Updating BIOS on Dell 12G PowerEdge Servers

Author(s)

Wei Liu

Raja Tamilarasan

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.

April 2012| Rev 1.0

Contents

Figures

Introduction

Customers using the 12th generation Dell PowerEdge Servers have a variety of ways to update the system BIOS. Customers can use any of the following methods, based on their needs and environment.

- Executing the BIOS DUP (Dell Update Package) from the operating system (OS)
- Using the DOS-based BIOS flash utility
- Using the UEFI-based BIOS flash utility
- Using the Lifecycle Controller Platform Update option (F10)
- Using the WSMAN-based 1:Many Remote Update method (Remote Enablement)

1:1 Updates

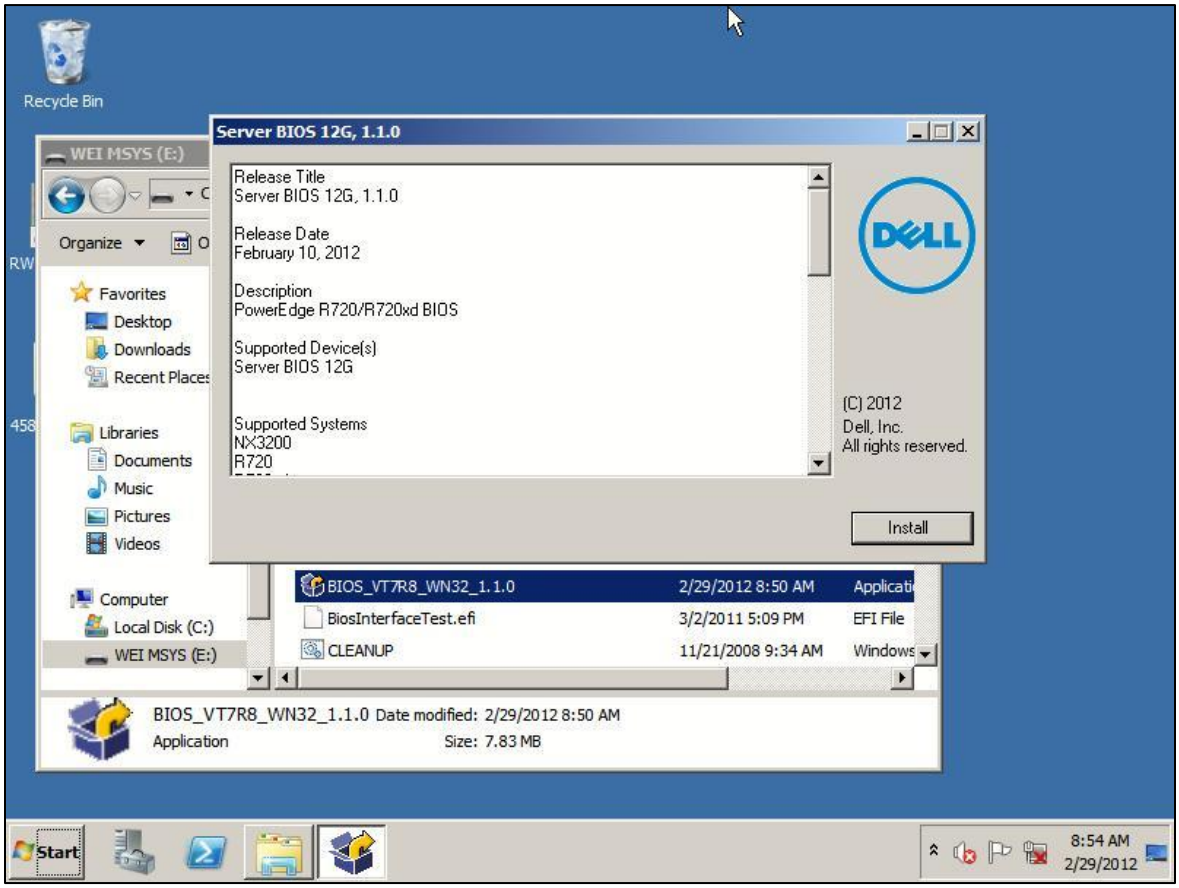
BIOS DUP (Dell Update Package) from the Operating System (OS)

Windows DUP

Installation steps:

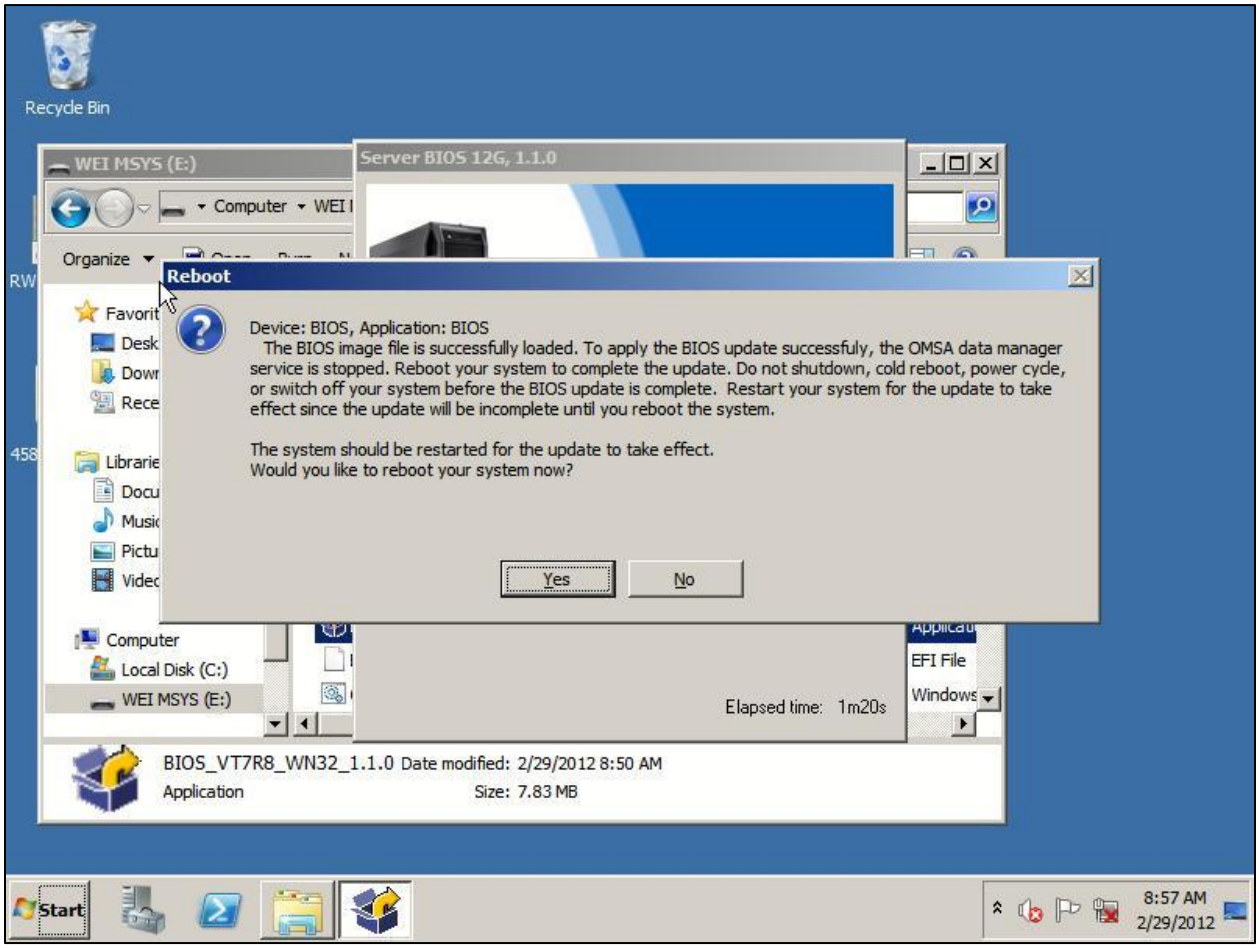
1. Browse to the location where you downloaded the file (for example, BIOS_VT7R8_WN32_1.1.0.EXE) and double-click the new file.
2. Read the release information presented in the dialog window (Figure 1).

