Recommended Methods for Updating Firmware on Dell Servers

AVS Sashi Kiran

November 2013

A Dell Technical White Paper

Revisions

Date	Description
December 2013	Initial release

THIS WHITE PAPER 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.

PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell logo, Dell Boomi™, Dell Precision™ ,OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-0S®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its

Table of Contents

Executive Summary

Dell provides various tools for applying the Dell Update Packages (DUPs) in various contexts for keeping Dell servers up to date. This technical paper describes recommended methods for updating Dell servers in various contexts such as in-band, out-of-band, and console.

A Dell Technical White Paper

Introduction

Dell provides software updates in the form of Dell Update Packages (DUPs).. DUPs can be deployed individually or in groups. This paper focuses on deploying DUPs in groups. Some of the tools provided by Dell are Dell Server Update Utility (SUU), Dell Repository Manager (DRM), Dell OpenManage Essentials, and so on. Dell publishes the catalogs at http://downloads.dell.com/catalog for facilitating the application of DUPs.

This technical paper provides a recommendation on the suitable methods for keeping Dell server up to date in various contexts:

1) In-band update deployment.
2) Out-of-band update deployment.
3) Console based update deployment.

1. In-band update

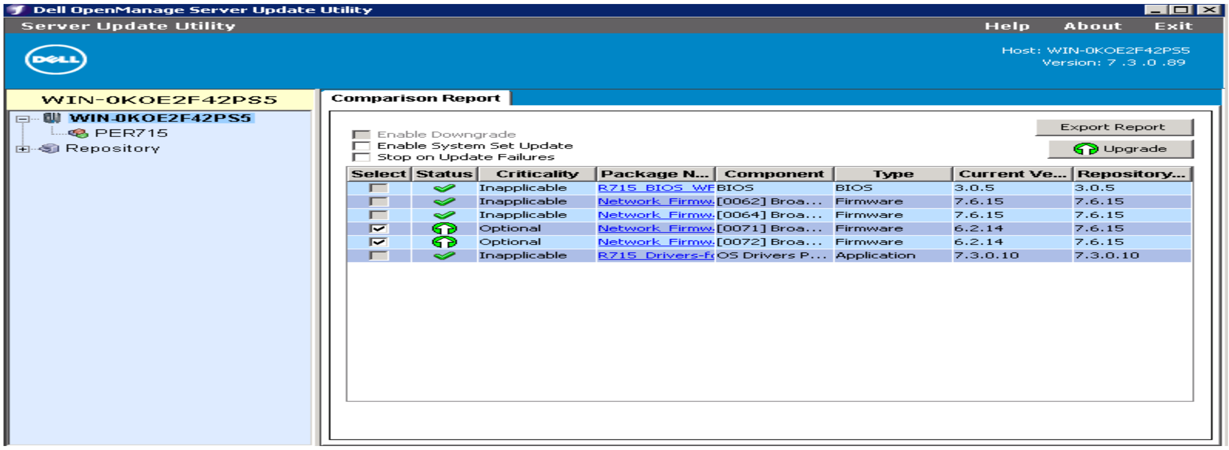
In in-band update the servers are updated in an operating system context. In-band updates on a server can be applied in different scenarios which are:

1) 1:1 scenario: at a time updates can be applied on single system.
2) 1: N scenario: at a time updates can be applied on multiple systems.

1.1 Single server updates (1:1 Scenario)

In case of single server updates, Dell recommends using SUU, which contains updates for all the servers supported by Dell. [Linux and Windows]. The SUU iso file in full can be downloaded from support.dell.com. The iso file is a large file containing the relevant updates for up to 4 generations of Dell PowerEdge servers. To assist in creating a smaller and focused SUU, Dell provides Dell Repository Manager (DRM). DRM allows the creation of an SUU for the required servers, which can be customized to include only the required updates. For more information on using DRM and creating a SUU iso from DRM, see www.delltechcenter.com/repositorymanager.

The SUU iso created via DRM or downloaded from support.dell.com can be used on the required servers. SUU provides the ease to end-user in inventorying the hardware present on a server and provides a report which displays all the hardware to be upgraded and also the importance level of each firmware or driver as displayed in Figure 1.



□ Enable Downgrade
□ Enable System Set Update
□ Stop on Update Failures

Select	Status	Criticality	Package N...	Component	Type	Current Ve...	Repository...
□	✓	Inapplicable	R715_BIOS_WF	BIOS	BIOS	3.0.5	3.0.5
□	✓	Inapplicable	Network_Firmw	[0062] Broa...	Firmware	7.6.15	7.6.15
□	✓	Inapplicable	Network_Firmw	[0064] Broa...	Firmware	7.6.15	7.6.15
☑	⇧	Optional	Network_Firmw	[0071] Broa...	Firmware	6.2.14	7.6.15
☑	⇧	Optional	Network_Firmw	[0072] Broa...	Firmware	6.2.14	7.6.15
□	✓	Inapplicable	R715_Drivers-f	OS Drivers P...	Application	7.3.0.10	7.3.0.10

Figure 1 Dell Server Update Utility

Based on the importance level, the servers can be upgraded. After selecting the desired updates, click on **Upgrade** and wait till the update is complete.

1.2 Multiple Server Updates (1: N Scenario)

Linux-Based Update:

In case of multiple server updates, if all are RPM-based Linux distributions, Dell recommends using yum (Yellowdog Updater, Modified). For more information on using Dell yum, see http://linux.dell.com/repo/hardware/latest/.

