Dell Management Plug-in for VMware vCenter: Enabling a Dell Server for Server Management in a vCenter

This Dell Technical White Paper describes necessary steps to enable Dell Servers ready for server management in vSphere client using Dell Management Plug-in for VMware vCenter.

Kaushal Gala
Irfan Azam
Muhammad Rahman
# Contents

Introduction .............................................................................................................. 8  
Audience and scope .................................................................................................. 8  
Prerequisites .............................................................................................................. 8  
Steps to enable Dell servers for management ....................................................... 8  
Connection Profiles .................................................................................................. 9  
Creating Connection Profiles .................................................................................. 9  
Test Connection Profiles ......................................................................................... 15  
Test Connection Failures ......................................................................................... 17  
Pre-Dell 12th Generation PowerEdge Servers ....................................................... 17  
Dell 12th Generation PowerEdge Servers ............................................................... 18  
Hardware inventory on Dell servers ........................................................................ 20  
Scheduling an inventory job ..................................................................................... 20  
Running an inventory job ......................................................................................... 23  
Reasons for Inventory Failures ................................................................................. 23  
Incorrect Error Messages for Inventory Failures .................................................... 23  
Compliance Issues .................................................................................................... 25  
Viewing non-compliant hosts .................................................................................. 25  
Fixing non-compliant hosts ..................................................................................... 27  
Fixing OMSA issues .................................................................................................. 32  
Common failures while fixing OMSA ...................................................................... 32  
Fixing CSIOR issues .................................................................................................. 32  
Common failures while fixing CSIOR ...................................................................... 33  
Conclusion ................................................................................................................ 33  
References ............................................................................................................... 33  

---

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Audience and scope</td>
<td>5</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>5</td>
</tr>
<tr>
<td>Steps to enable Dell servers for management</td>
<td>5</td>
</tr>
<tr>
<td>Connection Profiles</td>
<td>6</td>
</tr>
<tr>
<td>Creating Connection Profiles</td>
<td>6</td>
</tr>
<tr>
<td>Test Connection Profiles</td>
<td>11</td>
</tr>
<tr>
<td>Test Connection Failures</td>
<td>13</td>
</tr>
</tbody>
</table>
References ........................................................................................................ 24

Figures

Figure 1. Connection Profiles configuration wizard ........................................... 9
Figure 2. Connection Profiles ............................................................................. 10
Figure 3. Connection Profiles - Associated Hosts ............................................ 12
Figure 4. Connection Profiles - iDRAC Credentials ......................................... 12
Figure 5. Connection Profiles - Host Credentials ........................................... 14
Figure 6. Complete Connection Profile Creation ............................................. 15
Figure 7. Select a Connection Profile .............................................................. 16
Figure 8. Test Connection Profile ..................................................................... 17
Figure 9. Example of test connection ............................................................... 18
Figure 10. Schedule Inventory - Configuration Wizard ....................................... 20
Figure 11. Settings - Inventory Schedule ......................................................... 21
Figure 12. Schedule Inventory via Settings ....................................................... 21
Figure 13. Job Queue - Inventory History ........................................................ 22
Figure 14. Change Inventory Schedule ............................................................ 23
Figure 15. View Non-compliant hosts from Overview page ................................ 25
Figure 16. View non-compliant hosts from Compliance page ........................... 26
Figure 17. Example of non-compliant hosts .................................................... 27
Figure 18. Host Compliance Wizard - Select Hosts ............................................ 28
Figure 19. Host Compliance Wizard - Fix Connection Profile Warning ............. 28
Figure 20. Host Compliance Wizard - CSI0R .................................................. 29
Figure 21. Host Compliance Wizard - OMSA .................................................. 30
Figure 22. Host Compliance Wizard - Reboot Hosts ....................................... 31
Figure 23. Host Compliance Wizard - Summary ............................................. 32
Figure 1. Connection Profiles configuration wizard ........................................ 6
Figure 2. Connection Profiles .......................................................................... 7
Figure 3. Create New Connection Profile .......................................................... 7
Figure 4. Connection Profiles - Name and Description ..................................... 8
Figure 5. Connection Profiles - Associated Hosts .......................................... 8
Figure 6. Connection Profiles - iDRAC Credentials ....................................... 9
Figure 7. Connection Profiles - Host Credentials ......................................... 10
Figure 8. Complete Connection Profile Creation ......................................... 11
Figure 9. Select a Connection Profile ............................................................ 12
Figure 10. Test Connection Profile ............................................................... 12
Introduction

The Dell Management Plug-in for VMware vCenter is a virtual appliance which can be used to reduce tools and tasks associated with management and deployment of Dell servers in your virtual environment. The plug-in reduces complexity by natively integrating the key management capabilities into the vCenter console, and it minimizes risk with hardware alarms, streamlined firmware updates, and deep visibility into inventory, health, and warranty details.