Figure 1. Windows DUP



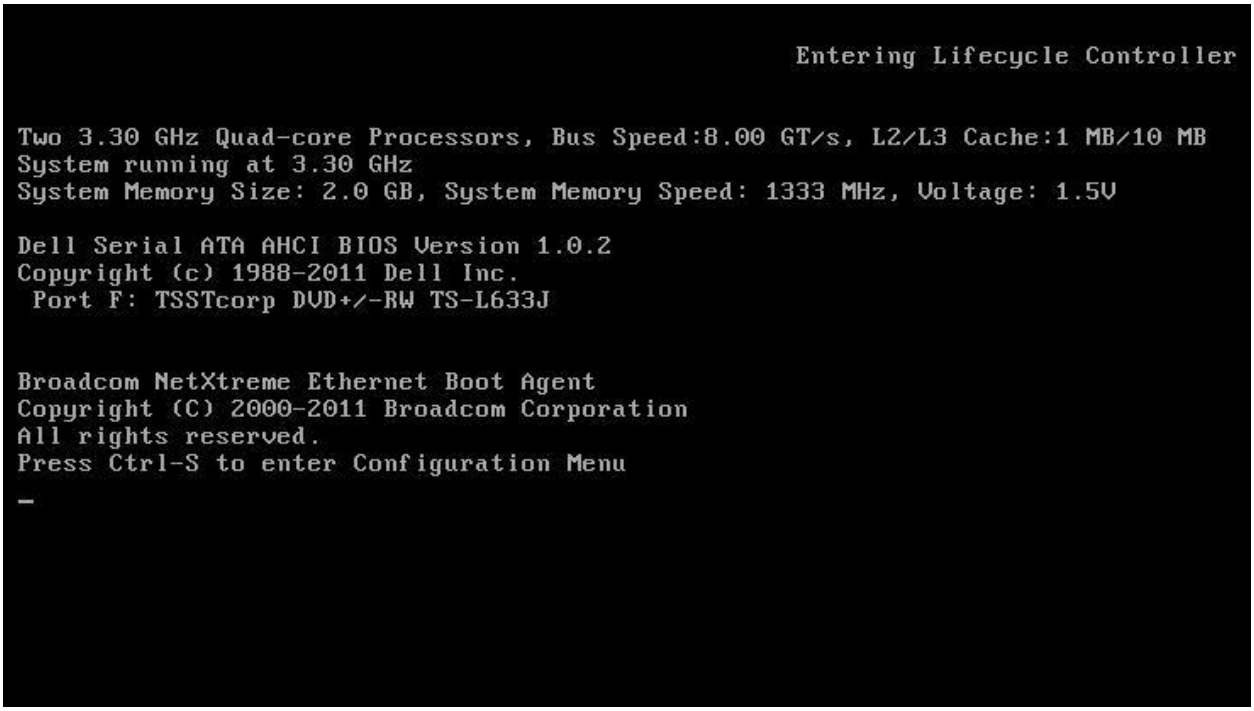
3. Click Install.
4. Follow the remaining prompts to perform the update (Figure 2).

Figure 2. After DUP installation, a system reboot is required for the update to be staged



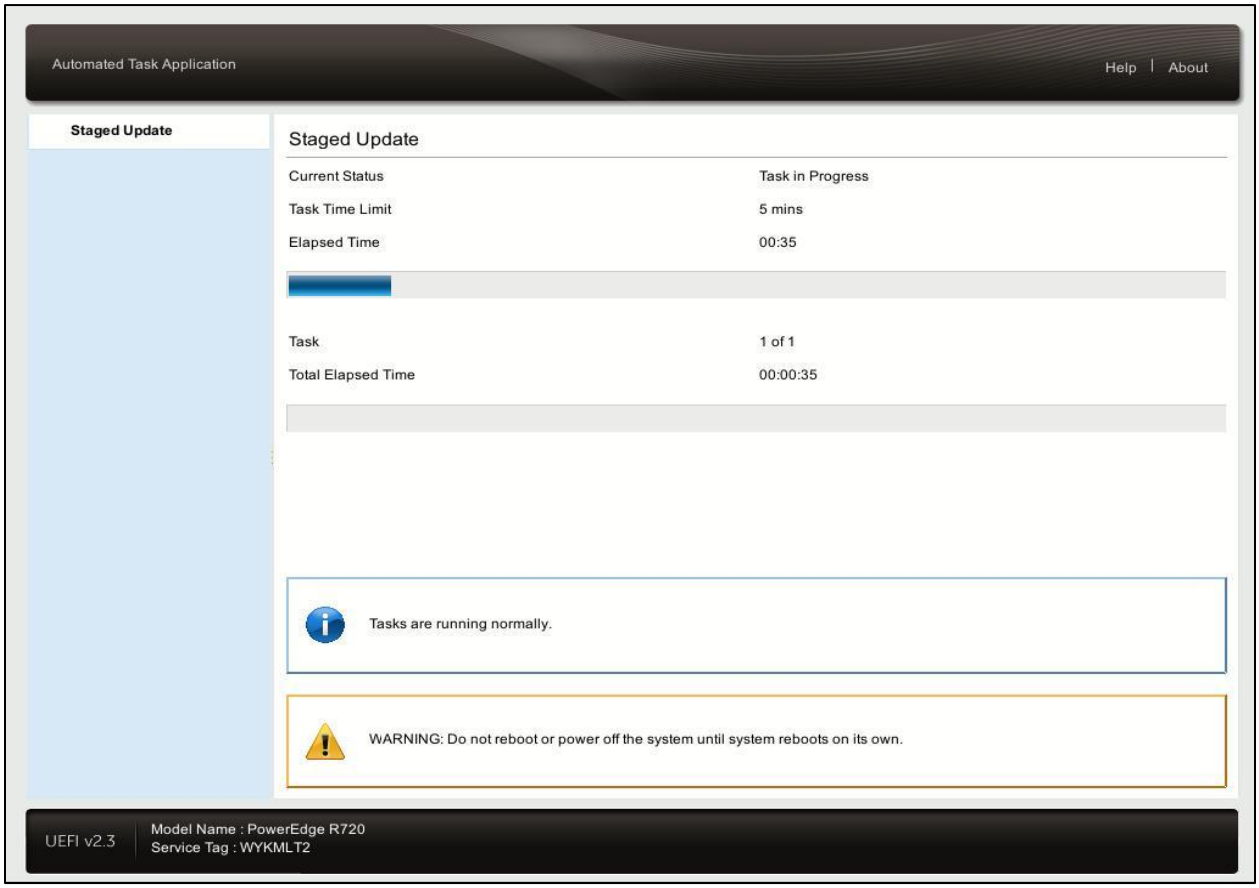
5. The system will reboot and launch Lifecycle Controller (Figure 3).

Figure 3. System reboots to Lifecycle Controller



6. The Lifecycle Controller will invoke the BIOS update (Figure 4). This may take a few minutes. After the BIOS is updated, a system reboot will automatically take place and boot back to the host operating system.

