



The science behind the report:

New VMware vSphere 7.0 features reduced the time and complexity of routine update and hardware compliance tasks

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report [New VMware vSphere 7.0 features reduced the time and complexity of routine update and hardware compliance tasks](#).

We concluded our hands-on testing on date July 21, 2020. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on date July 1, 2020 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

Table 1: Steps to perform tasks manually and with VMware vSphere® Lifecycle Manager (vLCM) and OpenManage Integration for VMware vCenter (OMIV). We used the manual approach as a baseline for determining savings.

Task	Approach	Steps	Savings over manual		
			Steps	Percentage	
Single node					
Update hypervisor	Manual	12	N/A	N/A	
	vLCM w/o Quick Boot	2	10	83.3%	
	vLCM w/ Quick Boot	2	10	83.3%	
Update hypervisor and firmware	Manual	19	N/A	N/A	
	vLCM and OMIV	2	17	89.4%	
Check hardware compatibility	Manual	21	N/A	N/A	
	vLCM	3	18	85.7%	

Task	Approach	Steps	Savings over manual	
Four-node cluster				
Update hypervisor	Manual	48	N/A	N/A
	vLCM w/o Quick Boot	2	46	95.8%
	vLCM w/ Quick Boot	2	46	95.8%
			Steps	Percentage
Update hypervisor and firmware	Manual	76	N/A	N/A
	vLCM and OMIVV	2	74	97.3%
Eight-node cluster				
Update hypervisor	Manual	96	N/A	N/A
	vLCM w/o Quick Boot	2	94	97.9%
	vLCM w/ Quick Boot	2	94	97.9%
Update hypervisor and firmware	Manual	152	N/A	N/A
	vLCM and OMIVV	2	150	98.6%

Table 2: Time to perform tasks manually and with automation tools. We used the manual approach as a baseline for determining savings. We abbreviate Quick Boot "QB."

Task	Approach	Admin time			System time			Total time		
		Time (h:mm:ss)	Savings (time)	Savings (%)	Time (h:mm:ss)	Savings (time)	Savings (%)	Time (h:mm:ss)	Savings (time)	Savings (%)
Single node										
Update hypervisor	Manual	0:09:31	N/A	N/A	0:13:23	N/A	N/A	0:22:54	N/A	N/A
	vLCM w/o QB	0:02:07	0:07:24	77.7%	0:08:22	0:05:01	37.4%	0:10:29	0:12:25	54.2%
	vLCM w/ QB	0:02:08	0:07:23	77.5%	0:06:13	0:07:10	53.5%	0:08:21	0:14:33	63.5%
Update hypervisor and firmware	Manual	0:18:45	N/A	N/A	0:27:24	N/A	N/A	0:46:09	N/A	N/A
	vLCM and OMIVV	0:02:12	0:16:33	88.2%	0:22:27	0:04:57	18.0%	0:24:39	0:21:30	46.5%
Check hardware compatibility	Manual	0:23:00	N/A	N/A	0:00:00	N/A	N/A	0:23:00	N/A	N/A
	vLCM	0:02:49	0:20:11	87.7%	0:00:00	N/A	N/A	0:02:49	0:20:11	87.7%
Four-node cluster										
Update hypervisor	Manual	0:42:50	N/A	N/A	0:47:41	N/A	N/A	1:30:31	N/A	N/A
	vLCM w/o QB	0:02:20	0:40:30	94.5%	0:24:02	0:23:39	49.6%	0:26:22	1:04:09	70.8%
	vLCM w/ QB	0:02:15	0:40:35	94.7%	0:16:24	0:31:17	65.6%	0:18:39	1:11:52	79.4%
Update hypervisor and firmware	Manual	1:37:35	N/A	N/A	2:10:47	N/A	N/A	3:48:22	N/A	N/A
	vLCM and OMIVV	0:02:51	1:34:44	97.0%	1:18:54	0:51:53	39.6%	1:21:45	2:26:37	64.2%

Task	Approach	Admin time			System time			Total time		
Eight-node cluster										
Update hypervisor	Manual	1:23:33	N/A	N/A	1:30:03	N/A	N/A	2:53:36	N/A	N/A
	vLCM w/o QB	0:02:56	1:20:37	96.4%	0:44:54	0:45:09	50.1%	0:47:50	2:05:46	72.4%
	vLCM w/ QB	0:02:21	1:21:12	97.1%	0:29:16	1:00:47	67.5%	0:31:37	2:21:59	81.7%
Update hypervisor and firmware	Manual	3:48:09	N/A	N/A	4:44:52	N/A	N/A	8:33:01	N/A	N/A
	vLCM and OMIVV	0:03:16	3:44:53	98.5%	2:38:46	2:06:06	44.2%	2:42:02	5:50:59	68.4%

Table 3: Time to update hypervisor in eight-node cluster using vLCM with and without Quick Boot enabled.

