Scripting WS-MAN Firmware Updates

This Dell Technical White Paper provides information about scripting WS-MAN Firmware Inventory and Firmware Updates on Dell PowerEdge servers with iDRAC.

Author(s)

Chris A. Poblete

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.

February 2012| Rev 1.0

Executive summary

This paper describes how to automate firmware inventory and updates through a secure and standards-based Web Services-Management (WS-MAN) service on Dell™ PowerEdge™ servers with Integrated Dell Remote Access Controller with Lifecycle Controller (iDRAC).

Contents

Introduction

WS-MAN provides secure, simple, scriptable, and standards-based remote management capabilities on Dell PowerEdge servers equipped with iDRAC.

WS-MAN is a network transport service that enables a user to access a number of Common Information Model (CIM) data access and methods supported by the target platform. WS-MAN can be scripted using command line interfaces (CLI) such as WinRM on Microsoft® Windows® systems and WS-MAN CLI on Linux systems.

This document uses the Python scripting platform, which run son both Windows and Linux systems. Some additional reading of specification documents may be required to understand the terminology and concepts in this paper.

In this document, you will learn how to:

- View firmware information/inventory on a system.
- Perform a firmware update.
- Perform a firmware rollback.

Before You Begin

Before you begin, it is recommended to take the following actions:

1. Make sure the target system is a PowerEdge server with iDRAC enabled, configured, and network accessible to communicate with WS-MAN.
2. For Windows, make sure the WinRM command line tool is configured and ready (for help, see *Installation and Configuration of Windows Remote Management*).

   For Linux, make sure the Openwsman CLI is built, installed, and ready (for help, go to the Openwsman Home and join the mailing list).
3. Make sure Python 2.7 is installed on the target system (for help, see Python Home).
4. Download the following Python scripts:

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

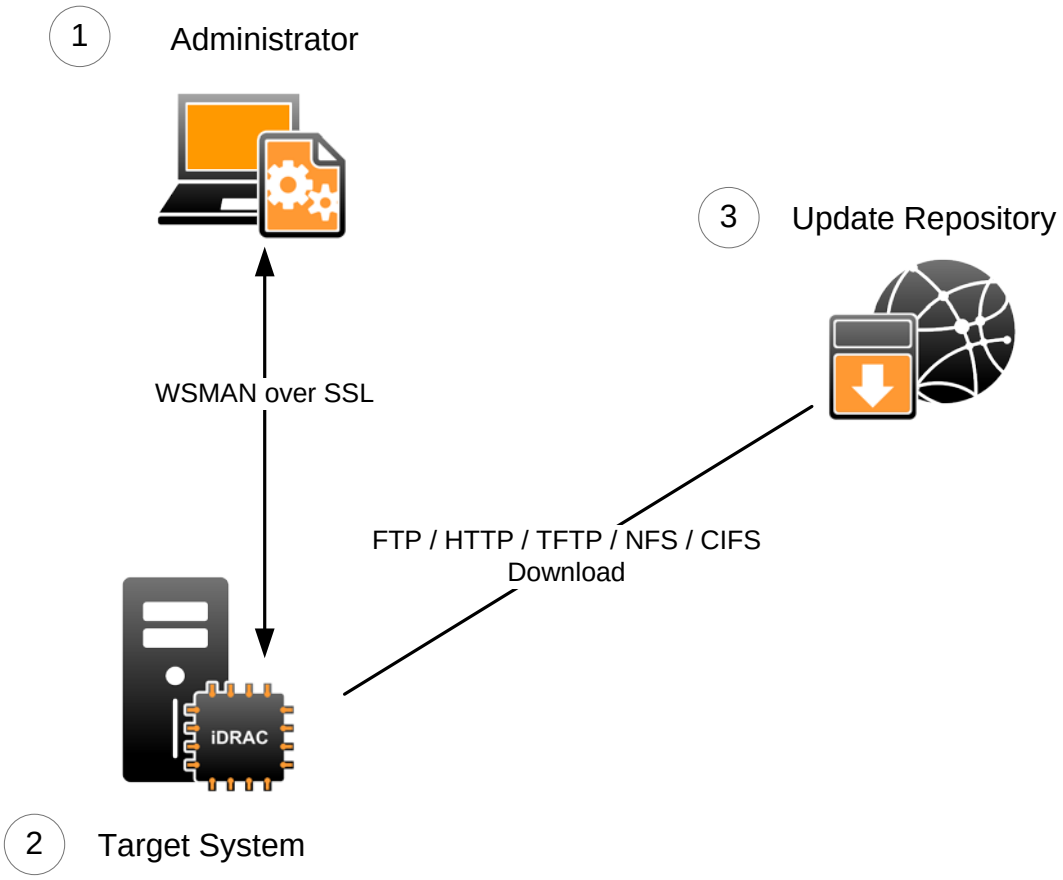

Figure 1 - Environment Diagram

Figure 2 shows an example of the target environment. It starts with the administrator (1) running scripts to send WS-MAN commands through an SSL connection. The target system (2) is equipped with iDRAC, which is a 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.