Figure 4. The BIOS update inside Lifecycle Controller

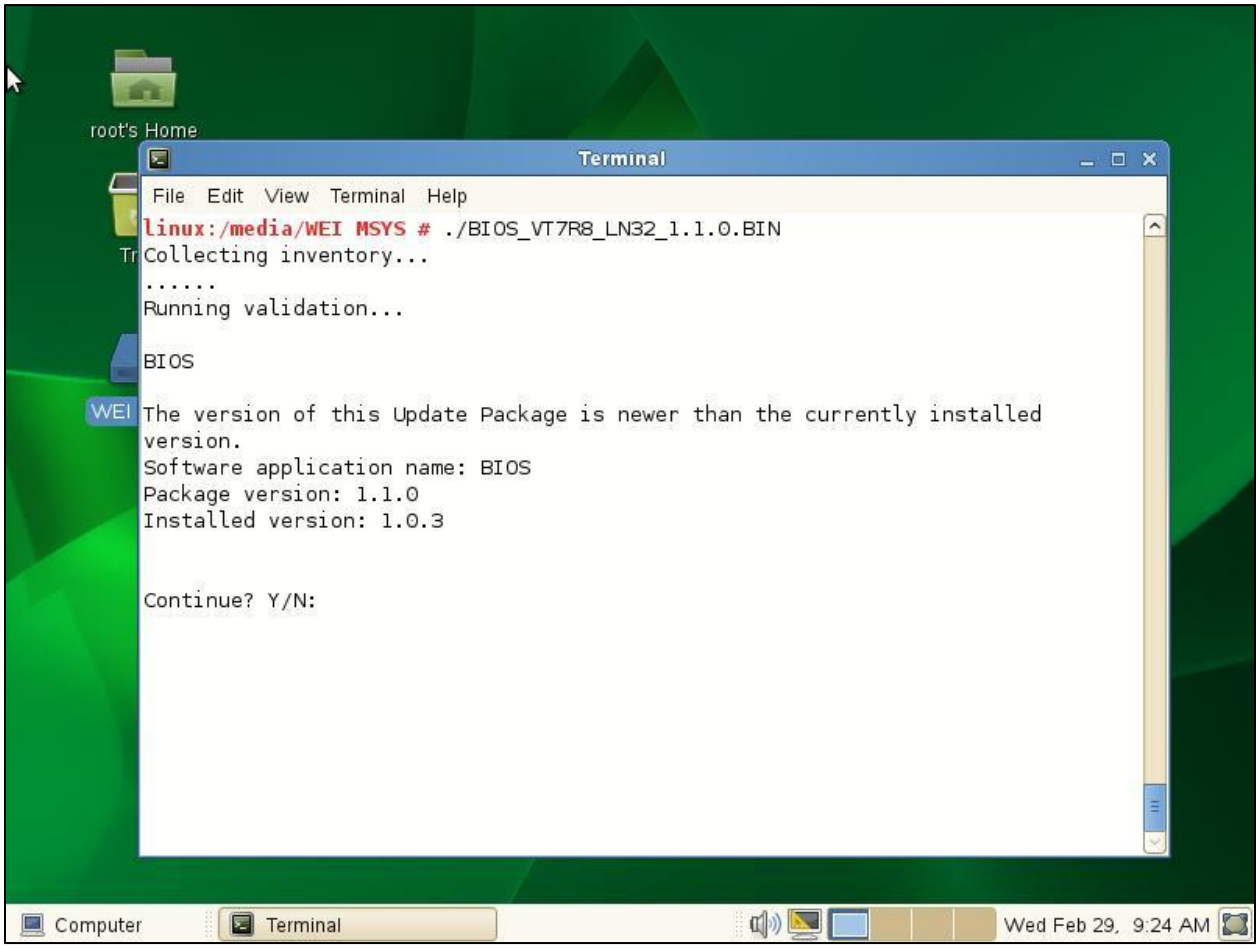


Linux DUP

Installation steps:

1. Read over the release information presented by executing the "./PER710_BIOS_LX_6.0.7.BIN" command from the shell.
2. Run the update by executing "./PER710_BIOS_LX_6.0.7.BIN" from the shell (Figure 5).

Figure 5. Linux DUP



3. Follow the remaining prompts to perform the update.
4. The system will reboot and launch Lifecycle Controller (Figure 3).
5. The Lifecycle Controller will invoke the BIOS update (Figure 4). This may take a few minutes. After the BIOS is updated, a system reboot will automatically take place and boot back to the host operating system.

DOS-based BIOS Flash Utility

The DOS or DRMK (Dell Real Mode Kernel)-based BIOS flash utility for each platform can also be found at the Dell support website. Note that you must have DOS bootable media, such as a USB key. To update the BIOS using this utility, perform the following steps:

1. Browse to the location where you downloaded the file.
2. Update the name of the file to DOS-recognizable format (8.3). If you do not update the filename to 8.3 format, the file name will be truncated to 8.3 format.
3. For more information on the 8.3 format, refer to http://en.wikipedia.org/wiki/8.3_filename.

4. Copy the file to the bootable device.
5. Boot the system to DOS by using the bootable device.
6. Run the executable under DOS. Follow the instructions provided by the flash utility. Figure 6 is a snapshot of the DOS flash utility. The update will take a minute or so, and a system reboot is required after the update is completed.

Figure 6. DOS-based BIOS flash utility

UEFI-based BIOS Flash Utility

Dell releases a UEFI-based BIOS flash utility for each 12th generation platform. There are two ways to utilize this utility, one is to run it from a UEFI shell, and the other is to load it directly from BIOS Boot Manager.

Run BIOS Flash Utility in a UEFI Shell

In this method, you must provide a UEFI-bootable device, such as a USB key. To make a USB key bootable in UEFI mode, you can download the UEFI shell binary from the UEFI open source website (ttp://sourceforge.net/apps/mediawiki/tianocore/index.php?title=UEFI_Shell) and save it as the following file on the USB key:

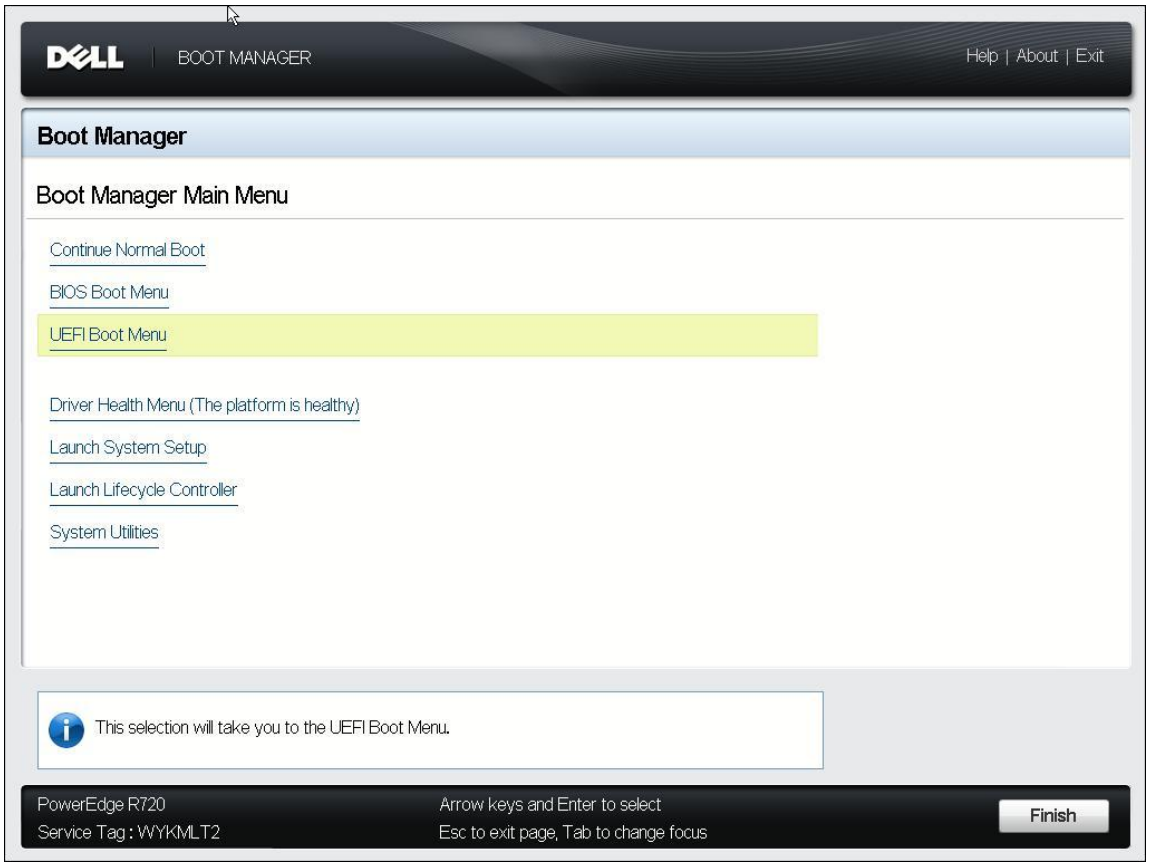
efi\boot\bootX64.efi

To update the BIOS under the UEFI shell, perform the following steps:

1. Copy the downloaded UEFI BIOS flash utility (for example, R720-010100.efi) to the USB key which has the UEFI shell.

2. Plug in the USB key and power on the system. Press F11 during POST to enter BIOS Boot Manager (Figure 7).

Figure 7. BIOS Boot Manager



3. Click UEFI Boot Menu and choose the UEFI-bootable USB key to boot.
4. From the UEFI shell prompt, locate the file system for the USB key, and launch the BIOS flash utility (Figure 8).

