere hosts list, but when you click the host for details, the information in **iDRAC License Type** is displayed as empty and **iDRAC License Description** is displayed as "Your license needs to be upgraded."

  Version affected: 4.0 and later

  Resolution: Perform any of the following:

  1. Fix CSIOR compliance and run the inventory.
  2. Log in to iDRAC to get the license information.

- **Issue 3**: Although deployment job fails due to inaccessible file share, the status is displayed as “Cancel.”

  Description: When you create an ISO profile with invalid credentials such as invalid credentials for CIFS share, and select the same ISO profile for deployment, the deployment task fails. However, the status displayed in the **Jobs** page as **Cancel** instead of **Failed**.

  Version affected: 3.0 and later

  Resolution: None

- **Issue 4**: Dell EMC icon is not displayed after unregistering vCenter from an earlier OMIVV version and then registering same vCenter with a later OMIVV version.

  Description: If you unregister an earlier OMIVV version with vCenter server, and then register a later OMIVV version with the same vCenter server, there is an entry in the vSphere-client-serenity folder, which is old data from the earlier OMIVV version. Hence, the Dell EMC icon is not displayed after registering the later OMIVV version as old data specific to the earlier OMIVV version exists in the vSphere-client-serenity folder of the vCenter appliance.

  Version affected: All

  Resolution: Perform the following steps:

  1. Restart vSphere Client on the vCenter server.
  2. If the issue persists:
     - For VMware vCenter, go to `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity` and for Windows vCenter, go to `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` folder in the vCenter appliance and see if the old data exists, such as: com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.xxx.
     - Manually deleted the folder corresponding to the earlier OMIVV version
     - Restart vSphere Client services for vSphere Client (HTML-5).

- **Issue 5**: The **OpenManage Integration** icon is not displayed after backup and restore from an earlier OMIVV version to a later OMIVV version.

  Description: The OpenManage Integration icon is not displayed after restoring an earlier OMIVV version appliance database to a later OMIVV version appliance.

  Version affected: 3.0 and later

  Resolution: The IP address of the OMIVV version appliance must be the same as the earlier OMIVV version appliance for the plug-in to work correctly after restore.

- **Issue 6**: Storage overview returning incorrect number of hard drives for inventory

  Description: Systems with software RAID show incorrect number of hard drives on the storage overview page.

Version affected: All

Resolution: None. The ESXi does not support software RAID. If the system has software RAID, it shows incorrect disks.

- **Issue 7**: System Event Logs are not showing in OpenManage Integration for VMware vCenter when power supply redundancy is lost.

  Description: When the power redundancy is lost on the PowerEdge modular servers, the system logs get cleared.

  Version affected: 3.0 and later

  Resolution: None

- **Issue 8**: Chassis and server health is displayed as warning on the **Chassis Summary** page when server becomes critical.

  Description: When a critical entry is made to SEL logs, the health of the server (modular) changes to critical. This is correctly reflected on the **Host Summary** page. However, this is not reflected on the **Chassis Summary** page. The server health is displayed as warning. If the chassis was normal earlier, the health of the chassis also changes to warning.

  Version affected: 3.0 and later

  Resolution: None. This is a known defect in the RACADM. The defect will be fixed in the next release of RACADM for chassis.

- **Issue 9**: The hard drive name is not displayed at data center and cluster level inventory in some situations.

  Description: Although the hard drive name is displayed when you view the inventory at the host level, the hard drive name is displayed empty when you view the inventory of the host at the data center and cluster level.

  Version affected: 3.0 and later

  Resolution: This issue does not affect the functionality of the features, and you can view the inventory at the host level to see the hard drive name.

- **Issue 10**: Hard disk option is not disabled in the Deployment wizard for all the servers that do not contain hard disk drives.

  Description: While navigating through the Deployment wizard, if the bare-metal servers do not have any hard disk drive, and then the hard disk option should be disabled on the **Select Deployment Options** page. However, the option is available for selection.