Else, Dell recommends using Dell OpenManage Deployment Toolkit (DTK) bootable Linux iso that can be created from Dell Repository Manager (DRM. For more information on creating a Linux bootable iso from DRM, see the technical paper at www.delltechcenter.com/repositorymanager.

Windows-Based Update:

In case of servers running Windows, Dell recommends using Dell Repository Manager (DRM).

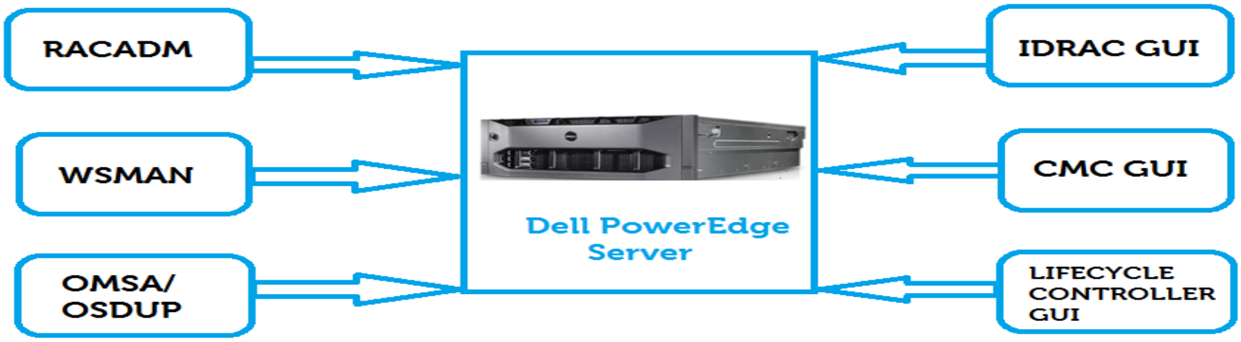
For example, Light Weight Deployment Packs (LWDP) can be used from DRM to deploy updates on a server running supported Windows operating system. For more information on using LWDP from DRM, see www.delltechcenter.com/repositorymanager.

2. Out-of-band update

From 11G onwards, Dell recommends using iDRAC and Lifecycle Controller (LC) for updating the firmwares on Dell servers in an out-of-band update. If a server does not have Lifecycle Controller, then Dell recommends using DTK bootable Linux iso created from Dell Repository Manager (DRM) to update the server. For more information on creating a Linux bootable iso from DRM, see www.delltechcenter.com/repositorymanager.

Out-of-band server updates are performed using the dedicated systems management channel running on the iDRAC service process or pre-OS UEFI environment such as Lifecycle Controller (LC).

- iDRAC and Lifecycle Controller support the following interfaces that perform firmware updates:



iDRAC and Lifecycle Controller provide the infrastructure for updating most of the firmwares on PowerEdge servers. The iDRAC and Lifecycle Controller (LC) are released as two individual firmware components, but are dependent on each other for various change management features and hardware that they support. It is recommended to update the two components together.

iDRAC and LC firmware should always be upgraded before upgrading other components on the server regardless of the methods used to perform firmware updates.

Following is the sequence recommended for updating the firmware on a Dell PowerEdge server:

1. iDRAC
2. Lifecycle Controller
3. BIOS
4. Diagnostics
5. OS Driver Pack
6. RAID
7. NIC
8. PSU
9. CPLD
10. Other update

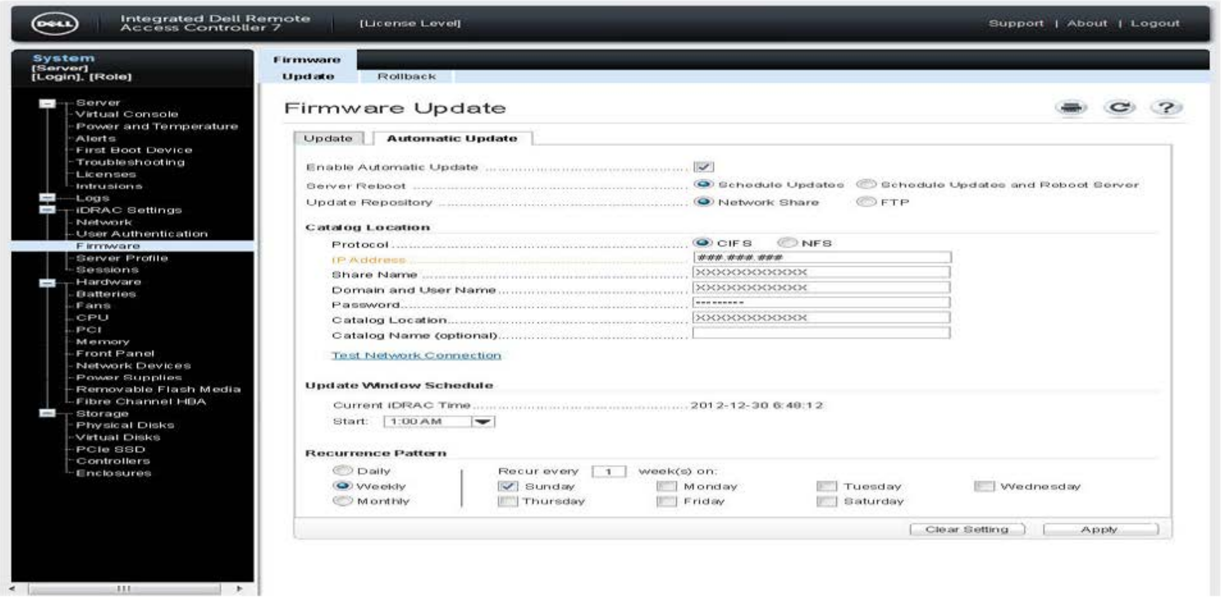
Staged updates can be applied in a single-host restart. For example, BIOS, RAID, NIC, PSU, and CPLD can be staged together and applied with a single-host restart.