Figure 8. Flash BIOS in UEFI shell

5. Follow the on-screen instruction to update the BIOS (Figure 9 and Figure 10).

Figure 9. UEFI-based BIOS flash utility

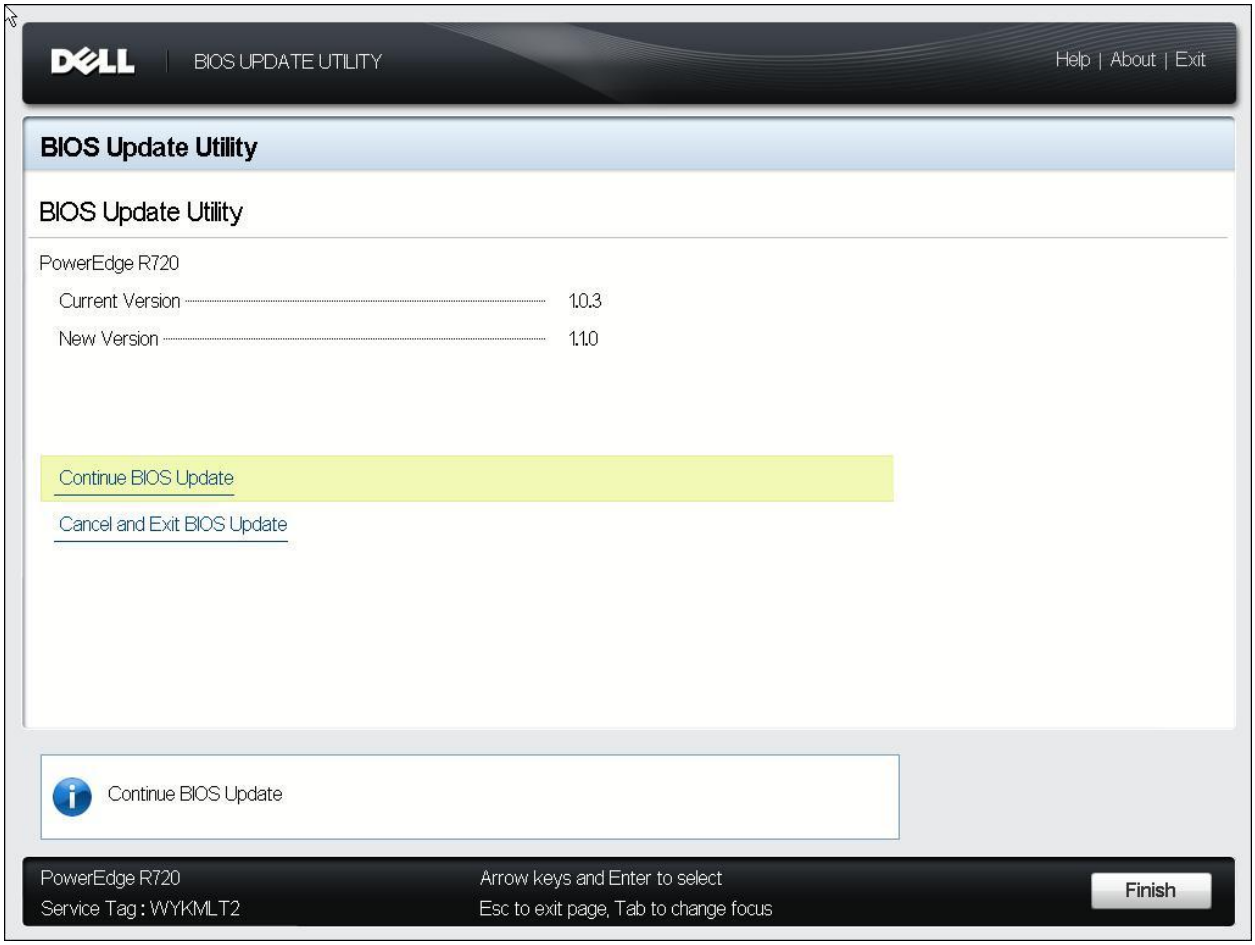


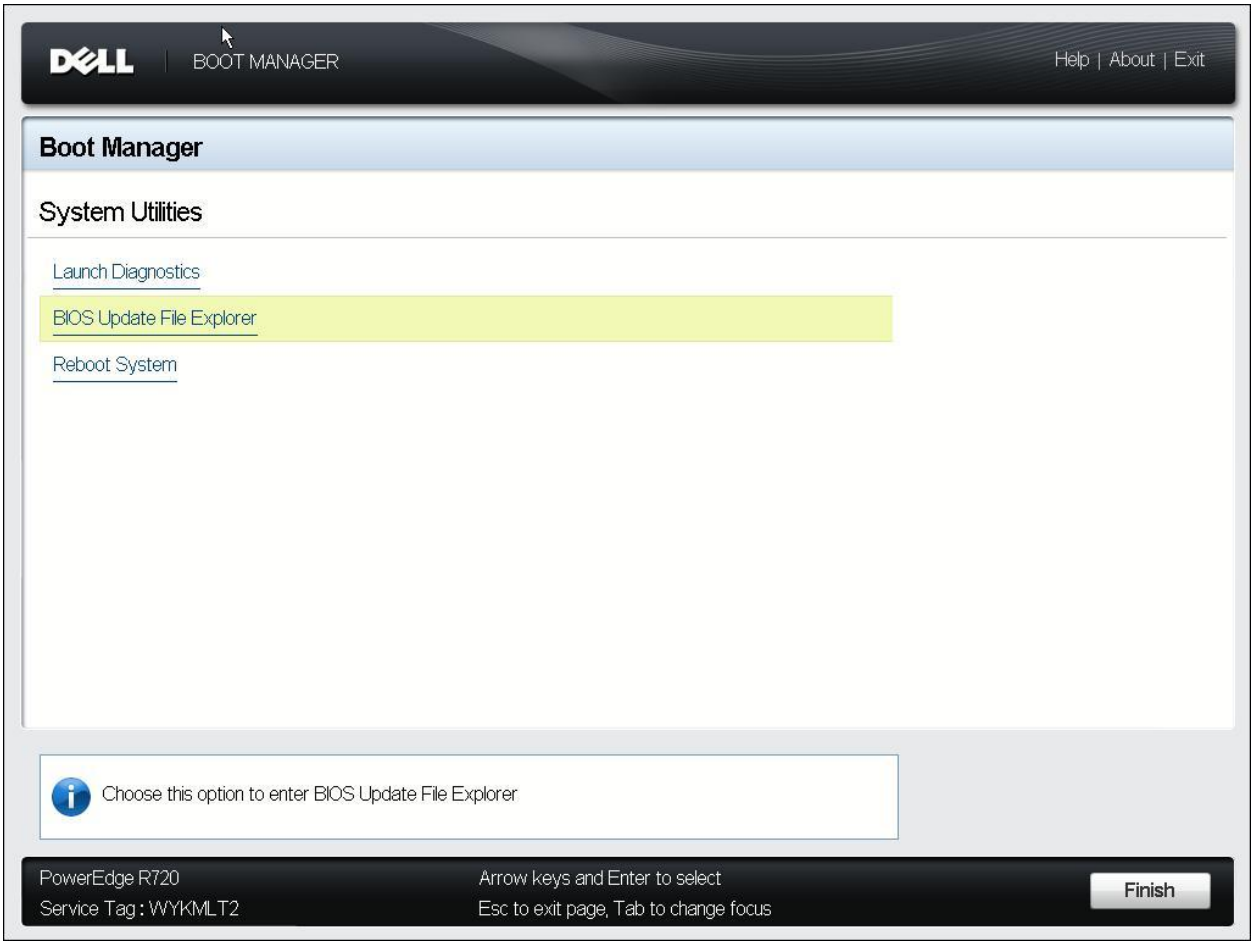
Figure 10. UEFI-based BIOS flash utility

Load the BIOS Flash Utility from BIOS Boot Manager

In case you don't have a UEFI shell, you can still use the following method to update the BIOS using the UEFI BIOS flash utility.

