SYSTEMS MANAGEMENT SAVINGS WITH DELL OPENMANAGE ON 13G DELL POWEREDGE SERVERS

SAVE ON SYSTEMS MANAGEMENT

WITH DELL™ OPENMANAGE™ ON DELL 13TH GENERATION POWEREDGE™ SERVERS

Save up to

785 hours

of administrator time over two years– a **91.3% reduction** in a 200 server datacenter compared to 200 four-year-old servers

Streamlined management means lower deployment, updating, monitoring, and maintenance costs.

POWERED BY INTEL® XEON® PROCESSORS E5-2600 v3 SERIES

If your datacenter is filled with older hardware, you probably aren't reaping the benefits of new systems management technologies. Using older hardware that makes administrators complete routine tasks manually bogs down staff and can keep your operating expenses high. By adding new 13G Dell PowerEdge servers to your infrastructure, you can manage your datacenter with the latest integrated Dell OpenManage systems management features to save administrator time and improve your bottom line.

In the Principled Technologies labs, we completed routine datacenter tasks on two solutions: 1) a new Dell PowerEdge R730 server with Dell OpenManage that automated many tasks and 2) an older Dell PowerEdge 2950 server that required us to complete the tasks manually. We compared the two and looked at the savings the new solution could provide a business with 200 servers over two years by automating tasks with Dell OpenManage.

We found that for the tasks we tested, Dell OpenManage streamlined server management enough that you could save as much as 785 administrative hours and 91.3 percent in administrator costs over two years for a 200-server deployment. In addition to savings in operating expenses, consolidating older servers onto technologically improved 13G Dell PowerEdge servers could reduce the number of servers you need to manage, which would give back even more time to administrators.

OCTOBER 2014

A PRINCIPLED TECHNOLOGIES TEST REPORT

Commissioned by Dell Inc.

DELL OPENMANAGE SUITE AND DELL 13G

Dell OpenManage is a systems management suite designed to help IT departments of all sizes manage their Dell PowerEdge server infrastructures. Without automated management, administrators must perform these tasks such as node deployment, error correction, and updates manually. The Dell OpenManage suite automates many processes, freeing up IT time for more strategic tasks. Using integrated systems management can improve the overall function of your infrastructure by allowing administrators to more quickly solve problems that arise in the datacenter.

With the introduction of 13G Dell PowerEdge servers, Dell has added a number of features to Dell OpenManage systems management to save administrator time and increase management flexibility (see Figure 1).

New systems management features in the Dell OpenManage Suite and iDRAC8 for 13G servers		
Faster deployment	OpenManage Essentials (OME) One-to-many deployment	Perform automated hardware configuration and Operating System deployment to multiple servers through centralized management
Improved connectivity	iDRAC Direct (cable)	Connect directly to the iDRAC using a front-side USB connection, without the need for a dedicated management network
	iDRAC Direct (key)	Rapidly deploy custom server profiles using plug-and-play technology
	Quick Sync (NFC)	Quickly inventory and modify server configurations using smartphone and tablets
Automated maintenance	Tech Support Report	Gather complete, advanced diagnostic information from a single location
	OME Managing Configuration Baseline	Manage your server configurations from a centralized location, without having to take a single server offline for inventory
Easier updating	Zero Touch Repository Manager and Self-updating firmware system	Build self-maintaining repositories and configure servers to automatically update to new versions of software on your own schedule
	OME Agent-free driver update	Deploy firmware and driver updates from the OME console without management software on your servers

Figure 1: New features in Dell OpenManage.

In our labs, we used these features to complete routine management tasks on a Dell PowerEdge R730 server with Dell OpenManage Suite and then performed the same tasks manually on a Dell PowerEdge 2950 server. We compared the time it took to complete these tasks and then calculated the time you could save over two years for a 200-server deployment. Using a salary estimate for a Systems Administrator I position[1],

[1] System Administrator I salary of $81,663 (US National average) reported on 10/02/2014 at http://swz.salary.com/SalaryWizard/Systems-Administrator-I-Salary-Details.aspx?hdcbxbonuse=off&isshowpiechart=true&isshowjobchart=false&isshowsalarydetailcharts=false&isshownextsteps=false&isshowcompanyfct=false&isshowaboutyou=false

we calculated the dollar amount you could save by automating these tasks with Dell OpenManage on a Dell PowerEdge R730 server.

For a detailed look at the system we used for testing, see Appendix A. For step-by-step details on how we tested, see Appendix B.

WHAT WE FOUND

As Figure 2 shows, completing the tasks using Dell OpenManage on a Dell PowerEdge R730 could save 785 hours over two years—a 91.3 percent reduction in administrator time. We took into consideration the number of times administrators would need to complete these tasks over the course of two years (read more about our assumptions below).

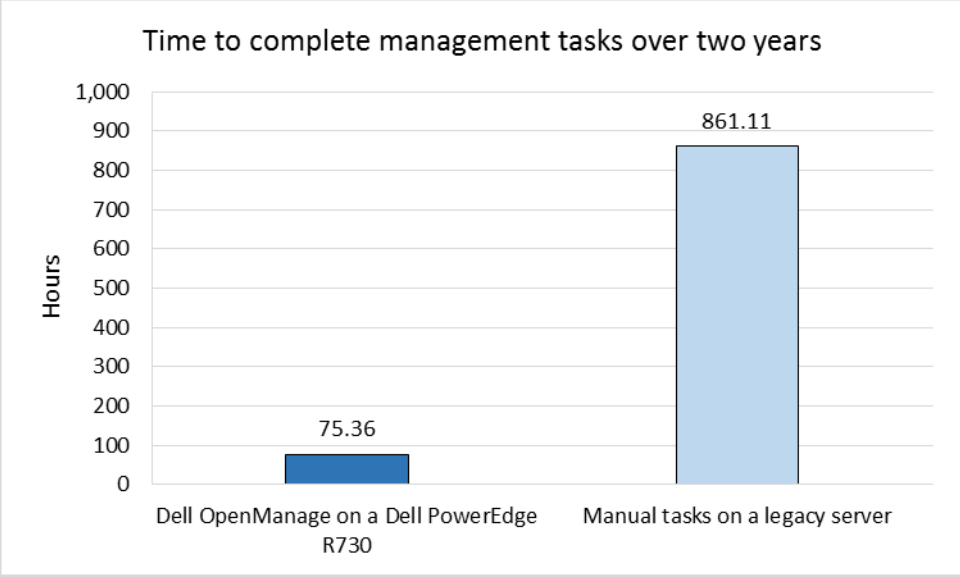


Figure 2: Automating the common server management tasks we tested with Dell OpenManage on a 13G Dell server could save up to 785 administrator hours over two years for a deployment of 200 servers versus manual management.

What could administrators do with all the time they'd save by automating routine tasks with Dell OpenManage on a 13G Dell PowerEdge server? For starters, they could manage a larger number of servers. They could also use that time to innovate elsewhere in the data center.

Administrator time translates directly to money. By automating these routine management tasks with Dell OpenManage, we estimate that you could save $30,849 in administrator time over two years for a 200-server deployment (see Figure 3). That reduces your operating expenditures by up to 91.3 percent.

