Updating BIOS on 13th Generation Dell PowerEdge Servers

Wei Liu
Dell Server BIOS Development

Raja Tamlarasan
Dell Server Lifecycle Controller Development

August 2014
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2014</td>
<td>Initial draft</td>
</tr>
</tbody>
</table>

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.

© 2014 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the DELL logo, and the DELL badge are trademarks of Dell Inc. Intel, the Intel Logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. Microsoft, Windows, and Windows Server are 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 any proprietary interest in the marks and names of others.
# Table of contents

Revisions .................................................................................................................................................. 2  

Executive summary ................................................................................................................................. 4  

1. Executing the BIOS DUP from within the operating system .............................................................. 4  
   1.1 Using Microsoft Windows DUP .................................................................................................... 4  
   1.2 Using Linux DUP ......................................................................................................................... 8  
   1.3 Using an UEFI-based BIOS flash utility ...................................................................................... 9  
   1.3.1 Run BIOS flash utility in UEFI shell ....................................................................................... 10  
   1.3.2 Loading the BIOS flash utility directly from the Boot Manager ............................................ 16  
   1.4 Updating the BIOS using the iDRAC web GUI ......................................................................... 17  
   1.5 Updating BIOS using Lifecycle Controller ............................................................................... 19  
   1.6 Remote BIOS update using WS-MAN ....................................................................................... 23  
   1.6.1 Before you begin .................................................................................................................. 24  
   1.6.2 Performing a firmware update on your system ................................................................. 25
Executive summary

The 13th generation of Dell PowerEdge servers offer a variety of methods - local or remote, with or without an operating system, to update the system BIOS. The different methods are listed below. You can choose the method that best suits your need and environment.

- Executing the BIOS Dell Update Package (DUP) from within the operating system.
- Using the UEFI-based BIOS flash utility in a pre-boot environment.
- Using the Lifecycle Controller Platform Update option (F10).
- Using the Update and Rollback feature in iDRAC web GUI.
- Using the WS-MAN based 1:many Remote Update method (Remote Enablement)

Note: Legacy DOS-based BIOS update utility is no longer supported.

1. Executing the BIOS DUP from within the operating system

1.1 Using Microsoft Windows DUP

Installation steps:

1. Browse to the location where you downloaded the file (e.g. BIOS_K44R7_WN32_1.0.2.EXE) and double-click the new file.
2. Read the release information and click Install.
Fig. 1 Windows DUP

3. Follow the instructions on the screen to perform the update. (Fig. 2).
Fig. 2 After DUP installation, a system reboot is required for the update to be staged.

The system reboots and launches Lifecycle Controller.
Lifecycle Controller invokes the BIOS update (Fig.4). This may take a few minutes. Ensure that you do NOT shutdown or reset the system during this operation. After the BIOS update is completed, the system reboots automatically.
1.2 Using Linux DUP

Installation steps:

1. Read the release information before running the "./BIOS_K44R7_LN_1.0.2.BIN" command from the shell.

2. Run the update by executing "./BIOS_K44R7_LN_1.0.2.BIN" from the shell (Fig.5).
3. Follow the instructions on the screen to perform the update.

The system reboots and launches Lifecycle Controller (Fig. 3). Lifecycle Controller invokes the BIOS update (Fig. 4). This may take a few minutes. After the BIOS is updated, the system reboots automatically.

1.3 Using an UEFI-based BIOS flash utility

Dell releases a UEFI-based BIOS flash utility for each 13th generation of server platform. You can use this utility using any of the following methods:

- Run it from a UEFI shell
- Load it directly from the BIOS boot manager.
1.3.1 Run BIOS flash utility in 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 must download the UEFI shell binary from the UEFI open source website (http://tianocore.sourceforge.net/wiki/UEFI_Shell) and save it as efi\boot\bootX64.elf file on the USB key.

To update the BIOS under UEFI shell, follow the below steps:

1. Copy the downloaded UEFI BIOS flash utility (for example, R730-010002.elf) to the USB key which has the UEFI shell.
2. Connect the USB key and turn on the system.
3. Press &lt;F11&gt; during POST to enter the BIOS Boot Manager (Fig. 6).