  Version affected: 2.0 and later

  Resolution/Workaround: None

- **Issue 11**: Using OpenManage Integration to update an Intel Network card with the firmware version of 13.5.2 is not supported.

  Description: There is a known issue with Dell EMC PowerEdge 12th generation servers and some Intel network cards with the firmware version of 13.5.2. Updating some models of the Intel network cards at this version of firmware fails when the firmware update is applied using the iDRAC with Lifecycle Controller.

  Version affected: All

  Resolution: Update the network driver software using an operating system. If the Intel network card has a version of firmware other than 13.5.2, you can update using OpenManage Integration.

  **NOTE:** When using the one-to-many firmware update, avoid selecting Intel network interface controllers that are at version 13.5.2, as this fails and stops the update task from updating remaining servers.

- **Issue 12**: Firmware upgrade or downgrade of Broadcom NetXtreme II 10-Gigabit Ethernet adapter (BCM57712) from firmware version of 6.2.x or earlier is not supported.

  Description: Using the OpenManage Integration to upgrade a Broadcom NetXtreme II 10-Gigabit Ethernet adapter (BCM57712) from firmware version of 6.2.x or earlier, or downgrade to a firmware version of 6.2.x or earlier is not supported.

  Version affected: All

  Resolution: There is a known issue with the Broadcom NetXtreme II 10-Gigabit Ethernet adapter (BCM57712) where updating the adapter from firmware version of 6.2.x or earlier, or downgrade to a firmware version of 6.2.x or earlier fails when the update is applied using the iDRAC with Lifecycle Controller.

  When attempting to perform this update using the OpenManage Integration, the update may incorrectly show that it completed successfully. However, the firmware update has failed and remains at the previous level. One way to successfully update the adapter software for the Broadcom NetXtreme II 10-Gigabit Ethernet adapter (BCM57712) is to update the adapter firmware from an operating system.

- **Issue 13**: Associated host credential profile is not displayed on the management compliance page when inventory is not able to get iDRAC IP for the host.

  Description: If the iDRAC IP is not retrieved because of nonresponsive iDRAC, the inventory fails and host to be associated with the host credential profile is not displayed on the management compliance page.

  Version affected: 1.6 and later

  Resolution: Reset the iDRAC to fix the issue of iDRAC not being responsive, and then rerun the inventory. If the inventory can get the iDRAC IP, then the host is associated with the correct host credential profile.

- **Issue 14**: Unable to boot to service partition while deploying OS ISO.

  **Description**: OS deployment is failing on 12th generation PowerEdge servers with the following error on the screen during POST: "Warning: Unable to boot to Service Partition." There is a BIOS issue to identify the network ISO when there is a local USB CD-ROM installed on the system and that USB CD- ROM is the only USB mass storage device plugged into the system.

  Version affected: 1.5.1 and later

  Resolution: Remove the local USB CD-ROM (not all local CD-ROM would expose this issue), or plug in extra USB floppy or USB drive on the system, or attach the virtual media (virtual floppy and virtual CD) from the iDRAC.

- **Issue 15**: A firmware update fails with an error message saying that USC is in use and it must be retried after 30 seconds.

  Description: During a firmware update, the update fails with the error message: If USC is in use, wait until USC has exited and retry the action. Otherwise retry after 30 seconds to check if network connectivity caused this error.

  Version affected:1.5.1 and later

  Resolution: To fix this issue, reset iDRAC and wait until iDRAC boots properly and try the firmware update again.

- **Issue 16**: Events from different vCenter are posted to another vCenter from a shared OMIVV appliance.

  Description: This situation can occur when a bare-metal server that was deployed in one vCenter is rediscovered again as bare-metal server but then selected for an OS deployed in another vCenter. This situation occurs if the host that was already on one of the registered vCenter was added to another registered vCenter. In this case, the host on first vCenter opens as disconnected.

