Update Dell™ Server Hardware with Dell OpenManage Essentials

This Dell Technical White Paper addresses the maintenance and enforcement of hardware revision baseline within a datacentre environment using Dell OpenManage Essentials.

Authors:

Lakshmi.K.S

Pavana Subbarao

Nitin Bhambere

Vineeth Valambra

Dell Enterprise Product Group

This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

© 2011 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell, the Dell logo, and PowerEdge are trademarks of Dell Inc. Intel and Xeon are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft, Windows, and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.

November 2012| Rev 1.1

Contents

Figures

Executive Summary

This white paper describes the process of maintaining and enforcing a hardware revision baseline within the Dell PowerEdge server environment using OpenManage Essentials.

This document explains the process to update servers without forcing an unplanned shutdown. Using OpenManage Essentials, IT administrator can keep the servers up to date without affecting the production environment. You can use a single console to update multiple Dell servers.

Introduction

IT Administrators face many challenges today, which include managing system updates (BIOS, firmware, driver) in the customer datacentre. Administrators find it challenging to keep track of new versions of firmware and drivers, which are released at frequent intervals.

This white paper explains how an IT Administrator can overcome the obstacles that come with managing system updates by using Dell OpenManage Essentials. This document includes:

- Deploying System Updates along with OMSA agent
- Obtaining the latest versions of drivers, firmware, and BIOS
- Determining the servers that should be updated and their respective packages (DUPs)
- Updating the hardware at the convenience of IT Administrator.

Obtaining the latest version of update packages

You must import the latest catalog.cab file to obtain the latest version of drivers, firmware, and BIOS. You can import the catalog from three different sources provided by Dell: Dell Server Update Utility (SUU) DVD, Dell FTP, and Dell Repository Manager (RM).

Figure 1. Select a catalog source

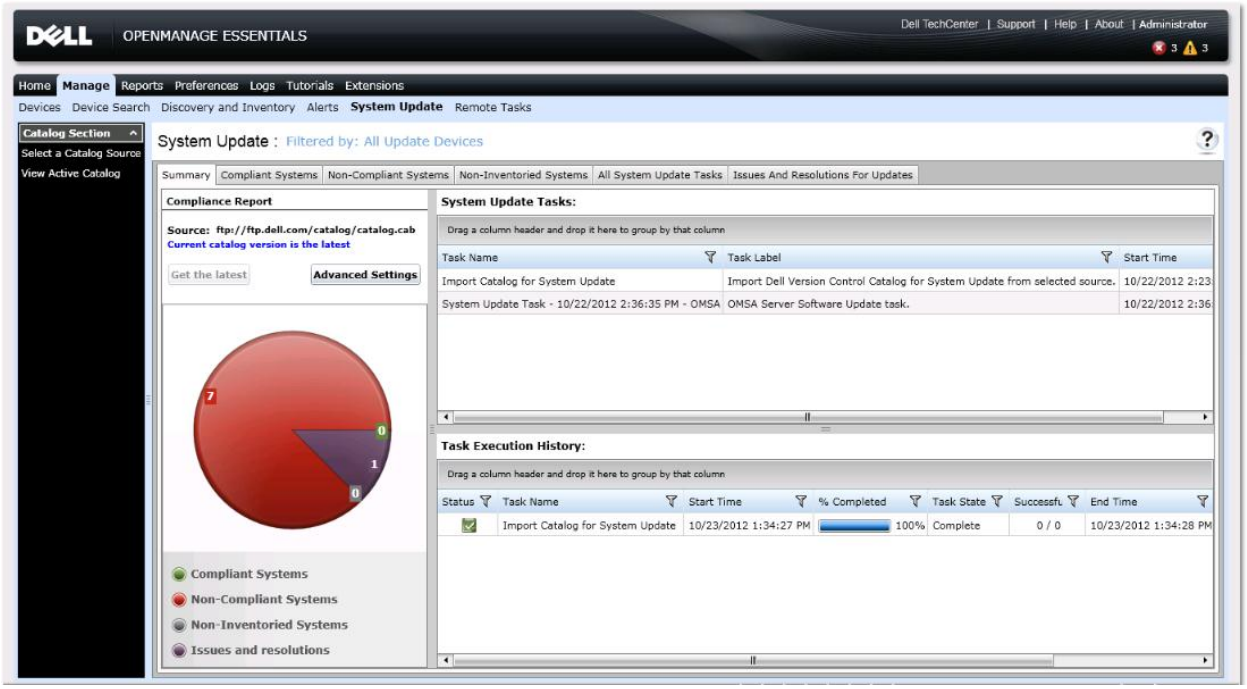
- **Dell Server update utility**: Dell server update utility DVD to import catalog. You can obtain the latest version of Dell SUU from support.dell.com. Dell recommends using this utility when Internet access is not available on the server where OpenManage Essentials is installed.

    1. Mount SUU DVD or iso image
    2. Launch OME console
    3. Navigate to Manage -> System update
    4. Click on “Select a catalog source”
    5. Select a catalog source windows is displayed – Select “Use file system source(SUU)” option
    6. Click on browse and navigate to the location where SUU is located
    7. Select catalog.xml or catalog.cab file located in the repository folder of SUU
    8. Click Import now to import catalog.

- **Dell FTP (Recommended):** Dell recommends using the Dell FTP site as the source if the Internet is accessible. Dell uploads the latest releases of firmware, drivers or BIOS on the FTP site so that the latest catalog is always available.

The **Get the Latest** button is automatically activated when a new version of catalog is posted on Dell FTP. To obtain the latest catalog, go to **Manage>System Update>Summary** and then click on the **Get the Latest button.**

Figure 2. Import latest Dell FTP catalog



To import catalog from FTP, configure proxy settings under the **Preferences** tab.

- **Dell Repository Manager:** Dell Repository Manager is a separate tool that you can install from the OpenManage Essentials installation package. With this tool you can create a custom repository to match required server model. Operating System and components to update.

  Here are the steps

  1. Discovery/Inventory Servers and iDRAC (using appropriate protocols) in OME
  2. Launch Dell Repository Manager (server).
  3. Click on Create and Choose Dell OpenManage Essentials Repository
  4. Enter name and description, click Next
  5. Choose Dell online repository , click Next
  6. Repository Manager will get OME inventory and all the devices are displayed in Repository Manager

7. Click next
8. Choose save and download repository and click Finish
9. Choose the location to save catalog and DUPs

Determining the servers that should be updated and their respective packages (DUPs)

- ### In-Band System Update along with OMSA agent

In-Band system update uses Operating System [Windows/Linux] environment to update Dell PowerEdge Server. The OS and OpenManage Server Administrator (OMSA) should be installed on Dell PE Server. It is recommended to IT Administrator to use In-Band System Update on Managed node with OS and OMSA installed.

To see the updatable servers in the datacentre, discover and inventory the server. Then you must import the baseline catalog. Discovered servers should have Dell OpenManage Server administrator installed on them. Discovered servers should also be classified under 'Servers' in the All Devices tree, under the Manage>Devices menu. Dell servers should be discovered using SNMP or WMI protocols only.

During a catalog import, the installed version of server packages is compared with the available version of packages in the baseline catalog to determine the updatable packages on the respective server. A comparison report is generated and the servers are classified as Compliant Systems, Non-Compliant Systems, or Non-Inventoried systems.

1. The servers that have the same versions of BIOS, Drivers and Firmware as that of the imported catalog are classified as "Compliant systems".
2. Servers which require BIOS, firmware or driver updates are classified as "Non-compliant Systems". This report also displays the level of importance of each applicable package (for example: critical, recommended, and optional packages). Refer to "Figure 4: Non-Compliant Report".
3. For the servers to be classified as compliant or non-compliant, installed package version information is available. This information is available in the "Software inventory information" table under the Device details (Refer to "Figure3: Software Inventory Information Table"). This table is populated when the server is inventoried. Servers which require inventory to be performed are classified under "Non-Inventoried Systems". You can run the server inventory task from this tab if necessary.

