OpenManage Integration for VMware vCenter: Enabling a Dell Host for Server Management in a vCenter

This Dell Technical White Paper describes necessary steps to enable Dell Server ready for server management in vSphere client using OpenManage Integration for VMware vCenter from vSphere Desktop Client

Kaushal Gala
Irfan Azam
Muhammad Rahman

October 2013

A Dell Technical White Paper

Revisions

Date	Description
August 2013	Initial release
October 2013	Ported to new Dell template

Table of contents

1 Introduction

The OpenManage Integration for VMware vCenter is a virtual appliance that 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 key management capabilities into the vCenter console, and minimizes risk with hardware alarms, streamlined firmware updates, and deep visibility into inventory, health, and warranty details.

The OpenManage Integration 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 OpenManage Integration for VMware vCenter will expand and enrich your data center management experience with Dell PowerEdge servers.

This whitepaper provides the information you need to prepare a Dell Server for server management in vCenter using the OpenManage Integration for VMware vCenter from vSphere Dekstop Client. We describe the steps you will take to set up a connection profile for Dell hosts in a vCenter, run inventory, and fix compliance issues on those hosts.

1.1 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 design, configuration, and operation of a dynamic datacenter. The scope of this document is to provide a detailed procedure that describes setting up a Dell Server for server management in vCenter. This document is intended to assist users in using the OpenManage Integration for VMware vCenter for managing vSphere hosts that are Dell Servers in a vCenter.

1.2 Prerequisites

Readers are expected to have a working knowledge of networking, VMware vSphere, virtual networking concepts, Windows™ and Linux server environment. 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 OpenManage Integration for VMware vCenter and register it to a vCenter. More information for installation and registering the plug-in to a vCenter can be found in OpenManage Integration for VMware vCenter User's Guide.

2 Steps to enable Dell servers for management

User need to perform the following steps in order to start managing Dell Host from the 'Dell Server Management' tab in vSphere Client:

1. Create a connection profile and associate Dell hosts to it
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

2.1 Connection Profiles

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

2.1.1 Creating Connection Profiles

1. Open OpenManage Integration for VMware vCenter using vSphere Client.
2. If you are using the OpenManage Integration for VMware vCenter for the first time, the Welcome page of the configuration wizard displays. Click **Next** or **Save and Continue** to see the Connection Profiles page.

If you have used the OpenManage Integration for VMware vCenter at least once, you will not see the Configuration Wizard automatically. Click **Connection Profiles** in the left navigation area.

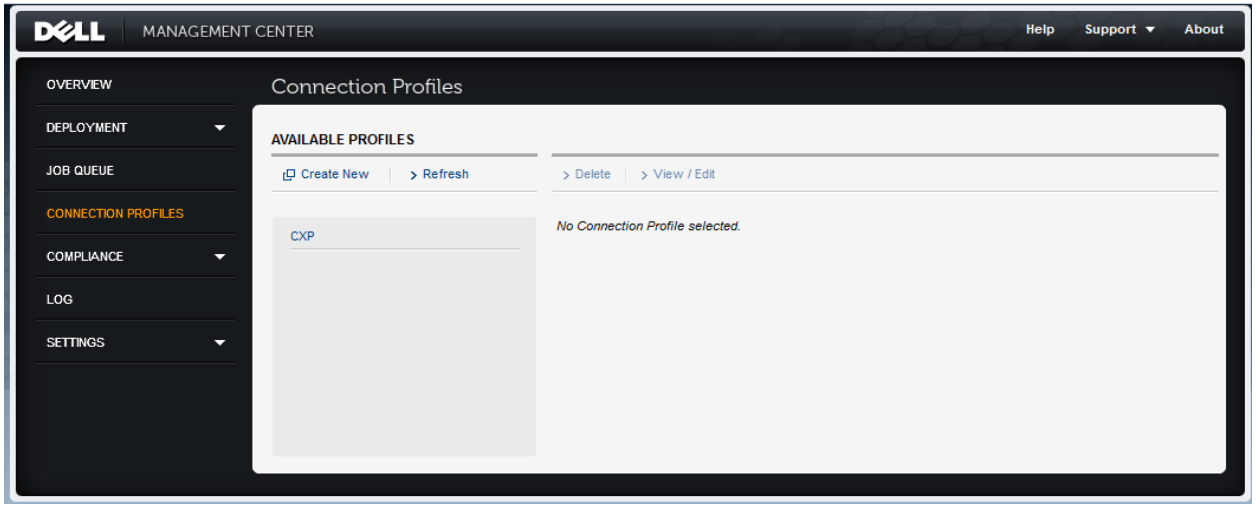

Figure 1 Connection Profiles

3. Click **Create New** to open the New Connection Profile screen.
4. Type a Profile Name and Description for the connection profile, and then click **Next**.
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**.