  Version affected: All

  Resolution: Remove the host from the first vCenter where it is now showing as disconnected.

- **Issue 17**: OS installation fails.

  Description: OS installation fails with the error message: **Mount network share failed – incorrect IP address or share name**.

  Version affected: 1.5 and later

  Resolution: Restart the appliance.

- **Issue 18**: Health status is showing Warning for chassis when one or more power supplies are critical.

  Description: The overall health information is displayed warning on summary page for VRTX chassis that has power supply in critical state.

  Version affected: All

  Resolution: Each power supply status is shown correctly as critical.

- **Issue 19**: Health status is showing as Healthy for chassis while Storage status is Warning.

  Description: The overall health information is displayed Healthy on summary page for VRTX chassis that has a storage component as Warning.

  Version affected: VRTX firmware version 2.0

  Resolution: Each power supply unit health status correctly shown as critical at OMIVV.

- **Issue 20**: Blower information is showing as N/A for a chassis when a Blower is removed.

  Description: Blower inventory information is displayed as N/A on the **Hardware** page for VRTX chassis when a Blower is removed from a slot.

  Version affected: 2.0 and later

  Resolution: You can see the correct status in the CMC console.

- **Issue 21**: I see a web communication error in the vSphere Client after changing the DNS settings in OpenManage Integration for VMware vCenter.

  Description: If you see any kind of web communication error in the vSphere Client while doing any OMIVV-related tasks after changing the DNS settings, clear the browser cache or log out and log in from the vSphere Client.

  Version affected: 2.x and later

  Resolution: Clear the browser cache or log out and log in from the vSphere Client.

- **Issue 22**: OMIVV RPM Upgrade fails when Proxy is configured with Domain user authentication.

  Description: If OMIVV appliance is configured with proxy to reach the Internet and proxy is authenticated using NTLM authentication, then the RPM update fails due to the issues in the underlying yum tool.

  Version Affected: OMIVV 4.0 and later

  Resolution: Do back up and restore to update the OMIVV appliance.

- **Issue 23**: Unable to apply system profile that has PCIe card in the FX chassis.

  Description: The OS deployment fails on a target server if the source server has PCIe card information when using an FX chassis. The System profiles on the source server have different `fc.chassislot ID` than the one on the target server. OMIVV tries to deploy the same `fc.chassislot ID` on the target server but fails. The System profiles searches for exact instance( FQDD) while applying the profile, which works successfully on rack servers (identical), but may have few restrictions in modular servers. For example, in FC640, the System profiles that are created from one modular server cannot be applied on other modular servers in the same FX chassis because of NIC level restrictions.

  Version Affected: OMIVV 4.1 and later

  Resolution: System profile that is taken from an FC640 server in slot 1 of a FX2s chassis can only be applied on another FC640 server residing in the slot 1 of another FX2s chassis.

- **Issue 24**: The first inventory (immediately after creating a host credential profile) may fail in ESXi 6.5 and later version where the WBEM enablement is necessary.

  Resolution: Trigger the inventory again from Jobs.

- **Issue 25**: After backup and restore from an earlier OMIVV version to a later OMIVV version, the following issues may be observed:
  - The Dell EMC logo is not displayed at vCenter.
  - The 2000000 error
  - The 3001 error

  Resolution:

  - Restart vSphere Web Client on the vCenter server.
  - If the issue persists:
    - For VMware vCenter, go to `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity` and for Windows vCenter, go to `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` folder in the vCenter appliance and see if the old data exists, such as: com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.xxx.
    - Manually deleted the folder corresponding to the earlier OMIVV version

- **Issue 26**: Proactive HA-related features are not functioning as expected after modifying the vCenter credentials.

  Description: If the vCenter credentials are modified by using the OMIVV portal after registering the OMIVV to a vCenter, the Proactive HA-related features will not function as expected.

  Resolution: If you are using the Proactive HA feature along with OMIVV, do not modify the registered user credentials. If the credentials require modification, unregister and register OMIVV appliance to vCenter with new username.