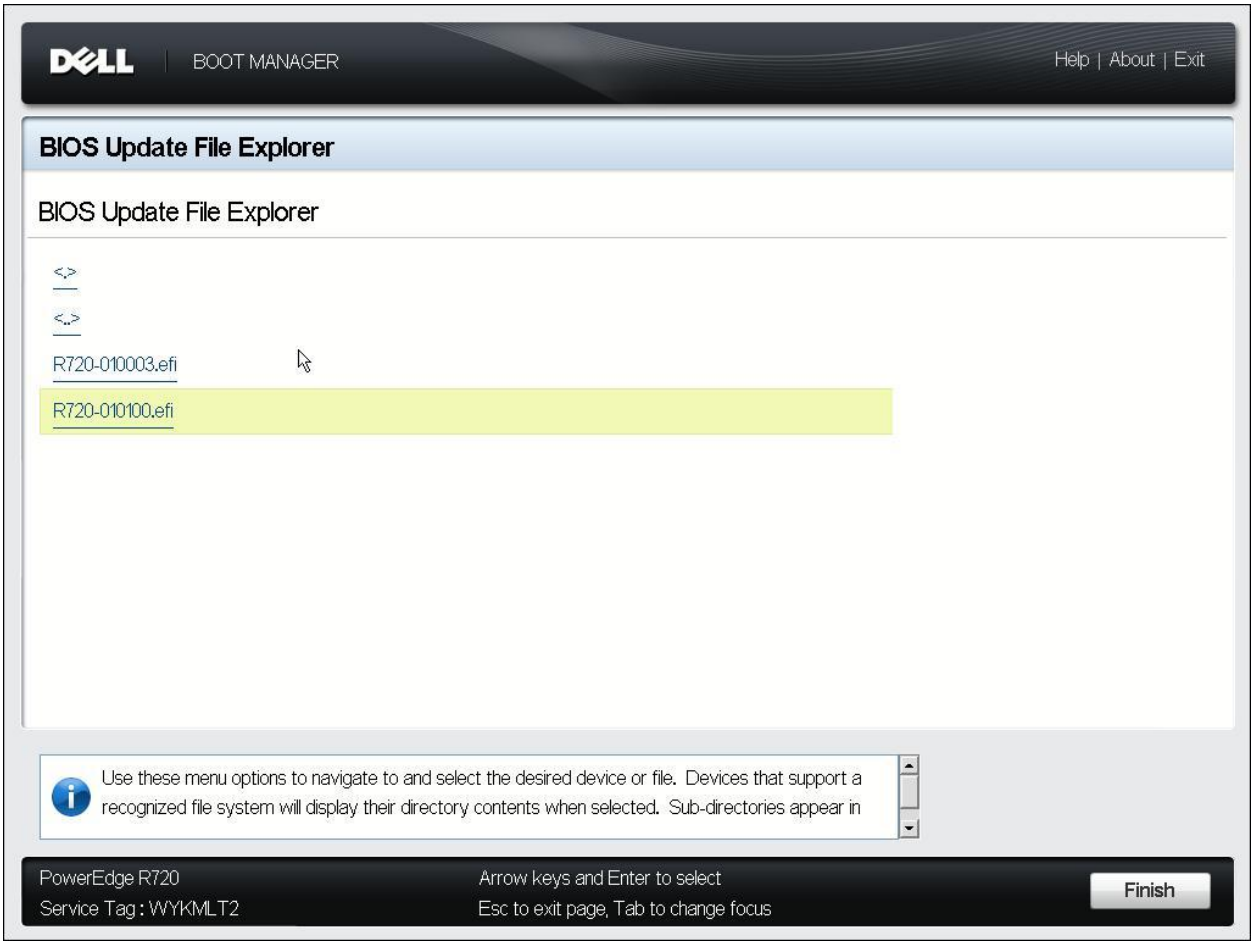
1. Copy the downloaded UEFI BIOS flash utility (.efi) to a USB key.
2. Plug in the USB key and power on the server. Press F11 during POST to enter the BIOS Boot Manager (Figure 7).
3. Navigate to the System Utilities menu and select BIOS Update File Explorer (Figure 11).

Figure 11. BIOS Update File Explorer



4. Select the USB key, and navigate through the directory contents to find the UEFI BIOS flash utility (for example, R720-010100.efi) (Figure 12).

Figure 12. Use BIOS Update File Explorer to select the BIOS UEFI flash utility file to update



5. The BIOS flash utility will launch when you select the file and press Enter. Then follow the on-screen instructions to update the BIOS (Figure 9 and Figure 10).

Update BIOS via Lifecycle Controller (F10)

Lifecycle Controller provides a Platform Update wizard that can be used to flash the BIOS and other firmware as well. You can use the Platform Update wizard to view the current versions of the installed applications and firmware, display the list of available updates, and select the required updates, downloads, and apply the updates. Different methods, such as FTP server, local USB devices, and network share, can be set up to access the updates in your organization. For detailed usage, please refer to the Lifecycle Controller User's guide. In this document we use the local USB device as an example.

Lifecycle Controller can be entered by pressing F10 during POST. To update the BIOS using Lifecycle Controller, perform the following steps.

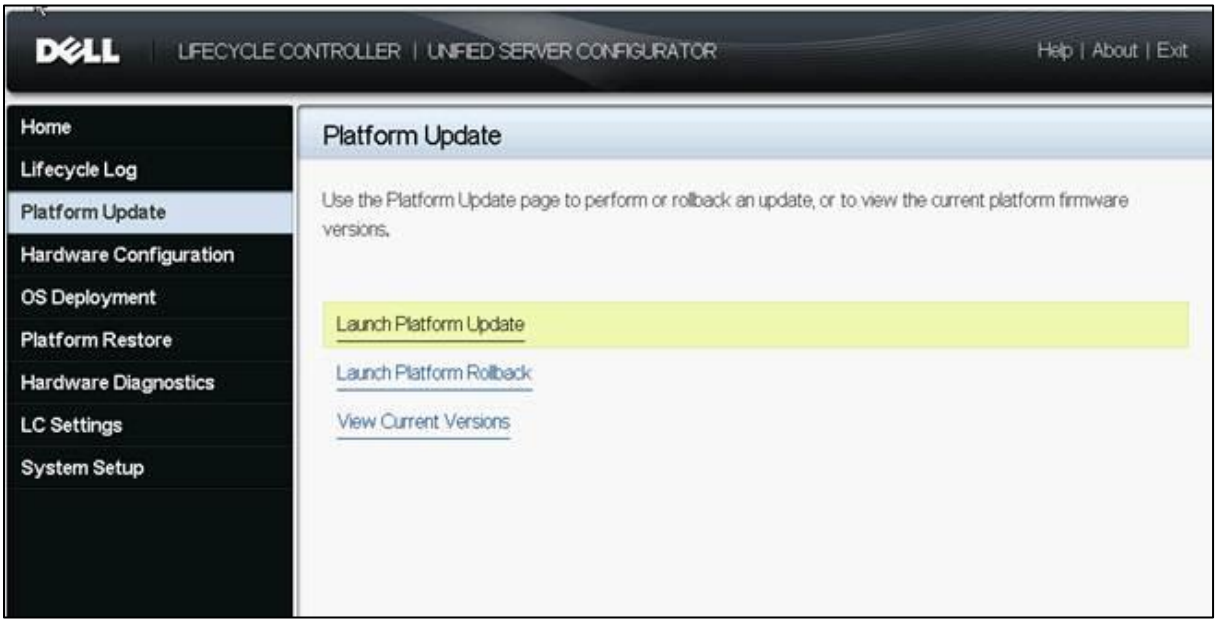
1. Plug the USB into the host.