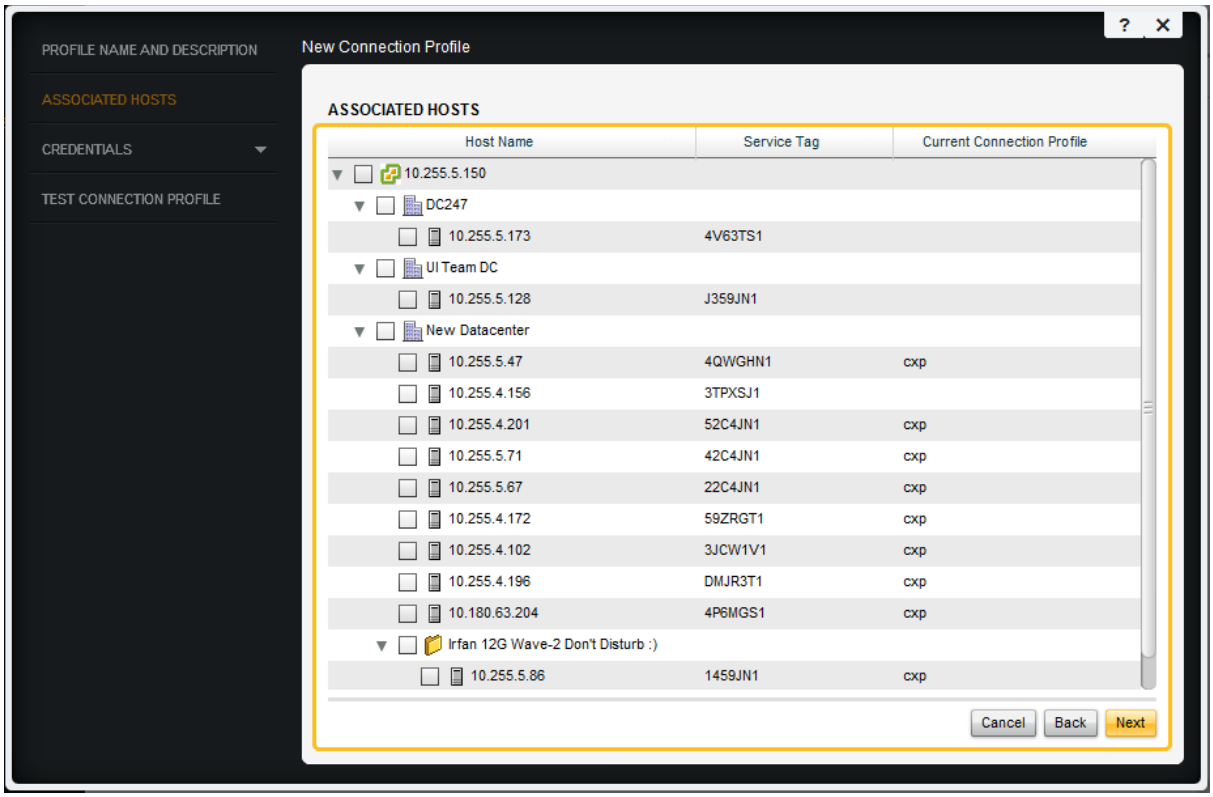

Figure 2 Connection Profiles - Associated Hosts

6. Read the information on Credentials screen, 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.

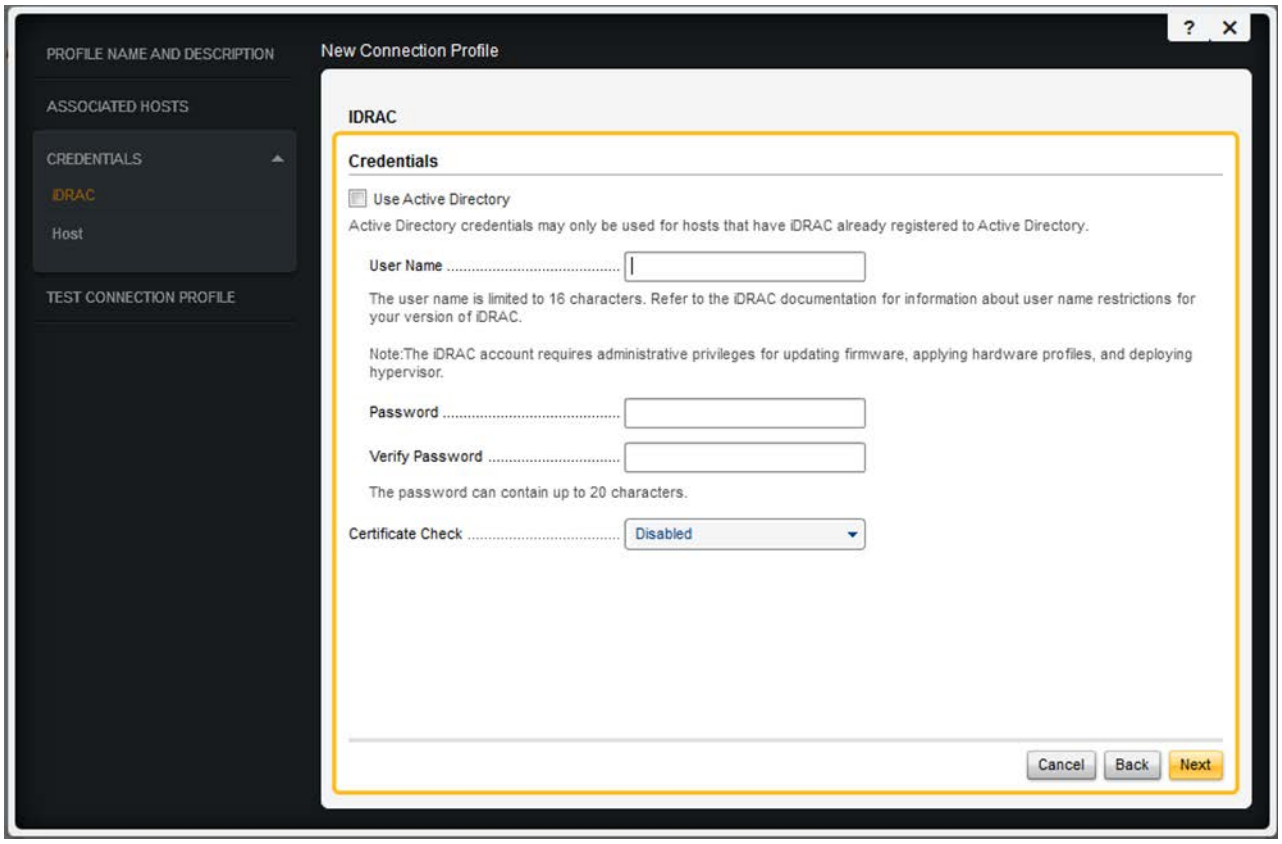

Figure 3 Connection Profiles - iDRAC Credentials

8. 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.

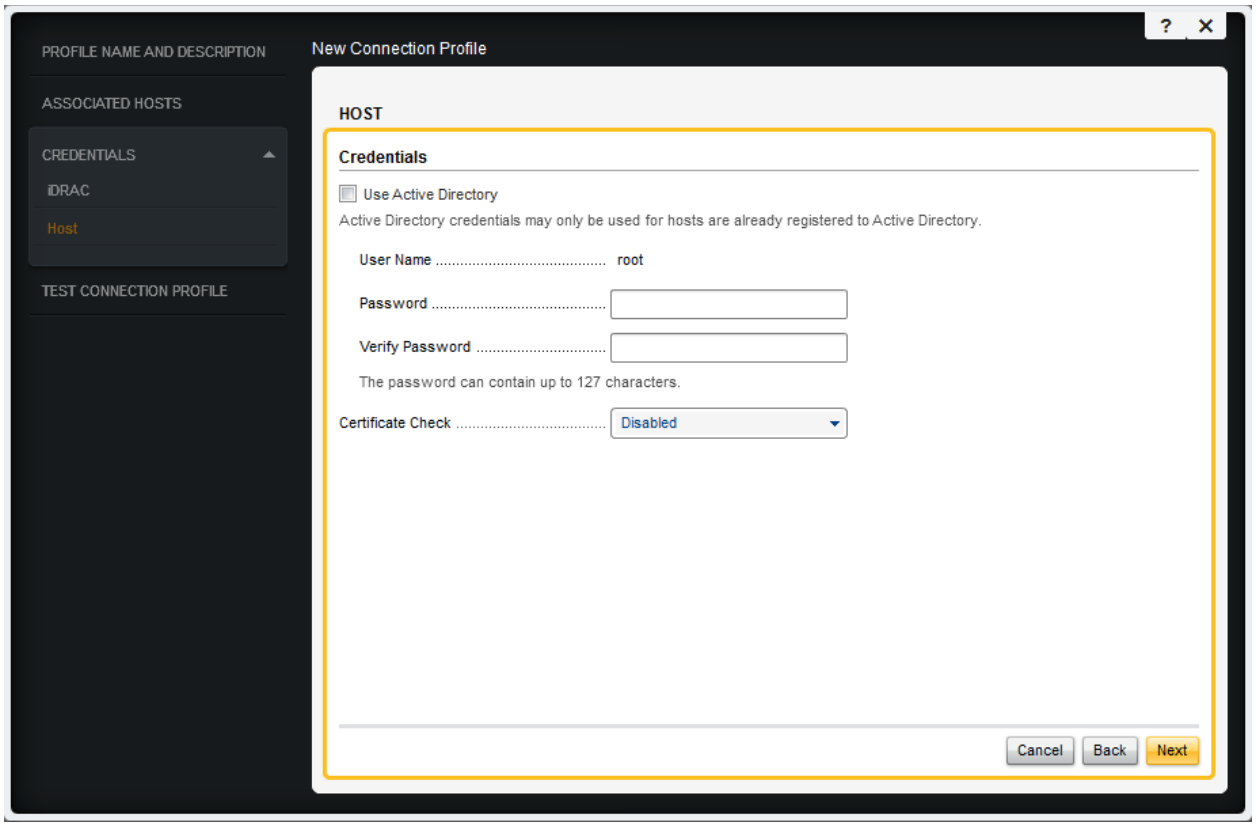

Figure 4 Connection Profiles - Host Credentials

At any time, the user can cancel profile creation action using the **Cancel** button, or move back and forth between the wizard screens using the **Back** and **Next** buttons.