Note : If multiple updates are staged together from consoles such as iDRAC GUI, CMC GUI, Lifecycle Controller GUI, or any other Dell-supported consoles such as OpenManage Essentials, the updates are automatically reordered on the basis of the time to install the optimizations built in for those management tools.

Automatic Update using iDRAC

Remote repository updates is the newest and the most advanced firmware update mechanism to update a wide variety of firmware and applications installed on the PowerEdge server. This feature uses an update repository created using the Dell Repository Manager to download and install the updates. The repository could either be ftp.dell.com or a user generated repository on the local network share. Remote repository updates provides a simple and easy way to automatically figure out the latest updates that are available for your PowerEdge server and install it all at once at the click of a button. The Automatic update is available on iDRAC from 12G (For example PowerEdge R720) onwards.

iDRAC web user interface can be used for scheduling automatic updates as shown in the following figure below:



Firmware Update

Enable Automatic Update ☑

Server Reboot ● Schedule Updates ○ Schedule Updates and Reboot Server

Update Repository ● Network Share ○ FTP

Catalog Location

Protocol ● CIFS ○ NFS

IP Address ###.###.###

Share Name XXXXXXXXXXXX

Domain and User Name XXXXXXXXXXXX

Password *********

Catalog Location XXXXXXXXXXXX

Catalog Name (optional)

Update Window Schedule

Current IDRAC Time 2012-12-30 6:48:12

Start: 1:00 AM

Recurrence Pattern

○ Daily
● Weekly
○ Monthly

Recur every 1 week(s) on:

☑ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday
☐ Thursday ☐ Friday ☐ Saturday

The figure displays Automatic Update with Network share and CIFS. The selected recurrence pattern displays the schedule of the update.
Similarly Automatic Updates can also be scheduled through FTP (**ftp.dell.com**)

RACADM behavior on Automatic update

The Automatic Updates creates a recurring schedule to run the updates automatically from the repository.
To enable automatic job update, schedule a recurrent update by using the following LC attribute.

/admin->racadm set lifecycleController.lcattributes.AutoUpdate.Enable <0-Disabled | 1-Enabled>

You can enable or disable the automatic update using the given command. If the attribute is set to Disabled, no action is taken. If the attribute is set to Enabled, the update operation is initiated at the pre-set time.

To check whether the automatic update is enabled or not, use the following command:

/admin->racadm get lifecycleController.lcattributes.AutoUpdate

To start a recurrent automatic update job using RACADM, use the following command through CIFS/NFS method:

/admin->racadm AutoUpdateScheduler create -u username –p password –l <location> [-f catalogfilename -pu <proxyuser> -pp<proxypassword> -po <proxy port> -pt <proxytype>] -time < hh:mm> [-dom < 1 – 28,L,'*'> -wom <1-4,L,'*'> -dow <sun-sat,'*'>] -rp <1-366> -a <applyserverReboot (1-enabled | 0-disabled)>

Update through WS-MAN

Firmware update through WS-MAN is performed remotely, and may be executed directly or by the staged mechanism based on the component that is being updated. In case of direct updates, the update package is downloaded from a repository and applied without rebooting the host machine. In staged updates, the update package is downloaded to iDRAC and the update is scheduled for application following a host reboot. The host reboot can be scheduled for immediate or later implementation using the Lifecycle Controller. This method can be used effectively to minimize the downtime of the server during peak hours.

While the firmware update using the WS-MAN protocol uses a programming interface, the other update methods are interactive, and use a user interface. Essentially, you can incorporate the update process into any application. Since the WS-MAN client is implemented in different programming languages, this is very useful. You can immediately put this method into use using a couple of popular WS-MAN client command line interfaces. The client server and the server hosting the repository can be in the same hardware.

Windows offers the WinRM CLI as well as the more capable PowerShell WS-MAN client, while Linux provides the open source OpenWS-MAN CLI (a standard component in Linux distributions). If your version of Linux does not have it, download it from www.sourceforge.net. Windows and Linux tools have different options, but similar WS-MAN client capabilities.

For more information on WS-MAN, see **http://en.community.dell.com/techcenter/systems-management/w/wiki/3244.remote-firmware-update.aspx**

2.1 Platform or Firmware Update Methods

The following are the various methods of performing platform or firmware updates:

1) FTP (Non-Proxy and Proxy)
2) Local Drive (SUU DVD or USB drive)
3) Network Share (CIFS or NFS)

Using FTP Server

Lifecycle Controller provides options to update a server using the latest firmware available on the Dell FTP server or on an internal FTP server.