2. Press F10 during POST. Lifecycle Controller will open (Figure 13).

Figure 13. Lifecycle Controller screen after pressing F10 during POST

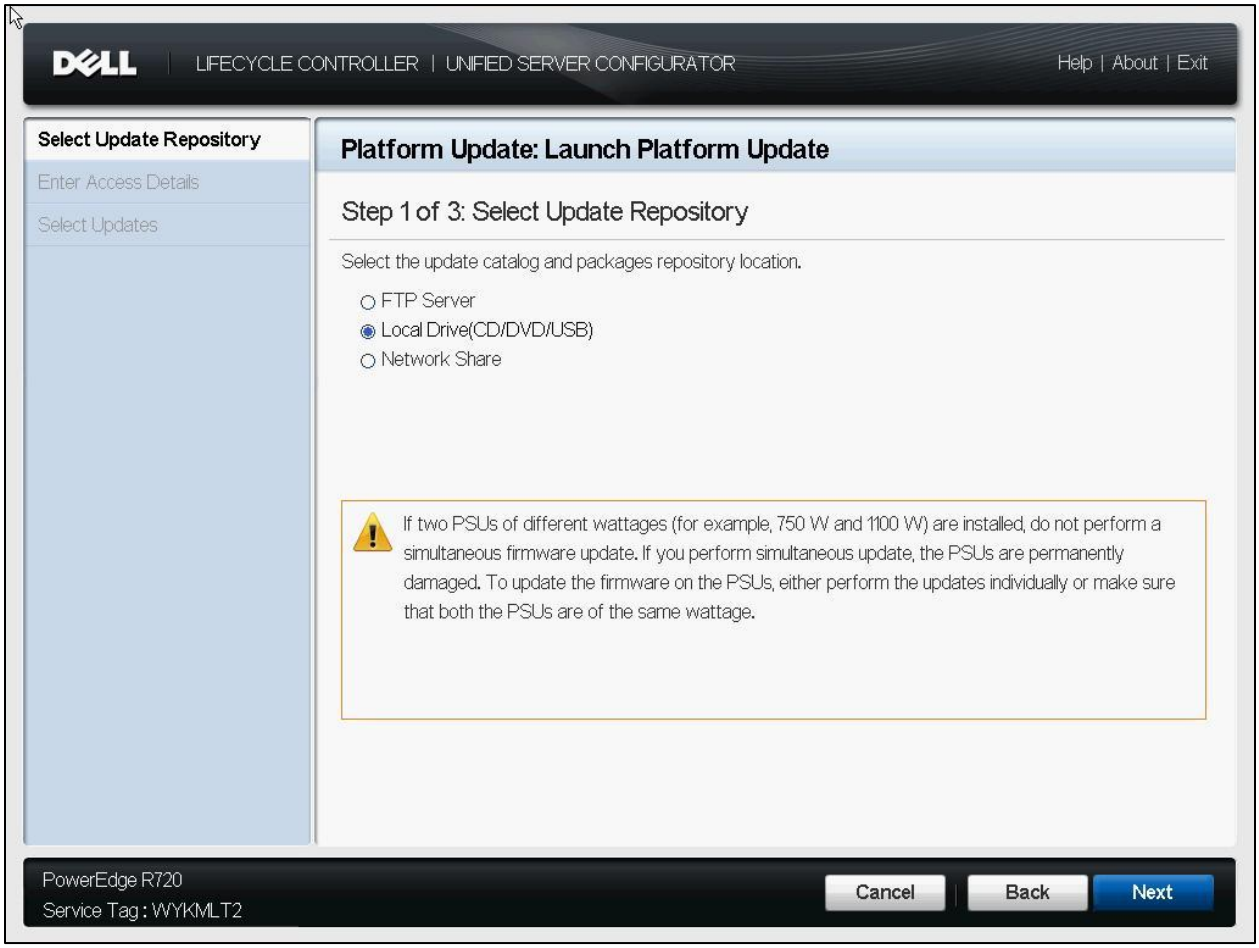
1. Click on Platform Update → Launch Platform Update (Figure 14).

Figure 14. Platform Update screen



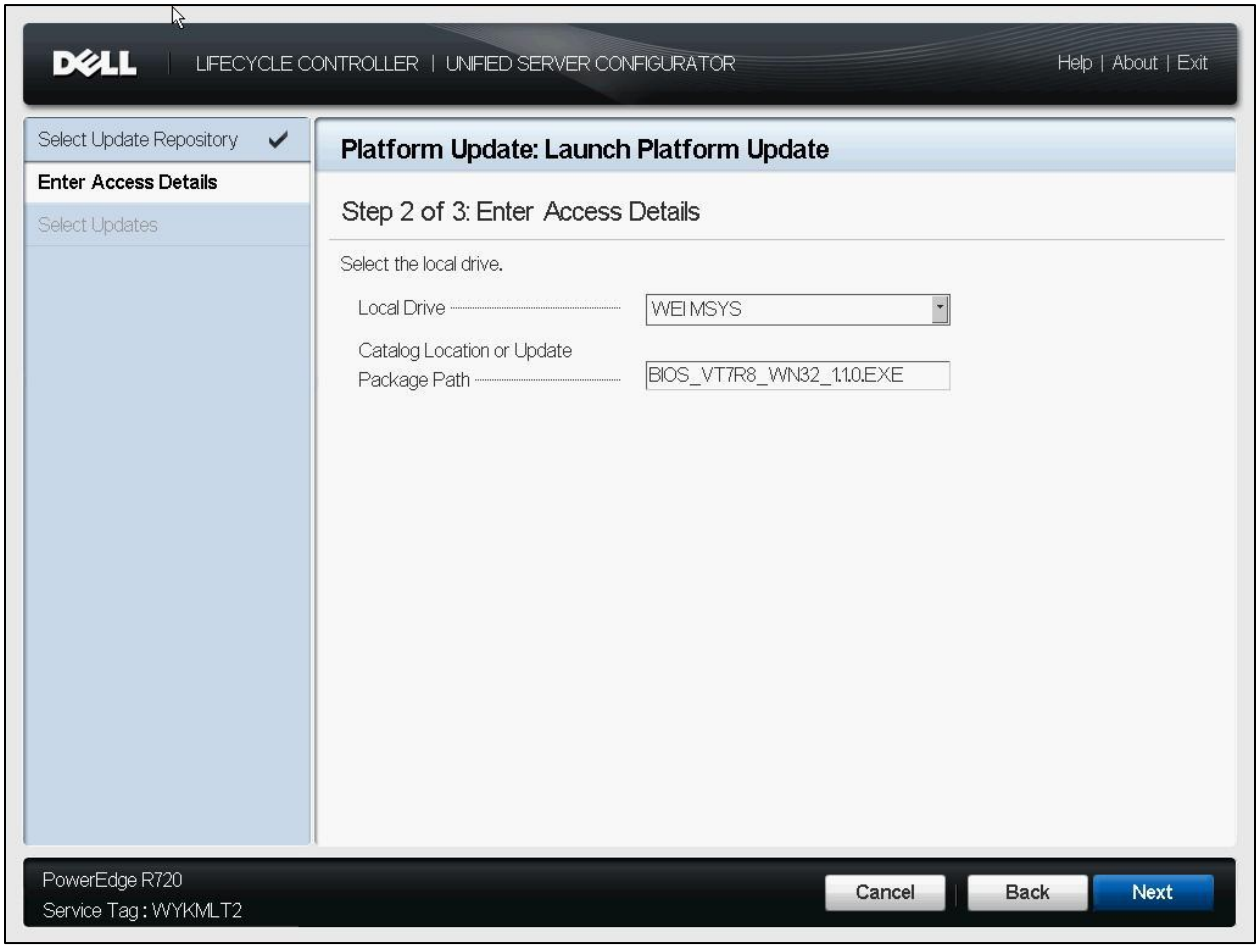
2. Select Local Drive (Figure 15).

Figure 15. Select Update Repository in Platform Update



3. Select your USB device from the Local Drive drop-down list. Type in the name of the DUP (for example, BIOS_VTR78_WN32_1.1.0.EXE) to be used to update.