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

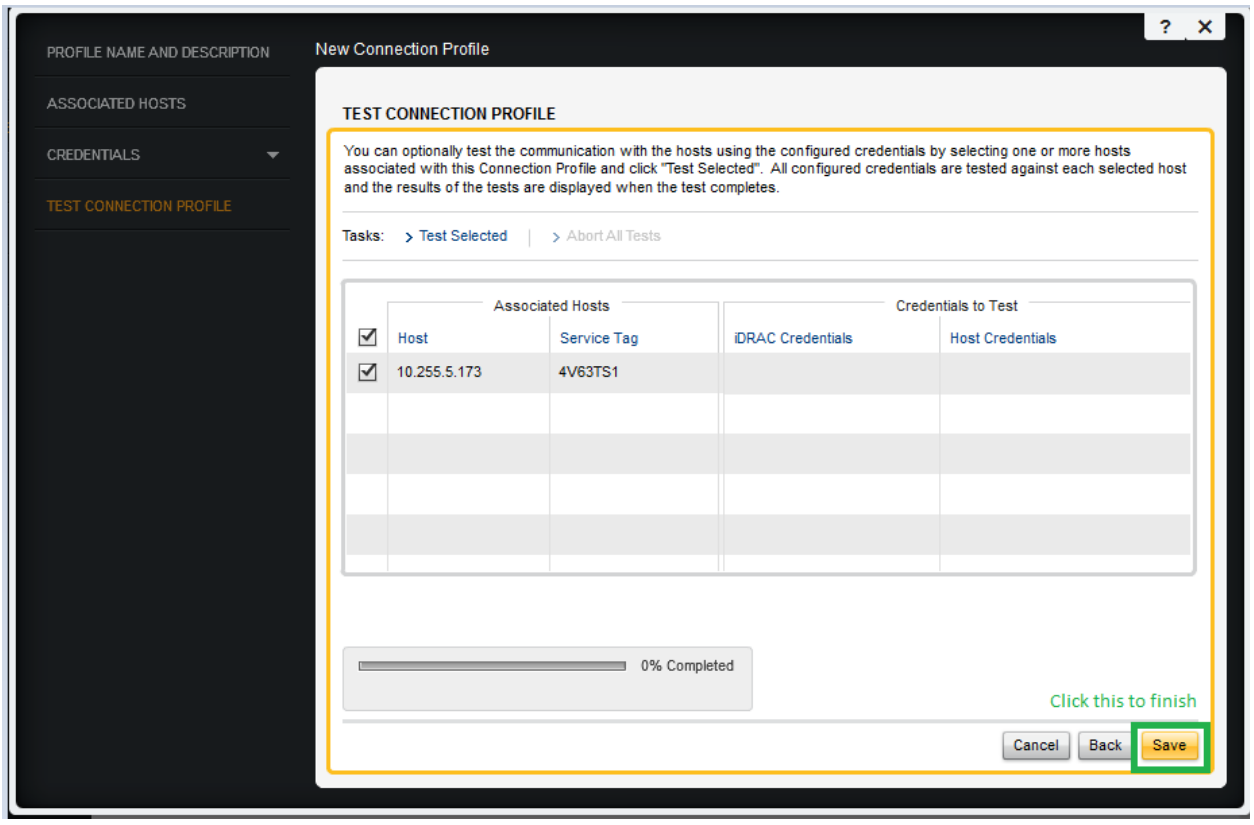

Figure 5 Complete Connection Profile Creation

2.1.2 Test Connection Profiles

You can test the credentials for connection profiles either at the end of the profile creation process or by using the **Test Connection** link on the Connection Profiles screen:

1. On the **Connection Profiles** screen, You will see the all the hosts attached to that connection profile. Click the connection profile you want to test.

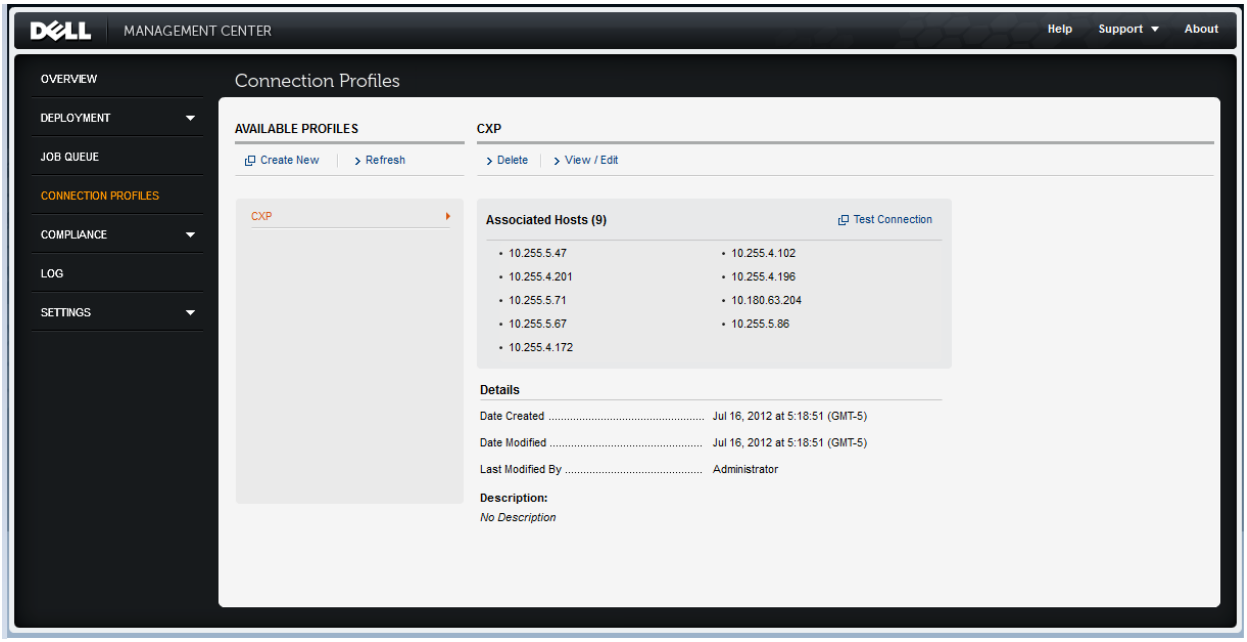

Figure 6 Select a Connection Profile

2. Click Test Connection above the attached hosts to open a popup screen.

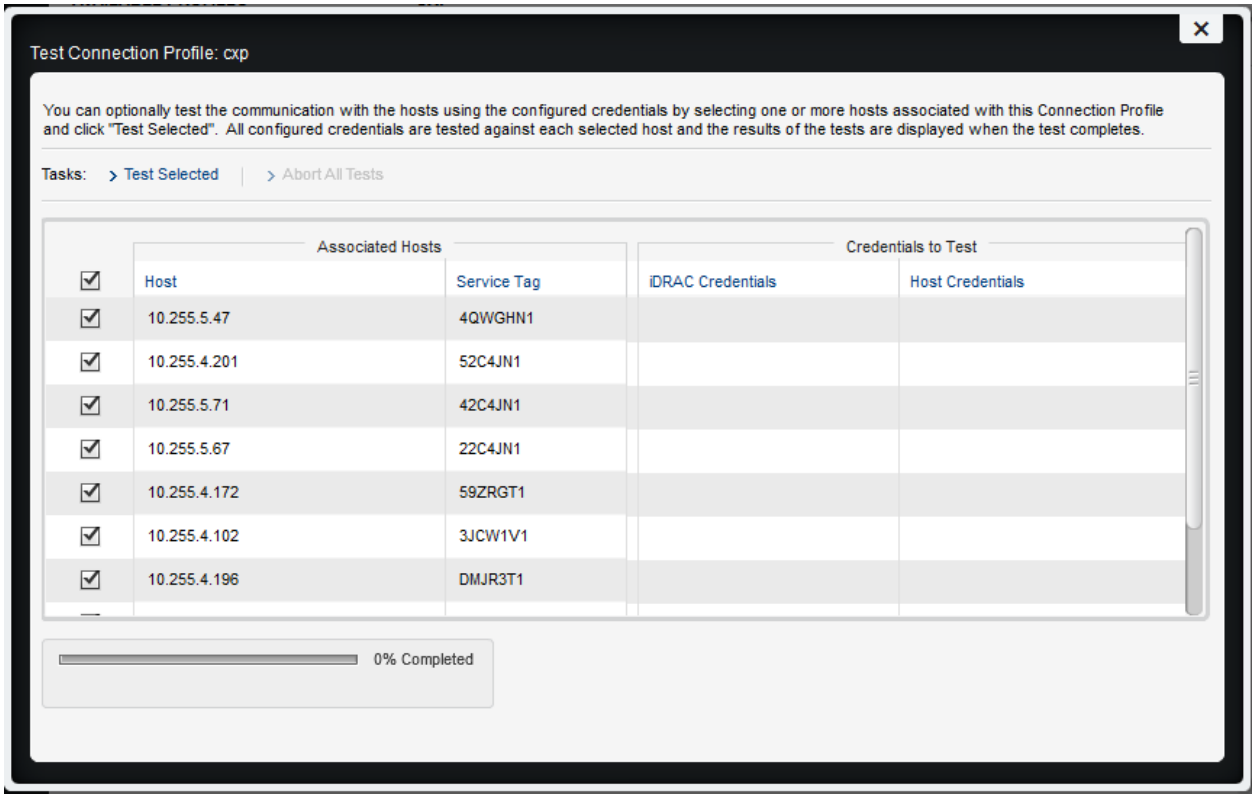

Figure 7 Test Connection Profile

3. Place a checkmark in the box beside the hosts you want to select, and click Test Selected.

2.1.3 Test Connection Failures

The following cases explain situations that can cause Test Connection Failures.