Figure 3. Software Inventory Information Table

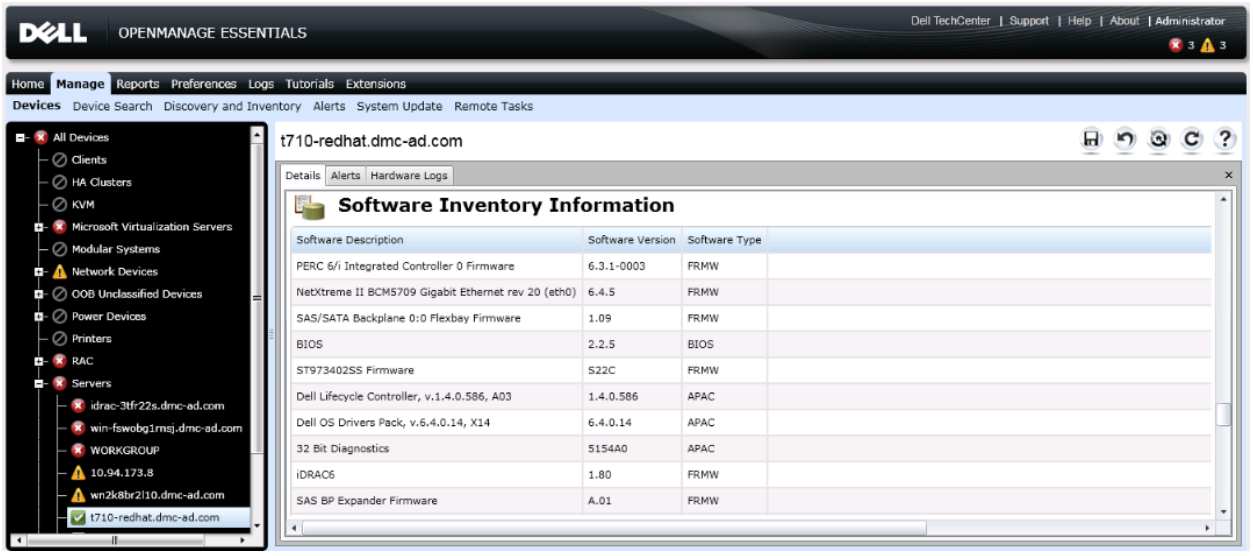
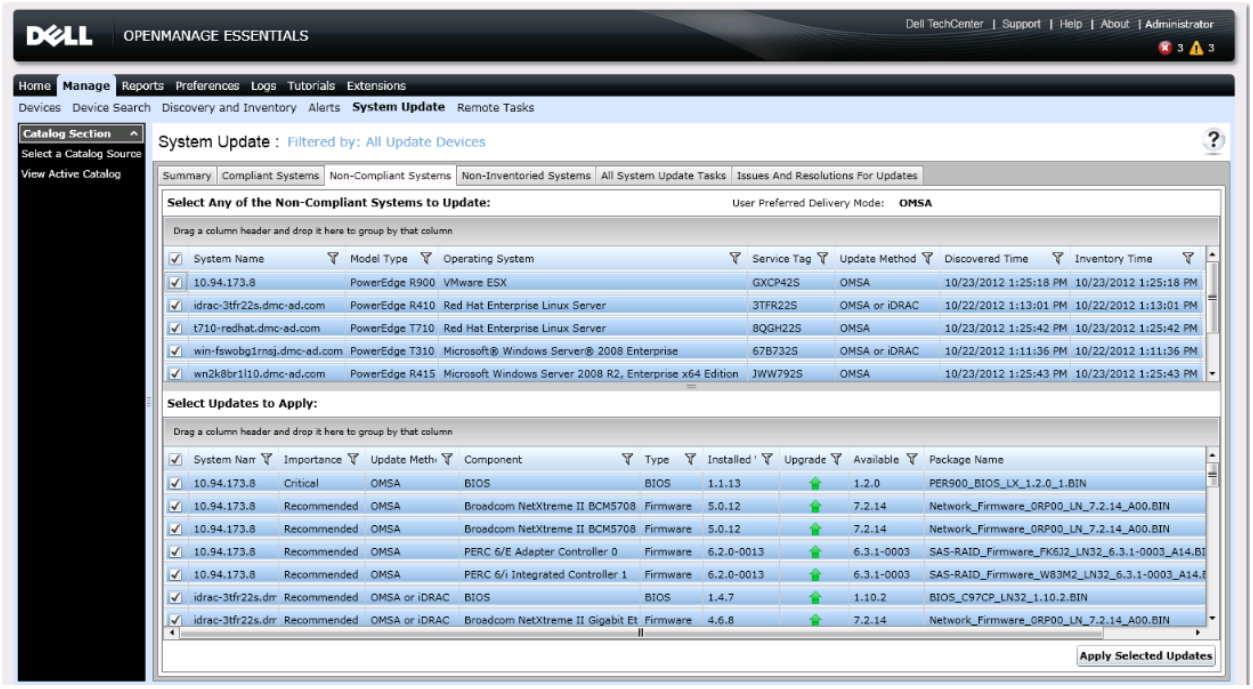


Figure 4. Non-Compliant Report



Updating the hardware at the convenience of IT Administrator

You must create a system update task and schedule to apply applicable updates to the non-compliant servers. Refer to “Figure 5: Create System Update Task” to view the update task creation page.

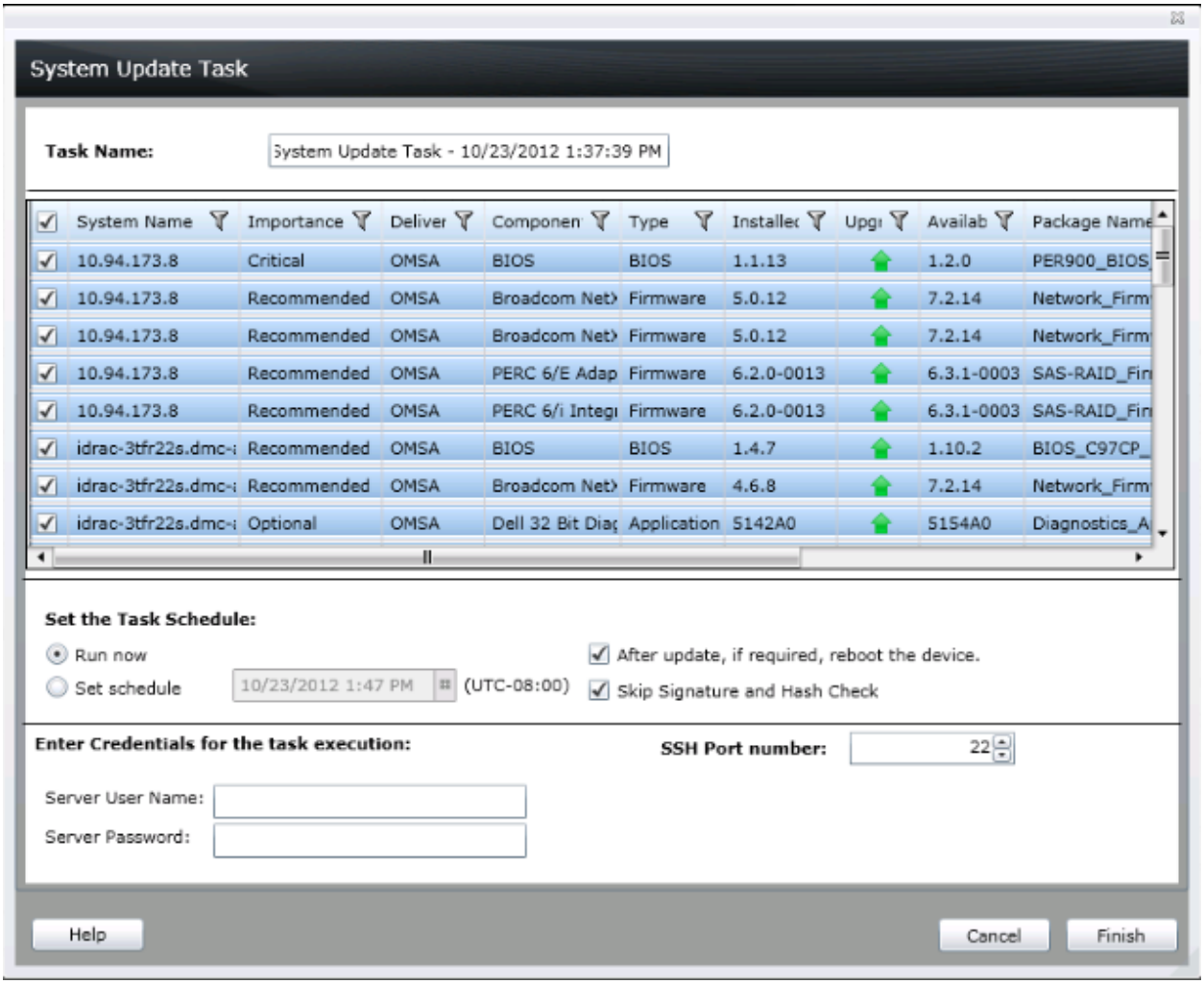
- **You can select various combinations to update servers:**
  - *Single update on a single server:* You can select one package to be applied on an individual server.
  - *Multiple update on a single server:* You can select all packages (BIOS, Drivers and Firmware) to be applied on an individual server using a single update task.
  - *Single update on multiple servers:* You can select one package applicable to multiple servers to be applied on multiple servers. Example: If there are 10 Dell PowerEdge R515 servers that require a BIOS update, then the update can be applied on all the 10 servers using a single task. All 10 servers must have the same credentials for the task to run successfully.
  - *Multiple updates on multiple servers:* You can select all applicable packages on multiple servers to be applied using a single task. All servers being updated using the task must have the same credentials for the task to run successfully.

    Note: You cannot update Windows and Linux servers in a single task.

- **Reboot device option:**
  - Packages like BIOS, Network firmware, storage controller firmware and drivers PERC, and SAS require a system reboot for the update to be successful. By default, the Reboot option is enabled in an update task. If you do not want to reboot at the time of update, you can uncheck this option and you can manually reboot the servers later during non-working hours. In this case, the updates are applied to the servers but the process is not complete until the server is rebooted.