Approach	Admin time			System time			Total time		
	Time (mm:ss)	Savings with Quick Boot enabled		Time (mm:ss)	Savings with Quick Boot enabled		Time (mm:ss)	Savings with Quick Boot enabled	
		Time (mm:ss)	%		Time (mm:ss)	%		Time (mm:ss)	%
vLCM w/o QuickBoot	02:56	N/A	N/A	44:54	N/A	N/A	47:50	N/A	N/A
vLCM w/ QuickBoot	02:21	00:35	19.8%	29:16	15:38	34.8%	31:37	16:13	33.9%

System configuration information

Table 4: Detailed information on the systems we tested.

Server configuration information	3x Dell EMC™ PowerEdge™ R640	Dell EMC PowerEdge R630	Dell EMC PowerEdge R730
BIOS name and version	Dell 2.6.4	Dell 2.11.0	Dell 2.11.0
Non-default BIOS settings	N/A	N/A	N/A
Operating system name and version/build number	VMware ESXi™ 7.0b- 16324942	VMware ESXi 7.0b- 16324942	VMware ESXi 7.0b- 16324942
Date of last OS updates/patches applied	07/16/20	07/16/20	07/16/20
Power management policy	Performance	Performance	Performance
Processor			
Number of processors	2	2	2
Vendor and model	Intel® Xeon® Silver 4114	Intel Xeon E5-2670 v3	Intel Xeon E5-2690 v3
Core count (per processor)	10	12	12
Core frequency (GHz)	2.20	2.30	2.60
Stepping	A0	M1	M1
Memory module(s)			
Total memory in system (GB)	64	128	128
Number of memory modules	4	8	4
Vendor and model	Hynix HMA82GR7CJR8N-VK	Hynix HMA42GR7MFR4N-TF	Samsung M386A4G40DM0-CPB
Size (GB)	16	16	32
Type	PC4-21300	PC4-17000	PC-17000
Speed (MHz)	2,666	2,133	2,133
Speed running in the server (MHz)	2,666	2,133	2,133
Storage controller			
Vendor and model	Dell PERC H740p mini	Dell PERC H730p	Dell PERC H730 mini
Cache size (GB)	8	2	1
Firmware version	50.9.4	25.5.6.09	25.5.6.09
Driver version	7.712.50.00	7.712.50.00	7.712.50.00
Local storage			
Number of drives	2	2	2
Drive vendor and model	Toshiba AL15SEB060NY	Seagate ST9300605SS	ATA LK1600GEYMV
Drive size (GB)	600	300	1600
Drive information (speed, interface, type)	12Gb SAS, HDD	6Gb SAS, HDD	6Gb SATA, SSD

Server configuration information	3x Dell EMC™ PowerEdge™ R640	Dell EMC PowerEdge R630	Dell EMC PowerEdge R730
Network adapter			
Vendor and model	Broadcom® BCM57416 NetXtreme-E 10Gb Ethernet Adapter	Broadcom BCM5720 NetXtreme-E 1Gb Ethernet Adapter	Intel I350 Ethernet 10GbE 4P
Number and type of ports	2x 10 GbE	2x 1 GbE	4x 10 GbE
Driver version	216.0.72.0	4.1.4.1-1	1.4.11.0
Network adapter			
Vendor and model	Broadcom BCM5720 NetXtreme-E 1Gb Ethernet Adapter	Intel X540- AT2 10 Gigabit Ethernet Adapter	N/A
Number and type of ports	2x 1 GbE	2x 10 GbE	N/A
Driver version	4.1.4.1	1.8.9.0	N/A
Cooling fans			
Vendor and model	2x Sunon PG40561BX-Q100-S99 1x Delta GFC0412DS-D	Delta GFM0412SS	NMB 06038DA-12S-EWH
Number of cooling fans	8	7	6
Power supplies			
Vendor and model	Dell E750E-S1	Dell GFM0412SS	Dell L750E-S0
Number of power supplies	2	2	2
Wattage of each (W)	750	750	750

Table 5: Detailed information on the systems we tested.