Pre-Dell 12th Generation 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 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:
    i. Host is not online or rebooting.
    ii. 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.
    iii. Any other networking and/or routing problems; check the network and DNS configuration in the appliance.

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:
    i. iDRAC is not online or rebooting/resetting.
    ii. iDRAC is not reachable from appliance; check appliance's network configuration.

Dell 12th Generation 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.

iDRAC Credentials will fail for one of the following cases:

a. Any condition mentioned above for Dell 12th Generation PowerEdge Server 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.

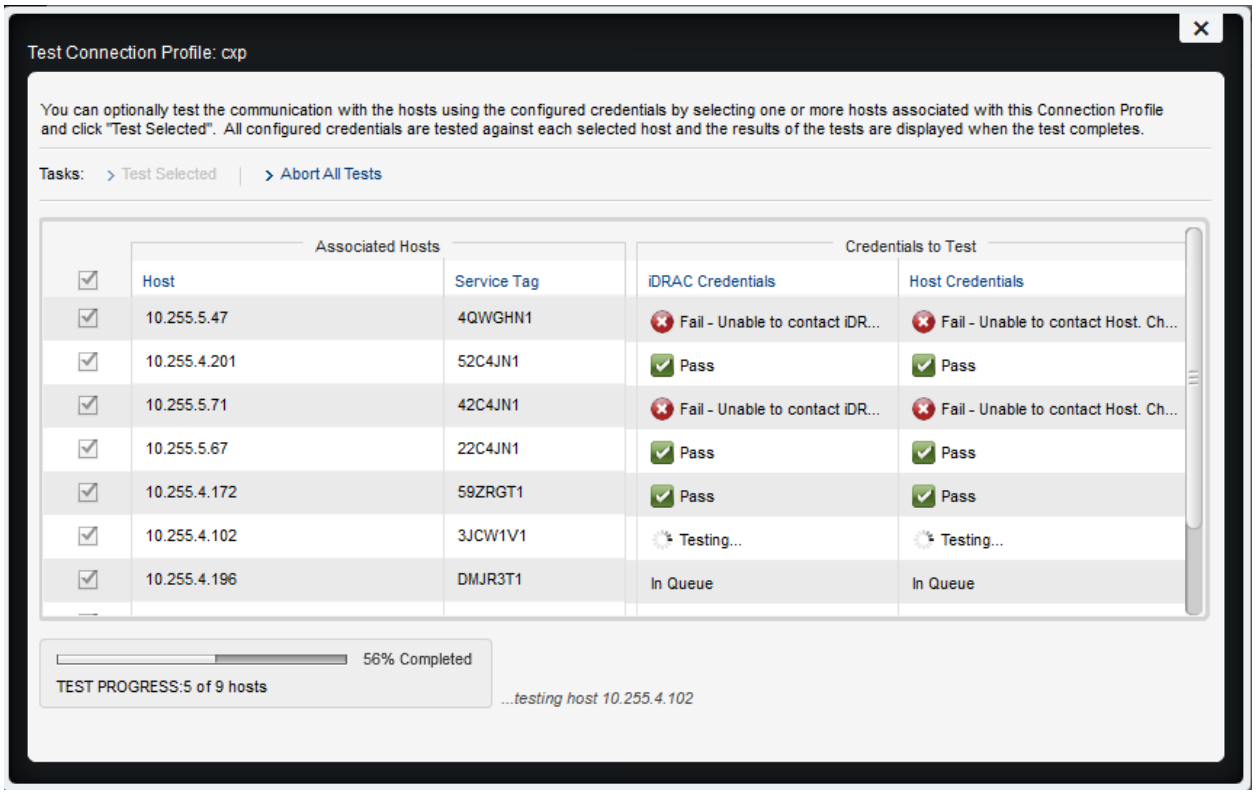

Figure 8 Example of test connection

2.2 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.

2.2.1 Scheduling an inventory job

Hardware inventory can be scheduled in any of three ways:

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

Figure 9 Schedule Inventory - Configuration Wizard

c. Click **Save and Continue** to save the inventory schedule.

2. Using the Settigs screens
   a. Click **Settings** in the left navigation area.
   b. Click **Inventory Schedule**.

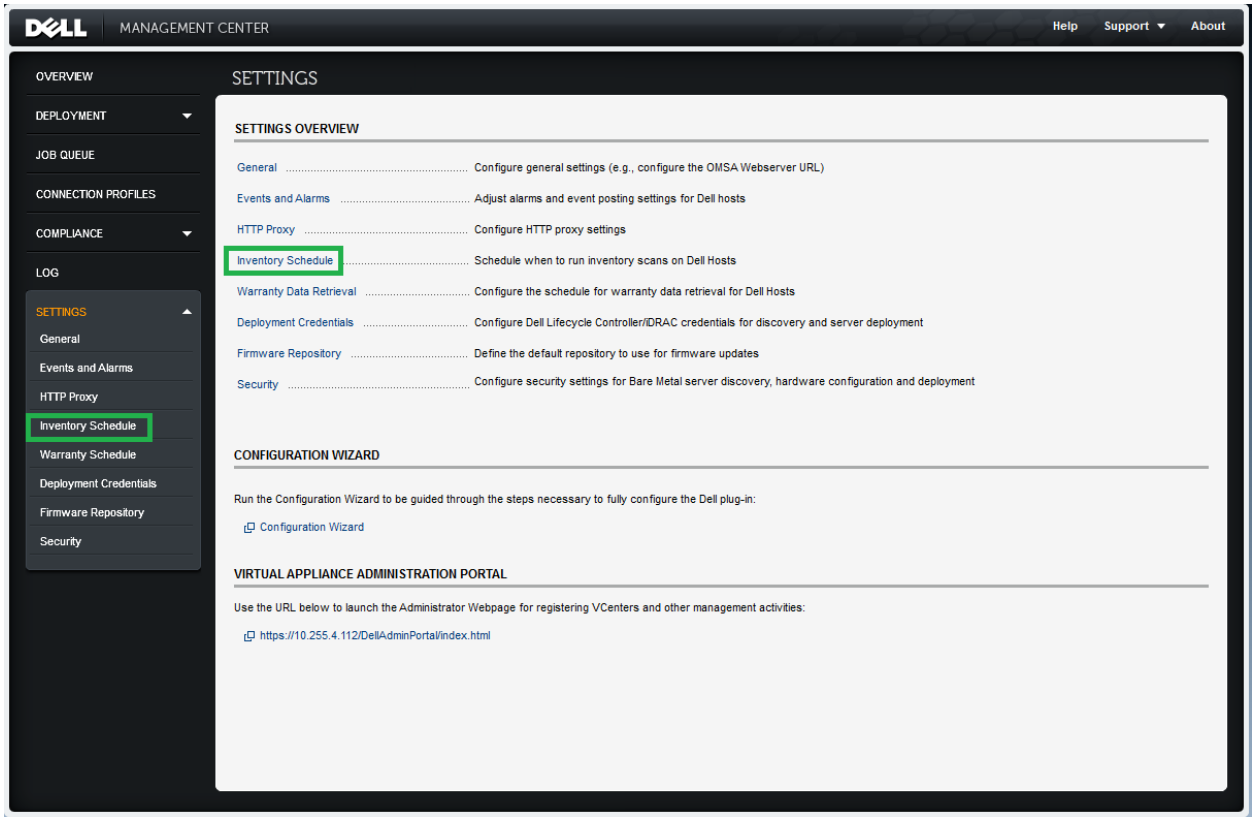

Figure 10 Settings - Inventory Schedule

c. Click on "**Edit**" on upper-right.
d. Select the days to run the inventory and set the time. Click **Save**.