- **Skip Signature Hash Check**:
  - Select this option to skip the signature and hash check on the system update package.

Figure 5. Create (In-Band) system update task



Once the update task is complete, OpenManage Essentials inventories the updated servers. Comparison between the installed packages version and baseline catalog are automatically completed and the servers are classified as compliant or non-compliant systems accordingly. The System Update functionality of OpenManage Essentials ensures that an IT Administrator can always be aware of the status of servers in the data-centre environment.

When BIOS, drivers, firmware and application packages are selected for updates on a server, packages are applied in the following order:

1. Drivers
2. Firmware
3. ESM firmware
4. BIOS
5. Application

During the system update process, packages are downloaded from the selected source and saved under the “Packages” folder under the “Essentials>System update” folder (C:\Program Files (x86)\Dell\SysMgt\Essentials\SystemUpdate\Packages).

Supported models for system update

Using OpenManage Essentials, you can update the following:

- All 8th generation and above servers
- Dell monolithic and modular servers
- All rack, tower, and blade servers
- Chassis(PowerEdge M1000e)

Table 1. Supported server models

Supported Server Model	
8G PowerEdge Servers	PE800, PE830, PE840, PE1800, PE2800, PE6800, PE6850
9G PowerEdge Servers	PE1900, Pe1950, PE2900, PE2950, PE2970, PE6950
10G PowerEdge Servers	R900, R905, R805, R200, T605, T300, T105, T100, M600, M605
11G PowerEdge Servers	R210II, T110II, R415, R515, R715, R310, R910, R810, R710, R610, T710, T610, T410, R410, T310, T110, R210, R510, M7610x, M710HD, M910, M710, M610, M915
12G PowerEdge Servers	T420, T320, R520, R420, R320, R820, R720, R620, T620, M820, M420, M520, M620

Dell OpenManage Server Administrator (OMSA)

Dell™ OpenManage Server Administrator (OMSA) is a software agent that provides a comprehensive, one-to-one systems management solution in two ways: from an integrated, Web browser-based graphical user interface (GUI) and from a command line interface (CLI) through the operating system. OpenManage Server Administrator is designed so that system administrators can manage server systems both locally and remotely on a network.

To learn more about Dell OpenManage Server Administrator (OMSA):
http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.aspx

Installing or Upgrading OMSA agent using OpenManage Essentials

You can use Dell™ Open Manage Essentials (OME) to install or update the OMSA agent on multiple Dell PowerEdge servers. Server can have Windows or Linux operating system.

Note: Deploying OMSA VIB on ESXI servers is not supported.

Prerequisites of OMSA install or upgrade

To manage any server from OpenManage Essentials it needs to be discovered using the relevant protocol.

1. Every server must have the relevant protocol enabled/configured. The protocol used for discovery is dependent on the operating system of the managed server.
   For more details about protocol configuration, refer to:-
http://en.community.dell.com/techcenter/extras/m/white_papers/20061808.aspx

2. Discover the server in OpenManage Essentials using the protocol configured.
   On discovery, server is classified under 'Unknown' if it does not have the OMSA agent installed else the server is classified under the 'Servers' group in the device tree.
   For more details about discovery and inventory configuration, refer to:-
http://en.community.dell.com/techcenter/extras/m/white_papers/20061803.aspx

3. Download the OMSA package form Dell Support site (http://support.dell.com/).

4. Configure the firewall, if enabled, on both the OpenManage Essentials machine as well as the server to be updated.
   To configure the firewall:

   A. On the OpenManage Essentials machine, open TCP port 135.

   B. Add the application "omremote.exe" (located in Essentials\bin to the firewall exception list).

C. On the managed system that you are going to update, run the following command using the command prompt on a Windows managed system: "**netsh firewall set service RemoteAdmin**".

For more information on connecting through the Windows firewall, see Microsoft's MSDN website for Platform SDK: Windows Management Instrumentation (Connecting through Windows Firewall) at
http://msdn.microsoft.com/en-us/library/aa389286(VS.85).aspx
http://support.microsoft.com/kb/875605

For Windows Server 2008 onwards, see the following link:
http://msdn.microsoft.com/en-us/library/aa822854(VS.85).aspx

For Linux:
http://www.physics.umd.edu/pnce/user-docs/Linux/firewall.html

Package types supported for OMSA agent install

On a server that is running a Windows based operating system, the Sysmight.msi OMSA package type is supported for installation. This package is available at the Dell Support site as an executable, which you have to extract.

After extraction, by default, Systemgmt.msi is available at "C:\OpenManage\windows\SystemsManagement\" The package is also available with the Dell™ OpenManage System Build and Update Utility (SBUU) DVD. You can use this package for installation and upgrade of the Dell OMSA agent.

Package types supported for OMSA agent upgrade

On a server running Windows based operating system, the following OMSA package type is supported for upgrade:

- OM-SrvAdmin-Dell-DUP-WIN-****.exe

  This package is available on the Dell Support site and Dell™ OpenManage Server Update Utility (SUU) DVD.

  You can use this package to update the Dell OMSA agent only with the following upgrades paths:
  - 5.5 >> 6.0
  - 6.x >> 6.5
  - 6.5 >> 7.x

  This package is only used for upgrading the Dell OMSA agent.

- OM-SrvAdmin-Dell-SP-WIN-****.exe

This package is available on the Dell Support site. You can only use this package for upgrading OMSA agent from N to N+1 version; for example, upgrading OMSA version 6.4 to 6.5.

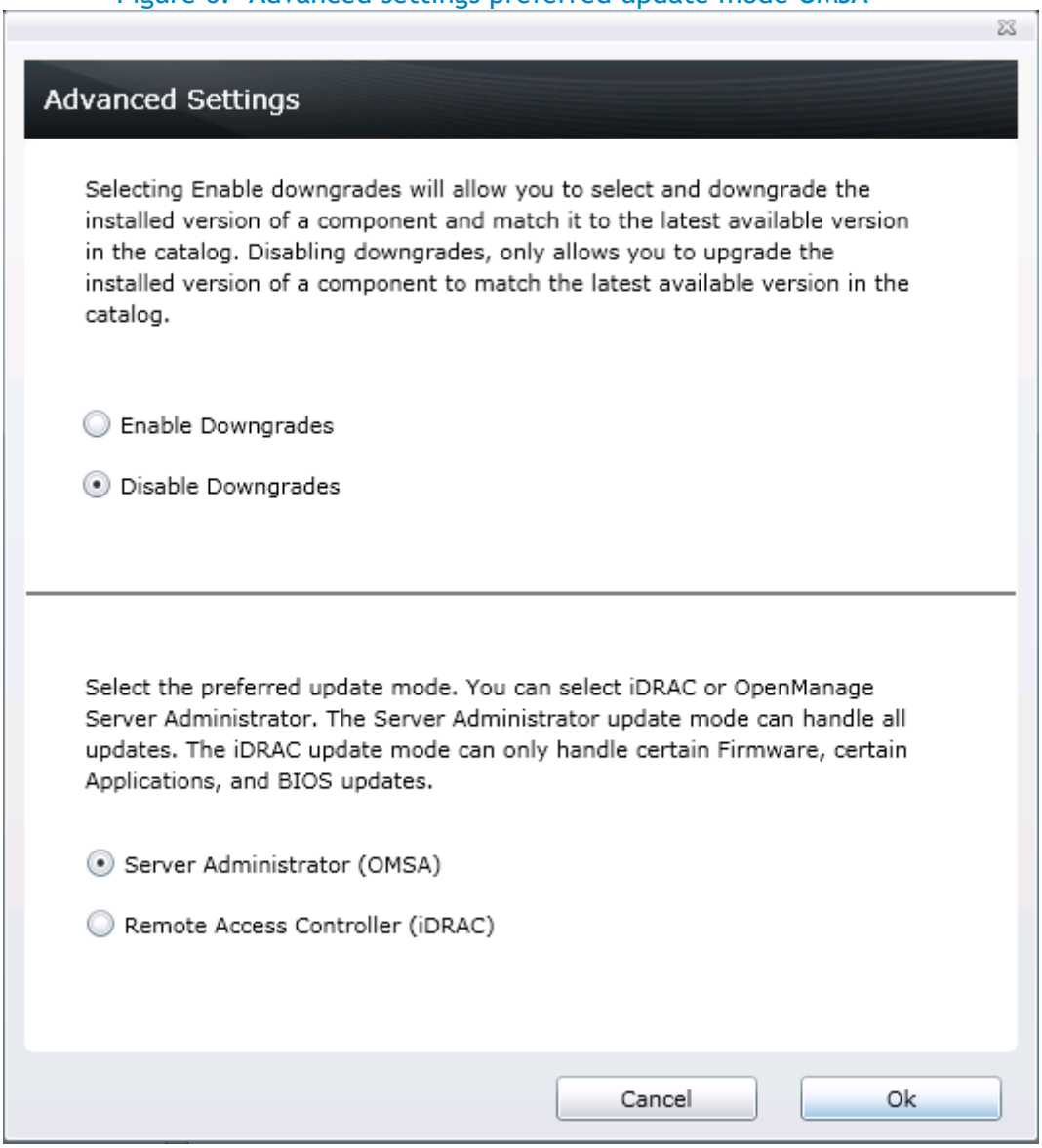
For more information about how to install/Upgrade OMSA using OpenManage Essentials, refer to “Deploying Server Administrator using OpenManage Essentials” white paper.