Performing a firmware update

The remote firmware update process involves the following steps

1. View the current firmware inventory of the system
2. Begin the update process
3. Monitor the update process

Install firmware information on the system

1. 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)
```

2. Enter requested 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 argument is the user name; if the user is an Active Directory account, then the syntax is USER@DOMAIN. The third argument is the user password.

3. 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
```

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

   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       0.3.32 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

1. 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.
```

2. Enter requested 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 argument is the user name; if the user is an Active Directory account, then the syntax is USER@DOMAIN. The third argument is the user password.

3. 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
```

4. Once a successful connection is established, the fwupdate.py script performs a Software Inventory and lists the components that are available to be updated.

Sample output:

```
 [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 a device that can either be updated to firmware located on a network share (ftp/http/tftp/nfs/cifs) or rolled back to a previous firmware version stored on the iDRAC.

5. Select the component alias (from step 3) for the component you would like to inventory. Once a component type is selected, the script lists options that are available for rollback and update for that particular component.

```
View component firmware inventory: n

OPTION       Component   Status      Comp ID   Version      Type

1(rollback)  FRMW        Available   None      7.0.47       Broadcom Gigabit Ethernet
BCM5720 - 18:03:73:0F:45:48

2(rollback)  FRMW        Available   None      7.0.46       Broadcom Gigabit Ethernet
BCM5720 - 18:03:73:0F:45:48

3(rollback)  FRMW        Available   None      7.0.46       Broadcom Gigabit Ethernet
BCM5720 - 18:03:73:0F:45:48

4(update)    FRMW        Installed   None      7.0.47       Broadcom Gigabit Ethernet
BCM5720 - 18:03:73:0F:45:48

5(update)    FRMW        Installed   None      7.0.47       Broadcom Gigabit Ethernet
BCM5720 - 18:03:73:0F:45:48

6(rollback)  FRMW        Available   None      7.0.47       Broadcom Gigabit Ethernet
BCM5720 - 18:03:73:0F:45:48

7(rollback)  FRMW        Available   None      7.0.47       Broadcom Gigabit Ethernet
BCM5720 - 18:03:73:0F:45:49

8(rollback)  FRMW        Available   None      7.0.46       Broadcom Gigabit Ethernet
BCM5720 - 18:03:73:0F:45:49

9(update)    FRMW        Installed   None      7.0.47       Broadcom Gigabit Ethernet
BCM5720 - 18:03:73:0F:45:49
```

Once the firmware inventory is listed, you can either continue with the firmware update or quit. To perform a firmware update, select one of the options that are available for update.

The script will prompt for the location of the Dell Update Package (DUP) to be used. 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 all-caps portions of the syntax 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 required to access and download files from the share. [MOUNTNAME] refers to the share mount name.

Sample output:

```
Options

tftp://192.168.0.100/BIOS-2011.exe

nfs://192.168.0.100/BIOS-2011.exe;mountpoint=/pub

cifs://DOMAIN\\USER:PASS@192.168.0.100/pub/BIOS-2011.exe;mountpoint=E

http://192.168.0.100/BIOS-2011.exe

ftp://192.168.0.100/BIOS-2011.exe

    Enter the path of the image file: tftp://192.168.0.3/DUP.exe
```

6. The script will prompt for a reboot type that the host will use reboot before performing 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
```

7. The script asks for permission to delete all existing jobs in iDRAC. It is recommended to choose yes for a clean start.

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

Deleting all iDRAC jobs

Completed job deletion
```

8. The script requests a start time for the job. The job can be scheduled immediately or for a future time.

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

The format of the StartTime argument is defined by the CIM Infrastructure Specification. Enter now to schedule the jobs immediately, or enter schedule to schedule the job for a future time. The schedule option will prompt for a start time, which you must enter in 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.

The update package is downloaded from the repository. This may take some time depending on the size of the package and network state. After the update package is successfully downloaded, the update and the reboot job are scheduled for the specified start time.

Sample output of successful command:

```
nic update successfully created

Creating reboot job

Reboot job successfully created.

Scheduling nic update job

Scheduling reboot job

The nic updating from version 7.0.21 to version
ftp://10.35.155.122/Release_DUPS/Network_Firmware_JXJWY_WN_7.0.46_X36.EXE
```

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

Sample output of failed command:

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

If the command fails, check that the InstanceID you provided is accurate by comparing it with output from the previous step. Remember that characters are case sensitive. Also, check the accuracy of the source URI to ensure it is accessible with proper permission. Once verified, try the command again.

After the specified start time elapses, the host reboots and launces System Services to perform the firmware update.

Monitor the update execution

The final step in the update process is to monitor when the update executes, and then to verify the update by checking the new version from the inventory enumeration.

1. 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
```

2. Enter requested information:

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

1. The first argument is the IP address of the iDRAC on the target system. The second argument is the user name; if the user is an Active Directory account, then the syntax is USER@DOMAIN. The third argument is the user password.