Using Non-Proxy FTP Server

Lifecycle Controller can access the latest firmware from ftp.dell.com. Lifecycle Controller downloads the DUPs from the FTP location to perform platform firmware update.
The updates can also be downloaded using Dell Repository Manager and the repository will be created on an internal FTP server.

Using Proxy FTP Server

Lifecycle Controller can be used to perform latest updates with the firmware available at ftp.dell.com or by using an internal, or service provider's FTP server, when you are connected to internet through a proxy server.

Using a Local Drive

Use either SUU DVDs or custom DVDs (SUU iso downloaded from support.dell.com) to perform firmware updates. You can also use a USB drive to update the firmwares.

Using a Network Share (CIFS or NFS)

If you are using a network share such as CIFS or NFS, select the appropriate network share depending on the availability of the update repository. The repository can be created using Dell Repository Manager to create the catalog and download the selected updates.

For more information on updating the firmwares using the mentioned methods, see http://en.community.dell.com/techcenter/extras/m/white_papers/20101309.aspx .

3. Console-based updates

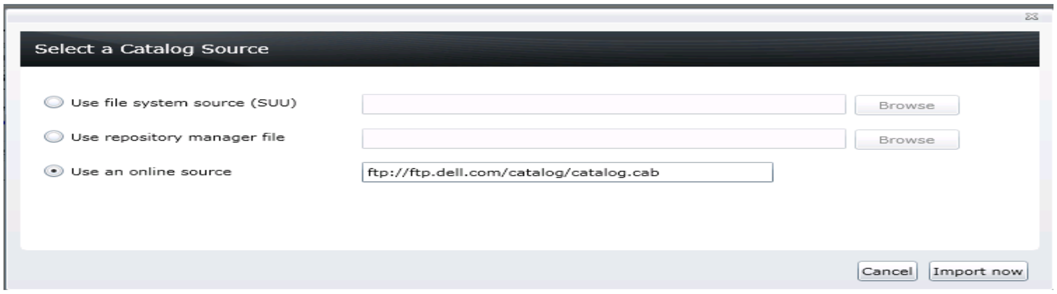
Dell recommends using Dell OpenManage Essentials (In-band with Dell OpenManage System Administrator (OMSA) and Out-of-Band without OMSA agent).

3.1 Update methods from Dell OpenManage Essentials

3.1.1 In-band update for in-band server updates

Windows Management Instrumentation service must be running on the selected targets. The sources for obtaining firmwares and drivers are displayed in the following figure:

- Online Source – ftp.dell.com.
- File system source – SUU media.
- Repository Manager file – Selected drivers and firmware generated from Dell Repository Manager Tool.



Select a Catalog Source

○ Use file system source (SUU)

○ Use repository manager file

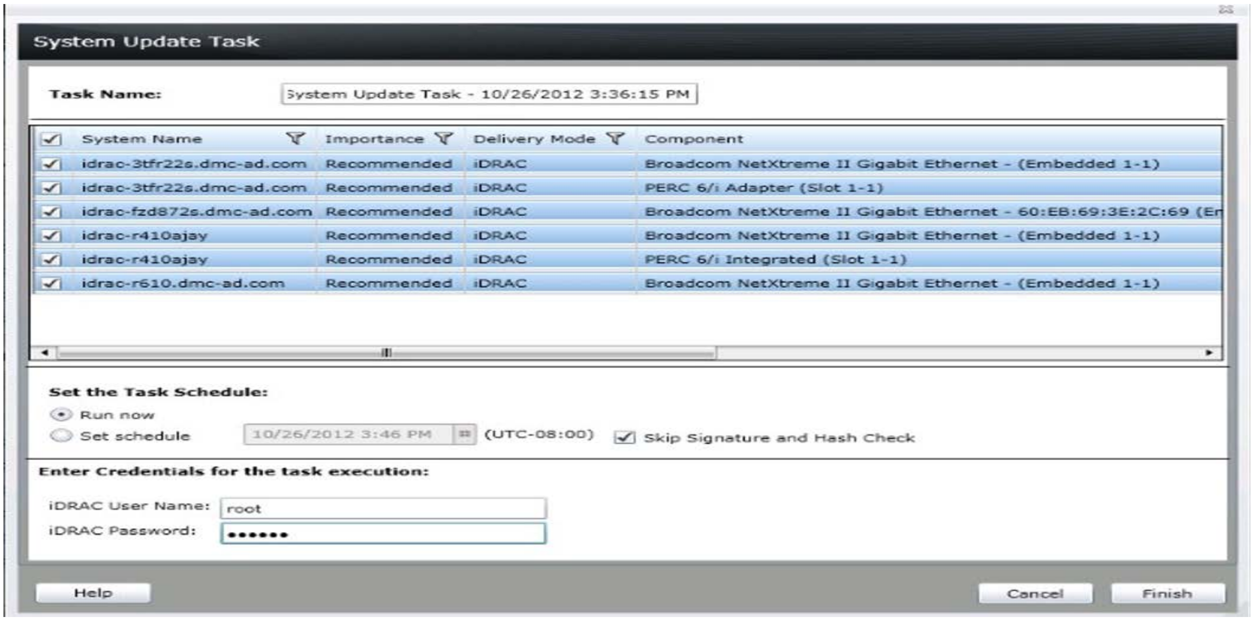
● Use an online source ftp://ftp.dell.com/catalog/catalog.cab

Figure Selecting source in OpenManage Essentials

3.1.2 Out- of- Band Server Update without OMSA agent - Agent Free System Update

Out- of- band server update uses iDRAC with Life Cycle controller to update Dell servers. Out- of- band server update is used for managing Dell servers with or without an operating system and without Dell OpenManage Server Administrator (OMSA).