Updating System via OpenManage Server Administrator

1. Enable OMSA update mode from advanced settings

   Go to System Update →Summary → Advanced Settings → Enable “Server Administrator (OMSA) mode.

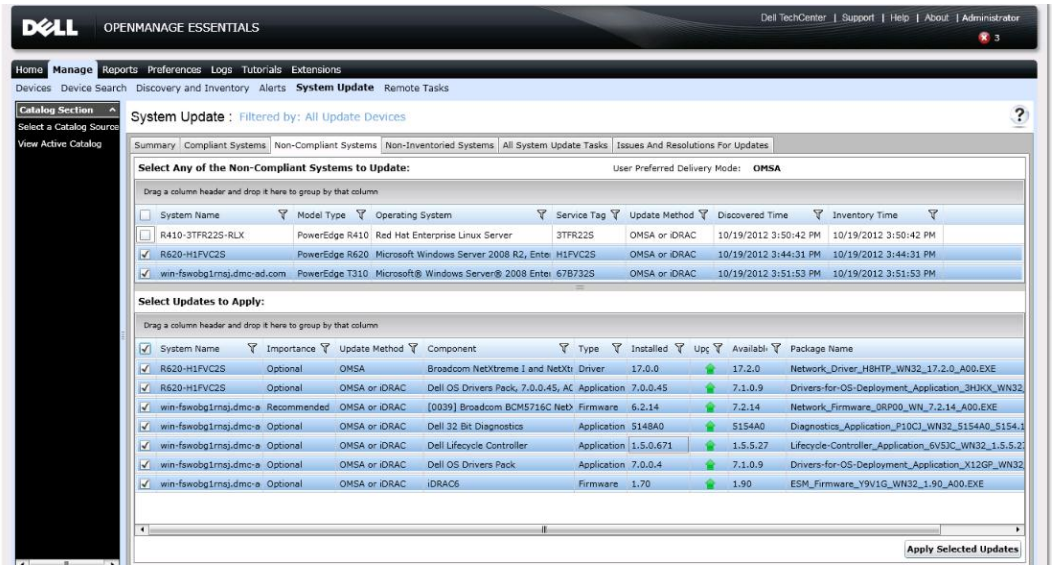
Figure 6. Advanced settings preferred update mode OMSA



2. Select Non-Compliant Systems to update.

   Go to System Update →Non-Compliant Systems →Select Systems from “Select Any of Non-Compliant Systems to Update:”

Figure 7. Non-Compliant Systems



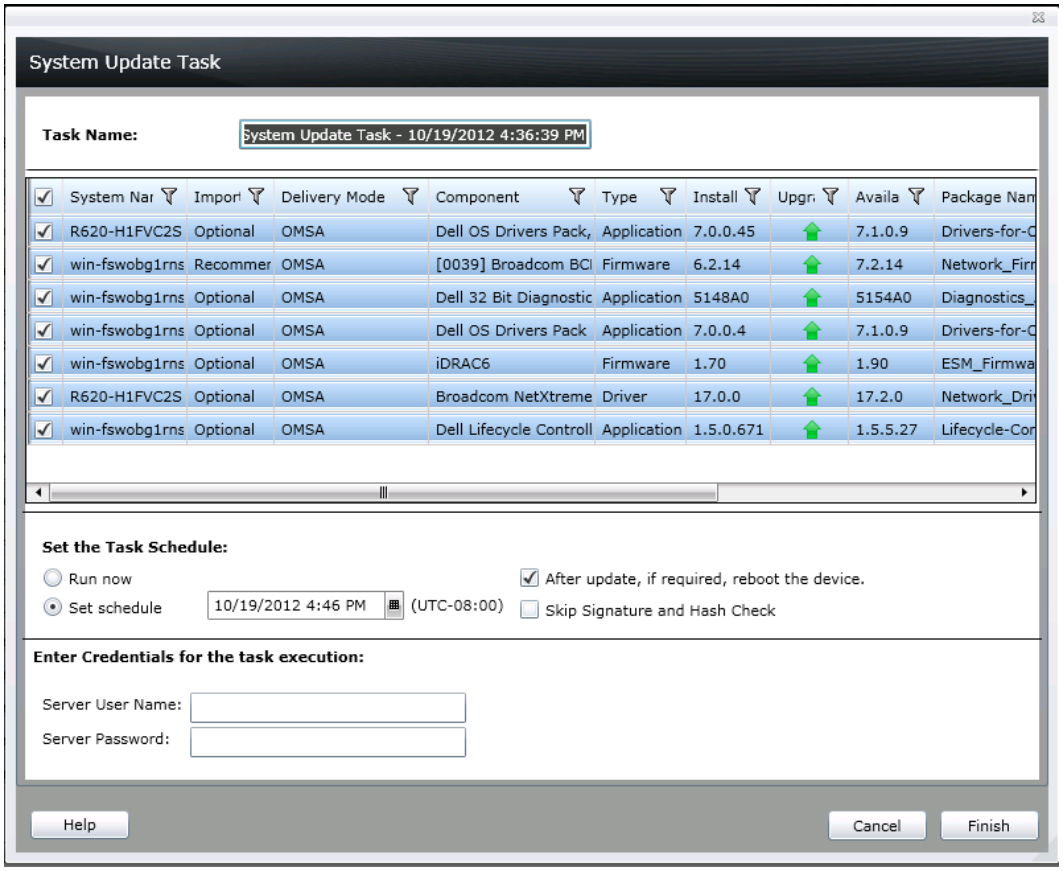
Note:

- User Preferred Delivery Mode OMSA.
- Update Method for Selected Systems – OMSA or iDRAC.
- Update Method for Selected Components – OMSA or iDRAC & OMSA.

3. Create an OMSA update mode System update task.
4. Select available components to update from “Select Updates to Apply:” (BIOS, Firmware, Drivers and Applications), Select “Apply Selected Update” button

5. Enter Task name, set the task schedule – Choose Run now or Set Schedule option, Select "After update, if required, reboot the device" and "Skip Signature and Hash Check" check box. Enter Server User name & Password. Click on "Finish" button. System update OMSA task will be created and completed.

Figure 8. Create OMSA delivery mode system update task



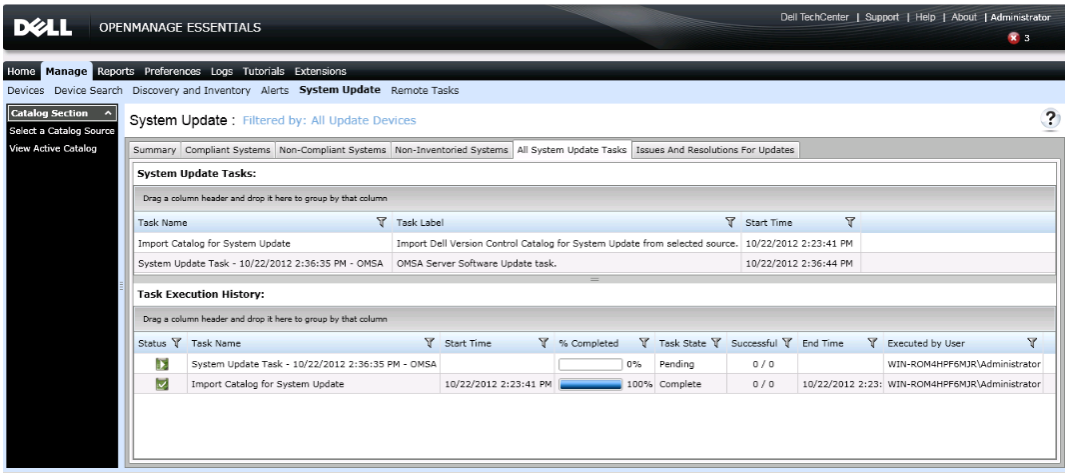
Note:

- Delivery Mode – OMSA.
- Updatable components BIOS, Firmware, Drivers & Applications.
- Server Credentials asked.
- All above packages can be updated using OMSA update mode.

6. View the System update task status.

    - System Update → Summary →Task Execution History: OR
    - System Update → All System Update Tasks →Task Execution History:

Figure 9. System Update Task (OMSA) Execution Status



Note: On completion of system update task the Task State set to Completed, an auto inventory task is run after 20 minutes to fetch updated inventory data.

Agent Free System Update - Out Of Band System Update without OMSA agent

Out Of Band system update uses iDRAC with Life Cycle controller mechanism to update Dell PowerEdge servers. Out Of Band system update is useful for IT administrator when there is managed PE server with/without Operating System and without OpenManage Server Administrator (OMSA).

