DELL UPDATE PACKAGES FOR LINUX

Version 7.4

Release Notes

Release Type and Definition

This Readme contains updated information for your "Dell Update Packages for Microsoft Windows Operating Systems User's Guide" and any other technical documentation included with the Dell Update Packages for Linux.

Version

7.4

Release Date:

December 2013

Previous Version

7.3

Importance

Dell Update Packages offer ease and flexibility for updating the system software on Dell PowerEdge systems. Update Packages are available for the following software components:

- System BIOS
- System firmware, also known as the Embedded Systems Management
- (ESM) firmware
- Dell Remote Access Controller (DRAC)/Integrated Dell Remote Access Controller (IDRAC) firmware, which also includes Embedded Remote Access (ERA) firmware
- PowerEdge Expandable RAID Controller (PERC) firmware
- Software RAID Controller firmware
- Baseboard Management Controller (BMC) firmware
- SCSI Backplane (BP) firmware
- SAS BP firmware
- SAS Expander firmware
- SSD firmware
- SED firmware
- SAS HDD Firmware
- SAS Controller firmware
- SEP firmware
- PowerVault 100T firmware
- PowerVault 110T firmware
- PowerVault MD1000 firmware
- PowerVault MD1120 firmware
- PowerVault MD1200 firmware
- PowerVault MD1220 firmware
- PowerVault RD1000 firmware
- Power Supply firmware
- Broadcom Network Adapter Firmware
- Intel Network Adapter Firmware
- QLogic Network Adapter Firmware
- Emulex Network Adpater Firmware
- OpenManage Server Administrator updates
- Mellanox Network Adapter Firmware

CONTENTS

- CRITICALITY
- MINIMUM REQUIREMENTS
- UPDATE PACKAGES: SUPPORTED COMPONENTS
- KNOWN ISSUES

CRITICALITY

2 – Recommended
It is recommended that you apply this update during your next scheduled update cycle. The update contains feature enhancements or changes that will keep your system software current and compatible with other system modules (firmware, BIOS, drivers, and software).

MINIMUM REQUIREMENTS

The Update Packages support Dell systems running the following Linux operating systems:

* Red Hat Enterprise Linux 5.8 x86
* Red Hat Enterprise Linux 5.8 x86_64
* Red Hat Enterprise Linux 5.9 x86
* Red Hat Enterprise Linux 5.9 x86_64
* Red Hat Enterprise Linux 6.3 server (64-bit)
* Red Hat Enterprise Linux 6.4 server (64-bit)
* SUSE Linux Enterprise Server 10 SP4 x86_64
* SUSE Linux Enterprise Server 11 SP2 x86_64
* SUSE Linux Enterprise Server 11 SP3 x86_64
* VMware ESX Server version 4.1 Update 3
* Citrix Xen Server 6.1
* Citrix Xen Server 6.2

NOTE: For the latest information about the various systems and operating systems that Dell Update Packages are supported on, see the "Dell Systems Software Support Matrix". This guide is available on the Dell Support website at "dell.com/support/manuals".

Update Packages may also be applied in a pre-operating system environment that uses the embedded Linux (ELI) environment through the Dell OpenManage Deployment Toolkit (DTK).

UPDATE PACKAGES: SUPPORTED COMPONENTS

Update Packages currently do not support all system component types. Dell will continue to make Update Packages available on additional devices in future.

This release of Update Packages supports updates to the devices listed in the following table.

Component Type	Supported Components
BIOS	
DRAC firmware	DRAC 5, iDRAC6, iDRAC7
RAID firmware	PERC H200, PERC S300 Adapter, PERC 5/E, PERC 5/i, SAS 5/i,

	SAS 5/iR Adapter, SAS 5/E, SAS 5/iR, SAS 6/iR, SAS 6/iR Adapter, PERC 6/E, PERC 6/i, PERC 6/i Adapter, CERC6/i PERC H310 Adapter,PERC H310 Mini Blade, PERC H710P Mini Blade,PERC H810 Adapter, PERC H710P Adapter,PERC H710 Mini Monolithic, PERC H310 Mini Monolithic,PERC H710 Adapter PERC H710P Mini Monolithic,PERC H710 Mini Blade PERC H700 Adapter,PERC H700 Modular,PERC H800 Adapter, PERC H700 Integrated
BMC firmware	BMC
SCSI BP firmware	BP
SAS BP, SEP firmware	BP
Storage enclosure	PowerVault MD1000, PowerVault MD1120, PowerVault MD1200, PowerVault MD1220
Tape drives firmware	PowerVault 100T DDS4, PowerVault 110T DAT72, PowerVault 110T LTO1, PowerVault 110T LTO2, PowerVault 110T LTO2-L, PowerVault 110T LTO3, PowerVault 110T LTO3-HH, PowerVault 110T LTO4, PowerVault 110T SDLT320, PowerVault 110T DLT VS80, PowerVault 110T DLT VS160, PowerVault 110T SDLT
Removable disk drive backup firmware	PowerVault RD1000
Network adapter firmware	Broadcom NetXtreme family of adapters Broadcom NetXtreme II family of adapters Intel PRO PCI-E Gigabit family of adapters QLogic Network family of adapters Emulex Network family of adapters Mellanox-Alpha Centauri Network family of adapters Mellanox Network Adapter Firmware Mellanox ConnectX-3 Dual Port 10 GbE DA/SFP + Ethernet Adapter.