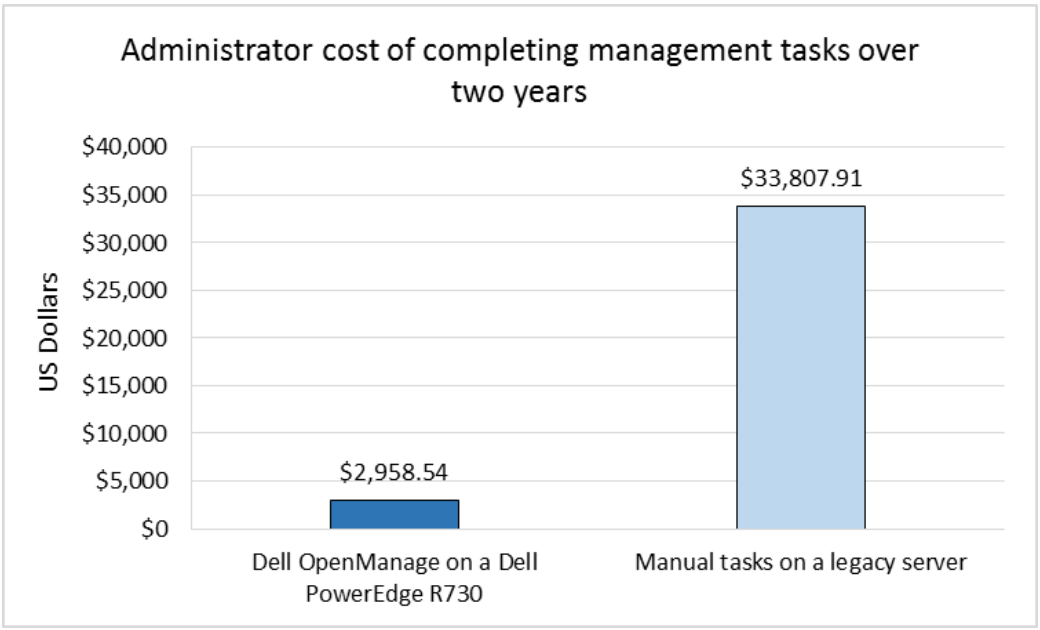


Figure 3: By automating the tasks we tested with Dell OpenManage on a Dell PowerEdge R730 server, you could save over $30,000 in administrator salary costs.

Figure 4 breaks down the tasks we tested and shows exactly where the time savings come from over the two-year period. We found that Dell OpenManage on 13G Dell PowerEdge servers had the biggest effect on routine maintenance tasks with 61.0 percent of the savings coming from automating quarterly firmware updates.

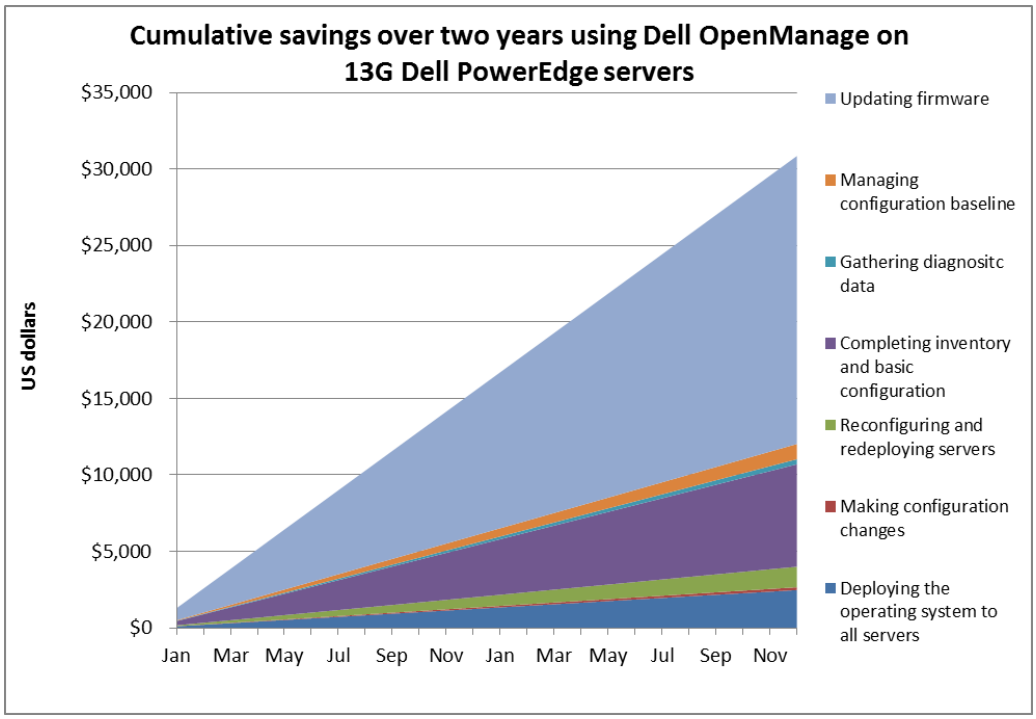


Figure 4: Cumulative savings, by task, over two years for a 200-server deployment of Dell PowerEdge servers using Dell OpenManage for management tasks.

REDUCING MANAGEMENT TIME WITH DELL

We investigated the new features of the Dell OpenManage Suite and the Dell 13G line on a new Dell PowerEdge R730 server to see how they simplified management tasks compared to doing them manually on a Dell PowerEdge 2950. These features fit into four categories:

- Deployment
- Connectivity
- Maintenance
- Updating

We found that the new features simplified all these tasks, saving administrator time and steps, as Figure 5 shows. Please note that some tasks must be completed only once for each server, while some tasks are ongoing and require varying amounts of repetition over two years. In each detailed section below, we detail our assumptions regarding the number of times an administrator would need to complete these tasks.

Scenario	Automation		Manual		Difference	
	Time (s)	Steps	Time (s)	Steps	Less time (s)	Fewer steps
Configure hardware information for deployment	95	23	226,800	19,000	226,705	18,977
One server	95	23	1,134	95	1,039	72
Make configuration changes using cable	7,600	1,200	24,500	1,800	16,900	600
One server	76	12	245	18	169	6
Make configuration changes using USB key	4,000	400	36,400	3,280	32,400	2880
One server	50	5	455	41	405	36
Redeploy servers with those changes	95	23	90,720	7,600	90,625	7,505
Complete inventory and configuration[2]	249,600	57,600	864,000	54,400	614,400	-3,200
One server (read and write combined)	156	36	540	34	384	-2
Gather diagnostic data	9,840	880	40,160	1,840	30,320	960
One server	123	11	502	23	379	12
Manage configuration baseline	50	5	91,000	8,200	90,950	8,195
One server	50	5	455	41	405	36
Complete firmware updates	0	0	1,726,400	48,000	1,726,400	48,000
One time	0	0	1,079	30	1,079	30

Figure 5: Detailed time and steps to complete tasks on 200 servers, with single server results shown in gray.

[2] The complete inventory and configuration automated process requires more steps than the manual process, but takes considerably less time. This is because the automated process requires steps to open the application on your tablet, but once configured is automated to get inventory and configuration information. The manual process requires more human interaction and time due to requiring a server reboot and hands-on activity. The automated process is a faster and less intrusive process as it doesn't require the system reboot.

Dell OpenManage Essentials one-to-many deployment

Servers take time to configure and deploy, so naturally the more servers you must deploy, the more efficiencies you seek to shorten the time. Configuring and deploying servers manually also increases the possibility of human error when setting up your infrastructure.

Dell OpenManage Essentials uses one-to-many deployment to deploy configuration profiles and operating systems quickly and easily to relieve this management burden. In our hands-on tests, we deployed a configuration profile and OS to a Dell PowerEdge R730 server in just 95 seconds; it would take no longer to deploy these to all 200 servers. In contrast, performing the same task manually takes 18 minutes 54 seconds, which adds up to 63 hours for a 200-server deployment. Figure 6 compares the estimated time for this task for a manual 200-server deployment versus using the automated approach. Larger infrastructures would see even greater savings by automating this procedure with Dell OpenManage Essentials.