![Fig. 6 Boot Manager]

4. If the boot mode is set to UEFI already, then select the One-shot UEFI Boot Menu and choose the UEFI bootable USB key to boot from. Proceed to step 7.
If the boot mode is set to BIOS, then navigate to the System Utilities menu and select the BIOS Update File Explorer (Fig. 8).
5. Select the USB key, and navigate through the directory contents to find the UEFI shell (namely bootX64.efi) (Fig. 9).
Fig. 9 Select the UEFI shell from the File Explorer

6. Select the file and press <Enter> to launch the BIOS flash utility.
7. From the UEFI shell prompt, locate the file system on the USB key, and launch the BIOS flash utility (Fig.10).
### Fig. 10 UEFI shell prompt

8. Follow the instructions on the screen to update the BIOS (Fig.11 and Fig.12).
Fig. 11 UEFI-based BIOS Update Utility
1.3.2 Loading the BIOS flash utility directly the from Boot Manager
In case you do not have a UEFI shell, you can use the Boot Manager to update the BIOS using the UEFI BIOS flash utility.

1. Copy the downloaded UEFI BIOS flash utility (e.g. R730-010002.efi) to a USB key.
2. Connect the USB key and turn on the server.
3. Press <F11> during POST to enter the BIOS Boot Manager (Fig. 6).
4. Navigate to the **System Utilities** menu and select **BIOS Update File Explorer** (Fig. 8).
5. Select the USB key, and navigate through the directory contents to find the UEFI BIOS flash utility (e.g. R730-010002.efi) (Fig.13).
6. Select the file and press <Enter> to launch the BIOS flash utility.
7. Follow the instructions on the screen to update the BIOS (Fig.11 and Fig.12)

### 1.4 Updating the BIOS using the iDRAC web GUI

1. Launch the iDRAC web GUI.
2. Click **iDRAC Settings** -> **Update and Rollback**.
3. From the Update tab, browse to the BIOS update package file (Windows DUP) and upload it. Both the Win32 and Win64 DUPs are supported in this method.
Fig. 14 Upload the BIOS DUP file in Firmware Update

4. Select the update and click either of the following options:

- **Install and reboot** – This option restarts the server and launches into Lifecycle Controller to perform the update.

- **Install next reboot** – This option stages the update for the next server restart.

You should see similar screen shots as Fig. 3. And Fig. 4 in the next reboot.
Fig. 15 Update the BIOS via iDRAC Firmware Update

5. Navigate to the **Job Queue** page to monitor the status of the update jobs.

**Note:** Only the Windows DUPs (both 32-bit and 64-bit) are supported in this method.

The BIOS update using the iDRAC **Firmware Update** method starts only if the server is not in POST. Make sure that the server is up and running in the operating system or is turned off before invoking the update process.

### 1.5 Updating BIOS using Lifecycle Controller

Lifecycle Controller provides a **Platform Update** wizard which allows you to flash the BIOS and other firmware. You can use the **Platform Update** wizard to view the current versions of the installed applications and firmware, display the list of available updates, select the required updates, download and apply the updates. You can set up different methods, such as FTP server, local USB devices, and network share to access the updates in your organization. For more information, see the Lifecycle Controller User’s guide.
Perform the steps below to update the BIOS using Lifecycle Controller:

1. Connect the USB flash drive that contains the Windows DUP file (both Win32 and Win64 versions are supported) to the server.
2. Press <F10> during POST to launch Lifecycle Controller.
3. In the left pane, click **Firmware Update**.
4. In the right pane, click **Launch Firmware Update**.

\[
\text{Fig. 16 Platform Update Screen in Lifecycle Controller}
\]

5. Select **Local Drive (CD or DVD or USB)** as the Update Repository.
6. Select the USB device you connected from the Local Drive drop down list. Type the name of the DUP in the File Path or Update Package Path (e.g. BIOS_K44R7_WN32_1.0.2.EXE) (Fig. 18).
Fig. 18 Select the local drive and type in the DUP file to use

7. Click **Next** and follow the instructions on the screen to complete the BIOS update (Fig. 19 then Fig. 4).
1.6 Remote BIOS update using WS-MAN

This topic explains the remote BIOS update feature using a CIM method based on the DMTF standard through the WS-MAN protocol, a network transport service that enables you to access a number of CIM style data access and methods supported by the target platform. The WS-MAN protocol is transmitted through an SSL-encrypted HTTP connection.
Fig. 20 Remote Firmware Update

Fig. 20 shows the pictorial view of the environment.

