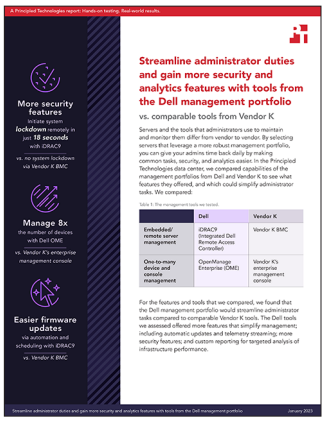

The science behind the report:

Streamline administrator duties and gain more security and analytics features with tools from the Dell management portfolio

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 Streamline administrator duties and gain more security and analytics features with tools from the Dell management portfolio.

We concluded our hands-on testing on September 14, 2022. 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 September 14, 2022 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

To learn more about how we have calculated the wins in this report, go to http://facts.pt/calculating-and-highlighting-wins. Unless we state otherwise, we have followed the rules and principles we outline in that document.

Table 1: Detailed results of our testing.

Use case	Dell iDRAC9		Vendor K			
	Time (s)	Steps	Available?	Time (s)	Steps	Manual
Security						
System lockdown	18	3	No	N/A	N/A	No
MFA	62	7 or 12	No	N/A	N/A	No
Dynamic USB	**37**	**4**	**No**	**290**	**14**	**Yes**
Ease of use						
Automatic updates	74	7	No	N/A	N/A	
Server profile Configuration	**91 + 51**	**12**	**Mixed**	**72 + 57**	**11**	
Telemetry streaming	49	5	No	N/A	N/A	
BIOS configuration	N/A	N/A	Yes (limited)	N/A	N/A	

Table 2: Comparison of the two management portfolios.

Use Case	Dell OME		Vendor K			
	Time (s)	Steps	Available?	Time (s)	Steps	Manual
Analytics						
Sending telemetry data	N/A	N/A	No	N/A	N/A	Yes
Reporting	N/A	N/A	No	N/A	N/A	Yes
Ease of use						
Scalability	N/A	N/A	Yes	N/A	N/A	
Alert-based actions	68	13	No	68	7	
Third-party device monitoring	N/A	N/A	No	N/A	N/A	
Third-party device monitoring with MIB import	N/A	N/A	No	N/A	N/A	
Carbon emission analysis	N/A	N/A	No	N/A	N/A	
Plug-in based architecture	N/A	N/A	Yes	N/A	N/A	

System configuration information

Table 3: Detailed information on the systems we tested.

System configuration information	Vendor K systems	Dell™ PowerEdge™ R750	Dell PowerEdge R7525
BIOS name and version	Undisclosed	Dell 1.6.5	Dell 2.5.6
Operating system name and version/build number	ESXi_7.0.2 build-17867351	DellEMC-VMware ESXi 7.0 Update 3 Build-19193900 (A03)	DellEMC-VMware ESXi7.0 Update 2 Build-17867351 (A06)
Date of last OS updates/ patches applied	Nov 1, 2022	09/15/22	09/15/22
Power management policy	Balanced	Balanced	Balanced
Processor			
Number of processors	1	2	2
Vendor and model	Intel® Xeon(® Gold 6334 CPU @ 3.60GHz	Intel Xeon Silver 4314 CPU @ 2.40GHz	AMD EPYC 7252 8-Core Processor
Core count (per processor)	8	16	8
Core frequency (GHz)	3.60	2.40	3.1
Memory module(s)			
Total memory in system (GB)	64	128	64
Number of memory modules	4	4	4
Vendor and model	Undisclosed	Hynix HMAA4GR7CJR8N-XN	Hynix HMA82GR7CJR8N-XN
Size (GB)	16	32	16
Type	PC4-25600	PC4-25600	PC4-25600
Speed (MHz)	3,200	3,200	3,200
Speed running in the server (MHz)	3,200	2,666	3,200
Storage controller			
Vendor and model	Undisclosed	Dell HBA355i	Dell PERC H345
Cache size	Undisclosed	N/A	0
Firmware version	Undisclosed	17.15.08.00	51.16.0-4076
Local storage (type A)			
Number of drives	2	2	2
Drive vendor and model	Undisclosed	SKhynix HFS480G3H2X069N	SKhynix HFS480G3H2X069N
Drive size	240	447 GB	447 GB
Drive information (speed, interface, type)	M.2 SATA SSD	6Gb SATA, SSD	6Gb SATA, SSD

System configuration information	Vendor K systems	Dell™ PowerEdge™ R750	Dell PowerEdge R7525
Local storage (type B)			
Number of drives	2	n/a	n/a
Drive vendor and model	Undisclosed	n/a	n/a
Drive size	600	n/a	n/a
Drive information (speed, interface, type)	10K 12Gbps SAS 2.5"	n/a	n/a
Network adapter A			
Vendor and model	Intel X710 2x10GbE SFP+ Adapter	1x Broadcom® Gigabit Ethernet BCM5720	1x Broadcom Gigabit Ethernet BCM5720
Number and type of ports	2 x 10GbE	2 x 1Gb	2 x 1Gb
Firmware version	Undisclosed	1.2829.0	1.2829.0
Network adapter B			
Vendor and model	Intel X710-T2L 10GBASE-T 2-port OCP Ethernet Adapter	1x Intel® Ethernet 10G 4P X710-T4L-t OCP	Broadcom Adv. Dual 25Gb Ethernet
Number and type of ports	2 x OCP	4 x 10GbE	2 x 25GbE
Firmware version	Undisclosed	20.5.13	20.5.13
Cooling fans			
Vendor and model	Vendor K	Dell Gold	Dell Gold
Number of cooling fans	5	4	4
Power supplies			
Vendor and model	Vendor K	Dell 0CYHHJA02	Dell
Number of power supplies	1	2	2
Wattage of each (W)	750	1400	800

How we tested

Comparing Dell iDRAC vs Vendor K BMC

System lockdown (iDRAC)

1. Open a web browser and connect to the iDRAC login page. Enter a username and password, and click Login.
2. In the upper-right corner of the browser, click the Lock icon, and select Enable.