  Version Affected: 4.3 and later

- **Issue 27**: When upgrading or downgrading some iDRAC firmware versions using OMIVV, even when the firmware update is successful, OMIVV may indicate that the job is failed.

  Description: During firmware update, when you downgrade or upgrade the iDRAC versions such as 3.20.20.20, 3.21.21.21, and 3.21.21.22, the job status is indicated as failed even when the job was successfully run.

  Resolution: Refresh the inventory after the job failure and rerun the job for other components.

  Version Affected: 4.3 and later

- **Issue 28**: Configuring the System Lockdown mode at a cluster level sometimes displays a message "No hosts under the cluster has successful inventory."

  Description: Configuring the System Lockdown mode at a cluster level sometimes displays a message "No hosts under the cluster has successful inventory." This message is displayed even when the cluster has successfully inventoried the 14G hosts that are managed by OMIVV.

  Resolution: Reboot the vCenter.

  To reboot the vCenter, do the following:

  1. Log in to the vSphere Client with a vCenter Single Sign-on Administrator account.
  2. Go to **Administration** > **Deployment** > **Deployment** > **System Configuration**.
  3. Click **Nodes**, select the vCenter Server Appliance node, and click the **Related Objects** tab.
  4. Reboot the vCenter node.

  Version Affected: 4.3 and later

- **Issue 29**: Sometimes post RPM upgrade of OMIVV appliance, multiple entries in the logs are seen in vCenter Recent Tasks.

  Description: Sometimes, after RPM upgrade, multiple entries are displayed in logs when viewed on vCenter Recent Tasks.

  Resolution: Restart the vCenter services.

  Version Affected: 4.3 and later

- **Issue 30**: Sometimes, the storage inventory data is not displayed for the host managed using chassis credential profile and present in member chassis.

  Description: The storage data may not be displayed for an MX host managed using the chassis credential profile and for a host present in the member chassis. Though the inventory data of other components is displayed, only the storage-related data is not displayed

  Resolution: Do one of the following:

  1. Update the MX7000 chassis firmware version to 1.00.10.
  2. Manage the host using iDRAC.
  3. Reinstall the host in another slot of the same MX7000 chassis and retry the operation.

  Version Affected: 4.3 and later

- **Issue 31–148132**: For a non-administrator user, inventory fails indicating that the enabling WBEM service is failed on host.

  Resolution: For more information about the required privilege for non-administrator user, see the OMIVV 5.0 User's Guide. Assign the required privilege to user and run the inventory again.

  Version Affected: 5.0

- **Issue 32–147023**: Host firmware update fails, if a canceled firmware update job of related chassis is present.

  If you cancel the firmware update job of a PowerEdge MX chassis, subsequent host firmware update job for hosts present in the same chassis is blocked.

  Resolution: Purge the canceled chassis firmware update job to release the lock on the related hosts.

  Version Affected: 5.0

- **Issue 33–143173**: OMIVV page displays invalid session, or time out exception, or two million errors in Firefox browser.

  If the OMIVV page is idle for some time (5–10 minutes), the invalid session, or time out exception, or two million errors is displayed.

  Resolution: Refresh the browser. `If the issue persists, log out and log in from vCenter.`

  To see the correct data in OMIVV, ensure that you complete the task listed in resolution.

  Version Affected: 5.0

- **Issue 34–148838**: Unable to delete the ISO profile.

  Resolution: None. You can edit the profile and use the same profile for different deployment task.

  Version Affected: 5.0

- **Issue 35–156807**: Invalid task name might be displayed for OMIVV tasks under VMware Task Console.

  Resolution: None

Version Affected: 4.3.1 and later

- **Issue 36–157172**: After you modify the **Data Retrieval Schedule** settings, Event Posting Level settings are cleared.

  Resolution: Reconfigure the Event Posting Level settings.