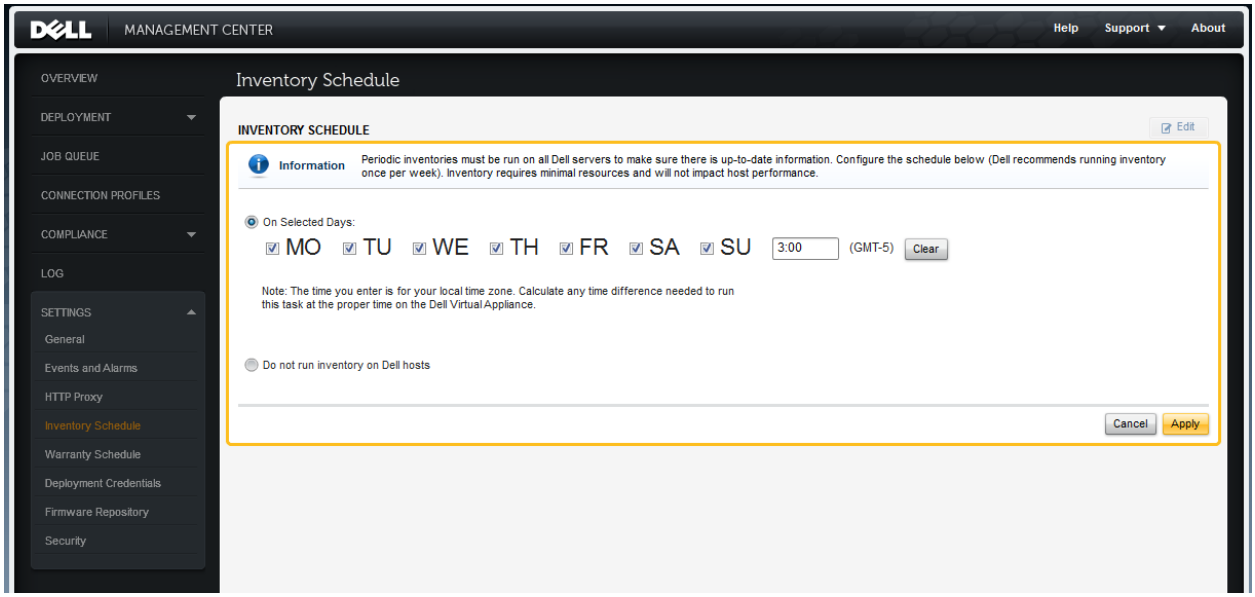

Figure 11 Schedule Inventory via Settings

3. Using the Job Queue
   a. Click **Job Queue** in the left navigation area.
   b. Click **Inventory History** to see details on Inventory Jobs.

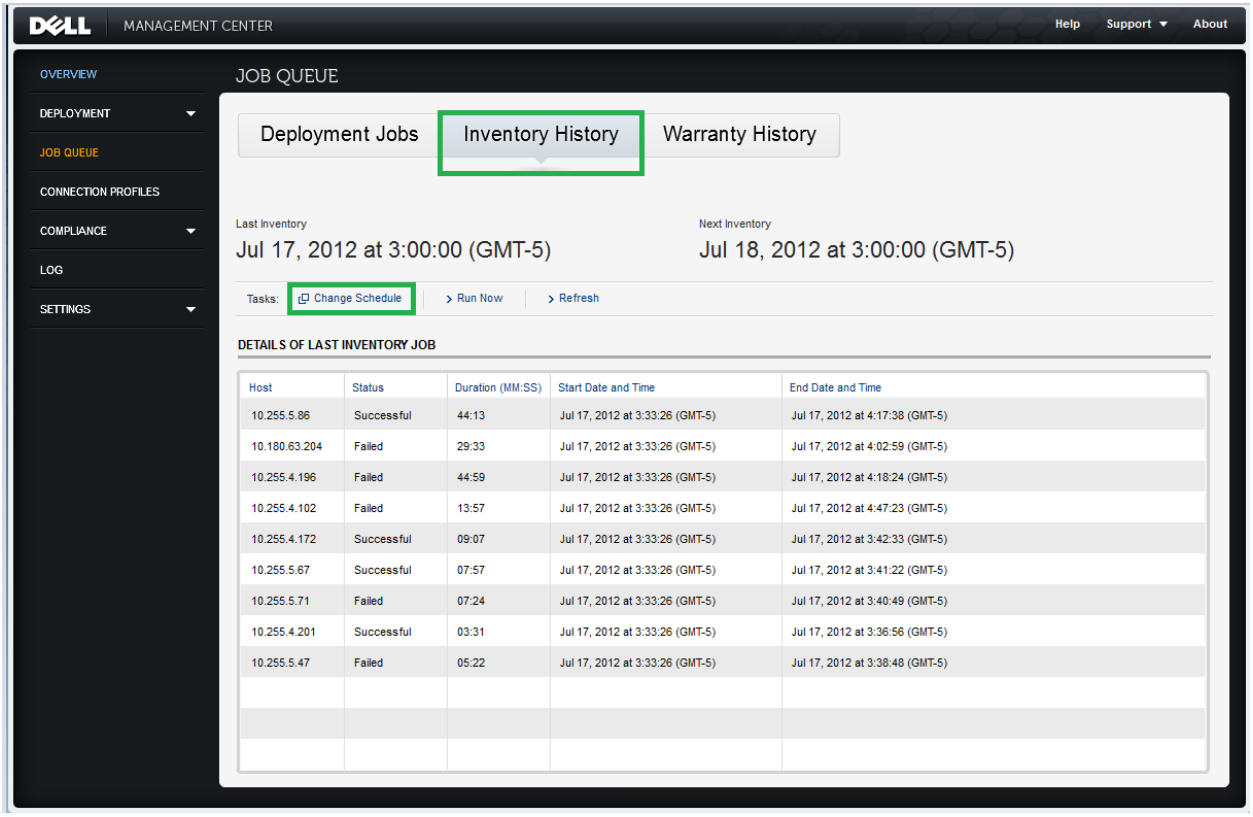

Figure 12 Job Queue - Inventory History

   c. Click **Change Schedule** to open a popup for changing inventory schedule.
   d. Click **Edit**, select the days to run the inventory, and set the time.
   e. Click **Apply**.