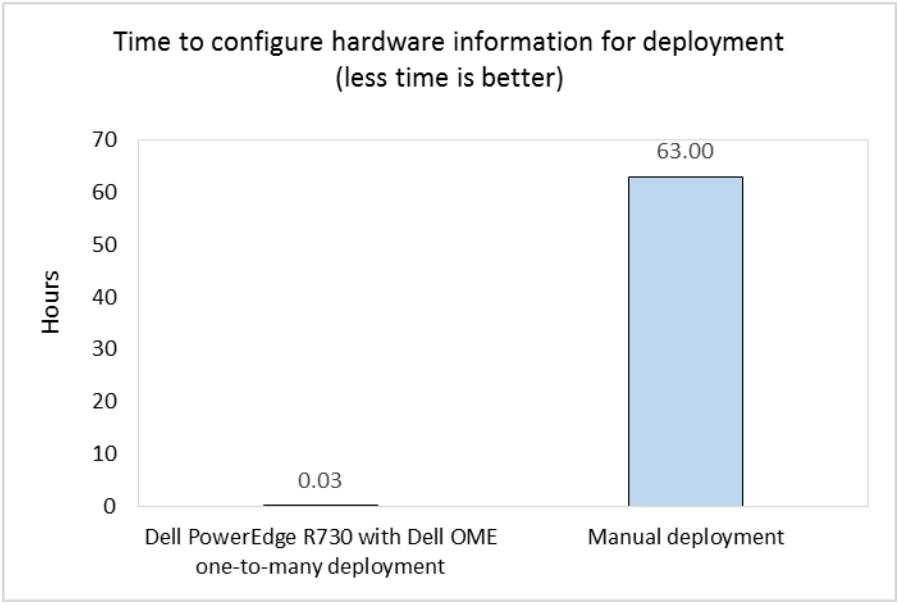


Figure 6: Configuring 200 servers with Dell OME one-to-many deployment would take up to 99.96 percent less time than configuring older servers manually.

For our cost calculations, we compared the time it would take to deploy the OS to all 200 servers. Administrators would need to do this only once to each server, during initial deployment. For specific steps we measured in this scenario, see Appendix B.

iDRAC Direct (cable)

Often, it's important that administrators be able to connect to servers quickly with minimal disruption to service, perhaps to make a quick configuration change or to check diagnostics. We found that connecting using a cable via iDRAC Direct could eliminate the need for cumbersome "crash carts" and reduce the time it took to make changes to a server configuration compared to using KVM and manual setup on an older server. Using the legacy method required connecting KVM hardware to the server,

rebooting, and manually entering system setup at the boot screen. With Dell OpenManage Essentials and iDRAC Direct, administrators need only plug in a USB cable and open a browser to make necessary configuration changes.

We found that for a 200-server deployment, Dell OpenManage Essentials on a 13G Dell PowerEdge server could save over four hours over two years by connecting using iDRAC Direct (see Figure 7). We assumed that administrators would connect using this method 25 percent of the time, or to 50 servers per year, to make necessary changes to servers. For specific steps we measured in this scenario, see Appendix B.

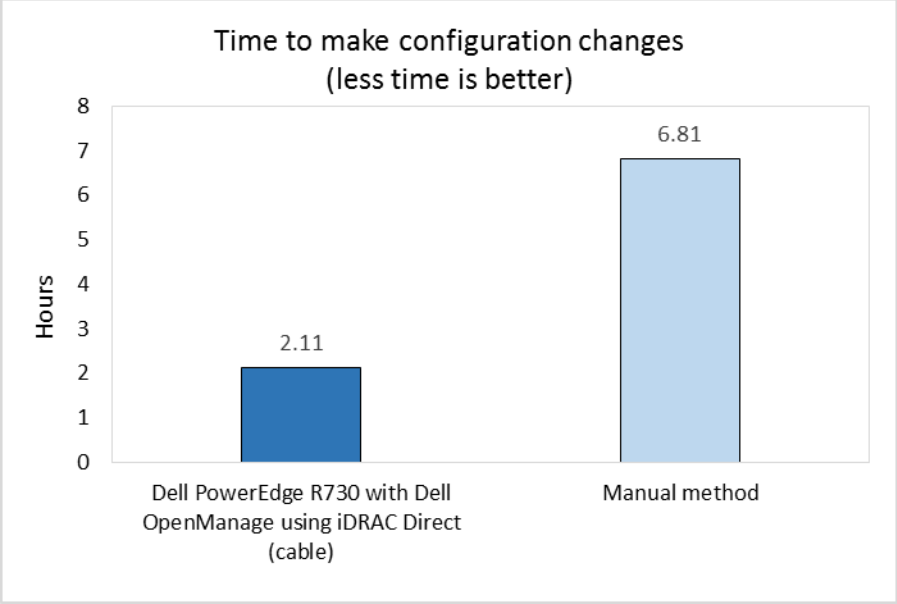


Figure 7: Changing the server configuration using iDRAC Direct (cable) would require up to 68.98 percent less time than connecting using KVM and manual setup.

iDRAC Direct (key)

Dell OpenManage and iDRAC Direct also allow administrators to easily connect to servers using a USB key. Using iDRAC Direct (key), we were able to redeploy a server with a new hardware profile in up to 96.78 percent less time than performing this task manually (see Figure 8). We estimate that administrators would connect and redeploy servers using this method 20 percent of the time over a two-year period, or to 40 servers per year. For specific steps we measured in this scenario, see Appendix B.

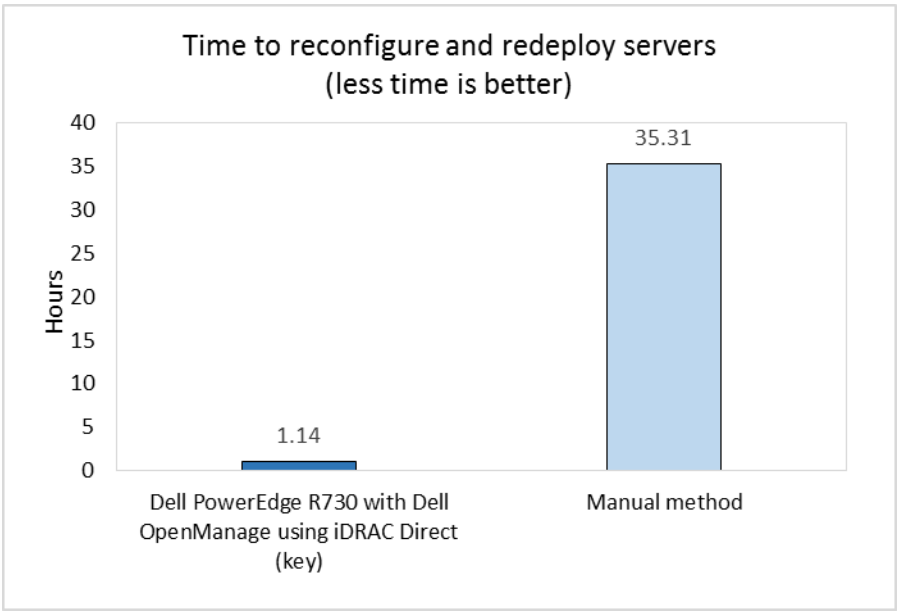


Figure 8: Connecting to iDRAC at the box using iDRAC Direct (key) would require up to 96.78 percent less time than deploying a server profile using KVM and manual setup.

Quick Sync

Being able to manage systems from smartphones and tablets can be a real advantage to admins who favor the portability of smaller devices, and with mobile systems able to wirelessly connect to the server infrastructure, administrators don't need to be tethered to the server to make changes. 13G Dell PowerEdge servers contain a near field communications (NFC) device as part of their front bezels. This allows admins to do basic inventory, health checks, and configuration updates using an NFC-enabled tablet or smartphone.