Agent free system update in OME does not need OS and OMSA on the managed system to gather inventory and deploy firmware and BIOS updates. Agent free updates are applied via Integrated Dell Remote Controller (iDRAC6/iDRAC7) on 11G and 12G Servers.

Prerequisities for Agent free(iDRAC) System Updates.

1. 11G servers
   - Modular : Minimum iDRAC6 firmware version 2.20 and higher
   - Monolithic : Minimum iDRAC6 firmware version 1.40 and higher
2. 12G servers
   - Express or Enterprise license
3. iDRAC is discovered and inventoried using Ws-Man protocol

   For more information on iDRAC

   http://content.dell.com/us/en/enterprise/d/solutions/integrated-dell-remote-access-controller-idrac.aspx

Updating System via Intergrated Dell Remote Access controller

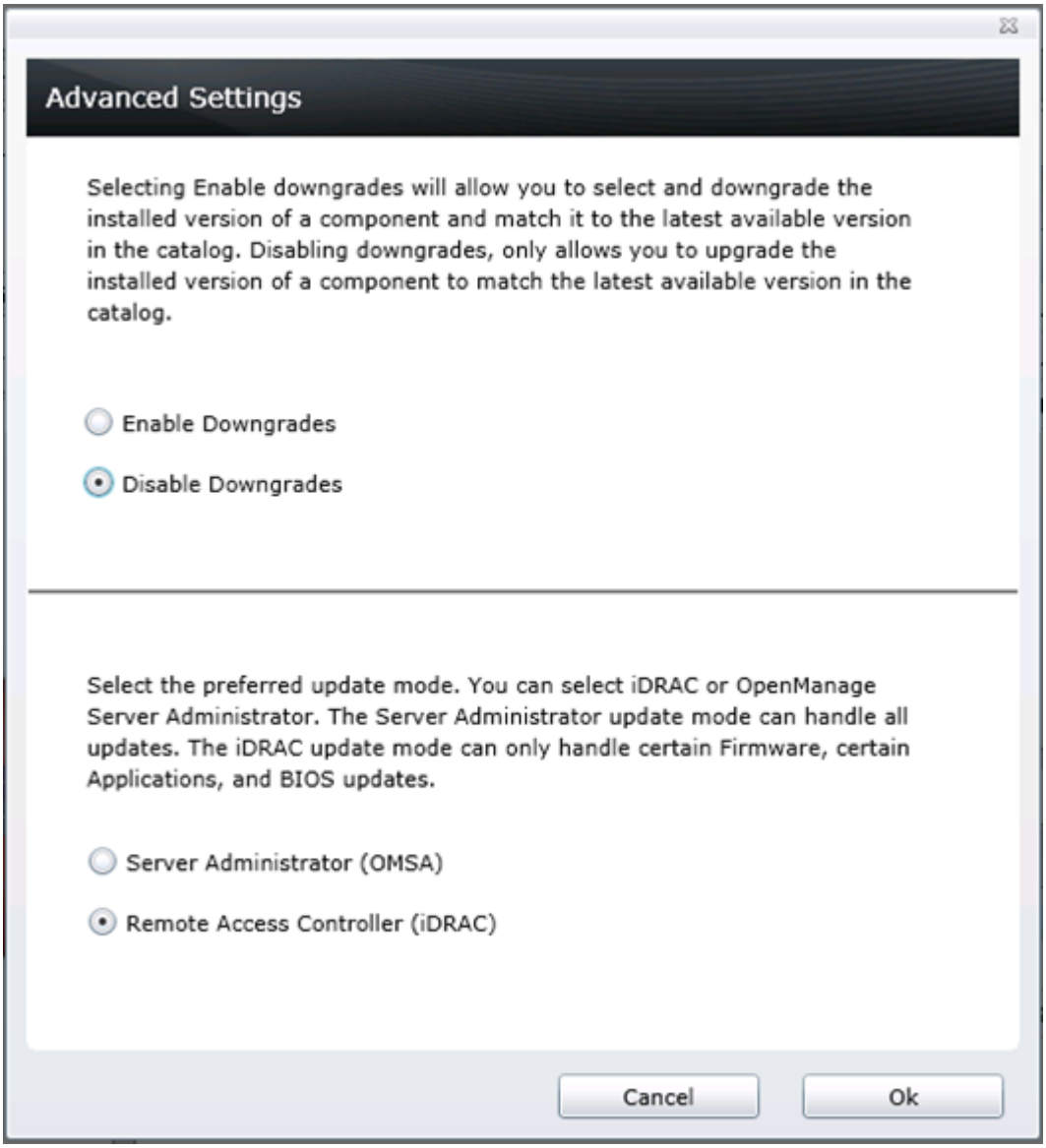
The following updates can applied via iDRAC

- BIOS
- Firmware
- Applications (Dell 32 Bit Diagnostics, Dell Life Cycle Controller.)

1. Discover and Inventory of iDRAC6/iDRAC7 using WS-Man protocol –
2. Navigate to Manage > Discovery and Inventory >Add discovery range.
3. Add iDRAC6 and iDRAC7 IPs. Click Next and Deselect SNMP protocol.
4. Click Next select Enable WS-Man Discovery, enter USERID, Password, Select “Secure Mode” Check box, and Select “Skip Common name check and “Trusted Site” check boxes
5. Click Next, On Discovery Range Action page select “Perform both discovery and Inventory.
6. Click Finish.
7. Navigate to Manage > Devices. Verify that the device is discovered and classified under RAC device group.

   Note: Discovered iDRAC will be either present under compliant or non-compliant systems section in the compliance pie-chart.
8. Click on “Advanced Settings”. Set preferred update mode to “Remote Access Controller (iDRAC)” Click OK to save the settings and close the “Advanced Settings” window

Figure 10. Advanced Settings preferred update mode iDRAC

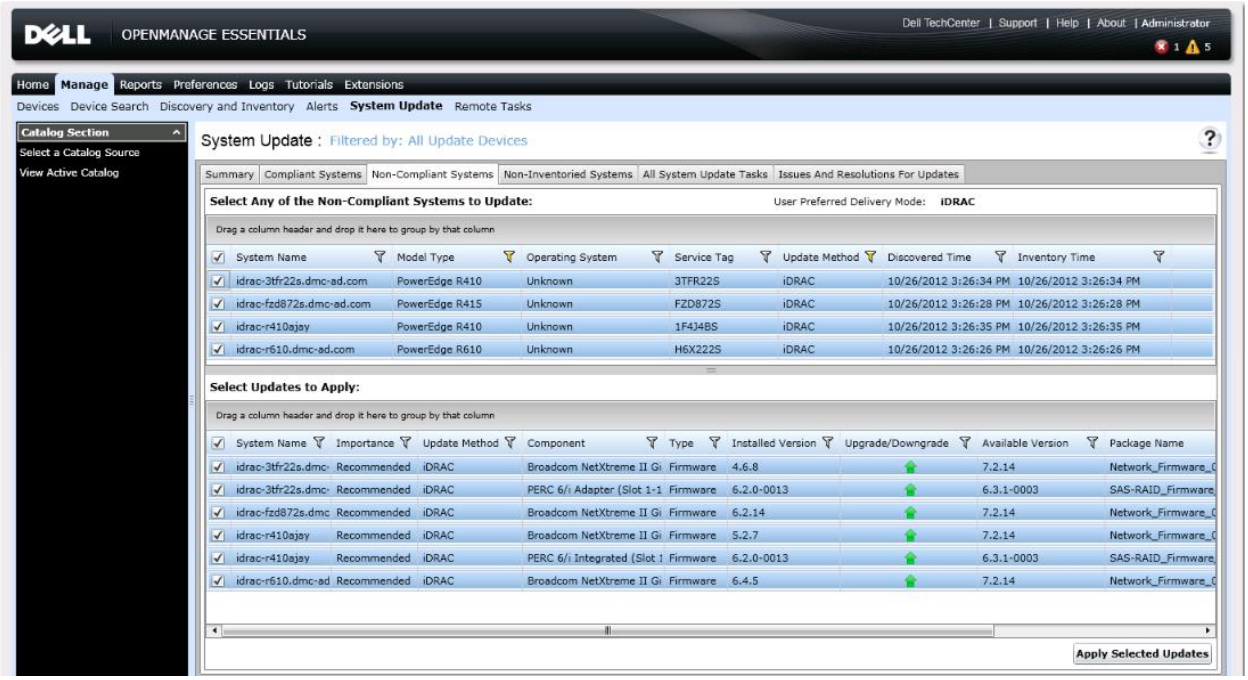


9. Download latest catalog – Refer “Obtaining the latest version of update packages” section
10. Click on Non-compliant tab if the discovered iDRAC is non-compliant. Verify that the “User Preferred Delivery Mode” is set to “iDRAC”

11. Select the iDRAC that is non-compliant and package to be updated on the System and click on Apply Selected updates.

    When **"User Preferred Delivery Mode"** is set to iDRAC, the "Update Method" will show iDRAC for all the available components (DUPs).