Agent- free server update in OpenManage Essentials does not need an operating system and OMSA on the managed server 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.



System Update Task

Task Name: ystem Update Task - 10/26/2012 3:36:15 PM

☑	System Name	Importance	Delivery Mode	Component
☑	idrac-3tfr22s.dmc-ad.com	Recommended	iDRAC	Broadcom NetXtreme II Gigabit Ethernet - (Embedded 1-1)
☑	idrac-3tfr22s.dmc-ad.com	Recommended	iDRAC	PERC 6/i Adapter (Slot 1-1)
☑	idrac-fzd872s.dmc-ad.com	Recommended	iDRAC	Broadcom NetXtreme II Gigabit Ethernet - 60:EB:69:3E:2C:69 (En
☑	idrac-r410ajay	Recommended	iDRAC	Broadcom NetXtreme II Gigabit Ethernet - (Embedded 1-1)
☑	idrac-r410ajay	Recommended	iDRAC	PERC 6/i Integrated (Slot 1-1)
☑	idrac-r610.dmc-ad.com	Recommended	iDRAC	Broadcom NetXtreme II Gigabit Ethernet - (Embedded 1-1)

Set the Task Schedule:

● Run now

○ Set schedule 10/26/2012 3:46 PM (UTC-08:00) ☑ Skip Signature and Hash Check

Enter Credentials for the task execution:

iDRAC User Name: root

iDRAC Password: ••••••

Figure Out-of-Band Server Update Task

3.1.3 Recommendations on Firmware Updates from OpenManage Essentials

- Use online source ftp.dell.com to ensure that the latest drivers and firmwares are available or use SUU for a qualified set of drivers and firmwares.
- Create custom catalogs, which gives maximum control over driver and firmware revisions in the environment because they get selected individually either from SUU or online source using the DRM.

3.2 Various other combinations

Single update on a single server

Single package can be selected to update single server.

Multiple update on a single server

Multiple packages (BIOS, drivers, and firmwares) can be selected to update individual server using a single update task.

Single update on multiple servers

Multiple servers can be selected to update with a single package.

Example: If there are 10 Dell PowerEdge R720 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

All applicable packages on multiple servers can be applied using a single task. All the servers must have the same credentials for the task to run successfully.

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

3.3 Using Dell Repository Manager to update Firmware through Dell OpenManage Essentials

An inventory- based repository can be created using DRM to update the firmwares through Dell OpenManage Essentials.

Provide DRM, the details of the server (IP address or host name, username, and password) having OpenManage Essentials. Once the required details are obtained, DRM tries to gather the list of servers discovered by OpenManage Essentials.

After successful operation, a repository gets created. The repository contains bundles for each discovered server under OpenManage Essentials. Updates for the same servers are grouped under the same bundle.

The repository created from the OpenManage Essentials inventory can be saved as a full repository using the save option available in DRM on to a desired location. The saved repository can be used to update the firmware later from OpenManage Essentials. Alternatively a customized SUU can be created by selecting the Export option and using the tool creation wizard.

Best Practice is to save the file and contents to a network location that OpenManage Essentials has access to.

For detailed usage, refer the technical paper on using Dell Repository Manager with Dell OpenManage Essential at www.delltechcenter.com/repositorymanager.

3.4 Updating Firmware through SCCM Console

The Microsoft System Center Configuration Manager (SCCM) offers a solution to comprehensively asses, deploy, and update servers, clients, and devices across physical, virtual, distributed, and mobile environments. Optimized for the Microsoft Windows operating system and extensible beyond, the tool suite is a suitable choice for gaining enhanced insight into and managing and administering IT systems.

3.4.1 Using System Center Update Publisher (SCUP) with SCCM

System Center Update Publisher (SCUP) is an add-on application designed to extend the software update management functionality in System Center Configuration Manager (SCCM). It helps IT administrators to import, create, and publish custom software update information to SCCM server.

Dell Catalog along with Microsoft System Center products SCUP, WSUS, and SCCM helps IT administrators in updating the BIOS, firmware, drivers, and applications of Dell servers.

Dell recommends the following for updating the server through SCUP and SCCM:

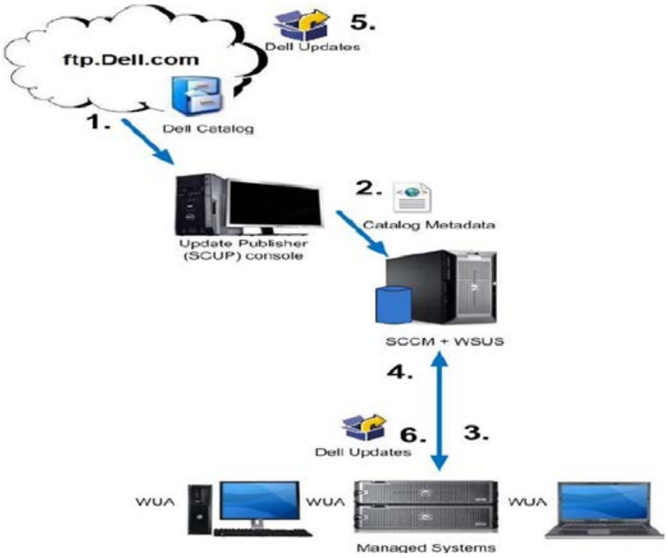
1) Import the Dell catalog to Windows Server Update Services (WSUS) using SCUP tool.