KNOWN ISSUES

For all Dell Update Packages

- On a Hyper-V virtual machine setup, while updating the Host OS components, ensure that the Guest OS's is not running.

- If you try to run the inventory for after the Broadcom Inventory Collector is run, then Mellanox Inventory Collector fails. To resolve, run the Mellanox Inventory Collector prior to running the Broadcom Inventory Collector or install Mellanox Ethernet drivers.

- Do not run other applications while executing Dell Update Packages.

- For firmware Dell Update Packages, an update package will not inventory the device if only a native non-Dell driver is installed. Thus the firmware update packages will not upgrade a device with a native driver.

- If the following error is displayed, Error while loading shared libraries: libstdc++.so.5: cannot open shared object file: No such file or directory", install the compatibility libraries from your Linux distribution. To install the compatibility libraries, use the following command:

  ```
  "rpm -ivh compat-libstdc++-33-3.2.3-47.3.i386.rpm"
  ```

  SLES 10 and SLES 11 (all service packs) uses
  "libstdc++-33-32bit-3.3.3-11.9.x86_64.rpm"

- If Update Packages stop abruptly due to a power outage or abnormal termination, perform the following steps:
  1. Remove the lock file.
  2. Type the following command to do so: "rm -f /var/lock/.spsetup"
  3. Run the Update Package again.

- If you see the message, "This Update Package is not compatible with any of the devices detected on your system", for a supported device, ensure that you have the latest Dell drivers for your system from the Dell Support website at www.support.dell.com.

- Some distributions of Linux may automatically mount a USB flash drive with the "-noexec" option. This prevents the execution of any wfile on that drive, including Dell Update Packages. If you are attempting to run a Dell Update Package from a USB flash drive under Linux, and are experiencing problems, remount the drive without the "-noexec" option, or copy the Dell Update Package to a drive mounted without the "-noexec" option.

- Dell Update Packages do not require new refreshes of existing SWB's to be reinstalled since the firmware image or driver does not change when the SWB is refreshed. A new DUP with different SWB is available if changes have been made to the firmware image or driver.

- If the console terminal displays USB connection status messages, ignore them as they do not affect the system.

- On all versions of ESX the following the USB Connection message with errors, these messages can also be ignored. The following shows a typical message:

  ```
  Vendor: iDRAC     Model: MAS022          Rev: 1.00
  Type:   Direct-Access                    ANSI SCSI revision: 02

  VMWARE SCSI Id: Supported VPD pages for sdc : 0x1f
  VMWARE SCSI Id: Could not get disk id for sdc
  VMWARE: Unique Device attached as scsi disk sdc at scsi3, channel 0, id 0, lun 0

  Attached scsi removable disk sdc at scsi3, channel 0, id 0, lun 0
  SCSI device sdc: 327680 512-byte hdwr sectors (168 MB)
  sdc: Write Protect is on
  SCSI disk error: host 3 channel 0 id 0 lun 0 return code = 8000002

  Current sd08:21: sense key Data Protect
  Additional sense indicates Write protected

  I/O error: dev 08:21, sector 1
  SCSI disk error : host 3 channel 0 id 0 lun 0 return code = 8000002
  ```

```
  Current sd08:21: sense key Data Protect
  Additional sense indicates Write protected
  I/O error: dev 08:21, sector 1

 Vendor: iDRAC     Model: SECUPD           Rev: 0329
   Type:   Direct-Access                   ANSI SCSI revision: 02
```

- DRAC5 updates are not supported on ESX 4.1. But if you run DRAC5 updates on ESX 4.1, console messages show up asking for IPMI installations, however later the updates goes through successfully.

- DUPs are designed to run only on a 32-bit environment. To run DUPs on a pure 64-bit environment, use the Dell YUM repository.

- If you attach VMedia on a system with the iDRAC Firmware version 1.5 some DUPs may fail to work. To resolve this issue, run the following command:
  racadm config -g cfgRacVirtual -o cfgLCDriveEnable 1 where cfgLCDriveEnable is an option implemented in iDRAC 1.5 with a default of 0 (disabled)

  NOTE: This command enables LCDrive from the iDRAC console or the OS. If the LCDrive is not enabled, DUPs may not work. After the DUP update is complete, to ensure the LCDrive is invisible, run the following command:
  racadm config -g cfgRacVirtual -o cfgLCDriveEnable 0.