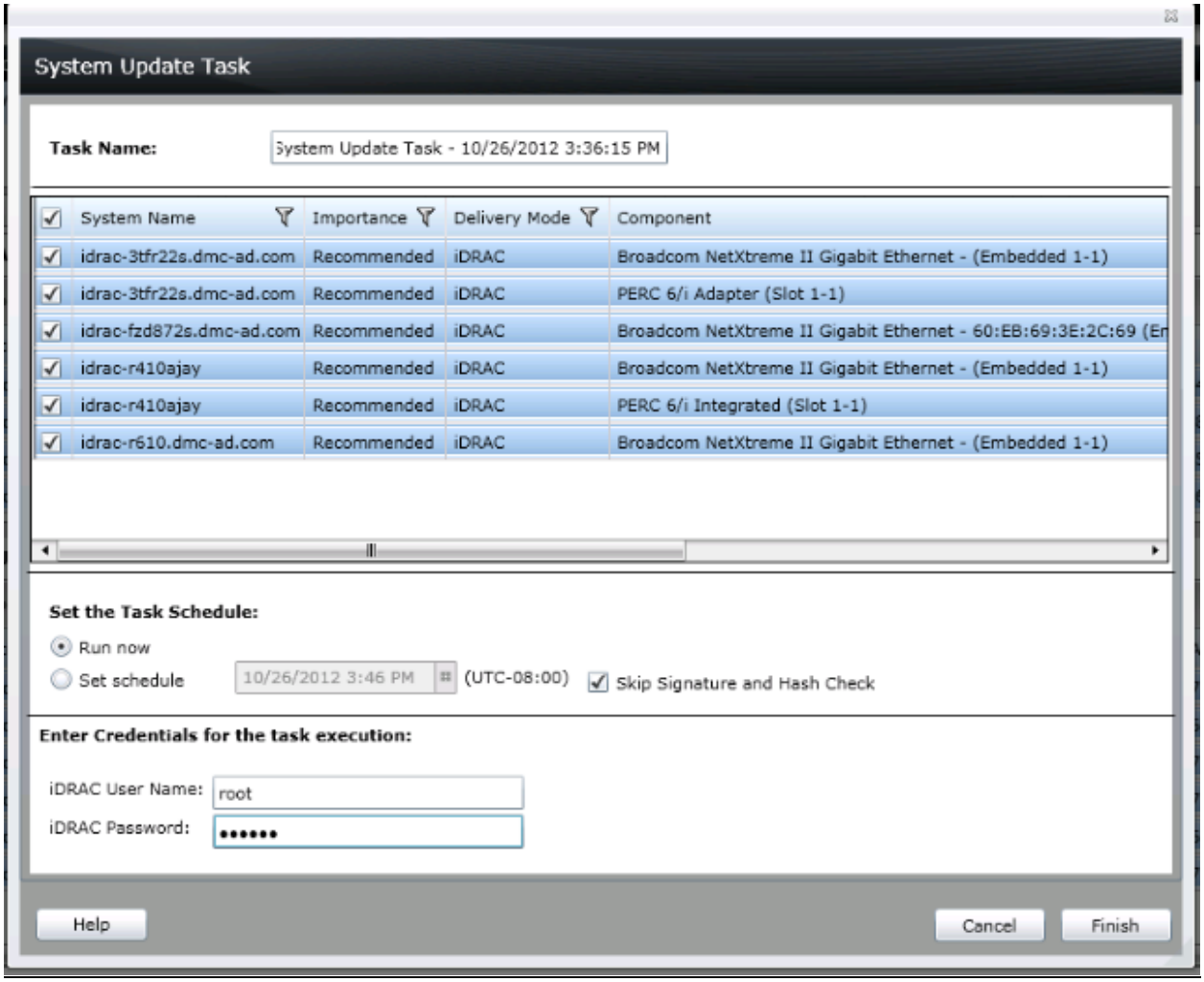
Figure 11. iDRAC Non-Compliant Report



12. "System Update Task" window is displayed.

    - Enter Task name
    - Set the Task Schedule – Choose Run now or Set Schedule
    - Enter iDRAC credentials
    - Click on "Finish" button to create system update task.

Figure 12. Create OOB system update task



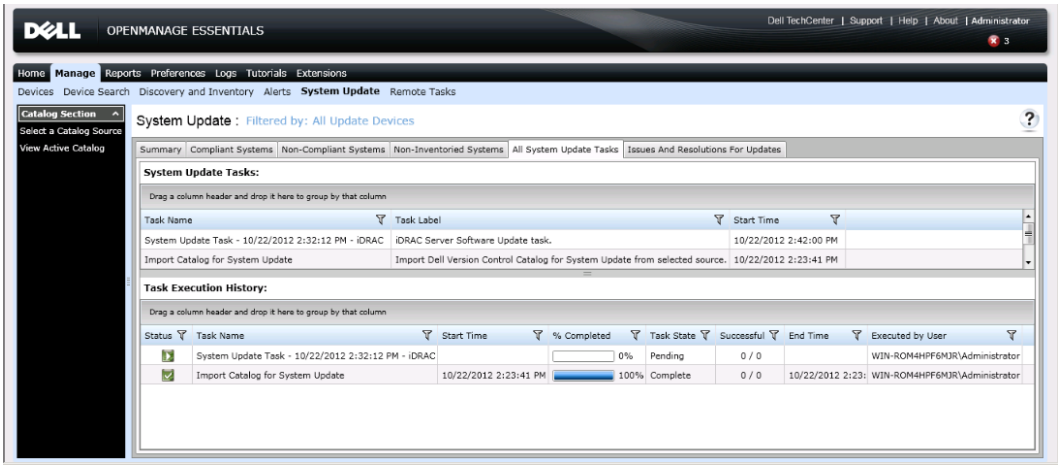
Note: Check "Skip Signature and hash check" to Skip signature and hash check.

13. System update task is created with name specified and "- iDRAC" appended to the task name. This indicates that preferred mode of deliver was iDRAC. The task is in pending state when the packages are being downloaded to local OME system. Once the packages are downloaded, task status changes to "Running". Once all the selected components (DUPs) are successfully applied

on the selected managed system, the task status set to “Complete”. An Inventory task is run 20 minutes after the software update task completion to fetch updated inventory.

14. To view the “Execution Details” of the task, double click on the task or right click on the task and select “Details” To copy execution details result, click on “Copy Results”

Figure 13. System Update Task (iDRAC) Execution Status



Note: Server will be rebooted after the system update task is complete. Inventory task runs automatically 20 minutes after system update task is completed and inventory of the server will be updated.

System Updates on correlated devices – Servers and iDRACs

Correlation is the process of relating resources to each other. OpenManage Essentials manages and identifies the relationship between resources (Server and iDRAC) that are discovered by different protocols.

Dell PowerEdge servers can be updated using OMSA & iDRAC method. IT administrator can use OMSA & iDRAC update method when there is a specific requirement to update System components BIOS, Firmware, Applications & Drivers or only BIOS, Firmware and Applications.

Table 2. Supported devices and protocol(correlation)

Dell PE Servers	iDRAC	iDRAC Firmware Versions.	Protocol Correlation
11G [Tower, RAC & Modular]	iDRAC6	1.40 above & 2.2 above	SNMP+WS-Man, WMI+WS-Man
12G [Tower, RAC & Modular]	iDRAC7	1.0 & above	SNMP+Ws-Man, WMI+WS-Man

- Perform discover and inventory of Dell PowerEdge server SNMP [Server IP] and WS-Man [iDRAC IP], Windows and Linux OS.
- Perform discovery and inventory of Dell PowerEdge server WMI [Server IP] and WS-Man [iDRAC IP], Only Windows OS.

  After performing above discovery and Inventory, To update correlated devices

  - Go to System Update and import a latest catalog (perfered online ftp.dell.com) (Refer to Obtaining the latest version of update packages
  - Perform system updates using either

    1. OMSA as preferred mode (refer to Updating System via OpenManager Server Administrator section)
    2. iDRAC as perferrred mode (refer to Updating System via Intergrated Dell Remote Access controller)

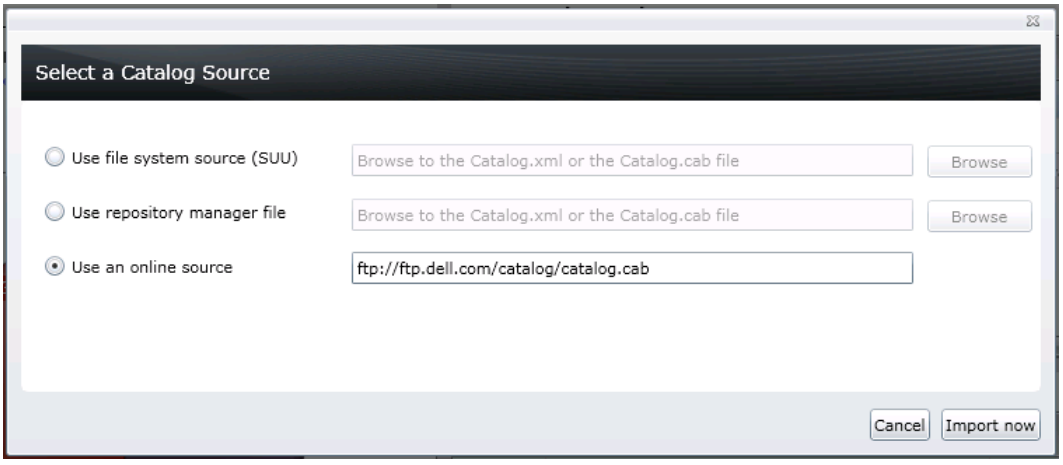
System Update – preferred mode is "iDRAC" & delivery mode is both OMSA & iDRAC

When IT administrator Discovers/Inventories multiple Dell PE 11G & 12G servers using Server IP and iDRAC IP. He is enable to update all the components in a single update task irrespective of component types (i.e. BIOS, Firmware, Drivers and Applications)

1. Discovery/Inventory PE (11G & 12G) Servers along with iDRAC (iDRAC6 & iDRAC7) or iDRAC alone using supported protocol. Ex: server with SNMP/WMIi & iDRAC with WS-Man.
2. Import latest catalog from online source (ftp.dell.com) –

   Go to Manage →System Updates → (LHS) Catalog Section → Select a Catalog Source and select option "Use an online source" click on "Import Now" button.