1 - Administrator runs the scripts to send WS-MAN command using an SSL connection.

2 - A target system equipped with iDRAC which is the management controller with advanced capabilities.

3 – DUPs used to update the firmware on the target system.

1.6.1 Before you begin

Before you begin, make sure that the following prerequisites are met:

- Ensure that the target system is a Dell PowerEdge server with iDRAC enabled, configured and network reachable to talk WS-MAN.
- On a server running Windows operating system, check if the `winrm` command line tool is configured and ready. For more information on the command, see Installation and Configuration of Windows Remote Management.
On a server running the Linux operating system, check if the openwsman command line tool is built, installed and ready. For more information on the command, go to the Openwsman Home and join the mailing list for access to the technical help.

Check if Python version 2.7 is installed on your system. For more information on the installation, see Python Home.

Download the following Python scripts from http://en.community.dell.com/dell-groups/dtcmedia/m/mediagallery/20011473

- [fw_inventory.py]
- [fwupdate.py]
- [fw_poll.py]

**1.6.2 Performing a firmware update on your system**

Perform the following steps to remotely update the firmware:

1. Get Firmware Information Installed on your System
2. Begin the update process.
3. Monitor the update process.

**1.6.2.1 Get firmware information installed on your system**

Run the following script to collect a firmware inventory on your system:

```bash
./fw_inventory.py
```

**Usage:** fw_inventory.py [options]

**Options:**
- `--help` show this help message and exit
- `--verbose` Prints information verbosely
- `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 prompts you for the following information:

   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 is the user password.

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

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

3. After a successful connection is established, the `fw_inventory.py` script performs a software inventory and lists out the components that are installed and the available version you can roll back to.

A sample output:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>Component</th>
<th>Status</th>
<th>Comp ID</th>
<th>Version</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1(update)</td>
<td>FRMW</td>
<td>Installed</td>
<td>26018</td>
<td>0.12 BP12G+ 0:2</td>
<td></td>
</tr>
<tr>
<td>2(update)</td>
<td>FRMW</td>
<td>Installed</td>
<td>68138</td>
<td>D505 Physical Disk 0:2:0</td>
<td></td>
</tr>
<tr>
<td>3(update)</td>
<td>FRMW</td>
<td>Installed</td>
<td>Empty</td>
<td>7.0.21 Broadcom NetXtreme Gigabit Ethernet</td>
<td></td>
</tr>
<tr>
<td>4(update)</td>
<td>FRMW</td>
<td>Installed</td>
<td>Empty</td>
<td>7.0.21 Broadcom NetXtreme Gigabit Ethernet</td>
<td></td>
</tr>
<tr>
<td>5(update)</td>
<td>BIOS</td>
<td>Installed</td>
<td>159</td>
<td>1.0.2 BIOS</td>
<td></td>
</tr>
<tr>
<td>6(update)</td>
<td>FRMW</td>
<td>Installed</td>
<td>Empty</td>
<td>7.0.21 Broadcom NetXtreme Gigabit Ethernet</td>
<td></td>
</tr>
<tr>
<td>7(update)</td>
<td>FRMW</td>
<td>Installed</td>
<td>26041</td>
<td>03.10.13 Power Supply.Slot.1</td>
<td></td>
</tr>
<tr>
<td>8(update)</td>
<td>FRMW</td>
<td>Installed</td>
<td>25227</td>
<td>1.00.00 Integrated Dell Remote Access Controller</td>
<td></td>
</tr>
<tr>
<td>9(rollback)</td>
<td>FRMW</td>
<td>Available</td>
<td>25227</td>
<td>1.00.00 Integrated Dell Remote Access Controller</td>
<td></td>
</tr>
<tr>
<td>10(update)</td>
<td>APAC</td>
<td>Installed</td>
<td>25806</td>
<td>4216.1 Dell Enterprise UEFI Diagnostics</td>
<td></td>
</tr>
<tr>
<td>11(update)</td>
<td>APAC</td>
<td>Installed</td>
<td>28897</td>
<td>1.0.0.3551 Dell Lifecycle Controller 2, 1.0.0.3551, X69</td>
<td></td>
</tr>
<tr>
<td>12(update)</td>
<td>FRMW</td>
<td>Installed</td>
<td>27763</td>
<td>0.5.3 System CPLD</td>
<td></td>
</tr>
<tr>
<td>13(update)</td>
<td>APAC</td>
<td>Installed</td>
<td>18981</td>
<td>7.0.0.38 Dell OS Driver Pack, v.7.0.0.38, X38</td>
<td></td>
</tr>
<tr>
<td>14(update)</td>
<td>FRMW</td>
<td>Installed</td>
<td>Empty</td>
<td>3.0.0-0135 PERC S110 Controller</td>
<td></td>
</tr>
<tr>
<td>15(update)</td>
<td>FRMW</td>
<td>Installed</td>
<td>Empty</td>
<td>20.10.1-0066 PERC H310 Mini</td>
<td></td>
</tr>
</tbody>
</table>