Server configuration information	Dell EMC PowerEdge R730	Dell EMC PowerEdge R730xd	Dell EMC PowerEdge R740
BIOS name and version	Dell 2.11.0	Dell 2.11.0	Dell 2.11.0
Non-default BIOS settings	N/A	N/A	N/A
Operating system name and version/build number	VMware ESXi 7.0b- 16324942	VMware ESXi 7.0b- 16324942	VMware ESXi 7.0b- 16324942
Date of last OS updates/patches applied	07/16/20	07/16/20	07/16/20
Power management policy	Performance	Performance	Performance
Processor			
Number of processors	2	2	2
Vendor and model	Intel Xeon E5-2699 v4	Intel Xeon E5-2699 v4	Intel Xeon Silver 4108
Core count (per processor)	22	22	8
Core frequency (GHz)	2.20	2.20	1.80
Stepping	B0	B0	U0

Server configuration information	Dell EMC PowerEdge R730	Dell EMC PowerEdge R730xd	Dell EMC PowerEdge R740
Memory module(s)			
Total memory in system (GB)	128	256	256
Number of memory modules	24	16	16
Vendor and model	Hynix HMA42GR7AFR4N-TF	Samsung M393A2K43BB1-CRC	Samsung M393A2K43BB1-CRC
Size (GB)	16	16	16
Type	PC4-17000	PC4-19200	PC4-19200
Speed (MHz)	2,133	2,400	2,400
Speed running in the server (MHz)	2,133	2,400	2,400
Storage controller			
Vendor and model	Dell PERC H730 mini	Dell PERC H730 mini	Dell PERC H740P
Cache size (GB)	1	2	8
Firmware version	25.5.6.09	25.5.6.09	50.9.4-3025
Driver version	7.712.50.00	7.712.50.00	7.712.50.00
Local storage			
Number of drives	2	2	2
Drive vendor and model	ATA LK1600GEYMV	Seagate ST9300653SS	Toshiba THNSF8120CCSE
Drive size (GB)	1,600	300	120
Drive information (speed, interface, type)	6Gb SATA, SSD	15K, 6Gb SAS, HDD	6Gb SATA, SSD
Network adapter			
Vendor and model	Intel I350 Ethernet 10GbE 4P	Broadcom BCM5720 NetXtreme-E 1Gb Ethernet Adapter	Broadcom BCM5720 NetXtreme-E 1Gb Ethernet Adapter
Number and type of ports	4x 10 GbE	2x 1 GbE	2x 1 GbE
Driver version	1.4.11.0	4.1.4.1	4.1.4.1
Cooling fans			
Vendor and model	Sunon VF60381B1-Q000-S99	Delta PFR0612DHE	NMB 06038DA-12S-EWH
Number of cooling fans	6	6	6
Power supplies			
Vendor and model	Dell L750E-S0	Dell D750E-S6	Dell D1100E-S0
Number of power supplies	2	2	2
Wattage of each (W)	750	750	1,100

How we tested

In the Principled Technologies data center, we configured a VMware vSphere environment with the following Dell EMC PowerEdge servers: 3x R640, 1x R740, 1x R630, 2x R730, and 1x R730xd. We chose a mix of 13th generation and current-generation Dell servers to simulate a typical data center with multiple generations of servers. We installed the generally available version of ESXi 7.0 (build 15843807) on each server. Additionally, we configured a Dell EMC PowerEdge R720 with ESXi 7.0 to host our vCenter 7.0 appliance and the latest version of the OpenManage Integration for the VMware vCenter virtual appliance (5.1.0.1828).

We ran the following three scenarios, comparing the time and effort required to complete each task manually versus using automation features in vSphere Lifecycle Manager and OpenManage Integration for VMware vCenter::

- Updating the hypervisor
- Updating the hypervisor and firmware
- Hardware compatibility check

When updating the hypervisor, we updated each server to ESXi version 7.0b (build 16324942) with the Dell EMC add-on for PowerEdge servers (version A02). For additional updating of the firmware, we focused on updating the BIOS and the network firmware only. The specific running versions and updated versions of the BIOS and network firmware varied in our multigenerational testbed. For information on the exact versions used for each server, see Table 4: Update version list). We ran our test scenarios against three configurations: a single ESXi server, a four-node cluster, and an eight-node cluster. We timed each test, separating administrator time (when the test required user interaction) and system time (when the server took a significant time to process an update and system reboots). We report time in h:mm:ss. We did not include the time necessary to download patches from the VMware website since this would be a one-time cost and highly variable depending on internet connection speeds.