- When you run USC-related DUPs with Citrix Xenserver 5.6.0-x, you need to set the virtual media in iDRAC to Detach. If you set the virtual media to Attach, the following error message is displayed:
  "Inventory Failure: Secure Copy Failure - The Secure copy function has failed"
  For BIOS updates, the following message is displayed:
  "doDepCheck failed"
  For other USC access related DUPs (PSU, NIC, SAS, PERC, BackPlane), the update is successful but the following error message may be displayed:

  ```
  "... mount: block device /dev/secmasupd-SECUPD is write-protected ...
     /bin/cp: cannot create regular file ..."
  ```

- When you try to execute DUPs on a 64-bit RHEL operating system, it fails to execute since DUP is a 32-bit application. To work around this issue, manually install the following RPMs:

  ```
  glibc.i686
  compat-libstdc++.i686
  libstdc++.i686
  zlib.i686
  libxml2.i686
  ```

- While executing some DUP's on 11G servers and When virtual media is in attached mode, a window with name SECUPD will popup and close automatically. Due to this there will be no functionality impact on DUP. This behaviour is observed across all RHEL OS flavours.

- Linux CLI Options
  For options beginning with '--', abbrevations are also supported.

Power Supply Unit (PSU) Dell Update Packages (DUPs)

After a Successful Power Supply firmware update, the system turns off, for up to 5 to 10 minutes, and reboots automatically. If you perform a cold boot (AC Power cycle) during the firmware update, the system does not boot.

Unified Server Configurator (USC) Dell Update Packages (DUPs)

- Lifecycle controller updates require system services to be enabled.

- For the first time, before you attempt to run Driver Package Diagnostics DUPs, execute the USC DUP.

- Before running DUPs, ensure that there are no external devices mounted to /media or /tmp.

- If the operating system is installed from "Operating System Deployment", select "Reboot and Exit" in the USC environment before booting to the operating system. This closes the USC session which is held for 18 hours. If you do not want to enter the USC and select "Reboot and Exit", but want to execute the DUPs within 18 hours, unplug the power supply of the system, wait for 10 seconds, and then power on the system.

- Due to the USB arbitration services of VMWare ESX 4.1, the USB devices appear invisible to the Hypervisor. So, when DUPs or the Inventory Collector runs on the Managed Node, the partitions exposed as USB devices are not shown, and it reaches the timeout after 15 to 20 minutes. This timeout occurs in the following cases:

- If you run DUPs or Inventory Collector on VMware ESX 4.1, the partitions exposed as USB devices are not visible due to the USB arbitration service of VMware ESX 4.1 and timeout occurs. The timeout occurs in the following instances:

- When you start "DSM SA Shared Service" on the VMware ESX 4.1 managed node, it runs Inventory Collector. To work around this issue, uninstall Server Administrator or wait until the Inventory Collector completes execution before attempting to stop the "DSM SA Shared Service".
- When you manually try to run DUPs or the Inventory Collector on the VMware ESX 4.1 managed node while USB arbitration service is running. To fix the issue, stop the USB arbitration service and run the DUPs or the Inventory Collector.

  To stop the USB arbitration service:
  1. Use the "ps aux|grep usb" to check if the USB arbitration service is running.
  2. Use the "chkconfig usbarbitrator off" command to prevent the USB arbitration service from starting during boot.
  3. After you stop the usbarbitrator, reboot the server to allow the DUPs and/or the Inventory collector to run.

Note: If you require the usbarbitrator, enable it manually. To enable the usbarbitrator, run the command - chkconfig usbarbitrator on.

12 G BIOS

- BIOS updates require system services/Lifecycle controller to be enabled.

- If the operating system is installed from "Operating System Deployment", select "Reboot and Exit" in the USC environment before booting to the operating system. This closes the USC session which is held for 18 hours. If you do not want to enter the USC and select "Reboot and Exit", but want to execute the DUPs within 18 hours, unplug the power supply of the system, wait for 10 seconds, and then power on the system.

- BIOS DUP will use LC to update BIOS. BIOS DUP will stage the BIOS firmware to maser partition and create a SSIB update task, which is executed by the SSM manager on reboot. The update task in the SSIB is a call to update wrapper in LC which has BIOS update logic.

BIOS

- A BIOS update requires enough free physical memory to load the entire BIOS image into the physical memory. If there is insufficient free physical memory available on the system to load the BIOS image, the Dell Update Package for BIOS may fail. In this instance, you may attempt running the Dell Update Package immediately after reboot or after adding more memory. If this does not resolve the issue, update the BIOS using the Diskette method.