2) Import updates from WSUS into SCCM.
3) Scan Dell managed servers using SCCM.
4) Deploy necessary updates to the Dell servers using SCCM.

You can do the following using SCUP:

- Create the correct applicability and deployment metadata for an update that can be managed through SCCM.
- Import update catalogs from third parties such as Dell or from own organization.
- Export and share the software update catalogs.
- Manage custom software update information

The same is illustrated in the following figure.



For more information on SCCM/SCUP, see http://en.community.dell.com/techcenter/os-applications/w/wiki/2536.dell-updates-catalogs.aspx

3.5 OpenManage Integration for VMware venter

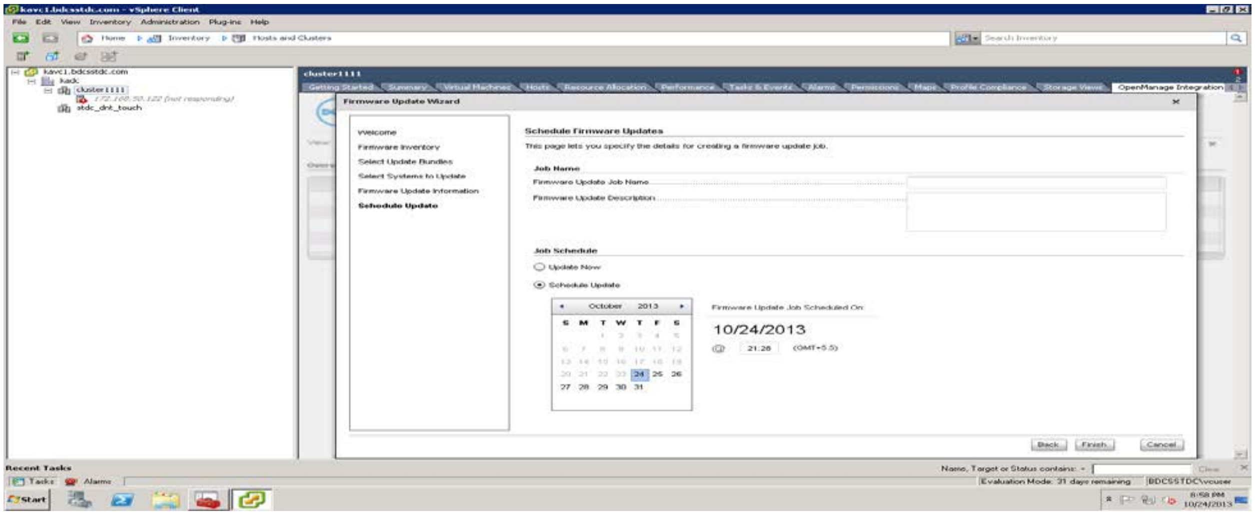
The OpenManage Integration for VMware venter is a virtual appliance that streamlines tools and tasks associated with the management and deployment of Dell servers in a virtual environment. It reduces complexity by natively integrating the key management capabilities into the VMware vSphere Client console. It minimizes the risks of hardware alarms, streamlines firmware updates and provides deep visibility into inventory, health, and warranty details.

The OpenManage Integration enables to schedule firmware updates for clusters within VMware vCenter. In addition, you can schedule the firmware update. This feature helps to perform the firmware updates during the scheduled maintenance window without your manual intervention

3.5.1 Scheduling an update from OpenManage VMWare vCenter through LC

You can use WinRM commands to update a server using Lifecycle Controller (LC). You can also update multiple servers as follows:

1) Schedule an update:


kavc1.bdcsstdc.com - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
Search Inventory
kavc1.bdcsstdc.com
kadc
cluster1111
172.168.50.122 (not responding)
stdc_dnt_touch
cluster1111
Getting Started Summary Virtual Machines Hosts Resource Allocation Performance Tasks & Events Alarms Permissions Maps Profile Compliance Storage Views OpenManage Integration
Firmware Update Wizard
Welcome
Firmware Inventory
Select Update Bundles
Select Systems to Update
Firmware Update Information
Schedule Update
October 2013
S M T W T F S
Back
Finish
Cancel
Recent Tasks
Tasks Alarms
Name, Target or Status contains:
Clear
Evaluation Mode: 31 days remaining
BDCSSTDC\vcuser
Start
8:58 PM
10/24/2013

Schedule Firmware Updates

This page lets you specify the details for creating a firmware update job.