The Dell Management Plug-in for VMware vCenter is designed to streamline the management processes in your data center environment by allowing you to use VMware vCenter to manage your entire infrastructure—both physical and virtual. From firmware updates to bare metal deployment, the Dell Management Plug-In for VMware vCenter will expand and enrich your data center management experience with Dell PowerEdge servers.

This whitepaper provides all necessary information you need to enable-prepare a Dell Server ready for server management in vCenter using the Dell Management Plug-in for VMware vCenter. This involves We describe the steps you will take to set up a connection profile for Dell hosts in a vCenter, running an inventory, and fixing compliance issues on those hosts.

Audience and scope

This whitepaper is intended for sale engineers, field application engineers, test engineers, architects, or IT administrators who are involved in the decision-making process for the planning, design, configuration, and operation of a dynamic datacenter. The scope of this document is to provide a detailed procedure towards that describes setting up a Dell Server for server management in vCenter. This whitepaper is intended for sale engineers, field application engineers, test engineers, architects, or IT administrators who are involved in the decision-making process for the planning, configuration, and operation of a dynamic datacenter.

This document is intended to assist users in using the Dell Management Plug-in for managing vSphere hosts that are Dell Servers in a vCenter.

Prerequisites

Readers are expected to have a working knowledge of networking, VMware vSphere, virtual networking concepts, Windows™ W2KR8, and the Linux environment. Requirements Software requirements are VMware ESX/ESXi™ 4.0 or later host installation and VMware vCenter™.

Readers are expected to know how to install a VMware ESX/ESXi™ hypervisor on a server and how to add it to a vCenter as a vSphere host.

Readers are also expected to know how to install Dell Management Plug-in for VMware vCenter and registering it to a vCenter. More information for installation and registering the plug-in to a vCenter can be found in Dell Management Plug-in for VMware vCenter User’s Guide.

Steps to enable Dell Servers for management

User needs to perform the following steps in order to start managing Dell hosts from the ‘Dell Server Management’ tab in vSphere Client:

1. Create a connection profile and associate the Dell hosts
2. Run hardware inventory on Dell hosts so that necessary hardware information is collected
3. Fix any compliance issues that are reported by vSphere Host Compliance
Connection Profiles

A Connection Profile associates a set of Dell hosts with necessary credentials needed for communication with ESX/ESXi™ and the Dell Remote Access Controller (iDRAC).

Creating Connection Profiles

2. If you are using the Dell Management Plug-in for the first time, you should see Welcome page of the Configuration Wizard displays. Click “Next” or “Save and Continue” to see the Connection Profiles page.

Figure 1. Figure 1—Connection Profiles Configuration Wizard — Connection Profiles
If you have used the Dell Management Plug-in at least once, you will not see the Configuration Wizard automatically. Click on **Connection Profiles** from in the left navigation area.

**Figure 2.** Connection Profiles

1. Click on **Create New** to open a popup for creating a new connection profile.

**Figure 3 Create New Connection Profile**

3. Enter a Profile Name and Description for the connection profile and, and then click **Next** to proceed.
4. **Figure 4 Connection Profiles – Name and Description**

5. Place a checkmark in the boxes beside the hosts in the vCenter tree that you want to be part of the Connection Profile, and then click **Next**.

   **Figure 4 Connection Profiles – Name**

   - Select the hosts that appear in vCenter tree via the checkboxes to make it part of the connection profile and then click “**Next**”. 
6. Read the information on "Credentials" page, and then click "Next".

7. Enter the required iDRAC credentials, and then click "Next". If you want to provide Active Directory credentials for the iDRAC, select the Use Active Directory check box before entering the Active directory credentials.

Figure 4. Figure 6. Connection Profiles - iDRAC Credentials
Enter Host Credentials (OS Admin login details), then click "Next". If you want to provide Active Directory credentials for the host, select the Use Active Directory check box before entering the Active directory credentials.
At any time, the user can cancel profile creation action using the via “Cancel” button. User can, or move/go back and forth via between the wizard screens using the “Back” and “Next” buttons.