We found that Quick Sync was able to reduce manual inventory and iDRAC configuration times, and with Dell OpenManage and the 13G Dell PowerEdge R730, we were able to complete faster inventory and hardware identification. Figure 9 compares the time it would take to complete inventory and basic configuration using Quick Sync versus the manual method. Based on our tests, it would take 71.11 percent less time to complete these tasks on a 200-server deployment. For our calculations, we assume that administrators would inventory all 200 servers quarterly over the course of the two years in our study, for a total of eight times in two years. For specific steps we measured in this scenario, see Appendix B.

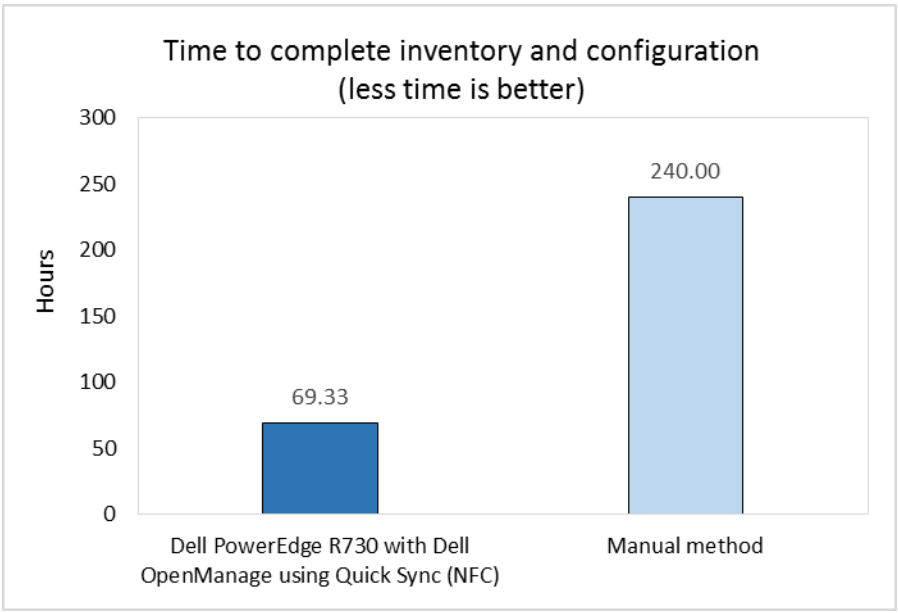


Figure 9: Completing inventory and configuration using Quick Sync would require up to 71.11 percent less time than manually inventorying the systems.

Tech Support Report

Improving and streamlining maintenance can have a dramatic effect on administrator time as well as operating expenses. Administrators spend a significant amount of time on support calls, so simplifying this process can help the health of your overall infrastructure by reducing the time it takes to fix any errors.

Manual methods of tech support require executing a separate data collection program within the OS to troubleshoot issues. 13G Dell PowerEdge servers eliminate this requirement and instead allow you to generate a Tech Support Report (TSR) that contains operating system diagnostic information.

We found that using Tech Support Report, a simplified information-gathering mechanism, saved time by reducing the variety of data that must be collected to simplify support calls. We estimate that for a 200-server deployment, this feature could save administrators over eight hours over two years (see Figure 10). We assumed that administrators would access tech support reports for 20 percent of the servers for two years. For specific steps we measured in this scenario, see Appendix B.

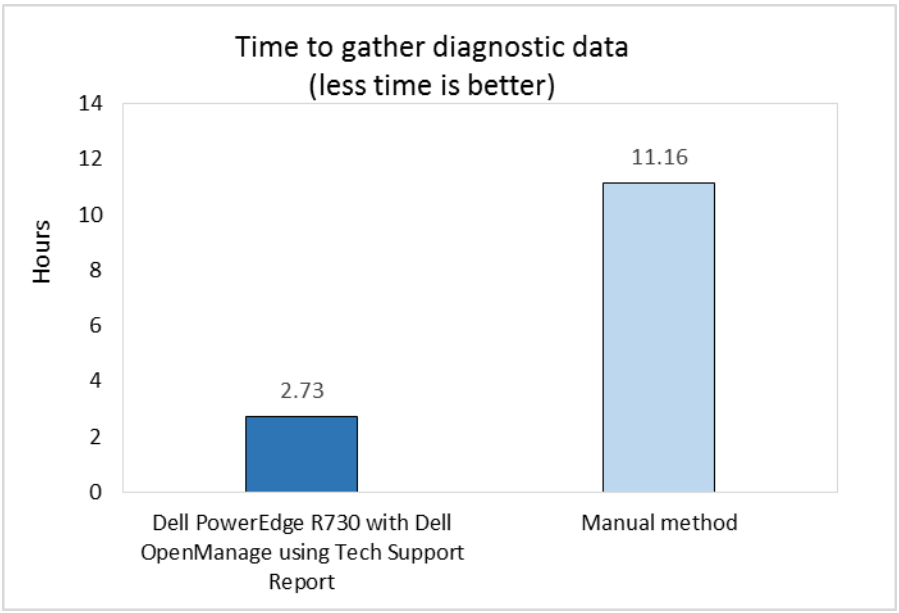


Figure 10: iDRAC8 with Tech Support Report would reduce the time to gather diagnostic data by up to 75.50 percent.

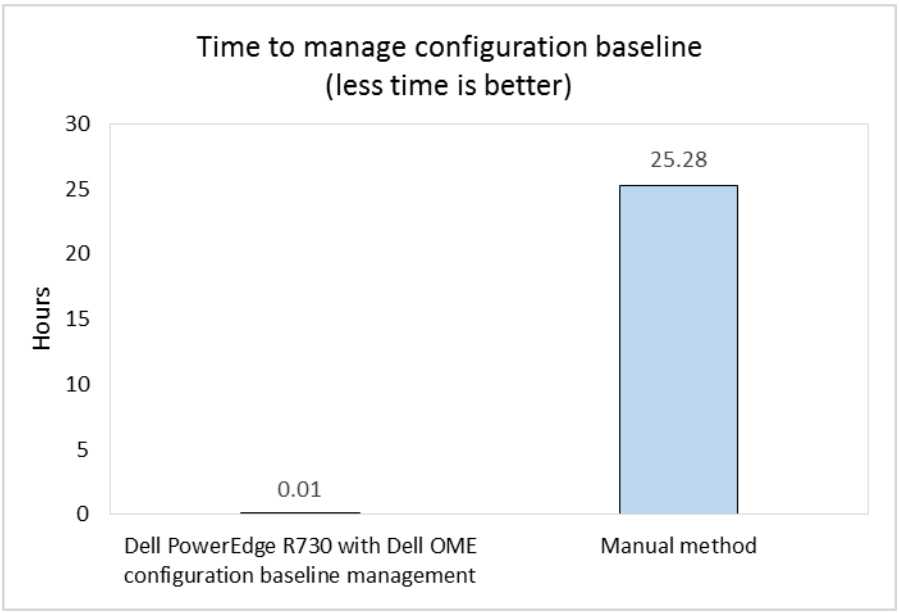
OME Managing Configuration Baseline

Server profiles let admins consistently configure servers for optimal performance in their intended roles. Sometimes administrators need to make changes to server configurations in the course of ongoing operations. With Dell OpenManage Essentials, an administrator can create baseline configurations that contain all the settings a particular group of servers should use, and then associate servers with those configurations. Dell OME can perform non-disruptive inventory on managed servers and find servers with configuration drift quickly and easily.

We found that inventorying a server with Dell OME took far less time than doing the same task manually. With a 200-server deployment, we estimate that Dell OME on a 13G Dell PowerEdge server would reduce the time to complete this task over two years by 99.95 percent.