1.6.2.2 Starting the update process

Run the following script to perform a firmware update on your system:

```
fwupdate.py
```

Usage: fwupdate.py [options]

Options:
- `--help` show this help message and exit
- `--file=CONFIG_FILE` Enter config file with parameters the script needs. Example of a file is fwupdate.cfg.
- `--verbose` Prints information verbosely
27

Updating BIOS on Dell 13th Generation of PowerEdge Servers

--cleanenv            Cleans .log, .xml, and .cer files in current directory.

1. The `fwupdate.py` script, prompts you for the following information:

   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 is the user password.

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

   Getting SSL Certificate. Waiting for response. Done

3. After a successful connection is established, the `fwupdate.py` script performs a software inventory and lists out the components that you can update.

   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

   The entries in the output displays the devices that can be:

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

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

4. Select the component alias (from step 3) for the component you would like to see the firmware inventory. After you select a component type, the list of options that are available for rollback and update for that particular component are displayed.

   View component firmware inventory: b
To perform a firmware update, select one of the options that are available for update.

A prompt for the location of the DUP is displayed. This location is referred as Update Repository in figure 17.

The following download methods are supported by iDRAC:

- 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]

You must provide the following details in the commands above:
- [IPADDRESS] is the IP address of the update package repository
- [LOCATION] is the path or directory where the update package is located
- [DUPFILENAME] is the name of the update package file name.

Note: Only Dell Update Package for Windows is supported. You can download the package from support.dell.com.

- [USER] and [PASSWORD] are the credential required to access and download the package from the share.
- [MOUNTNAME] is the share mount name.

The following is a sample output for the commands above:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>Component</th>
<th>Status</th>
<th>Comp ID</th>
<th>Version</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (update)</td>
<td>BIOS</td>
<td>Installed</td>
<td>159</td>
<td>1.0.2</td>
<td>BIOS</td>
</tr>
</tbody>
</table>

you can either continue with the firmware update or quit.
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
tftp://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. A prompt displaying the reboot type using which the host reboots to perform an update is displayed. 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. A prompt to delete all the existing jobs in iDRAC is displayed. It is recommended to select 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. A prompt to specify the start time for the job is displayed. 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

After the start time is specified, the update job is initiated.

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

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

The following shows the 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 1.0.2 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_poll.py script.

A sample output of a failed command:

The command failed with error code: CMPI_RC_ERR_INVALID_PARAMETER

When the command fails, check the InstanceID you provided is accurate by comparing it with the output from the previous step. Also, check the accuracy of the source URL. Ensure that it is accessible with proper permission. Once verified, try the command again.

After the specified Start Time elapses, the host reboots and launches System Services to perform the firmware update.

1.6.2.3 Monitoring the update execution

The final step of the update process is to monitor if the actual update is executed and verify the update by checking the new version from the inventory enumeration.

Run the following script to monitor the update execution:

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)
-v, --verbose          Prints information verbosity

The script prompts you for the following information:

- IP address of the iDRAC on the target system.
- User name. If the user is an AD account then the syntax is “USER@DOMAIN”.
- Password.
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 to list the current status of the job.

The script performs the executions in 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 starts to monitor the status of the data sync. At this time, the update executes and the device runs the new firmware level.