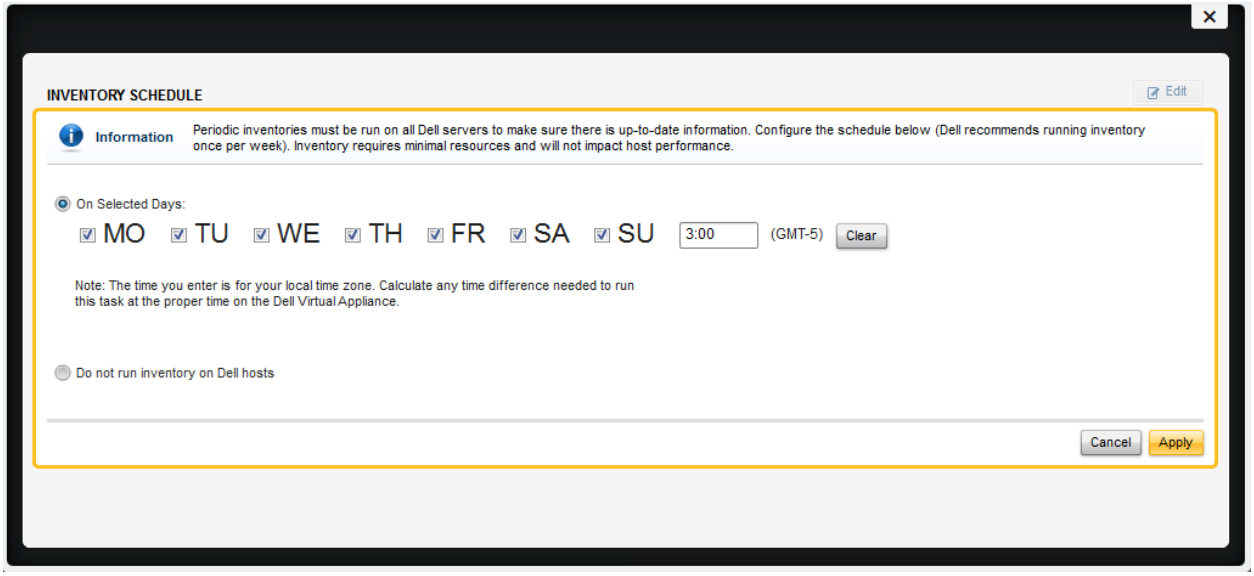

Figure 13 Change Inventory Schedule

2.2.2 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** 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.

2.2.3 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.

2.2.4 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.

2.3 Compliance issues

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

2.3.1 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 view non-compliant hosts:

1. Click **View Details** below **Non-compliant vSphere Hosts** on the **Overview** page as shown in Figure 15.

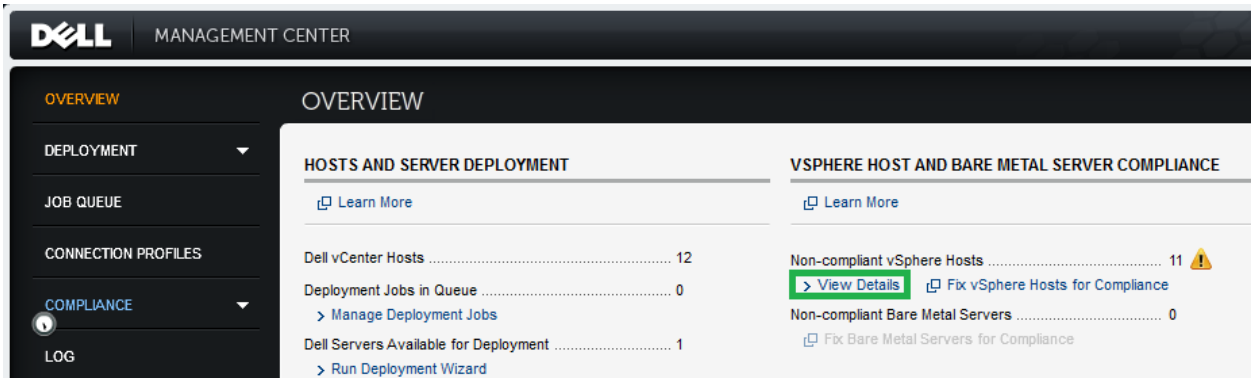

Figure 14 View Non-compliant hosts from Overview page

2. Click **vSphere Hosts** or **View non-compliant vSphere Host** Details on the Compliance page as shown in Figure 18.

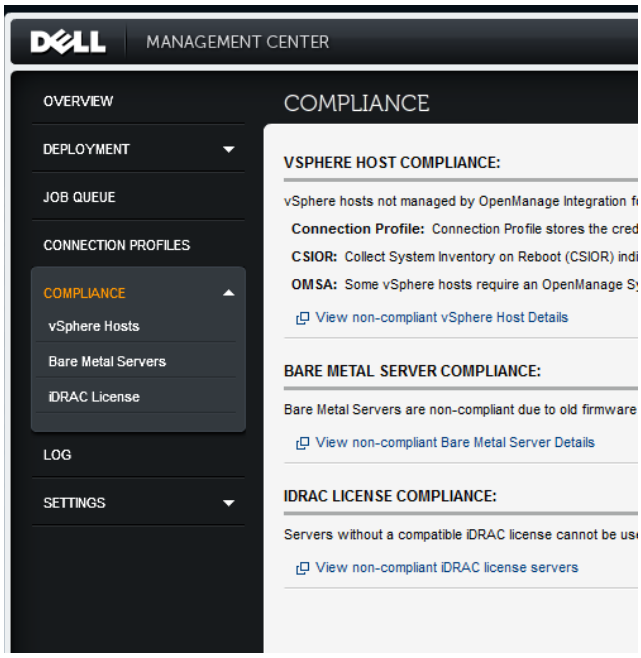

Figure 15 View non-compliant hosts from Compliance page

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

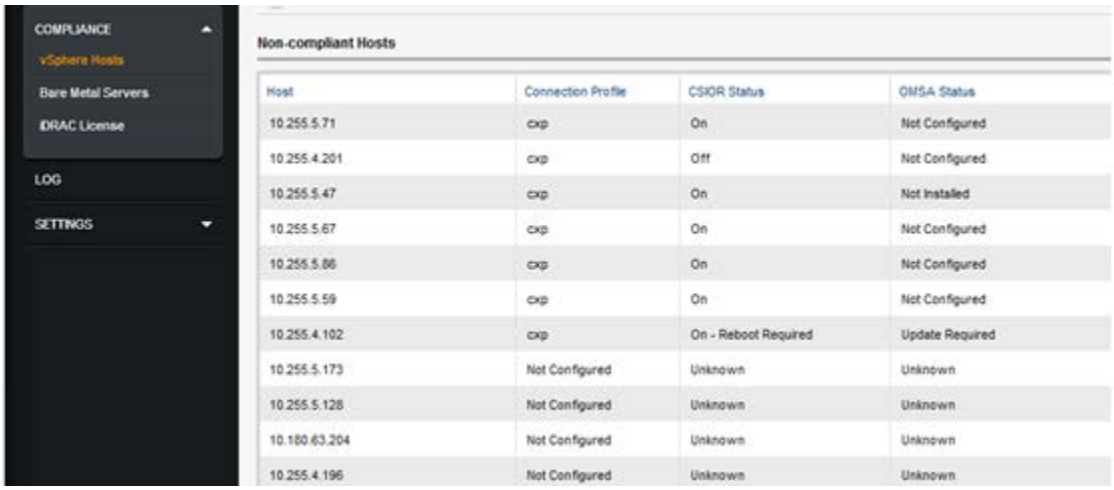

Figure 16 Example of non-compliant hosts

Due to security restrictions pertaining to Lockdown Mode, OpenManage Integration for VMware vCenter 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.

2.3.2 Fixing non-compliant hosts

OpenManage Integration for VMware vCenter 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 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:

1. Click **Fix non-compliant vSphere Hosts** on the **vSphere Hosts** page (alternatively, you can click **Fix vSphere Hosts for Compliance** on the **Overview** screen). The compliance wizard **Select Hosts** screen displays.