9. Test the credentials on “Click Test Connection Profile” to test the new profile credentials. See section Test Connection Profiles for further information. Click “Save” to finish creation of the connection profile.
Test Connection Profiles

You can test the credentials for connection profiles either at the end of creating a connection profile or by using the “Test Connection” link on the “Connection Profiles” page screen, as listed below:

1. On the “Connection Profiles” page screen, you will see all the hosts attached to that connection profile. Click on the connection profile you want to test. You will see all the attached hosts to that connection profile.
1. Figure 7. Select a Connection Profile

2. Click “Test Connection” right above the attached hosts to open a popup screen.
3. Place a checkmark in the box beside the hosts you want to select, and click **Test Selected**.

**Test Connection Failures**

iii. Check/select hosts and click "**Test Selected**".

The following cases below explain situations that can cause Test Connection Failures:

**Pre-dell 12th Generation Dell PowerEdge Servers**

- Host Credentials will fail for one of the following cases:
  a. Credentials changed to incorrect credentials for a host in a connection profile which has lockdown mode disabled.
  b. After adding a host to connection profile which has lockdown mode disabled, lockdown mode is enabled on that host. Test will fail for at least next 30 minutes for this host. If the connection still fails after 30 minutes, then either restart either host or the management agents on that host.
  c. No Agent (OMSA) is installed.
  d. Not able to reach host - common reasons include:
     1. Host is not online or rebooting.
2. Host is not reachable from appliance; if hosts are added with the DNS names or FQDN in the vCenter server, then make sure that appliance can access those hosts via the DNS configuration present in the appliance.

3. Any other networking and/or routing problems; check the network and DNS configuration in the appliance.

Pre-12th Generation Dell servers—iDRAC Credentials will fail for one of the following cases:

a. iDRAC is not present on the server.
b. Any condition mentioned above for Pre-Dell 12th Generation PowerEdge Server Host Credentials failure is true.
c. iDRAC credentials are incorrect.
d. Not able to reach the iDRAC - common issues included:
   1. iDRAC is not online or rebooting/resetting.
   2. iDRAC is not reachable from appliance; check appliance’s network configuration.

Dell 12th Generation Dell PowerEdge servers
—Host Credentials will fail for one of the following cases:

a. Credentials changed to incorrect credentials for a host in a connection profile which has lockdown mode disabled.
b. After adding a host to connection profile which has lockdown mode disabled, lockdown mode is enabled on that host. Test will fail for at least next 30 minutes for this host.

12th Generation Dell servers—iDRAC Credentials will fail for one of the following cases:

a. Any condition mentioned above for Dell 12th Generation PowerEdge Server 12th Generation Host Credentials failure is true.
b. Not able to reach the iDRAC, as mentioned above.

Here is an example screen of a “Test Connection” in action.

Figure 1. Figure 9. Figure 11. Example of Test Connection
### Figure 11: Example of Test Connection

![Test Connection Profile]

You can optionally test the communication with the hosts using the configured credentials by selecting one or more hosts associated with this Connection Profile and clicking "Test Selected". All configured credentials are tested against each selected host and the results of the tests are displayed when the test completes.

<table>
<thead>
<tr>
<th>Associated Hosts</th>
<th>Service Tag</th>
<th>DRAC Credentials</th>
<th>Host Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.5.47</td>
<td>4G/WNN1</td>
<td>Fail - Unable to contact DRAC</td>
<td>Fail - Unable to contact Host Credentials</td>
</tr>
<tr>
<td>10.255.4.201</td>
<td>52C/UN1</td>
<td>Pass</td>
<td>Pass</td>
</tr>
<tr>
<td>10.255.5.71</td>
<td>42C/UN1</td>
<td>Fail - Unable to contact DRAC</td>
<td>Fail - Unable to contact Host Credentials</td>
</tr>
<tr>
<td>10.255.5.67</td>
<td>22C/UN1</td>
<td>Pass</td>
<td>Pass</td>
</tr>
<tr>
<td>10.255.4.172</td>
<td>59Z/UT1</td>
<td>Pass</td>
<td>Pass</td>
</tr>
<tr>
<td>10.255.4.102</td>
<td>3JK/YV1</td>
<td>In Queue</td>
<td>In Queue</td>
</tr>
<tr>
<td>10.255.5.196</td>
<td>DM/RZT1</td>
<td>$\text{testing...}$</td>
<td>$\text{testing...}$</td>
</tr>
</tbody>
</table>

56% Completed

---

*NOTE: The screenshot and table are placeholders and should be replaced with actual content.*
Hardware Inventory on Dell Servers

A successfully completed inventory is required to gather the necessary hardware information for the Dell Server Management software to function. Also, periodic inventories ensure information is always up-to-date.