- If the above memory limitation occurs on VMware ESX Server, the problem is because the console operating system available memory is only 272 MB by default. Increase the console operating system memory to 800 MB temporarily and perform the firmware update. During ESX Server boot up, perform the following steps to increase the available memory:

1. While booting, press "e" on the VMware ESX line (Grub option display screen).

2. Press "e" again on the 'uppermem=' line and edit uppermem=819200.

3. Press "Enter".

4. Press "e" on the kernel line (below the uppermem line).

   i. Edit the kernel line with mem=800M and press “Enter”.

5. Press "b" to boot with these options.

6. Perform the firmware update.

- BIOS update may issue the following kernel messages on the console and in "/var/log/messages":

  dcd***: disagrees about the version of symbol struct_module

  dcd***: Unknown symbol get_user_size

  dcd***: Unknown symbol put_user_size

Ignore these messages because they do not refer to errors in BIOS update.

Dell Embedded Open Manage Server Administrator

The Dell Update Package for Dell Embedded Open Manage Server Administrator can only be applied in a pre-operating system environment that uses the Embedded Linux (ELI) through the Dell OpenManage Deployment Toolkit (DTK).

Intel firmware

The Linux FW DUP file requires DKMS (Version 2.2.x up to 2.2.0.2-1) and will not install correctly without it. It also requires that the appropriate kernel sources and the compiler be installed, because the Intel iqvLinux driver must be compiled on the target system.

Emulex firmware

Before running the Dell (Emulex) Network firmware DUP ensure that Dell (Emulex) driver packages are installed on the system.

DRAC 5 firmware

- Before updating the DRAC firmware, ensure that the following conditions are met:
  1. USB is enabled
  2. IPMI is working properly
  3. DRAC Virtual Flash is not in use either by the operating system or by any other application

The Linux DUP in this release may not work on RHEL 5. It works on earlier versions of RHEL. In cases where it does not work, use the web pack to perform this update.

Power Supply Unit firmware

Power Supply Unit firmware updates can be performed only on Life Cycle Controller enabled systems.

All PERC firmware and all SAS firmware

- Do not run storage controller update packages if the controller is in use by other applications. The firmware upgrade may fail if any of the RAID controllers in the system are performing an I/O background task (consistency check, background initialization, rebuild, or reconstruction). Allow the background task to complete before attempting to upgrade the firmware. "Patrol Read" tasks will not affect a firmware upgrade.
- Linux systems running one or more applications that interact with SCSI devices in certain ways are known to cause a kernel panic situation. Therefore, it is recommended that you stop Dell OpenManage Server Administrator and Dell OpenManage Server Administrator Storage Management Service before running storage controller firmware update packages.

  To stop the Dell OpenManage Server Administrator service,
  run "omconfig system webserver action=stop"

  To start the Server Administrator service,
  run "omconfig system webserver action=start"

  To stop the Server Administrator Storage Management Service,
  run "/etc/init.d/dataeng stop"

  To start the Server Administrator Storage Management Service,
  run "/etc/init.d/dataeng start"

PowerVault MD1000 firmware

The PowerVault update procedure requires the RAID controller to be in a known good state. If a problem occurs with the RAID controller during the update procedure, the Update Packages cannot communicate with the PowerVault system, inventory its firmware version, or perform the update. (138462)

PowerVault MD1000 firmware

Stop all input/output to the PowerVault MD1000 before running the PowerVault MD1000 firmware update package.

WARNING: THE SERVER MUST BE REBOOTED AFTER UPDATING THE FIRMWARE ON MD1000 ENCLOSURES IN ORDER TO MAINTAIN ENCLOSURE MANAGEMENT. ACCESS TO THE ENCLOSURES WILL BE LOST IF THE SERVER IS NOT REBOOTED.

When prompted for reboot after the update, select "Yes".

PowerVault 100T DDS4 firmware and all PowerVault 110T firmware (110T DDS4, 110T DAT72, 110T LTO1, 110T LTO2, 110T LTO2-L, 110T LTO3-HH, 110T LTO4, 110T SDLT320, 110T LTO3, 110T DLT VS80, 110T DLT VS160, and 110T SDLT)

- Before executing the firmware update, stop all tape backup activity and put all scheduled jobs on hold.
- After the firmware update is completed, restart your system for the updates to take effect.

Note: Tape automation devices are not supported by Dell Update Packages. Please disconnect or power off such devices before executing Dell Update Packages.

The tape automation devices are as follows:

1. PowerVault 120T
2. PowerVault 122T
3. PowerVault 124T
4. PowerVault 128T
5. PowerVault 130T
6. PowerVault 132T
7. PowerVault 136T
8. PowerVault 160T
9. PowerVault ML6000