Figure 16. Select the local drive and type in the DUP file to use



6. Click Next and follow the on-screen instructions to complete the BIOS update.

1:Many Updates

Remote BIOS Update using WSMAN

The option discussed here is a remote BIOS update feature using a CIM method based on the DMTF standard through the WSMAN protocol, a network transport service that enables the user to access a number of CIM-style data access methods supported by the target platform. The WSMAN protocol is transmitted through an SSL-encrypted HTTP connection.

Figure 17. Remote Firmware Update

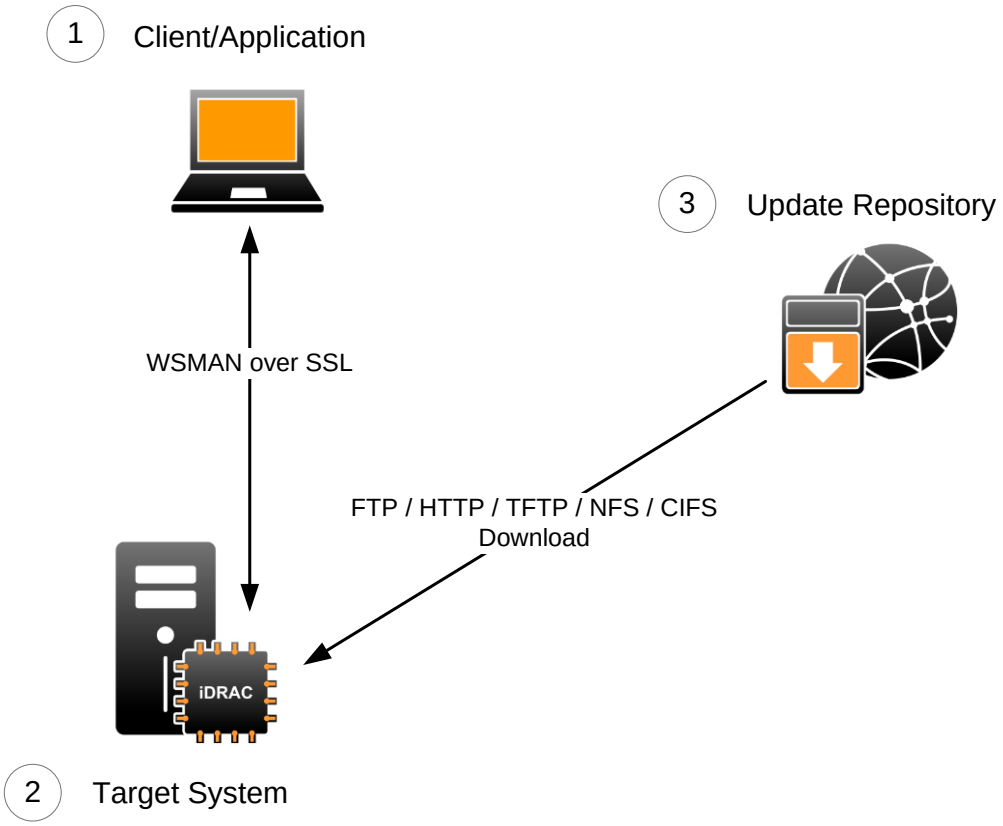


Figure 17 shows the pictorial view of the environment. It starts with the administrator (1) running scripts to send WSMAN commands through an SSL connection. The target system (2) is equipped with iDRAC, which is the management controller with advanced capabilities. The update repository (3) contains the Dell update packages (DUPs) that will be used to update the firmware on the target system.

Before you Begin

Here is a list of items that you need to prepare:

1. Verify that the target system is a Dell PowerEdge server with iDRAC enabled, configured, and network-reachable to talk WSMAN.

2. If you are using Windows, verify that the winrm command line tool is configured and ready. If you need help with this, read Installation and Configuration of Windows Remote Management.

3. If you are using Linux, verify that the openwsman command line tool is built, installed, and ready. If you need help with this, go to the Openwsman Home and join the mailing list for access to technical help.

4. Verify that Python version [2.7] is installed on your system. If you need help with this, refer to Python Home.

5. Download the Python scripts from [Click Here].

    a. [fw_inventory.py]
    b. [fwupdate.py]
    c. [fw_poll.py]

Performing a firmware update on your system

The remote firmware update process involves the following steps:

1. Get Firmware Information Installed on your System

2. Begin the Update Process

3. Monitor the update process

Get Firmware Information Installed on your System

The script to perform a firmware inventory on your system is:

`fw_inventory.py`

Run `fw_inventory.py –h` to see usage options.

```
./fw_inventory.py --help
Usage: fw_inventory.py [options]

Options:
-h, --help            show this help message and exit
-v, --verbose         Prints information verbosely
-f FWUPDATE, --firmware component=FWUPDATE
prints component information(nic, bios, idrac_fw,
drivers_pack, power_supply, raid,
lifecycle_controller, diagnostics)
```

1. The `fw_inventory.py` script will prompt for

```
Enter iDRAC IP Address: [iDRAC IP]
Enter User Name: [USER NAME]
Enter User Password: [PASSWORD]
```

The first argument is the IP address of the iDRAC on the target system. The second is the user name. If the user is an AD account, then the syntax is “USER@DOMAIN.” The third argument is the user password.

2. The script establishes a connection with the iDRAC and also performs certificate validation.

```
Pinging 192.168.0.206. Waiting for response. Done.
Getting SSL Certificate. Waiting for response. Done
```

3. Once a successful connection is established, the `fw_inventory.py` script performs a Software Inventory and lists the components that are installed and are available to be rolled back to.

A sample output:

```
OPTION       Component     Status      Comp ID   VersionType

1(update)    FRMW        Installed   26018     0.12 BP12G+ 0:2

2(update)    FRMW        Installed   68138     D505   Physical Disk 0:2:0

3(update)    FRMW        Installed   Empty     7.0.21 Broadcom NetXtreme Gigabit Ethernet

4(update)    FRMW        Installed   Empty     7.0.21 Broadcom NetXtreme Gigabit Ethernet

5(update)    BIOS        Installed   159       1.0.4 BIOS

6(update)    FRMW        Installed   Empty     7.0.21 Broadcom NetXtreme Gigabit Ethernet

7(update)    FRMW        Installed   26041     03.10.13 Power Supply.Slot.1

8(update)    FRMW        Installed   25227     1.00.00    Integrated Dell Remote Access
Controller

9(rollback)  FRMW        Available   25227     1.00.00    Integrated Dell Remote Access
Controller

10(update)   APAC        Installed   25806     4216.1   Dell Enterprise UEFI Diagnostics
Diagnostics Utility

11(update)   APAC        Installed   28897     1.0.0.3551 Dell Lifecycle Controller 2,
1.0.0.3551, X69

12(update)   FRMW        Installed   27763     0.5.3    System CPLD

13(update)   APAC        Installed   18981     7.0.0.38 Dell OS Driver Pack, v.7.0.0.38, X38

14(update)   FRMW        Installed   Empty     3.0.0-0135 PERC S110 Controller

15(update)   FRMW        Installed   Empty     20.10.1-0066 PERC H310 Mini
```

Begin the Update Process

The script to perform a firmware update on your system is:

fwupdate.py

Run `fwupdate.py –h` for usage options.

```
 ./fwupdate.py -h
Usage: fwupdate.py [options]

Options:
  -h, --help            show this help message and exit
  -f CONFIG_FILE, --file=CONFIG_FILE
                        Enter config file with parameters the script needs.
                        Example of a file is fwupdate.cfg.
  -v, --verbose         Prints information verbosely
  --cleanenv            Cleans .log, .xml, and .cer files in current directory.
```

1. On running the fwupdate.py script, you will be prompted for the following:

```
Enter iDRAC IP Address: [iDRAC IP]
Enter User Name: [USER NAME]
Enter User Password: [PASSWORD]
```

The first argument is the IP address of the iDRAC on the target system. The second is the user name. If the user is an AD account, then the syntax is "USER@DOMAIN." The third argument is the user password.

2. The script establishes a connection with the iDRAC and also performs certificate validation.

```
Pinging 192.168.0.206. Waiting for response. Done.
Getting SSL Certificate. Waiting for response. Done
```

3. Once a successful connection is established, the `fwupdate.py` script performs a Software Inventory and lists the components that are updatable.