  Version Affected: 5.0 and later

- **Issue 37–156357**: Firmware remediation from vSphere Lifecycle Manager fails on host having iDRAC version lower than 2.70.70 and IDSDM component.

  The support for IDSDM firmware update is introduced from iDRAC firmware version 2.70.70. When the machine gets updated to 2.70.70, it notices the presence of IDSDM and with older firmware. If you are managing cluster having iDRAC version lower than 2.70.70 and IDSDM component using vSphere Lifecycle Manager, the host remains in non-complaint after firmware remediation.

  Resolution: Perform the remediation operation twice. Alternatively, you can use the firmware update functionality from OMIVV to update the iDRAC to 2.70.70, and then use the vSphere Lifecycle Manager flow.

  Version Affected: 5.1

- **Issue 39–160776**: Unable to associate the cluster profile that is deleted and created using the same name in vSphere Lifecycle Manager.

  This issue occurs when the cluster profile that is associated with vSphere Lifecycle Manager image is deleted and if you create the cluster profile with the same name and try to associate the new cluster profile to vSphere Lifecycle Manager image.

  Resolution: Create a cluster profile with different name and associate the same in vSphere Lifecycle Manager image.

  Version Affected: 5.1

- **Issue 40–109760**: Proactive HA-related features are working after modifying user credentials in OMIVV Dell EMC administration console.

  If the credentials are modified using the OMIVV Dell EMC administration console after registering the OMIVV to a vCenter, the Proactive HA-related features will not function as expected.

  Resolution: If you are using the Proactive HA feature along with OMIVV, do not modify the registered user credentials. If the credentials require modification, unregister the old credentials and register by using the new credentials.

  Version affected: 4.3 and later

- **Issue 41–158524**: vSphere Lifecycle Manager shows firmware version for PCIe SSD or NVMe SSD as blank for vSAN cluster.

  When the Hardware compatibility is triggered, vSphere Lifecycle Manager does not validate PCIe SSD or NVMe SSD. If these components exist in the server, firmware version is shown as blank because vSphere Lifecycle Manager is not considering OMIVV output for these components.

  Resolution:

  - See that the firmware versions drifted in vSphere Lifecycle Manager firmware compliance page and compare the same with vSAN HCL supported firmware.
  - For vSAN cluster, see the supported or recommended firmware in health service.

  Version affected: 5.1 and later

- **Issue 42–170114**: During auto discovery, OMIVV allows you to apply lower complex password to iDRAC even if the password complexity level is set to high in iDRAC.

  This issue occurs when you set the password complexity as high in iDRAC and initiate auto discovery in OMIVV. During Auto discovery, iDRAC takes the simple password set on the **Deployment Credentials** page of OMIVV even if the password complexity is set high at iDRAC.

  Resolution: Perform any of the following:

  1. Update the password at **Deployment Credentials** with complexity meeting the level set at iDRAC.
  2. Update the password while deploying the System Profile in OMIVV.

  Version affected: 5.0 and later

- **Issue 43–176707**: The health status of the server node having storage sled in a chassis is listed twice on the **Chassis Health** page.

  The health status of a server node having storage sled in a chassis is listed twice in the **Storage** and **Server** sections of **Chassis Health** page. The corresponding slot health is shown as **Unknown** in the **Server** section.

Resolution: To view the correct health status of that server node having storage sled, see the health status that is displayed in the **Storage** section. Ignore the health status reported in the **Server** section.

Version Affected: 5.0 and later

- **Issue 44–180099**: IDSDM component firmware version is not reflecting in inventory after firmware update.

  After you update the IDSDM firmware version, firmware inventory is not reflecting the updated firmware version.

  In vSphere Lifecycle Manager, remediation fails if server has IDSDM component for upgrade.

  In firmware drift report, IDSDM firmware is marked as drifted even if the firmware is upgraded.

  Resolution: None. This is an iDRAC issue. Firmware update is completed successfully.