Job Name

Firmware Update Job Name

Firmware Update Description

Job Schedule

○ Update Now

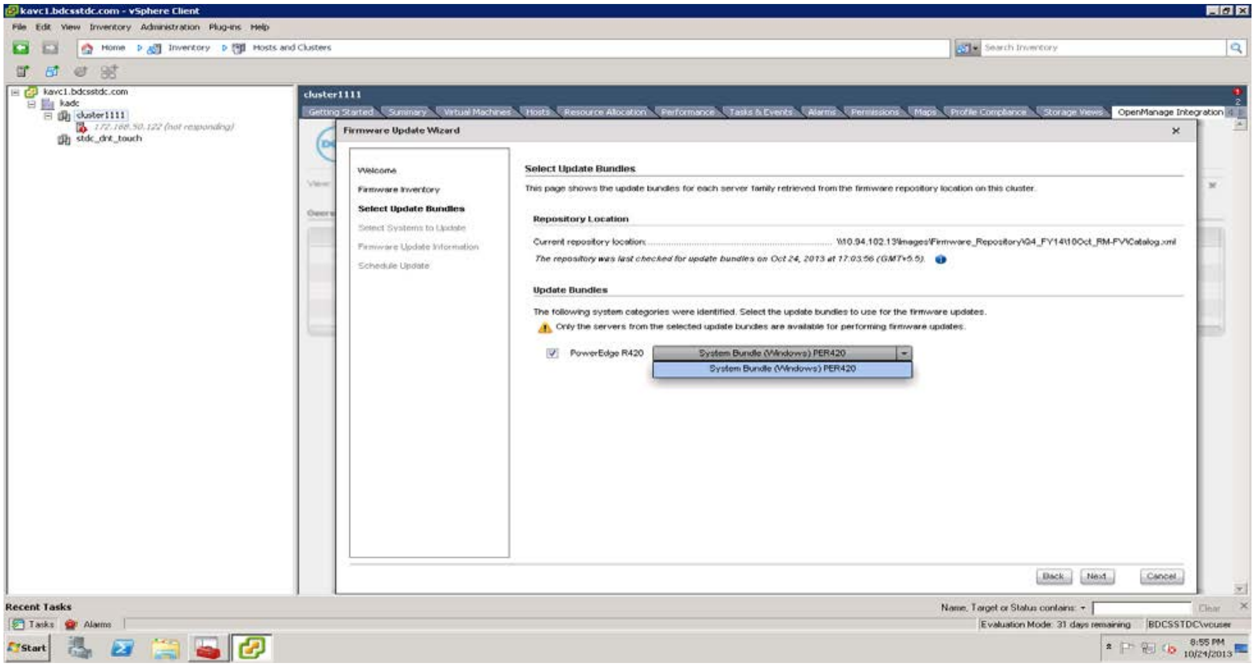
● Schedule Update

Firmware Update Job Scheduled On:

10/24/2013

21:28 (GMT+5.5)

2) Select the required bundle. If there are multiple servers, then select the multiple servers accordingly.


kavc1.bdcsstdc.com - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
Search Inventory
kavc1.bdcsstdc.com
kadc
cluster1111
172.168.50.122 (not responding)
stdc_dnt_touch
cluster1111
Getting Started Summary Virtual Machines Hosts Resource Allocation Performance Tasks & Events Alarms Permissions Maps Profile Compliance Storage Views OpenManage Integration
Firmware Update Wizard
Welcome
Firmware Inventory
Select Update Bundles
Select Systems to Update
Firmware Update Information
Schedule Update
Back
Next
Cancel
Recent Tasks
Tasks Alarms
Name, Target or Status contains:
Clear
Evaluation Mode: 31 days remaining
BDCSSTDC\vcuser
Start
8:55 PM
10/24/2013

Select Update Bundles

This page shows the update bundles for each server family retrieved from the firmware repository location on this cluster.

Repository Location

Current repository location: \\10.94.102.13\Images\Firmware_Repository\Q4_FY14\10Oct_RM-FV\Catalog.xml

The repository was last checked for update bundles on Oct 24, 2013 at 17:03:56 (GMT+5.5).

Update Bundles

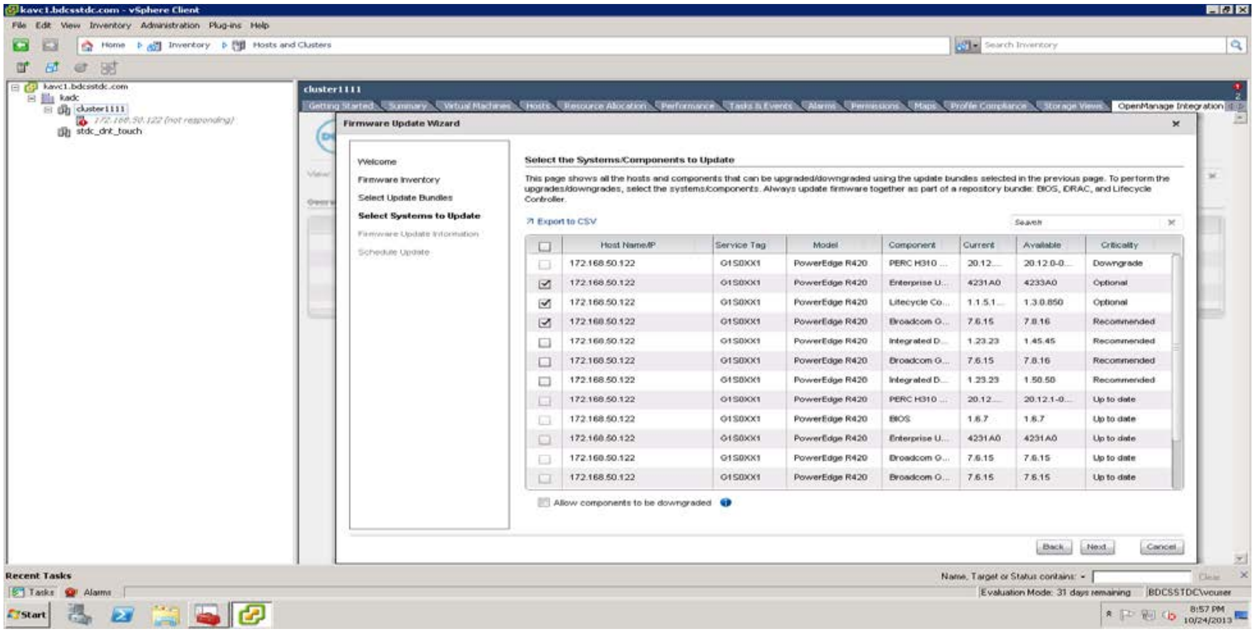
The following system categories were identified. Select the update bundles to use for the firmware updates.