   A sample output of the command:

```
[Firmware Component Inventory List]
b   - bios
dp  - drivers_pack
i   - idrac_fw
n   - nic
p   - power_supply
r   - raid
lc  - lifecycle_controller
d   - diagnostics
a   - all
```

   Each entry in the output lists the device that can either be:

   a. Updated to firmware located on a network share (ftp/http/tftp/nfs/cifs).

      (or)

   b. Rolled back to a previous version of the firmware that is stored on the iDRAC.

4. Select the component alias (from Step 3) of the component for which you would like to see the firmware inventory. Once a component type is selected, the script lists options that are available for rollback and updates for that particular component.

```
  View component firmware inventory: b

OPTION       Component   Status      Comp ID   Version      Type

1 (update)    BIOS      Installed   159       1.0.4        BIOS
```

5. Once the firmware inventory is listed, you can either continue with the firmware update step or exit.

6. To perform a firmware update, select one of the options that are available for updating.

```
1 (update)    BIOS      Installed   159       1.0.4 BIOS
```

7. The script will prompt for the location of the Dell Update Package (DUP) to be used. This location is called the Update Repository; see item 3 in **Error! Reference source not found.**. iDRAC supports the following download methods with source URI syntax:

   - FTP
     ftp://[IPADDRESS]/[LOCATION]/[DUPFILENAME]
   - HTTP
     http://[IPADDRESS]/[LOCATION]/[DUPFILENAME]
   - TFTP
     tftp://[IPADDRESS]/[LOCATION]/[DUPFILENAME]
   - CIFS
     cifs://[USER]:[PASSWORD]@[IPADDRESS]/[LOCATION]/[DUPFILENAME];mountpoint=[MOUNTNAME]
   - NFS
     nfs://[IPADDRESS]/[LOCATION]/[DUPFILENAME];mountpoint=[MOUNTNAME]

The portions of the syntax in all capital letters represent user-provided values. The [IPADDRESS] is the IP address of the update package repository. The [LOCATION] is the path or directory. The [DUPFILENAME] is the update package file name. The only supported update package is the "Dell Update Package for Windows" that can be downloaded from support.dell.com. [USER] and [PASSWORD] refer to the user credentials allowed to access and download from the share. [MOUNTNAME] refers to the share mount name.

The following is a sample output:

```
 Options

tftp://192.168.0.100/BIOS_VT7R8_WN32_1.1.0.EXE

nfs://192.168.0.100/BIOS_VT7R8_WN32_1.1.0.EXE;mountpoint=/pub

cifs://DOMAIN\\USER:PASS@192.168.0.100/pub/BIOS_VT7R8_WN32_1.1.0.EXE;mountpoint=E

http://192.168.0.100/BIOS_VT7R8_WN32_1.1.0.EXE

ftp://192.168.0.100/BIOS_VT7R8_WN32_1.1.0.EXE
```

Enter the path of the image file: tftp://192.168.0.100/BIOS_VT7R8_WN32_1.1.0.EXE

8. The script prompts for a reboot type with which the host will be rebooted to perform the update. Select an appropriate reboot type.

```
  Reboot Type Options (1,2,3, and 4)

  1  =   Forceful shutdown and reboot
```

```
2  =   Graceful shutdown and reboot (Recommended)

3  =   Forceful shutdown if graceful shutdown does not succeed

4  =   No reboot
```

9. The script prompts for deleting all existing jobs in iDRAC. Dell recommends that you choose “yes” to have a clean start.

```
Erase all previous jobs stored in the iDRAC? (yes/no) yes

 Deleting all iDRAC jobs

 Completed job deletion
```

10. The script prompts you to specify the start time for the job. The job can be scheduled either immediately or for a future time.

```
Schedule the bios update now or schedule later (now, schedule)? now
```

    The format of the StartTime argument is defined by the CIM Infrastructure Specification. Select the “now” option to schedule the jobs immediately. Use the “schedule” option to schedule the job for a future time. The “schedule” option will prompt for a start time, which should be of the format MM-DD-YYYY hh:mm:ss

```
Y = Year, M = Month, D = Day, H = Hour, m = minute, S = second

12-13-2011 11:11:11
```

    Once the start time is specified, the Update job is initiated.

11. The update package is downloaded from the repository and may take some time depending on the size of the package and network state.

12. Once the update package is successfully downloaded, the update and the reboot job are scheduled for the specified start time.

The following is a sample output:

```
bios update successfully created

Creating reboot job

Reboot job successfully created.

      Scheduling bios update job

      Scheduling reboot job

The bios updating from version 1.0.4 to version
tftp://192.168.0.100/BIOS_VT7R8_WN32_1.1.0.EXE

Check the status of the reboot job and the bios update job by using the fw_pull.py
script.
```

A sample output of a failed command:

```
The command failed with error code: CMPI_RC_ERR_INVALID_PARAMETER
```

If the command fails, verify that the InstanceID you provided is accurate by comparing it with the output from the previous step. Compare each character. Characters are case-sensitive. Also, check the accuracy of the source URI. Ensure that it is accessible with proper permission. Once verified, try the command again.

13. Once the specified start time is reached, the host reboots and launches Lifecycle Controller to perform the firmware update.

Monitor the Update Execution

The final portion of the update process is to monitor when the actual update is executed and ultimately be able to verify the update by checking the new version from the inventory enumeration.

The script to monitor the update:

fw_poll.py

```
Run fw_poll.py –h for usage options
```

```
./fw_poll.py -h
Usage: fw_poll.py [options]

Options:
  -h, --help            show this help message and exit
  -j JOBID, --JobID=JOBID
                        Provide one of the JobIDs (begins with JID or RID)
                        within the fwupdate.out file
  -v, --verbose         Prints information verbosely
```

Once the script is run, it prompts for the following:

- The IP address of the iDRAC on the target system.
- The user name. If the user is an AD account, then the syntax is “USER@DOMAIN”.
- The user password.

The following is a sample output of the command:

```
Available JobIDs.

(1) JID_267336093962

   - bios updating to image located at tftp://192.168.0.100/BIOS_VT7R8_WN32_1.1.0.EXE

(2) RID_267336106745

   - reboot for bios update

(0) exit out
```

```
Enter a number to poll JobID or to exit. (1,2,etc): 1

   JobStatus = Scheduled

   Message = Task successfully scheduled.

   MessageArguments = NA

   MessageID = JCP001

   Name = update:DCIM:INSTALLED#701__BIOS.Setup.1-1

   Repeat get JobStatus command for JID_267336093962? (yes, no):
```

Select the number corresponding to your job and it will list of the current status of the job.

The script performs two steps. The first step is to monitor the status of the job associated with the update. When it detects the status is “completed”, it monitors the status of the data sync. At this time, the update has been executed and the device is running the new firmware level.

BIOS update using Repository Manager

Dell Repository Manager is an application that allows IT administrators to easily manage system updates. Repository Manager provides an easy-to-use, searchable interface to create custom collections known as bundles and repositories of Dell Update Packages (DUPs).

For more information on Repository Manager, refer to the techcenter link below.

http://en.community.dell.com/techcenter/systems-management/w/wiki/1767.repository-manager.aspx

BIOS update using Dell Management Plug-In for VMware vCenter

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.

For more information on the Dell Management Plug-In for VMware vCenter, refer to the following link:

http://en.community.dell.com/techcenter/systems-management/w/wiki/1961.aspx

BIOS update using Dell Chassis Management Controller (CMC)

The Dell Chassis Management Controller (CMC) is a systems management hardware and software solution for managing multiple Dell blade chassis. The CMC, which is a hot-pluggable module that sits in the back of a Dell blade Chassis, provides a secure web / browser-based interface that enables an

IT administrator to take inventory, perform configuration and monitoring tasks, remotely power on/off blades, and enable alerts for events on servers and components in the blade chassis.

For more information on performing updates using the Dell Chassis Management Controller, refer to the following link:

http://en.community.dell.com/techcenter/systems-management/w/wiki/dell-chassis-management-controller.aspx