  Version Affected: 5.0 and later

- **Issue 45–180664, 180631**: OMIVV RPM upgrade using proxy fails.
  - If proxy password contains @ character, OMIVV RPM upgrade using proxy fails.
  - Once if you enter the proxy credential in the OMIVV administration console, OMIVV continue to use the same the proxy credentials, even if credentials are disabled. RPM upgrade fails if credential entered in OMIVV administration console is not valid or proxy password contains @ character.

  Resolution:
  - Ensure that @ character is not used for proxy password.
  - Once if you enter the proxy credential in OMIVV administration console, continue to use proxy with right proxy local credentials (without @ character in password).

  Version affected: 5.2

- **Issue 46–180620**: Fan and temperature sensor details of FX chassis are not displayed on the **Hardware Overview** page of OMIVV.

  This issue occurs if storage sled is present in fourth slot of the chassis or fourth slot of the chassis is not populated. In this case, fan and temperature sensor details of FX chassis shows zero on the **Hardware Overview** page.

  Resolution: OMIVV displays health status and alerts details of fan and temperature sensor. For inventory details, go to Chassis Management Controller (CMC). To launch CMC, go to **Hosts & Chassis** and then click specific chassis URL.

  Version Affected: 5.2

- **Issue 47–181526**: Driver downgrade is not supported for ESXi 7.0 and later version.

  Driver downgrade is not supported in OMIVV for ESXi 7.0 and later versions. Though OMIVV wizard allows you to create the driver downgrade job, driver is not downgraded.

  Resolution: None

  Version Affected: 5.1 and later

- **Issue 48–201651**: The deployment job runs in a recurring manner on weekly basis even after the deployment job is successfully completed.

  The deployment job scheduled on host runs in a recurring manner on weekly basis even though the deployment job is successfully completed. This issue occurs when the deployment job is scheduled for future date or time in OMIVV. Because of the inadvertent triggering of deployment job, the hosts might move to disconnected state or maintenance mode and host might be reimaged based on the job configuration (ISO profile, system profile). This can also lead to a potential disruption to the workloads and clusters.

  Resolution: The issue is fixed in the latest version of OMIVV. For more information, see *OpenManage Integration for VMware vCenter version 5.3.1 Release Notes* available at https://www.dell.com/support.

  Version affected: 5.0 and later

# 7

# Features and fixes in previous releases

## Version

5.2

## Release Date

October 2020

## Features and enhancements

- Introduction of OMIVV Open API Specification (OAS) compliant RESTful APIs

  For more information, see the *OpenManage Integration for VMware vCenter Version 5.2 API Guide* available at **https://www.dell.com/support/**.
- Support for vSphere 7.0 U1
- Support for XE2420 PowerEdge server
- Support for R6515, R7515, R740, and M740c vSAN Ready Nodes
- Enhancement in host credential profile to handle the ESXi credentials in the newer version of ESXi and vCenter. For more information, see the host credential profile topic in OMIVV User's Guide.
- Support for IPv4 range-based bare-metal discovery
- Added filter option on the **Dell EMC Chassis** and **Dell EMC Hosts** pages to filter host and chassis health status.
- Enhancement in warranty reporting for host with multiple or different warranties
- Support for offline RPM update using local HTTPS.
- Addressed critical product issues. For more information about fixed issues, see the Fixed issues section.

## Fixed issues

This release provides fixes for the following issues:

- 159900—Unable to view the proper remediation failure message in vSphere Lifecycle Manager
- 167511— OMIVV becomes unresponsive when managing multiple vCenters
- 166045—OMIVV system profile capture fails for servers with BOSS controller
- 175806— Test connection fails for all hosts managed by vCenter 6.5
- 169195—OMIVV RPM Upgrade fails in proxy environment
- 169295—OMIVV management compliance page displays 200000 error
- 172937—OMIVV becomes unresponsive after restore from OMIVV 4.3
- 177420—Backup and restore failed after the RPM upgrade of the OMIVV appliance