Only the servers from the selected update bundles are available for performing firmware updates.

☑ PowerEdge R420 System Bundle (Windows) PER420

System Bundle (Windows) PER420

3) Select the components for all the selected servers.


kavc1.bdcsstdc.com - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
Search Inventory
kavc1.bdcsstdc.com
kadc
cluster1111
172.168.50.122 (not responding)
stdc_dnt_touch
cluster1111
Getting Started Summary Virtual Machines Hosts Resource Allocation Performance Tasks & Events Alarms Permissions Maps Profile Compliance Storage Views OpenManage Integration
Firmware Update Wizard
Welcome
Firmware Inventory
Select Update Bundles
Select Systems to Update
Firmware Update Information
Schedule Update
Export to CSV
Search
Back
Next
Cancel
Recent Tasks
Tasks Alarms
Name, Target or Status contains:
Evaluation Mode: 31 days remaining
BDCSSTDC\vcuser
Start
8:57 PM
10/24/2013

Select the Systems/Components to Update

This page shows all the hosts and components that can be upgraded/downgraded using the update bundles selected in the previous page. To perform the upgrades/downgrades, select the systems/components. Always update firmware together as part of a repository bundle: BIOS, iDRAC, and Lifecycle Controller.

□	Host Name/IP	Service Tag	Model	Component	Current	Available	Criticality
□	172.168.50.122	G1S0XX1	PowerEdge R420	PERC H310 ...	20.12....	20.12.0-0...	Downgrade
☑	172.168.50.122	G1S0XX1	PowerEdge R420	Enterprise U...	4231A0	4233A0	Optional
☑	172.168.50.122	G1S0XX1	PowerEdge R420	Lifecycle Co...	1.1.5.1...	1.3.0.850	Optional
☑	172.168.50.122	G1S0XX1	PowerEdge R420	Broadcom G...	7.6.15	7.8.16	Recommended
□	172.168.50.122	G1S0XX1	PowerEdge R420	Integrated D...	1.23.23	1.45.45	Recommended
□	172.168.50.122	G1S0XX1	PowerEdge R420	Broadcom G...	7.6.15	7.8.16	Recommended
□	172.168.50.122	G1S0XX1	PowerEdge R420	Integrated D...	1.23.23	1.50.50	Recommended
□	172.168.50.122	G1S0XX1	PowerEdge R420	PERC H310 ...	20.12....	20.12.1-0...	Up to date
□	172.168.50.122	G1S0XX1	PowerEdge R420	BIOS	1.6.7	1.6.7	Up to date
□	172.168.50.122	G1S0XX1	PowerEdge R420	Enterprise U...	4231A0	4231A0	Up to date
□	172.168.50.122	G1S0XX1	PowerEdge R420	Broadcom G...	7.6.15	7.6.15	Up to date
□	172.168.50.122	G1S0XX1	PowerEdge R420	Broadcom G...	7.6.15	7.6.15	Up to date

□ Allow components to be downgraded

3.5.2 Using DRM to update Firmware through OpenManage VMWare for vCenter

An inventory based repository can be created using DRM to update the firmwares through OpenManage VMWare for vCenter.

Provide the IP address or Host Name of the vSphere appliance, Username and Password of the server where OpenManage VMWare for vCenter resides to Dell Repository Manager. Once the required details are filled, Dell Repository Manager tries to gather the list of servers discovered by OpenManage VMWare for vCenter.

After successful operation, a repository gets created as shown in figure below. The repository contains bundles for each server discovered under OpenManage VMWare for vCenter. Updates for the same server are grouped under same bundle.

For more information on creating a repository using Dell Repository Manager, see the Technical paper "**Using Dell Repository Manager with OpenManage Essentials & Dell™ OpenManage Integration for VMware vCenter**" available at www.delltechcenter.com/repositorymanager.

4. Dell Repository Manager

Dell Repository Manager (DRM) is an application that allows you to easily manage system updates. DRM provides a searchable interface to create custom software collections known as bundles and repositories of Dell Update Packages (DUPs).

You can use the bundles and repositories for the deployment of multiple firmware updates at once. Additionally, DRM makes it easier to locate specific updates for a particular platform, which saves time.

DRM can also create repositories for multiple servers with multiple updates and export it to different deployment media such as a Light Weight Server Update Utility (SUU), Deployment Toolkit (DTK) Linux media, Light Weight Deployment Scripts, and so on.

For more information about Dell Repository Manager, see www.delltechcenter.com/repositorymanager.