Prerequisites

Installing VMware ESXi 7.0

We used the following steps to install and configure ESXi 7.0 on the systems under test. Prior to installing, we obtained the image needed and put it on a bootable USB.

1. Boot the VMware ESXi installation media using a USB.
2. To Continue, press Enter.
3. To Accept and Continue, press F11 key.
4. Under Storage Device, select the installation drive, and press Enter.
5. Select US Default for keyboard layout, and press Enter.
6. Enter root password twice, and press Enter.
7. At the Confirm Install window, to install, press F11.
8. At the Installation Complete window, to reboot, press Enter.
9. After reboot, press F2 to Configure System.
10. Log in with root user/password, and press Enter.
11. Scroll to Configure Management Network, and press Enter.
12. Scroll to IPv4 Configuration, and press Enter.
13. Scroll to Static IPv4, and use spacebar to select it.
14. Set the IPv4, and use spacebar to select it.
15. To continue, Press Enter.
16. Scroll to IPv6 Configuration, and press Enter.
17. Scroll to Disable IPv6, and use spacebar to select it.
18. To continue, press Enter.
19. Scroll to DNS Configuration, and press Enter.
20. Scroll to manually configure DNS, and use spacebar to select it.
21. Add Primary DNS Server and Alternate DNS Server, and provide the hostname for the system.
22. Scroll to Custom DNS Suffixes, and press Enter.
23. Add the suffix that is required for testing, and press Enter.
24. To accept the changes, press ESC.

Deploying the VMware vCenter Server appliance

We used the following steps to deploy and configure the VMware vCenter appliance on our infrastructure server. Prior to completing the following, we obtained the VMware-VCSA installer image from VMware.

1. On a Windows server or VM, download VMware-VCSA installer image from https://my.vmware.com/en/web/vmware/downloads/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/7_0.
2. Mount the image, navigate to the vcsa-ui-installer folder, and double-click win32.
3. Double-click installer.exe.
4. Click Install.
5. Click Next.
6. Accept the terms of the license agreement, and click Next.
7. Leave the default Center Server with an Embedded Platform Services Controller selected, and click Next.
8. Enter the FQDN or IP address of the host onto which you are deploying the vCenter Server Appliance.
9. Provide the server's username and password, and click Next.
10. To accept the certificate of the host you chose to connect to, click Yes.
11. Provide a name and password for the vCenter Appliance, and click Next.
12. Set an appropriate Appliance Size, and click Next.
13. Select the appropriate datastore, and click Next.
14. At the Configure Network Settings page, configure the network settings as appropriate for your environment, and click Next.
15. Review your settings, and click Finish.
16. When the deployment completes, click Continue.
17. At the introduction page, click Next.
18. At the Appliance configuration page, select the time synchronization mode and SSH access settings, and click Next.
19. Select Create a new SSO domain.
20. Provide an SSO Domain name and SSO Site name.
21. Provide a password and confirm it, and click Next.
22. At the CEIP page, click Next.
23. At the Ready to complete page, click Finish.
24. At the Warning pop-up, click OK.
25. After Stage 2 has completed successfully, click Close.

Creating a cluster

Before creating the clusters, we added the ESXi servers to the vCenter.

1. In the vSphere Client, right-click on the Datacenter, and select a new cluster.
2. On the New Cluster dialog box, provide a name for the cluster, enable vSphere DRS, and check Manage all host in the cluster with single image.
3. In the Image Setup box, verify the ESXi version and select the proper Vendor Addon (we selected Dell EMC because we tested R640s). Click OK.
4. In the Cluster quickstart pane, under Add hosts, select Add.
5. On the Add host dialog box, select Existing hosts, choose your desired hosts, and click Next.
6. On Host summary, review the hosts, and click Next.
7. On Ready to complete screen, review the cluster, and click Finish.
8. Under the Configure cluster pane, click Configure.
9. On Configure Cluster dialog box, check Configure networking settings later, and click Next.
10. For Advanced Options, input the IP address for the NTP server, and click Next.
11. Review the cluster configuration, and click Finish. Depending on the test scenario, we added either four hosts or eight hosts to the cluster.

Configuring the OpenManage Integration for VMware vCenter

We obtained the OMIVV Integration appliance from the Dell website, deployed the virtual appliance in the vCenter, and completed the following steps.