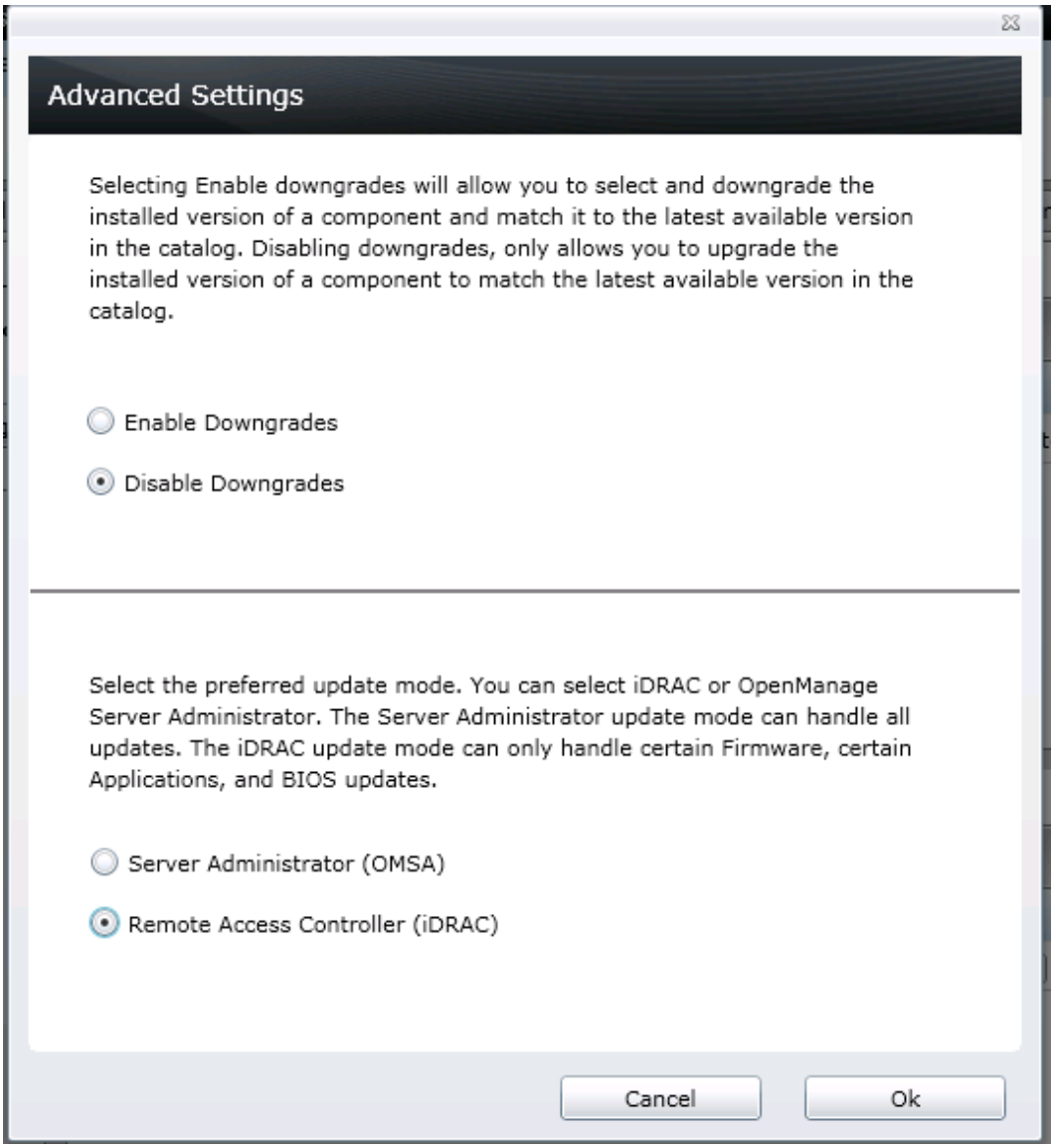
Figure 14. Catalog source



3. Enable iDRAC update mode from advanced settings.

   Go to System Update →Summary → Advanced Settings → Enable “Remote Access Controller (iDRAC) mode.

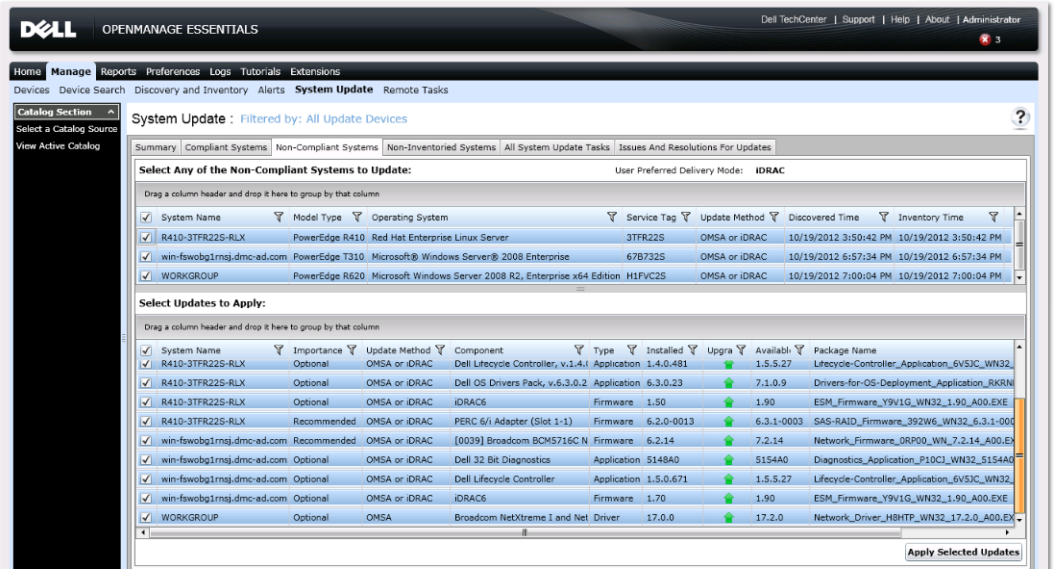
Figure 15. Advanced Settings



4. Select Non-Compliant Systems to update.

   Go to System Update →Non-Compliant Systems →Select Systems from “Select Any of Non-Compliant Systems to Update:”