We assumed that baseline configuration would be applied just once for all 200 servers. For specific steps we measured in this scenario, see Appendix B.

Figure 11: Dell OME would reduce the time to manage configuration baseline to the servers by up to 99.95 percent.



Auto-Updating firmware

Planned maintenance windows in off-peak hours allow administrators to make any updates without affecting customers, but require long shifts at odd hours. 13G Dell PowerEdge servers with iDRAC 8 can update firmware automatically to save administrators time and hassle. When coupled with the Zero-Touch Repository Management features of Dell Repository Manager, the ability to perform updates automatically during off hours means an administrator can set up maintenance activities during normal business hours.

We found that using Auto-Updating with Zero-Tough Repository Manager took no time at all for administrators—everything happened automatically. As Figure 12 shows, updating firmware manually is a laborious task that must be repeated several times each year, costing nearly 500 hours of administrator time in a two-year period.

We assumed that administrators would update firmware on items such as the BIOS, controller, iDRAC and network interface card for all 200 servers each quarter for two years. For specific steps we measured in this scenario, see Appendix B.

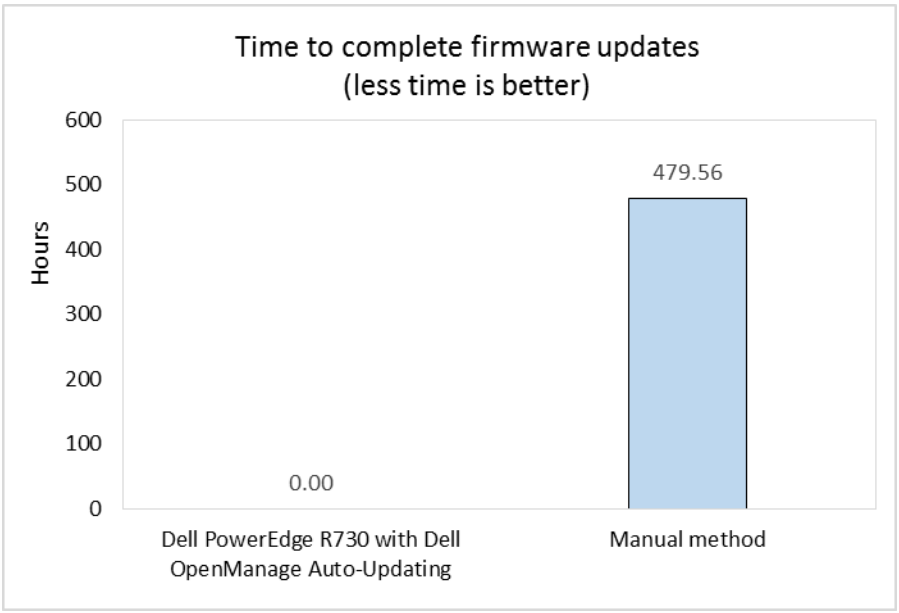


Figure 12: Updating firmware using automatic updating can reduce administrative effort by nearly 500 hours compared to manual methods over a two-year period.

WHAT WE TESTED

About the Dell PowerEdge R730

The 2U Dell PowerEdge R730 rack server is powered by two Intel Xeon E5-2600 v3 processors and is designed for functional flexibility in the datacenter. The PowerEdge R730 has 24 DIMM slots to support up to 1.5 TB of memory, supports up to two optional internal GPU processing accelerators, and can support up to four optional NVM Express™ Flash PCIe® SSDs to reduce storage bottlenecks.

With redundant power supply units, hot-swappable hardware, and Dual SD™ card for Failsafe Hypervisors, the Dell PowerEdge R730 supports hardware high availability. The PowerEdge R730 comes standard with iDRAC8 with Lifecycle Controller and Dell OpenManage, which all work to streamline management. For more details on the Dell PowerEdge R730, visit www.dell.com/us/business/p/poweredge-r730/pd.

CONCLUSION

Administrators can spend their time doing routine tasks such as firmware updates, or they can spend their time on other initiatives to make your data center and your business more successful. Older servers keep admins focused on routine tasks instead of innovation because they just don't have the capabilities to streamline management in a meaningful way to lessen the burden of routine management tasks.

In our hands-on tests, we found that Dell PowerEdge R730 servers with Dell OpenManage dramatically reduced the time it took to deploy, update, monitor, and maintain servers compared to completing the tasks manually on older systems. We estimate that you could save as much as 91.3 percent of administrator time—nearly 800 hours—over two years for a 200-server deployment.

Don't let your older servers continue to be a time sink for administrators. By upgrading to new Dell PowerEdge R730 servers with new systems management features to handle routine tasks, you can potentially redirect those resources to innovation in other areas.

APPENDIX A – SYSTEM CONFIGURATION INFORMATION

Figure 13 provides detailed configuration information for 13G Dell PowerEdge R730 we used for our automation testing with Dell OpenManage.

System	Dell PowerEdge R730
Platform	
Vendor and model number	Dell PowerEdge R730
BIOS name and version	1.0.2
General	
Number of processor packages	2
Number of cores per processor	12
Number of hardware threads per core	2
CPU	
Vendor	Intel
Name	Xeon
Model number	E5-2690 v3
Socket type	LGA2011-3
Core frequency (GHz)	2.6
Bus frequency	9.6 GT/s
L1 cache	12 x 32 KB
L2 cache	12 x 256 KB
L3 cache	30 MB
Memory module(s)	
Total RAM in system (GB)	16
Vendor and model number	Hynix Semiconductor® HMA41GR7MFR8N-TF
Type	DDR4
Speed (MHz)	2,133
Speed running in the system (MHz)	2,133
Size (GB)	8
Number of RAM module(s)	2
Chip organization	Dual-sided
Rank	Dual
Operating system	
Name	Microsoft® Windows Server® 2012 R2, Datacenter x64 Edition
Build number	Version 6.3 (Build 9600) (x64)
File system	NTSF
Language	English
RAID controller	
Vendor and model number	Dell PERC H730P Mini
Firmware version	25.2.1.0037
Driver version	6.602.07.00
Cache size (MB)	2,048

System	Dell PowerEdge R730
Hard drives	
Vendor and model number	Seagate® ST300MM0006
Number of drives	5
Size (GB)	278.88
RPM	10,000
Type	SAS
Power supplies	
Total number	2
Vendor and model number	Dell 0G6W6KX02
Wattage of each (W)	750
Cooling fans	
Total number	6
Ethernet adapters	
Vendor and model number	Intel 2P X520/2P I350 rNDC

Figure 13: System configuration information for the Dell PowerEdge R730.

Figure 14 details the system configuration information for the legacy Dell PowerEdge 2950 we used to test manual management tasks.

System	Dell PowerEdge 2950
Power supplies	
Total number	2
Vendor and model number	Z750P-00
Wattage of each (W)	750
General	
Number of processor packages	2
Number of cores per processor	4
Number of hardware threads per core	1
System power management policy	Max Performance
CPU	
Vendor	Intel
Name	Xeon
Model number	E5310
Socket type	LGA771
Core frequency (GHz)	1.60
Bus frequency	1066 MHz
L1 cache	4 × 32 KB
L2 cache	2 × 4 MB
L3 cache	0
Platform	
Vendor and model number	Dell PowerEdge 2950
Motherboard model number	0H603H

System	Dell PowerEdge 2950
Motherboard chipset	Intel 5000X R12
BIOS name and version	Dell 2.7.0
BIOS settings	Default
Memory module(s)	
Total RAM in system (GB)	32
Vendor and model number	Samsung® M395T5160QZ4-CE65
Type	PC2-5300F
Speed (MHz)	667
Speed running in the system (MHz)	667
Size (GB)	4
Number of RAM module(s)	8
Rank	Dual
Disks	
Vendor and model number	Seagate® ST300MM0006
Number of disks in system	3
Size (GB)	300
Type	HDD
Firmware	LS08
Disk controller	
Vendor and model	Dell SAS 6/ir
Controller cache (MB)	0
Controller driver	6.1.7600.16385
Controller firmware	0.25.47.00-IR
RAID configuration	1 with hot spare
Operating system	
Name	Windows Server 2008 R2 Datacenter 64-bit SP1
Build number	7601
File system	NTFS
Kernel	NT
Language	English
Ethernet	
Vendor and model number	Broadcom® BCM5708C NetXtreme® II GigE
Type	Integrated
Driver	7.10.6.0
Optical drive(s)	
Vendor and model number	TEAC CD ROM CD-224E-N
Type	CD Reader
USB ports	
Number	4 external, 1 internal
Type	2.0

Figure 14: System configuration information for the Dell PowerEdge 2950.