1. Under the Menu drop-down, select OpenManage Integration.
2. Select the Settings tab, and click Start Initial Configuration Wizard.
3. To proceed, click Get Started.
4. Select your vCenter, and click Next.
5. On the Create Host Credential Profile page, click Create Host Credential Profile.
6. Click Get Started.
7. On Name and Credentials, provide name for the host profile, enter the iDRAC credentials and host ESXi credentials, check Enable Certificate For both, and click Next.
8. On the Select Host screen, select the host, and click Next.
9. On the Associated Host dialog box, check the box next to host, and click Begin Test. Once all the hosts have passed, click Finish.
10. On Create Host Credential Profile, click Next.
11. On Configure Additional Settings page, under Expand Inventory Schedule, set a desired schedule for inventory check. Click Apply, and click Next.
12. On the Additional Settings Confirmation pop-up, click Proceed.
13. On the Next Steps dialog box, review the next steps, and click Finish.

Creating a system profile in OMIVV

1. In the OpenManage Integration Appliance, select the Compliance & Deployment tab.
2. Select System Profile, and click Create Profile.
3. Click Get Started.
4. On Name and Description, enter a name for the Profile, keep the default Profile Type, and click Next.
5. On the Reference Server dialog box, select the desired server. When Extraction Confirmation pop-up appears, click OK.
6. On Select a Reference Server, click Next.
7. On Profile Settings, expand the iDRAC tab, input the iDRAC password of the reference server in the value column of the iDRAC Embedded1 Password Attribute, and click Next.
8. On the Summary page, review the details of the profile, and click Finish.

Creating a cluster profile in OMIVV

1. Under the Compliance & Deployment tab, select Cluster Profile.
2. Click Create New Profile.
3. On the Profile Name and Description, enter name of profile, and click Next.
4. On Associate Profiles, check System profile, and choose the created system profile in the System Profile drop-down.
5. Check Firmware Repository Profile, choose the Dell Default Catalog in the Firmware Repository Profile drop-down, and click Next.
6. On Associate Clusters, click Browse, select the desired cluster, click OK, and click Next.
7. On Schedule Drift Detection, choose the days and time for your desired schedule, and click Next.
8. On the Summary, review the details of the profile, and click Finish.

Creating a vLCM desired image

1. Select the cluster under Host and Cluster.
2. Under the Update tab, select Image under Host.
3. In the right-hand corner, click the Edit button.
4. On Select Driver Addon, in the Select the hardware support manager drop-down, select Dell EMC OMIVV.
5. Select the cluster profile for the firmware and driver add-on, and click Select.
6. Click Validate, and click Save.

Scenario: Updating the hypervisor

We ran and timed the following test scenarios on a single server, a four-node cluster, and an eight-node cluster.

Installing ESXi patch updates manually

Total steps: 12

Prior to the installing, we obtained the required patches from the VMware product patches page.

1. Log into the ESXi host with the desired datastore you want to upload the patch file.
2. Select Storage, and click Datastore browser.
3. To make a new folder, click Create directory, name the folder, and click Create directory.
4. Select the newly created folder, click Upload, select the patch you downloaded from VMware, and click Open.
5. Place the server in maintenance mode.
6. Ensure that ESXi Shell and SSH services have started.
7. Through PuTTY connect, SSH to the host server using the proper credentials.
8. Navigate to the directory on the datastore where you uploaded the patch file, and verify that the file exists by running the following commands:

```
# cd /vmfs/volumes/Datastore/DirectoryName
# ls
```

9. From the home directory, to update the host with the patch, enter the following command:

```
# esxcli software vib update -d /vmfs/volumes/Datastore/DirectoryName/vib_update.zip
```

10. Verify that the VIBs are installed on your ESXi host:

```
# esxcli software vib list
```

11. After you have installed the patch, reboot the ESXi host:

```
# reboot
```

12. After the host has finished booting, exit maintenance mode.

Remediating image compliance using vLCM without Quickboot

Total steps: 2

1. In the Edit Image box, set ESXi version, Vendor Add-ons, and components, and click Validate and Save.
2. Once the compliance check completes, to push the updates to the servers, click Remediate.

Remediating image compliance using vLCM with Quickboot

Total steps: 2

We enabled QuickBoot in the Lifecycle Manager prior to performing the following tasks.

1. In the Edit Image box, set ESXi version, Vendor Add-ons, and components, and click Validate and Save.
2. Once the compliance check completes, to push the updates to the servers, click Remediate.

Scenario: Updating the hypervisor and firmware

We ran and timed the following test scenarios on a single server, a four-node cluster, and an eight-node cluster.