Figure 16. Non-Compliant Systems

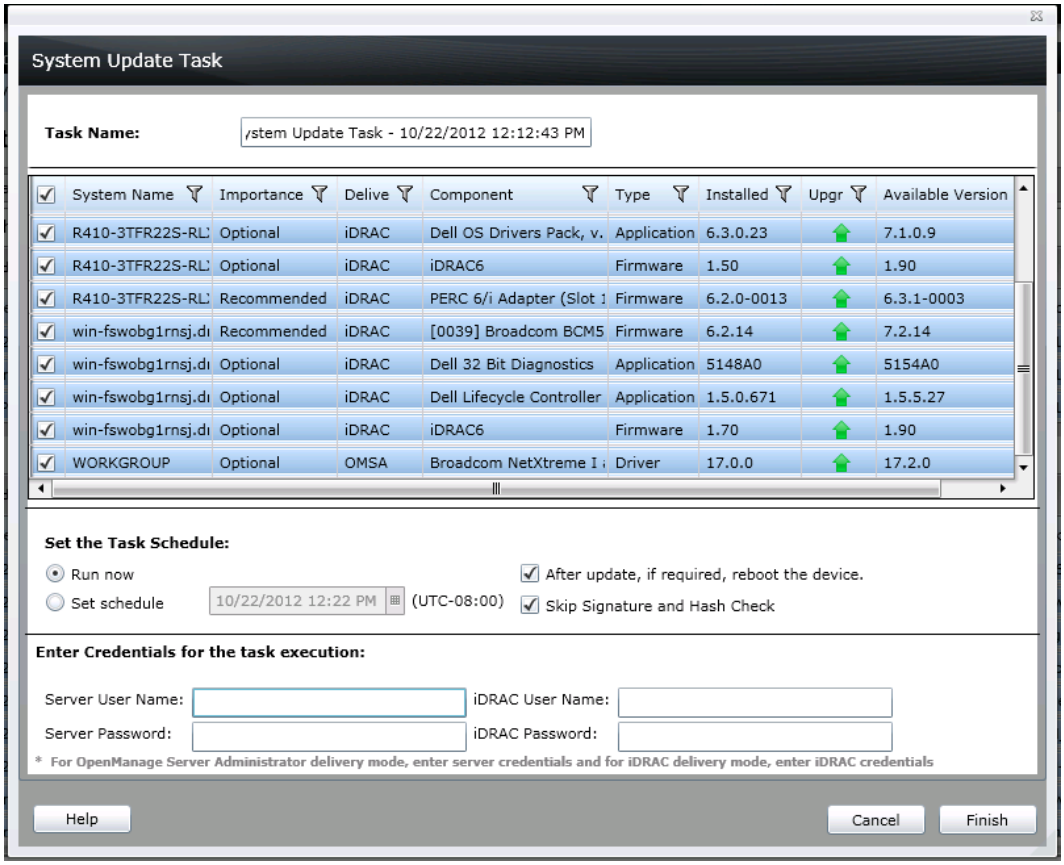


Note:

- User Preferred Delivery Mode - iDRAC
- Update Method for Selected Systems – OMSA or iDRAC.
- Update Method for Selected Components – OMSA or iDRAC & OMSA
- Select all PE-Servers which have same server credentials.
- Select all available components (BIOS, Firmware, Drivers & Applications)

5. Create an OMSA + iDRAC mode System update task.

Figure 17. OMSA + iDRAC mode system update task



Note:

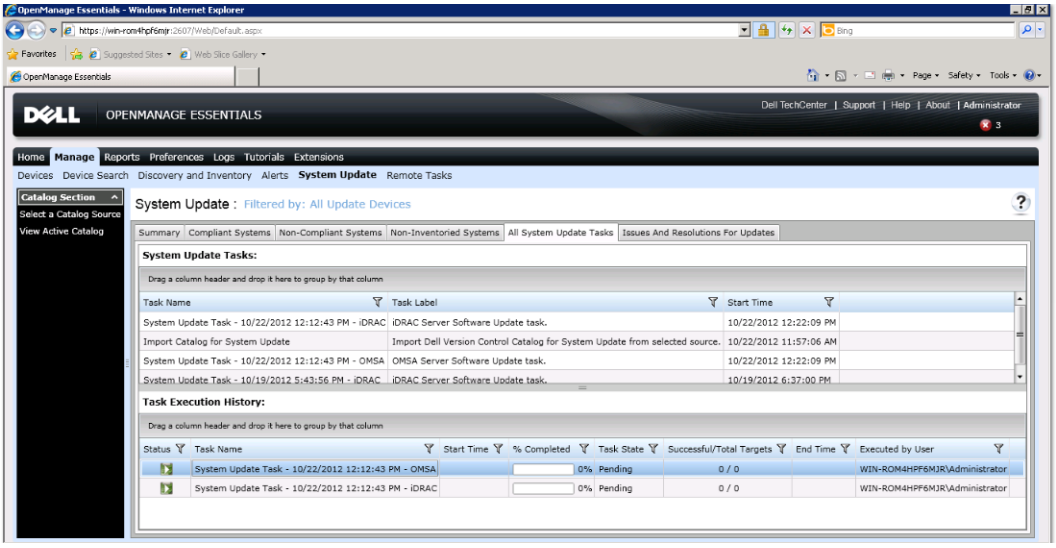
- Delivery Mode – iDRAC & OMSA
- Updatable components BIOS, Firmware, Drivers & Applications.
- Server and iDRAC Credentials asked.
- Enter Task name, set the task schedule – Choose Run now or Set Schedule option, Select “After update, if required, reboot the device” and “Skip Signature and Hash Check” check box, Enter Server and iDRAC credentials and Click on “Finish” button

System update OMSA and iDRAC task will be created and completed.

6. View the System update task status.

    - System Update → Summary →Task Execution History: OR
    - System Update → All System Update Tasks →Task Execution History:

Figure 18. System Update Task Execution Status



Note: On completion of system update task the Task State set to Completed, an auto inventory task is run after 20 minutes to fetch updated inventory data.

System Update Scalability

The scalability of System update is an important consideration for IT administrators of Enterprise Business, Medium Business and Small Business customers.

Test environment and methodology

The scalability and performance tests for Dell OME were performed on the following environments

- **Small business customer's environment**: This environment consisted of 100 managed systems. For example, a customer having 80 Dell PowerEdge Servers, 10 Dell EqualLogic storage devices and 10 Dell PowerConnect switches.
- **Medium business customer's environment:** Medium business environment consisted of 500 managed systems.
- **Enterprise business customer's environment:** This environment consisted of 2000 managed systems.

The hardware and software configuration of OME was different for these environments. Please refer to Table 1 for more details.

Table 3. Test Environments for OME1.1

Test Configuration	Test Environment		
	Small Business	**Medium Business**	**Enterprise Business**
NO. of Managed Systems	100	500	2000
RAM used on OME system	4 GB	6 GB	8 GB
Processor cores	2 cores	4 cores	8 cores
Operating System on which OME was installed	Windows Server 2008 x86 Standard Edition SP2	Windows Server 2008 x64 Standard Edition R2	Windows Server 2008 x64 Enterprise Edition SP2
Database version and Location	SQL 2008 Express (Local)	SQL 2008 Standard R2 (Local)	SQL 2008 Enterprise R2 (Remote)

Note: "Local" in the "Database version and Location" implies that the database is to be installed on the same machine as OME. "Remote" implies that the database is to be setup on a different machine

than OME. Please refer to the whitepaper “Installing Dell OpenManage Essentials” for more information about installing Dell OME on a remote Database.

Generic recommendations

Based on the analysis of the performance data collected for the various features tested, the following are the recommendations:

1. The minimum hardware and software mentioned in Table 1 must be used in order for better performance of OME. Higher hardware specifications i.e., increase in processor cores or RAM will yield better performance that that detailed out in the rest of the document.
2. Recommendation is to configure the “max server memory” of SQL server based on the available system resources. Please refer to the MSDN link for more information.
3. OME must be installed using a remote database when the number of managed system is >500 and if the hardware specification is that provided in Table 1.
4. Domain Name System (DNS) must be configured such that OME is able to resolve the hostname of all the managed systems.

Table 4. System Update Data

System Update Data	**Enterprise Business**		**Medium Business**	
Update Mode	In-**band update**	Out of band update	In-band update	Out of band update
Number of Discovered Nodes	2000		500	
Time taken to complete	1 hour 20 min	1 hour 40 min	1 hour 30 min	1 hour 50 min
Average CPU Utilization	55%	55%	55%	55%
Average memory utilization	3.5 GB	3.8 GB	2.3 GB	2.3 GB
Test Scenario	System Update of 30 targets where each target had 3 to 6 updatable components			
Catalog Source	Dell OpenManage Server Update Utility DVD (SUU)			

Note: Table 11 above provides the data for an Enterprise Business and Medium Business environment. The average memory utilization is higher due to devices being discovered and inventoried on the OME system.

These are the recommendations for using the patch feature, based on the analysis of the test results:

1. Recommendation is to update not more than 30 managed systems at any given time.
2. Dell SUU is recommended as the catalog source for system update as the packages are downloaded at a faster rate.
3. Separate system update tasks must be created for Windows and Linux targets in case of Inband system updates.

List of System and Device Firmware and its behavior on update

System Firmware

Table 5. System Firmware Data

Type of Firmware	Reboot Required
BIOS	YES
ESM	YES
BMC	NO

Device Firmware

Table 6. Device Firmware Data

Type of Firmware	Reboot Required
PERC	YES
RAC	NO
CERC	YES
SAS	YES
SCSI BP	YES
SAS BP	NO
Storage Enclosure	NO
Zappa	NO
Pompano	YES
Tape	NO
HDD DUP	NO
Catfish	NO

Note: None of the drive update requires reboot.

Conclusion

All that an IT administrator needs to do to keep servers up to date in a datacentre is to install Dell agent on servers, inventory the servers, and import the latest version of catalog.

Use the following three steps to keep the servers up to date in a datacentre environment using Dell OpenManage Essentials:

1. Discover and Inventory Dell servers.
2. Discover and Inventory Dell iDRAC6 and above.
3. Discover and Inventory Dell PE VMware ESXi server and its iDRAC6 and above.
4. Import the latest catalog.
5. Schedule the system update task.

Learn more

Visit DellTechcenter.com/OME for more information on Dell OpenManage Essentials.

© 2011 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell and the Dell logo are trademarks of Dell Inc. Microsoft, Windows, and the Windows logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Intel and Xeon are registered trademarks of Intel Corporation in the U.S. and other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.

November 2012 | Rev 1.0