## Version

5.1

# Release Date

April 2020

# Features and enhancements

- Support for vSphere 7.0
- Support for firmware management using vSphere Lifecycle Manager
- Support for XR2 and R7525 PowerEdge servers
- Support for parallel MX7000 chassis firmware updates

# Fixed issues

This release provides fixes for the following issues:

- 113924: When performing backup and restore, error message that is displayed is not informative in admin portal if the invalid username is entered.
- 124012: Testing iDRAC connectivity in a host credential profile using an incorrect password locks the iDRAC access to the appliance until the penalty time configured in iDRAC.
- 127439: When several traps for the same server are received, in under a minute, health metric and extended metric jobs for the server may fail to run. The health status of those servers will be reported as **Unknown** until the next successful health metrics job.
- 128822: The management compliance page shows incorrect credential profile name for hosts managed using chassis credential profile.
- 130791: If you try to manage all the OMIVV-managed hosts in a single host credential profile, it may take few minutes to display the Dell inventory notification in vCenter.
- 146440: Chassis firmware update fails on small deployment mode.
- 147679: Inventory or warranty job fails to trigger after backup and restore.
- 147664: Guest operating system details of OMIVV appliance are incorrectly displayed in ESXi.
- 144171: Chassis inventory fails in OMIVV after promoting backup lead as a lead.
- 135743: Time that is shown for Power Monitoring inventory of the hosts is incorrect when viewed from data center and cluster level.
- 133215: Loading information such as chassis health and active errors take up to one minute because the OMIVV gets live information from the chassis devices.
- 143733: Attribute is not applied after successful system profile RAID deployment.
- 144046: OMIVV lists the virtual IP of the lead when you try to add the member chassis in chassis credential profile.
- 146439: Unable to see the failure details in OMIVV logs for failed MX chassis firmware update job.
- 147683: On the configuration preview page of the deployment wizard, if you clear the target server after performing the configuration preview operation, an error message is displayed.
- 156506: OMIVV becomes unresponsive after alert management configuration.
- 160623: Warranty query does not work from OMIVV.
- 160584: Unregistration of vCenter fails from OMIVV when vCenter extension is removed from vCenter Managed Object Browser (MOB).
- 160809 and 160379: OMIVV conflicts with other third-party plugins

# 8

# Limitations

The following are the limitations for this release of OMIVV:

- If the Dell Cloud server model C6320 contains H730 controller and micro SD card in the riser, the micro SD card might not be detected in some situations. This limits the OS deployment on the SD card.
- In the Dell Cloud server model C6320, deployment through LSI 2008 is not supported.
- OMIVV cannot access files from SMB version 3 based CIFS.

# 9

# Instructions for installing

## Downloading the software package

For more information about downloading OMIVV, see the **Download OpenManage Integration for VMware vCenter** topic in the *OpenManage Integration for VMware vCenter Version 5.2 Installation Guide* at **www.dell.com/support**.

## Installation prerequisites

For the installation prerequisites, see the **Prerequisite checklist** topic in the *OpenManage Integration for VMware vCenter Version 5.2 Installation Guide* at **www.dell.com/support**.

## Installation process

For more information about installation process, see the **Install and Configure OMIVV** section in *OpenManage Integration for VMware vCenter Version 5.2 Installation Guide*.

## Upgrade prerequisites

For more information, see the **Update OMIVV appliance and repository location** topic in *OpenManage Integration for VMware vCenter Version 5.2 User's Guide*.

## Upgrade process

For more information about upgrade process, see the **Upgrade OMIVV appliance using RPM** and **Upgrade OMIVV appliance using backup and restore** topics in *OpenManage Integration for VMware vCenter Version 5.2 User's Guide*.

# 10

# Contacting Dell EMC

Dell EMC provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell EMC for sales, technical support, or customer service issues, see https://www.dell.com/contactdell.

If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or the product catalog.