Scheduling an inventory job

Hardware inventory can be scheduled in any of the three ways below:

a. 1. Using the Configuration Wizard
   i. a. Once you have created a connection profile in the Configuration Wizard as shown in Configuration Wizard - Connection Profiles above, click through the screens via using "Next" or "Save and Continue" until you land on "Inventory Schedule" page.
   ii. b. Using the checkboxes, select the days you want inventory to run via the checkboxes. Set the time you want the inventory to run on the selected days.

b. 2. Using the Settings screens
   i. a. Click on "Settings" from in the left navigation area.
   ii. b. Click on "Inventory Schedule".

Figure 10. Schedule Inventory - Configuration Wizard

Figure 12. Schedule Inventory - Configuration Wizard

iii. c. Click "Save and Continue" to save the inventory schedule.
Click on “Edit” on upper-right.

Select the days to run the inventory and set the time. Click “Save”.

On Selected Days:
- MO
- TU
- WE
- TH
- FR
- SA
- SU
3:00 (GMT-5)

Do not run inventory on Dell hosts.
4.3. Using the Job Queue

i. **a.** Click “Job Queue” from the left navigation area.

ii. **b.** Click “Inventory History” to see details on Inventory Jobs.

---

**Figure 15. Job Queue - Inventory History**

---

**Figure 13. Figure 15 Job Queue - Inventory History**

---

**Figure 15. Job Queue—Inventory History**

---

**Figure 13. Figure 15 Job Queue—Inventory History**

---

**Figure 15. Job Queue—Inventory History**

---

**Figure 13. Figure 15 Job Queue—Inventory History**

---

i. **c.** Click “Change Schedule” to open a popup for changing inventory schedule.

d. Click “Edit” to select the days to run the inventory and set the time.

e. **e.** Click “Apply”.
Running an inventory job

An inventory job can either run on scheduled days/time as explained in the section Scheduling an inventory job, or on demand when user clicks “Run Now” button as shown in Figure 13. After the inventory job finishes, the result of inventory on each host is displayed in inventory job details table with Successful or Failed status. The status is only for the last inventory job. The host with Successful inventory status is ready to be managed in Dell Server Management tab corresponding to that host.

Reasons for Inventory Failures

1. Any condition mentioned in the section Test Connection Profiles for Pre 12th Generation Host Credentials failure is true. See section Compliance issues to troubleshoot inventory issues.

2. Any condition mentioned in the section Test Connection Profiles for 12th Generation Host Credentials failure is true. See section Compliance issues to troubleshoot inventory issues.

3. An expired license or base license present for iDRAC on a 12th Generation host also fails inventory. To see more details, view “iDRAC License” page under “Compliance” in Dell Management Center.

To troubleshoot inventory failures, check host and iDRAC Network connections.

Incorrect Error Messages for Inventory Failures

Following incorrect errors can be seen during inventory for a connection failure with iDRAC:

1. Exception specifying that OMSA is not installed.
2. iDRAC License failure, for Pre 12th Generation Host.
Dell Management Plug-in for VMware vCenter: Enabling a Dell Server for Server Management in vCenter
Compliance issues

The Dell hosts must meet certain minimum criteria in order to be managed by the Dell Management Plug-in. If the Dell hosts do not meet the minimum criteria, they are treated as non-compliant vSphere hosts.

Viewing non-compliant hosts

A compliance check runs as a part of an inventory job on hosts that are part of a connection profile. This check identifies hosts that do not meet necessary minimum criteria, and marks such hosts as non-compliant specifying exact reasons.

There are two ways to look at the non-compliant hosts:

a. Click “View Details” link right below “Non-compliant vSphere Hosts” on the “Overview” page as shown in Figure 15.

b. Click “vSphere Hosts” or “View non-compliant vSphere Host Details” link on the “Compliance” page as shown in Figure 18.
The hosts shown are non-compliant because of one or more of the reasons listed below:

1. Inventory Job has not run on the host.
2. Inventory Job has not completed on the host.
3. Connection Profile not configured.
4. OMSA is not installed (applicable only to Pre 12th Generation Host)
5. OMSA update required (applicable only to Pre 12th Generation Host)
6. OMSA is not configured (applicable only to Pre 12th Generation Host)
7. CSIOR (Collect System Inventory on Reboot) is off
8. Reboot Required

The figure below shows an example screen of non-compliant hosts.
Due to security restrictions pertaining to Lockdown Mode, Dell Management Plug-in cannot communicate or run the full compliance check for hosts with Lockdown Mode set to Enabled state. Such hosts are not shown in the non-compliant and are marked with a message on top of the non-compliant hosts list.