System lockdown (Vendor K BMC)

1. There was no equivalent system lockdown feature in the Vendor K BMC we tested. It does appear a similar feature exists in one Vendor K purpose-built edge server.

Disabling USB ports (iDRAC)

Initial configuration

1. Open a web browser, and connect to the iDRAC login page. Enter a username and password, and click Login.
2. Click Configuration→BIOS Settings.
3. Expand Integrated Devices. Change the value of User Accessible USB Ports to All ports off (Dynamic). Click Apply, and Reboot.
4. Click OK.

Enabling or disabling USB ports dynamically

1. Open a web browser, and connect to the iDRAC login page. Enter a username and password, and click Login.
2. Select Configuration→System Settings.
3. Expand Hardware Settings→Front Ports. Use the drop-down menu to enable or disable the ports. Click Apply.

Disabling USB Ports (Vendor K BMC)

1. Open a web browser, and connect to the Vendor K BMC management page. Enter a username and password, and click Login.
2. Click to launch the remote control.
3. Click the top-down menu (far left)→Power→Restart server immediately. Wait for the system to enter pre-boot.
4. When visible, Press F1 to enter System Setup.
5. Select UEFI Setup→System Settings→Devices & I/O Ports→USB Configuration→USB Ports (Enabled/Disabled).
6. Select a setting. Click Save the settings, and reboot.
7.

Enabling multi-factor authentication

RSA SecurID option

1. Open a web browser, and connect to the iDRAC login page. Enter a username and password, and click Login.
2. Select iDRAC Settings→Users.
3. Expand Local Users. Select an existing user (we selected PT_Test), and click Edit.
4. Scroll down to the bottom of the page. If SecurID is not already configured, perform the following:
5. Click the link for the SecurID configuration.
6. If it has not already been installed, upload the RSA Server Certificate.
7. Enter the RSA SecurID Authentication Server URL, the Client ID, and the Access Key, and click Test Network Connection.
8. Click Configure.
9. Click OK.
10. Beside RSA SecurID State, use the drop-down menu to select Enabled. Click Save.
11. Click OK.

Easy 2FA option (requires an SMTP server)

1. Open a web browser, and connect to the iDRAC login page. Enter a username and password, and click Login.
2. Select iDRAC Settings→Users.
3. Expand Local Users. Select an existing user (we selected PT_Test), and click Edit.
4. Scroll down to the bottom of the page. If an SMTP server is not already configured, perform the following:
5. Click the link for Configure SMTP.

6. Enter the IP address or FQDN of the SMPT server. Click Configure.
7. Click OK.
8. Beside the Easy 2FA State, use the drop-down menu to select Enabled. Enter the IP address for the user, and click Test Connection.
9. Click OK.
10. Click Save.
11. Click OK.

Enabling automatic updates (iDRAC)

1. Open a web browser, and connect to the iDRAC login page. Enter a username and password, and click Login.
2. Click Maintenance→System Update.
3. Click Automatic Update.
4. At the bottom of the page, click Enable Automatic Update.
5. Click OK.
6. Select the Server Reboot type: Schedule Updates. From the Location Type drop-down menu, select HTTPS. Under HTTPS Server settings, enter downloads.dell.com. In the Update Window Schedule section, specify the start time for the firmware update (we chose 00:00), and the frequency of the updates (we selected daily). Click Schedule Update.

Exporting/importing server configuration profile (iDRAC)

Exporting a server configuration profile

1. Open a web browser, and connect to the iDRAC login page. Enter a username and password, and click Login.
2. Click Configuration→Server configuration profile.
3. Expand Export. Enter the filename (test) you want to save the profile under, and check the boxes for the components you want to capture (we selected all). From the Export Type drop-down menu, select Clone.
4. Click Export. Upon completion, click Save Locally. You can import this file (test.xml) to any server with identical hardware configurations, and it will replace the assigned values on the target with the values contained in the file.

Importing a server configuration profile

1. Open a web browser, and connect to the iDRAC login page. Enter a username and password, and click Login.
2. Click Configuration→Server configuration profile.
3. Expand Import. Next to File Path, select File.
4. Browse to the file location you want to import, select the file, and click Open.
5. Next to Import Components, check the box for All. Click Import.
6. Alternately, to test the profile for changes and view the Job Queue for status, click Preview. Then, repeat the process above to import the file.
7.

Telemetry streaming (iDRAC)

1. Open a web browser, and connect to the iDRAC login page. Enter a username and password, and click Login.
2. Click Configuration→System Settings.
3. Expand Telemetry Configuration. Enter the RSyslog Server1 address and port number, and click Apply.
4. Click OK.

Read the report ▶

This project was commissioned by Dell Technologies.

Principled Technologies®

Facts matter.®