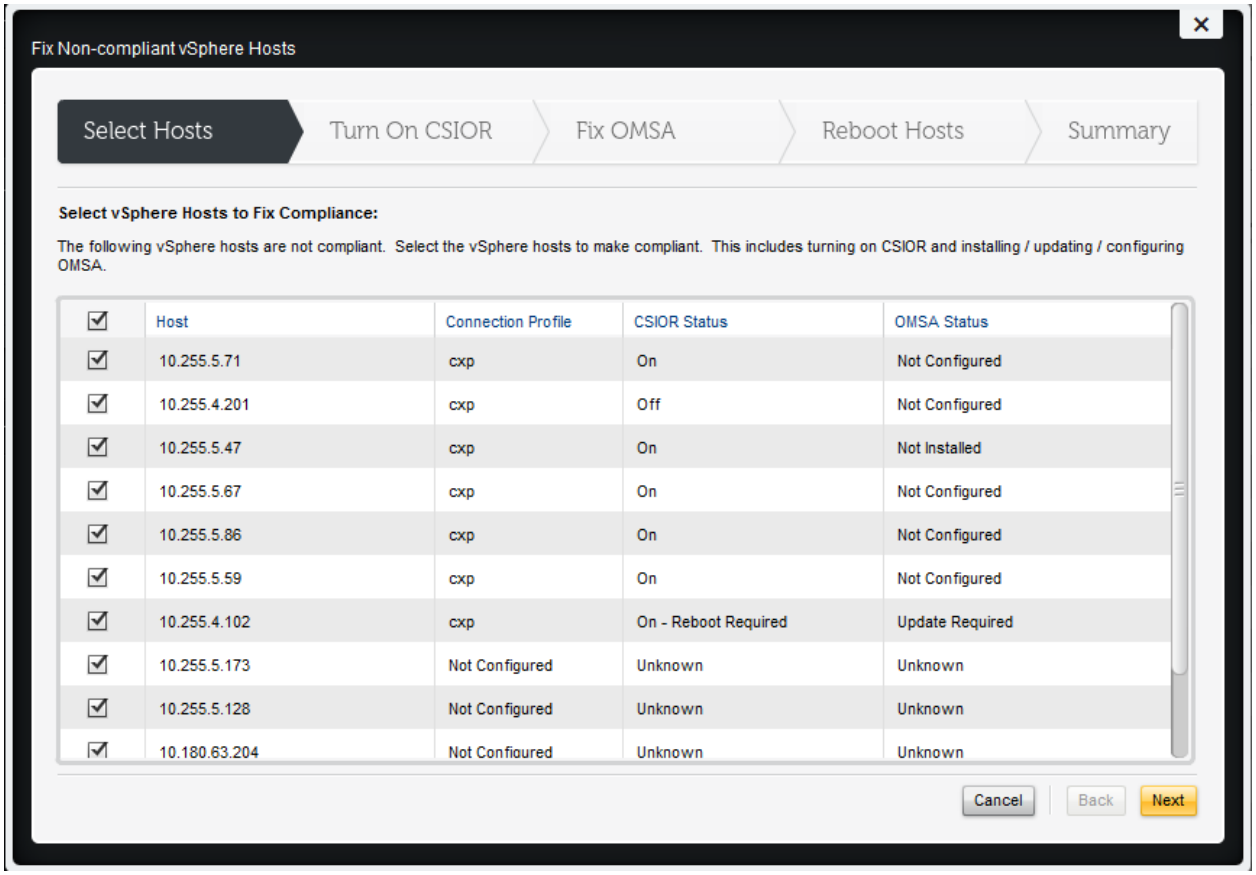

Figure 17 Host Compliance Wizard - Select Hosts

2. Select the hosts you want to fix on the Select Hosts page using the checkboxes on the left column. Click **Next**.

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.

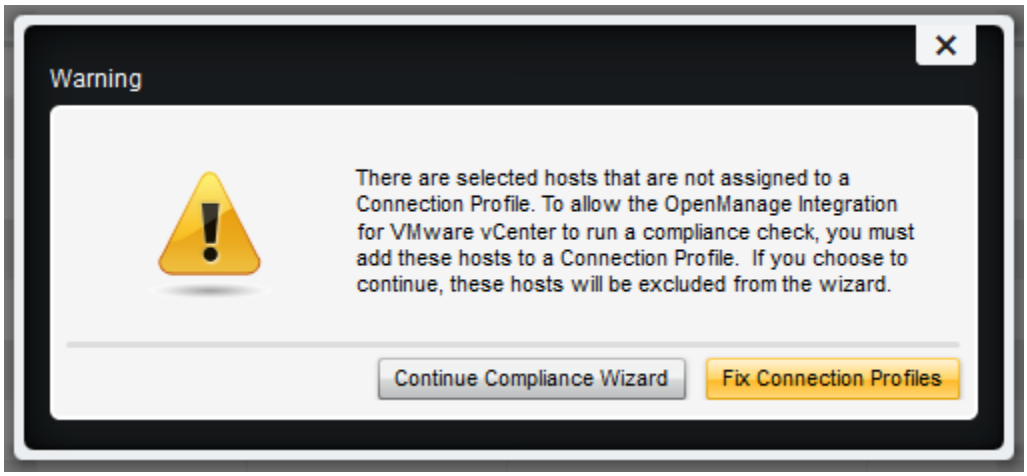

Figure 18 Host Compliance Wizard - Fix Connection Profile Warning

Click **Fix Connection Profiles** to proceed to the Connection Profiles screen.

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

3. 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.

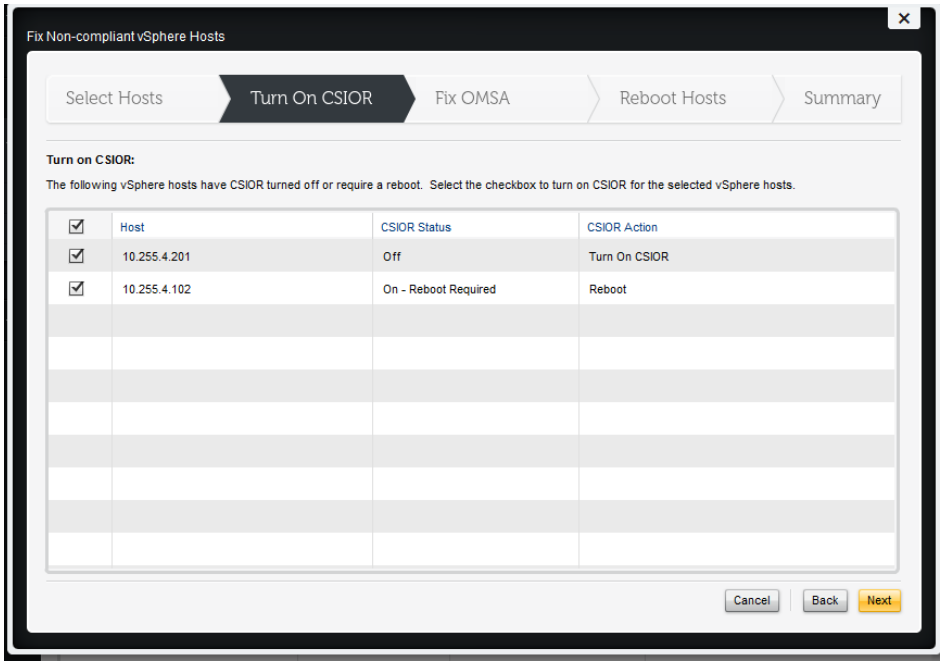

Figure 19 Host Compliance Wizard - CSIOR

4. Next you will be shown hosts (from the hosts you selected in Step 2) that are non-compliant due to OMSA state on the **Fix OMSA** page. Select hosts to fix OMSA state and click Next. See *Fixing OMSA issues* for details.