APPENDIX B – HOW WE TESTED

In this section, we show the steps it took to complete the tasks manually on a Dell PowerEdge 2950 (legacy solution) and then the steps to complete the same tasks with new features of Dell OpenManage on a Dell PowerEdge R730.

Completing tasks manually on the Dell PowerEdge 2950

Deploying a Manual Configuration

1. Open a Web browser from within the management network and navigate to the iDRAC IP address (`192.168.1.105`).
2. Log in with the iDRAC's username and password (Username: `root`; Password: `calvin`).
3. Click the Power Management tab to verify that the server is powered on. If the server's power status is OFF, select Power On System and click Apply.
4. Select the Alert Management tab.
5. Check Enable Platform Event Filter alerts.
6. Click Apply Changes.
   Note: For our test environment, we decided that the administrator should not receive alerts for warnings.
7. Click Battery Probe Warning.
8. Uncheck Enable.
9. Click Apply Changes.
10. Click Go Back to the Platform Events Page.
11. Click Temperature Probe Warning.
12. Uncheck Enable.
13. Click Apply Changes.
14. Click Go Back to the Platform Events Page.
15. Click Processor Warning.
16. Uncheck Enable.
17. Click Apply Changes.
18. Click Go Back to the Platform Events Page.
19. Click PS/VRM/D2D Warning.
20. Uncheck Enable.
21. Click Apply Changes.
22. Click Go Back to the Platform Events Page.
23. Select the Traps Settings subtab.
24. Click Destination: 1.
25. Verify the tick box for Enable Destination is checked and type the destination IP address (`192.168.1.50`).
26. Click Apply Changes.
27. Click Go Back to the Platform Event Alert Destination Page.
28. Verify that the Community String field is set to public.
29. Click Apply Changes.
30. Click the Email Alert Settings subtab.
31. Click E-mail Alert 1.
32. Check Enable E-mail Alert.
33. Type the Destination E-Mail Address (`adminpager@principledtechnologies.com`).
34. Type an E-mail Description (`Admin Pager`).

35. Click Apply Changes.
36. Click Go Back to the E-Mail Alert Destination Page.
37. Type the SMTP (e-mail) Server IP Address (192.168.1.51).
38. Click Apply Changes.
39. Click the Console tab.
40. Click Connect.
41. A Java® app will launch. Click Continue when the security warning appears.
42. Click Run when the Java warning appears. The remote console viewer will launch.
43. Restart the server.
44. Strike F2 to enter Setup when prompted.
45. Select CPU Information.
46. Verify that Execute Disable is Enabled.
47. Verify that Virtualization Technology is Enabled.
48. Verify that Adjacent Cache Line Prefetch is Enabled.
49. Verify that Hardware Prefetcher is Enabled.
50. Press Escape to exit the CPU Information menu.
51. Verify that Boot Sequence Retry is Enabled.
52. Select Integrated Devices.
53. Verify that Embedded SATA is set to Off.
54. Verify that Embedded Gb NIC1 is Enabled with PXE.
55. Verify that Embedded Gb NIC2 is Enabled with PXE (Default: Enabled).
56. Verify that OS Watchdog Timer is Disabled.
57. Press Escape to exit the Integrated Devices menu.
58. Select Serial Communication.
59. Verify that Serial Communication is On without Console Redirection.
60. Verify that External Serial Connector is COM1.
61. Verify that Failsafe Baud Rate is set to 115200.
62. Verify that Remote Terminal Type is set to ANSI.
63. Press Escape to exit the Serial Communication menu.
64. Scroll down to select System Security.
65. Scroll down to verify that NMI Button is Disabled.
66. Press Escape to exit the System Security menu.
67. Press Escape to exit the System Configuration menu.
68. Select Save Changes and Exit.
69. If prompted, press Ctrl-C to run SAS Configuration Utility. If no prompt is given, send the Ctrl-Alt-Del macro to restart the server and reinitiate the prompt.
70. When the SAS Configuration Utility launches, select the adapter from the list (SAS6IR) and press Enter.
71. Using the arrow keys to navigate, select RAID Properties, and press Enter.
72. Select Create R1 Volume.
73. Select the three physical disks to use as a RAID 1 by using the arrow keys to navigate to the RAID Disk column. Press the spacebar over No to change to Yes for the first two disks.
74. For the third disk, under the Hot Spr column, change the No to Yes.
75. Press C to Create array.
76. Select Save changes then exit this menu.
77. Press F3.

78. When the process is complete, press Escape.
79. Press Escape again.
80. Select Exit the Configuration Utility and Reboot.
81. When prompted, press Ctrl-E to Enter the Remote Access Configuration Utility.
82. Verify that IPMI Over LAN is On.
83. Select LAN Parameters.
84. Scroll down to verify that LAN Alert Enabled is On.
85. Verify that Alert Policy Entry 1 is Enabled.
86. Verify that Alert Destination 1 is correct (192.168.1.50).
87. Select Host Name String.
88. Verify the Current Host Name String is correct (localhost.ptnet.principledtech.com).
89. Press Escape.
90. Press Escape again.
91. Press Escape to exit.
92. Put the installation media in the server's CD drive.
93. Restart the server.
94. When prompted, press F11 to enter the Boot menu.
95. Select IDE CD-ROM device, and press Enter.

iDRAC Direct (cable)

Manual: Crash cart

1. Plug the crash cart power strip into a power outlet.
2. Connect a keyboard to the server front panel.
3. Connect a mouse to the server front panel.
4. Connect a monitor to the server front panel.
5. Power on or reboot the server.
6. When prompted, press Ctrl-C to run SAS Configuration Utility.
7. When the SAS Configuration Utility launches, select the adapter from the list (SAS6IR) and press Enter.
8. Using the arrow keys to navigate, select RAID Properties, and press Enter.
9. Select Create R1 Volume.
10. Select Create R1 Volume.
11. Select the three physical disks to use as a RAID 1 by using the arrow keys to navigate to the RAID Disk column. Press the spacebar over No to change to Yes for the first two disks.
12. For the third disk, under the Hot Spr column, change the No to Yes.
13. Press C to Create array.
14. Select Save changes then exit this menu.
15. Press F3.
16. When the process is complete, press Escape.
17. Press Escape again.
18. Select Exit the Configuration Utility and Reboot.

iDRAC Direct (USB key)

Manual configuration

We used the time and steps from the zero-touch manual configuration.

Quick Sync (NFC)

Manual read procedure

1. Plug the crash cart power strip into a power outlet.
2. Connect a keyboard to the server front panel.
3. Connect a mouse to the server front panel.
4. Connect a monitor to the server front panel.
5. Power on or reboot the server.
6. Press Ctrl-E when prompted to enter the Remote Access Configuration Utility.
7. Verify that Baseboard Management Controller Revision, Remote Access Controller Revision, and Primary Backplane Firmware Revision version numbers are up to date (2.50; 1.65; 1.05).
8. Select LAN Parameters.
9. Check the Ethernet IP Address and Default Gateway.
10. Press Escape.
11. Press Escape again to exit.
12. Remove the keyboard, monitor, and mouse.