Updating Dell EMC firmware using Lifecycle Controller

Dell EMC provides two recommended methods for running firmware updates on Dell EMC servers with ESXi: using Lifecycle Controller or booting to the platform-specific firmware update ISO available from the Dell EMC website for each server type. We chose to use Lifecycle Controller since this feature was available in all our test servers. We completed the steps for the manual hypervisor sections prior to running these. A total of 7 steps.

1. From boot, to enter the Lifecycle Controller during POST, press F10.
2. In the left pane, under Home, select Firmware Update.
3. In the Firmware Update pane, select Launch Firmware Update.
4. On Select Update Repository, select FTP Server.
5. Verify the default FTP share information, click Test Network Connection, and click Next.
6. After reading the Firmware Update Warning, click Yes.
7. On Select Updates, select the BIOS and network firmware, and click Apply. Allow the system to update and reboot itself.

Remediating image compliance using vLCM and OMIVV

We completed the configuration of OMIVV integration, created the necessary profiles (Host, Cluster, and System), and created a vLCM desired Image prior to the following steps. A total of 2 steps.

1. In the Edit Image box, set ESXi version, Vendor Add-ons, and components, and click Validate and Save.
2. Once the compliance check completes, to push the updates to the servers, click Remediate.

Scenario: Hardware compatibility

We ran and timed the following test scenarios on a single server. For a single server hardware compatibility check, vLCM performs the check automatically against the VMware Compatibility Guide (VCG). For our manual process, we searched the online VCG for our server components.

Manually checking hardware compliance on the VMware hardware compatibility list

Required steps: 10

We completed the following steps by utilizing iDRAC and the Host UI from a web browser. A total of 10 steps.

1. Log into the server iDRAC.
2. From the iDRAC, select the system drop-down menu, and click Inventory.
3. Gather the model name, Device ID, and firmware information of the BIOS, CPU, NIC, storage controller, and AHCI SATA controller.
4. Log into the ESXi host UI.
5. To collect the driver information, navigate to Manage → Packages.
6. Navigate to the VMware Compatibility guide <https://www.vmware.com/resources/compatibility/search.php>.
7. In the Search Compatibility Guide search bar, enter the device ID, and click Search.
8. On the results page, select the correct component model.
9. On the details page, select the Model release that corresponds to ESXi 7.0.
10. Repeat steps 7 through 9 for the other components.

Remediating image compliance using vLCM

Prior to completing the following steps, we added the hosts to the vCenter. A total of 3 steps.

1. Under the Host and Cluster menu, navigate to the server.
2. Select the Update tab, and click Hardware Compatibility
3. Go through each Compatible device, and verify that the current driver and firmware are listed on the Supported in VMware Compatibility Guide list.

Update version list

Table 6: Detailed information on the server update versions. We updated each server from ESXi 7.0 GA (15843801) to ESXi 7.0bs (16321839) with the Dell A02 vendor add-on driver pack.

	Previous firmware	Current firmware
Dell EMC PowerEdge R740		
BIOS	2.5.4	2.6.4
BCM5720	21.40.21	21.60.2
Dell EMC PowerEdge R730xd		
BIOS	2.10.5	2.11.0
BCM5720	21.40.21	21.60.2
Dell EMC PowerEdge R730		
BIOS	2.8.0	2.11.0
X520/I350	19.0.12	19.5.12
Dell EMC PowerEdge R730		
BIOS	2.7.1	2.11.0
X520/I350	18.0.17	19.5.12
Dell EMC PowerEdge R640		
BIOS	2.4.8	2.6.4
BCM5720	21.40.21	21.60.2
BCM57416	21.40.25.31	21.60.22.11
Dell EMC PowerEdge R640		
BIOS	2.3.10	2.6.4
BCM5720	21.40.21	21.60.2
BCM57416	21.40.25.31	21.60.22.11
Dell EMC PowerEdge R640		
BIOS	2.3.10	2.6.4
BCM5720	21.40.21	21.60.2
BCM57416	21.40.25.31	21.60.22.11
Dell EMC PowerEdge R630		
BIOS	2.9.1	2.11.0
BCM5720	21.40.2	21.40.21

Read the report at <http://facts.pt/chz3xgi> ►

This project was commissioned by Dell EMC.



Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc.
All other product names are the trademarks of their respective owners.

DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:

Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.'s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.'s testing. Customer's sole and exclusive remedies are as set forth herein.