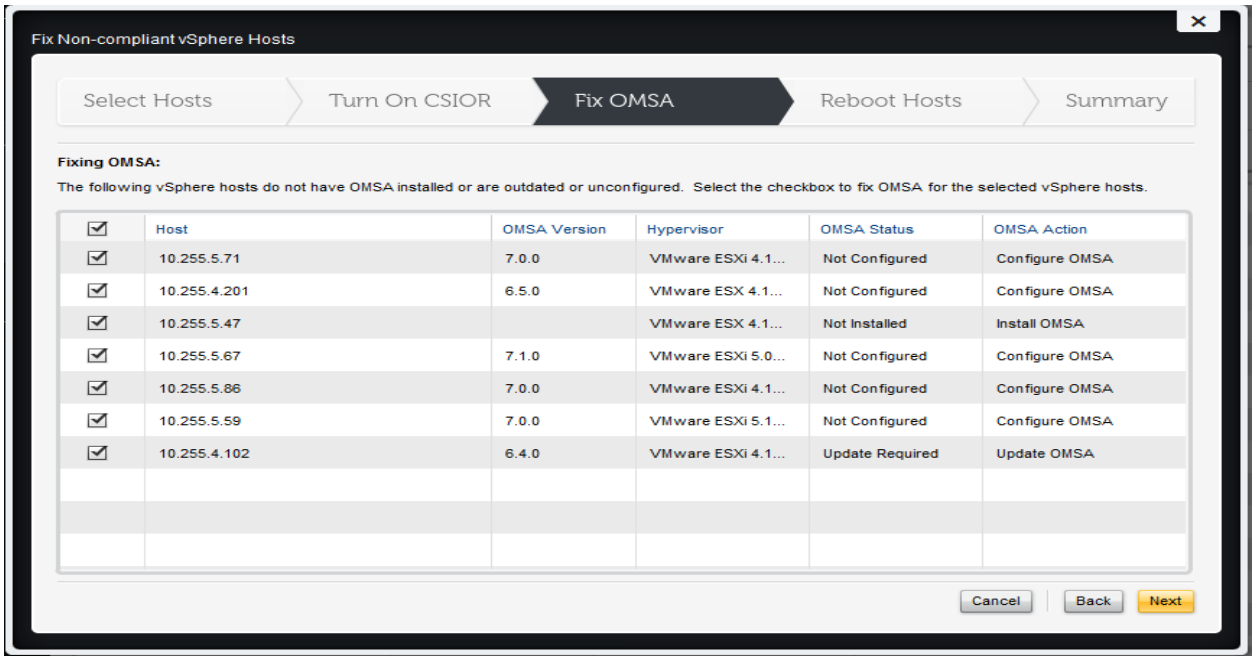

Figure 20 Host Compliance Wizard – OMSA

5. If you have selected hosts that may need reboot either while fixing OMSA or CSIOR, the Reboot Hosts screen displays with 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**.

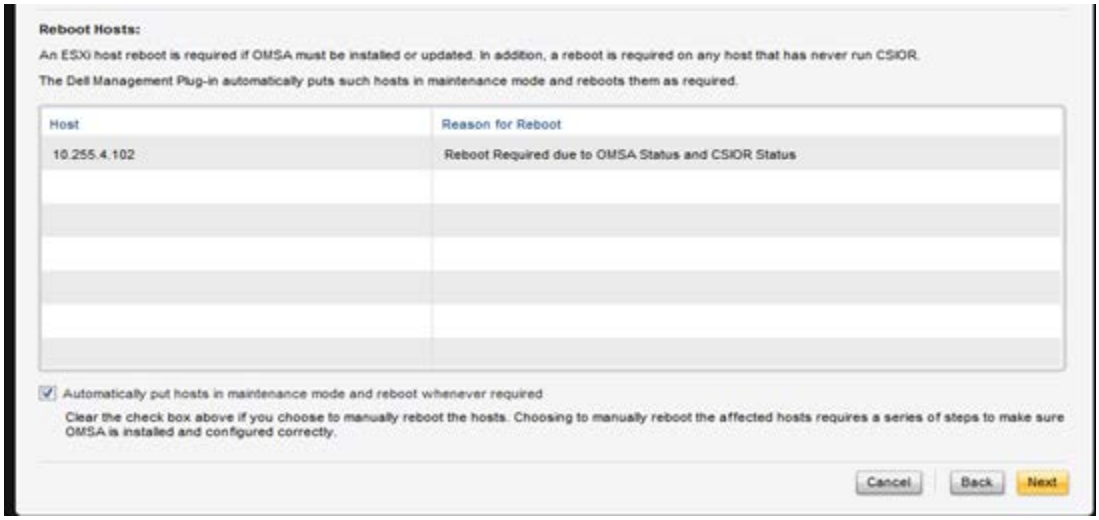

Figure 21 Host Compliance Wizard - Reboot Hosts

6. The **Summary** screen summarizes the actions that will be performed to correct compliance. Click **Finish** to initiate the fix process. You can go back and change your selections using the **Back** button.

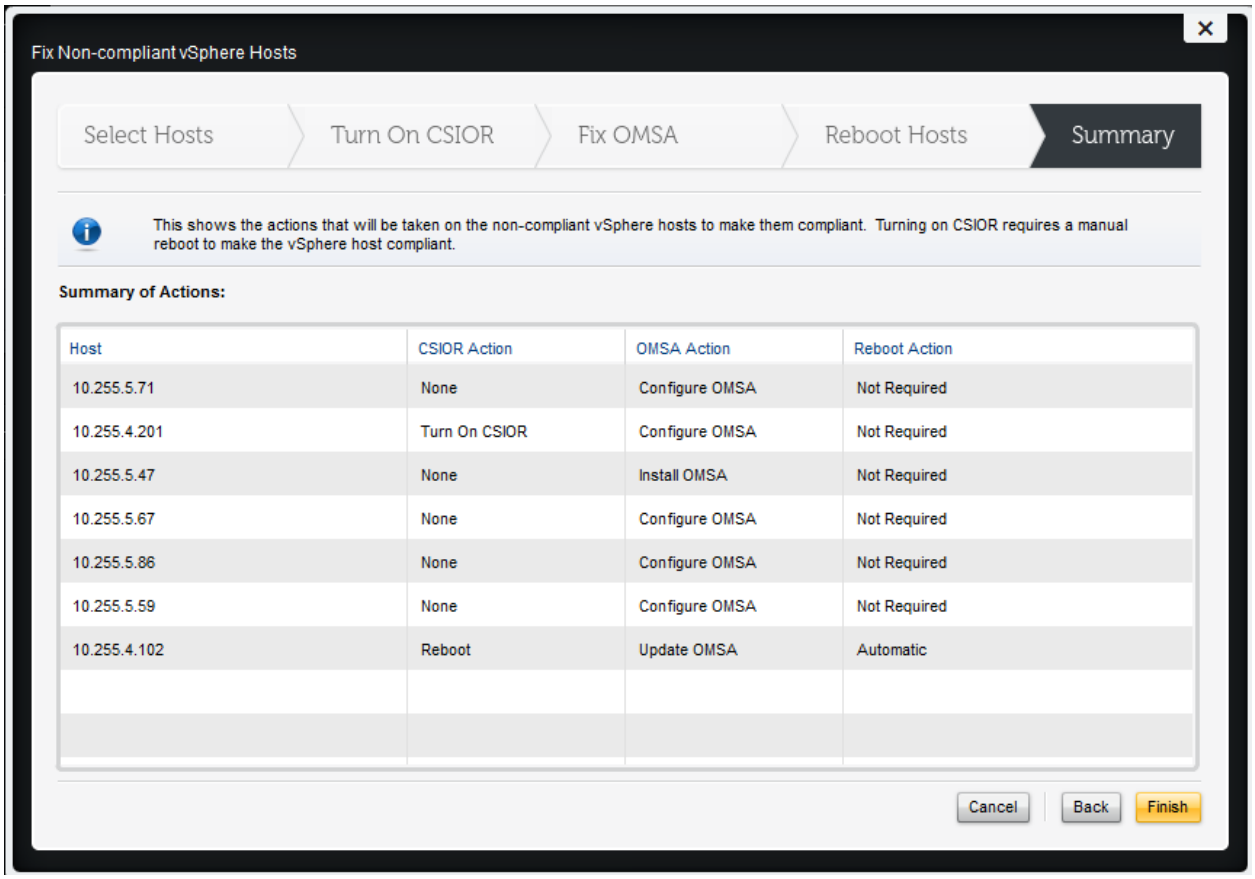

Figure 22 Host Compliance Wizard – Summary

2.3.3 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, a file on the host operating system is configured to send SNMP traps.

OpenManage Integration for VMware vCenter 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 Upate1.

2.3.4 Common failures while fixing OMSA

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

2.3.5 Fixing CSIOR issues

CSIOR is an iDRAC feature which needs to be ON to collect 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 checkbox to reboot hosts in the Reboot Host screen of the host compliance wizard.

2.3.6 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".

3 Conclusion

Now that you have successfully set up your Dell Servers and they are ready to be managed from your vSphere Client, you can start using the Dell Server Management tab to access desired management features. More information on this may be found in OpenManage Integration for VMware vCenter User's Guide.