Manual write procedure

1. Plug the crash cart power strip into a power outlet.
2. Connect a keyboard to the server front panel.
3. Connect a mouse to the server front panel.
4. Connect a monitor to the server front panel.
5. Power on or reboot the server.
6. Press Ctrl-E when prompted to enter the Remote Access Configuration Utility.
7. Select LAN Parameters.
8. Select IP Address Source and press space to change from DHCP to Static.
9. Select Ethernet IP Address, press Enter, and set the IP address for the DRAC. We used `172.16.10.120`. Type the first set of numbers and use tab to navigate between periods.
10. Press Enter.
11. Select the Subnet Mask and press Enter to set it. We used `255.255.0.0`. Type the first set of numbers and use tab to navigate between periods.
12. Press Enter.
13. Select the Default Gateway and press Enter to set it. We used `172.16.10.1`. Type the first set of numbers and use tab to navigate between periods.
14. Press Enter.
15. Press Escape.
16. Select Advanced LAN Parameters.
17. Select DNS Servers from DHCP and use the arrow keys to change from On to Off.
18. Select DNS Server 1 and set the IP address. We used `172.16.0.10`.
19. Select DNS Server 2 and set the IP address. We used `172.16.0.11`.
20. Press Escape.
21. Press Escape.
22. Select Save Changes and Exit.

Tech Support Report

Manual (DSET)

1. Open a Web browser from within the management network and navigate to the iDRAC IP address (`192.168.1.105`).
2. Log in with the iDRAC's username and password (Username: `root`; Password: `calvin`).
3. Click the Console tab.
4. Click Connect.
5. A Java app will launch. Click Continue when the security warning appears.
6. Click Run when the Java warning appears. The remote console viewer will launch.
7. Click Macros, and click Ctrl-Alt-Delete.
8. Log in to Windows with your username and password.
9. Open a Web browser and navigate to `dell.com/dset`
10. Download DSET for Windows.
11. Run the downloaded application.
12. Click Next.
13. Accept the license agreement.
14. Leave Create a One-Time Local System DSET Report as default, and click Next.
15. Enter the network file share location (`\\192.168.1.20\profiles`).
16. Check Enable Report Filtering and Automatically Upload the Report to Dell.
17. Click Next.
18. Leave Hardware Information, Storage Information, and Software Information checked by default.
19. Check Gather Advanced Log Files Information.
20. Click Next.
21. Click Start.
22. A command window will appear and update the report generation and upload status. The window will automatically close. Click Finish.
23. Sign out of the Windows server, and close the console session.

Compliance Baseline Management

Manual Compliance Check

We used a spreadsheet to keep track of all configuration items for the manual scenario. For every verification step in this methodology, if the setting is correct, mark C for compliant; if the setting is missing, mark M for missing; if the setting is different than the configuration baseline, mark D for different, and write the current setting in the non-compliant value cell in the compliance spreadsheet.

1. Connect a monitor.
2. Connect a keyboard.
3. Connect a mouse.
4. Power on the server.
5. Strike `F2` to enter Setup.
6. Select CPU Information.
7. Verify that Execute Disable is Enabled.
8. Verify that Virtualization Technology is Enabled.
9. Verify that Adjacent Cache Line Prefetch is Enabled. (Default: Disabled).
10. Verify that Hardware Prefetcher is Enabled.
11. Verify that Demand-Based Power Management is Disabled.
12. Verify that each processor reports the correct number of cores (4; 4).

13. Press Escape.
14. Verify that Boot Sequence Retry is Enabled.
15. Select Integrated Devices.
16. Verify that Embedded SATA is Off.
17. Verify that Embedded Gb NIC1 is Enabled with PXE.
18. Verify that Embedded Gb NIC2 is Enabled with PXE (Default: Enabled).
19. Scroll down to verify that OS Watchdog Timer is Disabled.
20. Press Escape.
21. Select Serial Communication.
22. Verify that Serial Communication is On with Console Redirection. (Default: On without Console Redirection).
23. Verify that External Serial Connector is COM1.
24. Verify that Failsafe Baud Rate is set to `115200`.
25. Verify that Remote Terminal Type is set to ANSI.
26. Press Escape.
27. Select System Security.
28. Scroll down to verify that NMI Button is Disabled.
29. Press Escape.
30. Press Escape again.
31. Select Discard Changes and Exit.
32. When prompted, press Ctrl-E to enter the Remote Access Configuration Utility. (If you are not prompted, send the Ctrl-Alt-Del macro to reboot the server and try again).
33. Select Network.
34. Verify that Enable IPMI Over LAN is On.
35. Verify that Enable Platform Event Filter Alerts is Enabled.
36. Select LAN Parameters.
37. Scroll down and verify that LAN Alert Enabled is On.
38. Verify that Alert Policy Entry 1 is Enabled.
39. Verify that Alert Destination 1 is `192.168.1.50`.
40. Press Escape.
41. Press Escape again.

Repository Manager and Automatic Updates

Manual firmware updates – iDRAC

1. Open a remote desktop r from within the management network and navigate to the iDRAC IP address (`192.168.1.105`).
2. Log in with the iDRAC's username and password (Username: `root`; Password: `calvin`).
3. Click the Console tab.
4. Click Connect.
5. A Java app launches. When the security warning appears, click Continue.
6. When the Java warning appears, click Run. The remote console viewer will launch.
7. If the server is not at the Windows Server log in screen, reboot. Once at the Windows log in screen, send the Ctrl-Alt-Del macro and log in with the username and password.
8. Locate the firmware update installation packages (for our tests, we used a folder on our desktop).
9. Run the network adapter firmware update installation package.
10. Click Install.

11. Click Next.
12. Accept the license agreement, and click Next.
13. Click Next.
14. Click Install.
15. Click Finish.
16. Run the SAS RAID firmware update installation package.
17. Click Install.
18. When the installation is finished, click No to manually restart the server later.
19. Run the Remote Access firmware update installation package.
20. Click Install.
21. During the firmware flash process, the console will lose connection to the server.
22. Navigate to the DRAC console from your management station (192.168.1.105) and attempt to login. Logins will be disabled until the firmware flash is complete. Open a command prompt, type `ping 192.168.1.105 -t` and wait for the DRAC IP to report successful pongs. Our test took around 15 minutes for the firmware flash to complete.
23. Log back into the DRAC.
24. Click the Console tab.
25. Click Connect.
26. A Java app launches. When the security warning appears, click Continue.
27. When the Java warning appears, click Run. The remote console viewer will launch.
28. If you are not logged into the server, send the Ctrl-Alt-Del macro and log in with the administrator credentials.
29. Verify that the update completed successfully.
30. Close all windows and restart the server.

Completing tasks with Dell OpenManage on the Dell PowerEdge R730

One-to-many deployment

OME Auto Deployment

This procedure assumes a CSV list of Service Tags and a baseline profile have already been created.

1. Open a Web browser and log in to OME.
2. Select Deployment.
3. Click Setup Auto Deployment.
4. Check the box for Deploy Template.
5. Check the box for Boot to Network ISO.
6. Click Next.
7. Expand Server Templates, and select the template to deploy.
8. Click Next.
9. Enter the ISO Filename you want to deploy. We used `windows2012r2.iso`
10. Enter the IP address of the OME server. We used `192.168.1.50`
11. Enter the share name of the deployment share. We entered `ServerConfig`
12. Enter the Share Username you configured for your deployment File Share. We used `test\administrator`
13. Enter the share password you configured for your deployment file sure user. We used `Password1`
14. Click Next.
15. Click Import.
16. Browse to the location of the CSV file containing hardware Service Tags, and click Open.
17. Click Ok. The servers from the CSV will be imported.