**Fixing non-compliant hosts**

Dell Management Plug-in can take necessary steps to resolve the compliance issue by installing software, updating software, configuring SNMP on host, turning on CSIOR on iDRAC etc. After doing completing all the required steps to make a host compliant, an automatic inventory job is triggered to re-collect the latest information on that host.

To fix compliance issues on non-compliant hosts, use “the Host Compliance Wizard” as explained below:

1. Click on “Fix non-compliant vSphere Hosts” link on the “vSphere Hosts” page (Alternatively, you can click “Fix vSphere Hosts for Compliance” on “the Overview” page screen). This will bring up the Host compliance wizard with “Select Hosts” page screen displays.
2. Select the hosts you want to fix on the “Select Hosts” page using the checkboxes on the left column, then click “Next” button.

If you select hosts that are not part of a connection profile, i.e. those with Connection Profile shown as “Not Configured”, you will be prompted with a warning message.
Click Fix Connection Profiles to proceed to the Connection Profiles screen.

You can proceed to Connection Profiles page using “Fix Connection Profiles” button.

Clicking on “Continue Compliance Wizard” will allow you to continue with the wizard, but will not include hosts that were not part of any connection profile.

Next you will be shown hosts (from the hosts you selected) that are non-compliant due to CSIOR state on “Turn On CSIOR” page. Select hosts to fix CSIOR state and click “Next”. See section Fixing CSIOR issues for details.

Next you will be shown hosts (from the hosts you selected in Step ii) that are non-compliant due to OMSA state on “the Fix OMSA” page. Select hosts to fix OMSA state and click “Next”. See section Fixing OMSA issues for details.
If you have selected hosts that may need reboot either while fixing OMSA or CSIOR, then the “Reboot Hosts” page is shown. The screen displays details on those hosts that need to be rebooted. You can check the checkbox on the bottom to opt-in for maintenance mode and reboot action. If you wish to manually reboot such hosts, simply uncheck the checkbox. Click “Next”.

---

**Figure 21.** Host Compliance Wizard - OMSA

**Figure 24.** Host Compliance Wizard - OMSA
6. The “Summary” page shown in the end screen simply summarizes the actions that will be performed to correct fixing the compliance. Click the “Finish” button to initiate the fix process. You can go back and change your selections using the “Back” button.
Fixing OMSA issues

When a host is selected for fixing an OMSA issue, a new OMSA package is installed or updated as needed. To fix OMSA configuration of OMSA, a file on the Host operating system is configured to send SNMP traps.

Dell Management Plugin-in uses vCenter for OMSA related issue on ESXi 4.x hosts but uses SSH on classic ESX 4.x and ESXi 5.0/5.0 Update1.

Common failures while fixing OMSA

a. Host is down
b. SSH is disabled for ESX 4.x and ESXi (5.0, 5.0 U1)
c. PasswordAuthentication=no in the SSH Configuration file on ESXi (5.0, 5.0 U1)
d. Network latency for OMSA configuration.

Fixing CSIOR issues

CSIOR is an iDRAC feature, which needs to be ON to collect the hardware information. When a host is selected for fixing CSIOR issues, this feature is turned ON. Sometimes, CSIOR may already be ON and simply needs the host to reboot. This is indicated in CSIOR status as “On - Reboot Required”. To fix
this, simply select the check-box to reboot hosts in the “Reboot Hosts” screen page of the host compliance wizard.

Common failures while fixing CSIOR

1. iDRAC not responding. Resetting iDRAC can resolve this problem.
2. Bad iDRAC credentials set in the connection Profile.
3. Old iDRAC Firmware that does not support CSIOR Configuration.

Note: Even after having run inventory, if the CSIOR status is “Unknown”, it is due to the same reasons as explained above in “Common Failures while fixing CSIOR”.

Conclusion

Now that you have successfully set up your Dell Servers and they are ready to be managed from your vSphere Client itself, you can start using the ‘Dell Server Management’ tab to access your desired management features. You can read more details in Dell Management Plug-in for VMware vCenter User’s Guide.

References

1. Dell Management Plug-in for VMware vCenter Quick Installation Guide