Sample output:

```
Available JobIDs.

(1) JID_267336093962

   - nic updating to image located at
ftp://10.35.155.122/Release_DUPS/Network_Firmware_JXJWY_WN_7.0.46_X36.EXE

(2) RID_267336106745
```

```
   - reboot for nic 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__NIC.Integrated.1-2-1

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

3. Select the number corresponding to your job to display the current status.

The script performs two step executions. 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.

Performing a firmware rollback

A firmware rollback applies a device's previously installed firmware version. This is useful when you encounter a new firmware level that was just updated and is causing problems or incompatibilities in the system.

To determine if firmware can be rolled back, examine the inventory list and look for "available" in the status. For example:

```
5(update)    FRMW        Installed   None      7.0.47       Broadcom Gigabit Ethernet
BCM5720 - 18:03:73:0F:45:48
```

To perform a rollback, select the firmware entry marked "available" and run the update script without the source URI. The script will detect that the request is a roll back and will execute the proper commands. Unlike an update, a rollback does not go through the download phase. Jump to scheduling the update and follow the rest of the process.

Sample output:

```
   ./fwupdate.py
    Enter iDRAC IP Address: 10.36.0.117
    Enter User Name: root
    Enter User Password:
Pinging 10.36.0.117. Waiting for response. Done.
Certificate exists!
```

```
[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

  View component firmware inventory: n
OPTION       Component   Status      Comp ID   Version      Type
1(rollback)  FRMW        Available   None      7.0.47       Broadcom Gigabit Ethernet BCM5720
- 18:03:73:0F:45:48
2(update)    FRMW        Installed   None      7.0.47       Broadcom Gigabit Ethernet BCM5720
- 18:03:73:0F:45:48
3(rollback)  FRMW        Available   None      7.0.46       Broadcom Gigabit Ethernet BCM5720
- 18:03:73:0F:45:48
4(update)    FRMW        Installed   None      7.0.47       Broadcom Gigabit Ethernet BCM5720
- 18:03:73:0F:45:48
5(rollback)  FRMW        Available   None      7.0.47       Broadcom Gigabit Ethernet BCM5720
- 18:03:73:0F:45:48
6(rollback)  FRMW        Available   None      7.0.47       Broadcom Gigabit Ethernet BCM5720
- 18:03:73:0F:45:49
7(rollback)  FRMW        Available   None      7.0.46       Broadcom Gigabit Ethernet BCM5720
- 18:03:73:0F:45:49
8(rollback)  FRMW        Available   None      7.0.46       Broadcom Gigabit Ethernet BCM5720
- 18:03:73:0F:45:48
9(update)    FRMW        Installed   None      7.0.47       Broadcom Gigabit Ethernet BCM5720
- 18:03:73:0F:45:49


Choices:
   d       Select different component
   OPTION              1,2,3
   ENTER: 1
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
   Enter reboot type: 1
   Erase all previous jobs stored in the iDRAC? (yes/no) yes
Deleting all iDRAC jobs
Completed job deletion
   Schedule the  nic rollback now or schedule later (now, schedule)? now
Creating nic rollback job
nic rollback successfully created
Creating reboot job
Reboot job successfully created.
Scheduling nic rollback job
Scheduling reboot job
The nic rollback from 7.0.47 to the image 7.0.47
Check the status of the reboot job and the nic rollback job by using the fw_pull.py script.
```

Exceptions

One exception to the process described in the previous sections is that certain updates do not require a reboot and scheduling. After the update package is downloaded, it is immediately applied to the device. This exception applies to Lifecycle Controller, Diagnostics, and OS Driver Pack firmware updates. System CPLD Updates are currently not supported by this method.

Summary

In this paper, you have learned how to perform an inventory of firmware installed on your system, a firmware update on select system devices, and a firmware rollback.

Additional Resources

Lear more about firmware inventory as defined by the Dell CIM profile specification:
http://www.delltechcenter.com/page/DCIM.Library.Profiles.DCIM+Software+Inventory+Profile+1.0

Lear more about firmware update as defined by the Dell CIM profile specification:
http://www.delltechcenter.com/page/DCIM.Library.Profile.DCIM+Software+Update+Profile+1.0

Lear more about job control as defined by the Dell CIM profile specification:
http://www.delltechcenter.com/page/DCIM+Job+Control+Profile+1.1

WS-MAN Interface Guide for Linux:
http://attachments.wetpaintserv.us/BMJk79WsVP3F0jwl50xR_w2088275

WS-MAN Interface Guide for Windows:
http://attachments.wetpaintserv.us/utYVFQFaHmnfG_LHEnx1YQ2026735

WS-MAN command line open source for Linux (OpenWS-MAN):
http://sourceforge.net/projects/openWS-MAN/

WS-MAN command line for Windows (WinRM):
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384291(v=VS.85).aspx

All about Lifecycle Controller in iDRAC:
http://support.dell.com/support/edocs/software/smusc/smlc/lc_1_5/index.htm