18. Click Next.
19. Click Next to accept defaults for template deployment.
20. Click Next to accept default iDRAC credentials.
21. Review the summary, and click Finish.
22. Click Yes to proceed.
23. Click Yes to confirm job creation.

iDRAC Direct (cable)

Automatic: USB A-A male-male cable

1. Remove the front bezel.
2. Connect a laptop to the server using a USB A/A cable. The USB cable must be connected to the server's USB management port, indicated on the front panel with a wrench icon.
3. Open a Web browser on the management laptop.
4. Connect to iDRAC at `169.254.0.3`, and accept any certificate or security warnings.
5. Log in with your username and password.
6. Click Storage→Virtual Disks.
7. Click Create.
8. For Layout, select RAID-1.
9. Under Internal Disks, check the boxes to select the disks to add to the array.
10. Click Create Virtual Disk.
11. Click OK. Alternatively, you can view the job status by clicking Job Queue.
12. Log off iDRAC.

iDRAC Direct (USB key)

Automatic: iDRAC Direct USB Key

1. Remove the bezel.
2. Connect a monitor to the server front panel, or observe the system through a remote console.
3. Insert a USB device with the necessary configuration profile.
4. Wait for the server to restart, as indicated by the monitor returning no signal.

Quick Sync (NFC)

Automatic read procedure (NFC + tablet)

1. Unlock the tablet.
2. Open the OpenManage application on the NFC-capable tablet.
3. Press the NFC button on front bezel.
4. Hold the tablet's NFC to the iDRAC Quick Sync and wait for tablet to refresh.
5. Touch Firmware Details.
6. Verify that the BIOS, Lifecycle Controller, PERC H730P Mini, and System CPLD are all up to date (0.3.23; 2.00.00.00; 25.2.1.0037; 0.5.1). Return to the main menu.
7. Touch the back arrow to go back to the main menu.
8. Touch Network Details.
9. Touch IPv4.
10. Check the IP Address, Default Gateway and DNS Address.
11. Touch the back arrow twice to return to the main menu.
12. Close the application.

Automatic write procedure (NFC + tablet)

1. Unlock the tablet.
2. Open the OpenManage application on the NFC-capable tablet.
3. Press the NFC button on the front bezel.
4. Place the tablet against the NFC area of the front bezel. The configuration will be imported.
5. Tap the gear icon at the top right of the page.
6. Tap iDRAC Configuration via Quick Sync (NFC bezel).
7. Tap IPv4 Settings.
8. Tap the checkbox for Enable DHCP to clear it.
9. Tap the top field for the IP address.
10. Using the tablet keyboard, enter the IP address. We used `172.16.10.120`.
11. Tap the middle field for the Gateway address.
12. Using the tablet keyboard, enter the IP address. We used `172.16.10.1`.
13. Tap the third field for the Subnet Mask.
14. Using the tablet keyboard, enter the IP address. We used `255.255.0.0`.
15. Tap the checkbox for Use DHCP for DNS to clear it.
16. Tap the fifth field for the primary DNS address.
17. Using the tablet keyboard, enter the IP address. We used `172.16.10.10`.
18. Tap the sixth field for the secondary DNS address.
19. Using the tablet keyboard, enter the IP address. We used `172.16.10.11`.
20. Tap Save.
21. Enter the username and password of the iDRAC you are going to update. We used the username `root` and the password `calvin`.
22. Press Sync Now.
23. Press the NFC button on the front bezel.
24. Touch the tablet to the NFC bezel to perform a Quick Sync.
25. Close the OpenManage app.

Tech Support Report

Automatic (13G TSR)

1. Log into iDRAC with your username and password.
2. Under Server in the vertical navigation menu, select Troubleshooting.
3. Select Tech Support Report in the horizontal navigation bar.
4. Select Advanced Export Options.
5. Check RAID Controller Log and OS and Application Data, and ensure Enable Report Filtering is checked.
6. Under Export Location, change the radio button to Network.
7. Fill out the required network information. For our tests, we used CIFS:
    a. IP Address: `192.168.1.20`
    b. Share name: `profiles`
    c. Domain Name: <blank>
    d. Username: Administrator
    e. Password: `Password1`
8. Check I agree to allow Technical Support to use this data.
9. Click Export.
10. View the status of the export by clicking the job queue button.
11. Refresh the page until the job status reports Completed.

OME Compliance Baseline Management

OME Baseline Configuration Compliance Check

1. Open a Web browser and connect to OME.
2. Select Manage→Configuration.
3. Click the red section of the pie chart indicated as non-compliant.
4. Double-click an entry in the pop-out table.
5. Note the missing and different settings. These are sortable and can be exported to HTML.

OME Agentless Driver Updates

Installing OMSA (one time task)

1. Log into remote server.
2. Browse to the location of the OMSA installation file.
3. Double-click setup.exe.
4. When prompted, click Run.
5. Correct any conditions that create an error, and click Install Server Administrator.
6. Click Next.
7. Select I accept the terms in the license agreement and click Next.
8. Click Typical and select Next.
9. Click Install.
10. Click Finish.

Performing Updates with OMSA

1. On the OME server, log in to OME.
2. Click Manage→System Update.
3. Click Select a Catalog Source in the left hand menu.
4. Select Use repository manager file.
5. Click Browse and select the catalog.xml file you want to use for the baseline.
6. Click Open to select the catalog.xml file.
7. Click Import Now. The compliance report will regenerate.
8. Click the red section of the chart indicating Non-Compliant Systems.
9. Check the box beside a non-compliant system. Note the preferred Delivery Method is In-Band Agent.
10. Under Select Updates to Apply, check the topmost box to select all updates.
11. Click Apply Selected Updates.
12. Select Run Now under Set the Task Schedule.
13. Check the box for Skip Signature and Hash Check.
14. Enter the server credentials for the task. We used `test\administrator` and `Password1`.
15. Click Finish.

Repository Manager and Automatic Updates

Automatic Updates (setup only – not counted as repetitive administrative task)

(Note: 72 seconds – not included in timed runs.)

1. Log into iDRAC with your username and password.
2. Select iDRAC Settings→Update and Rollback.
3. Click the Automatic Update tab.
4. Check the box for Enable Automatic Updates.
5. For Server Reboot, select Schedule Updates and Reboot Server.
6. For File Location, select Network.

7. For Protocol, select CIFS.
8. Enter the IP address of the repository host. We used `192.168.1.20`.
9. Enter the share name that houses the repository. We used `repoman`.
10. Enter the username with access to the repository share. We used `administrator`.
11. Enter the password of the user with access to the share. We used `Password1`.
12. Enter the start time for the maintenance window. We used `00:00`.
13. Select Monthly and use the pull-down menus to select the first Sunday of every one month.
14. Click Schedule Update.
15. Click OK to confirm that the Auto Update setup is complete.

ABOUT PRINCIPLED TECHNOLOGIES

Principled Technologies, Inc.
1007 Slater Road, Suite 300
Durham, NC, 27703
www.principledtechnologies.com

We provide industry-leading technology assessment and fact-based marketing services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from researching new technologies, to developing new methodologies, to testing with existing and new tools.

When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual requirements. Whether the technology involves hardware, software, Web sites, or services, we offer the experience, expertise, and tools to help our clients assess how it will fare against its competition, its performance, its market readiness, and its quality and reliability.

Our founders, Mark L. Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists, they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO of VeriTest.