



The science behind the report:

Dell server management tools can help improve security, sustainability, and management efficiency

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 Dell server management tools can help improve security, sustainability, and management efficiency.

We concluded our hands-on testing on May 13, 2024. 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 May 13, 2024 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

System configuration information

Table 1: Detailed information on the systems we tested.

System configuration information	Dell™ PowerEdge™ R760	Vendor K systems
BIOS name and version	Dell 1.8.2	Undisclosed
Non-default BIOS settings	Intel® Turbo Boost enabled, Virtualization enabled	Intel Turbo Boost enabled, Virtualization enabled
Date of last OS updates/patches applied	04/29/2024	05/15/2024
Power management policy	Balanced (initial) / Performance (post-test)	Balanced (initial) / Performance (post-test)
Processor		
Number of processors	2	2
Vendor and model	Intel® Xeon® Gold 6454S CPU @2.20 GHz	Intel Xeon Gold 6454S CPU @2.20 GHz
Core count (per processor)	32	32
Core frequency (GHz)	2.20	2.20
Stepping	8	8

System configuration information	Dell™ PowerEdge™ R760	Vendor K systems
Memory module(s)		
Total memory in system (GB)	256	256
Number of memory modules	16	16
Vendor and model	Hynix SYS-221H-TNR	Undisclosed
Size (GB)	16	16
Type	DDR5	DDR5
Speed (MHz)	4,800	4,800
Speed running in the server (MHz)	4,800	4,800
Storage controller		
Vendor and model	Dell PERC H965i Front (Embedded)	Undisclosed
Cache size	-	8 GB
Firmware version	17.15.08.00	Undisclosed
Local storage		
Number of drives	6	6
Drive vendor and model	Samsung MZILG1T6HCJRAD3	Undisclosed
Drive size (GB)	1,500	1,600
Drive information (speed, interface, type)	24 Gbps, SAS, SSD	24Gb SAS SSD
Network adapter		
Vendor and model	1x Broadcom Gigabit Ethernet BCM5720, 1x Broadcom Adv Dual 10GBASE-T Ethernet, 1x Broadcom BCM57504 4x25G SFP28 PCIE	Broadcom BCM5719 1Gb 4-p OCP Adapter Broadcom NetXtreme-E Dual-port 10GBASE-T Ethernet PCIe Adapter
Number and type of ports	2 x 1GbE, 2 x 10GbE, 4x25GbE	4 x 1 GbE, 2x 10GbE
Driver version	22.31.6, 22.31.13.70, 22.31.13.70	20.24.41, 223.1.96.0
Cooling fans		
Vendor and model	Dell Silver	Vendor K
Number of cooling fans	6	6
Power supplies		
Vendor and model	Dell 06C11WA02	Vendor K
Number of power supplies	2	2
Wattage of each (W)	1,400	1,000

How we tested

In our testing, we compared Dell Technologies Integrated Dell Remote Access Controller 9 (iDRAC9) to Vendor K baseboard management controller (BMC) and Dell Technologies OpenManage Enterprise (OME) to Vendor K's enterprise management console. In order to prevent the identification of Vendor K, we have omitted the detailed steps to complete the Vendor K testing. We took every measure to ensure a fair comparison between the competing management tools.

Enabling dynamic USB ports

iDRAC9

1. Log into iDRAC.
2. Navigate to Configuration → System Settings.
3. Expand Hardware Settings → Front Ports. Toggle Front USB port to Enabled/Disabled from iDRAC9. Click Submit.
4. To confirm, click OK.

Completing system lockdown

iDRAC9

1. Log into iDRAC9.
2. On the Dashboard, use the More Actions menu to select Turn on the System Lockdown Mode. A banner message will appear indicating the inability to make changes while lockdown is turned on.

Changing a BIOS configuration item

iDRAC9

1. Log into iDRAC.
2. Navigate to Configuration → BIOS Settings.
3. Expand System Profile Settings and select Performance from the pull-down menu beside System Profile. Click Apply, and click OK to confirm.
4. Scroll down and click At Next Reboot. Click OK to confirm.

Setting up alert-based actions

OME

1. Log into OME.
2. Click Alerts → Alert Policies.
3. Click Create.
4. Provide a name and description of the policy, and check the Enable checkbox. Click Next.
5. Select Built-in → iDRAC → System Health → Temperature. Click Next.
6. To skip the message IDs, click Next.
7. Click Select Devices.
8. Check the box next to the server or servers to which you want the policy applied, and click OK.
9. Click Next.
10. To accept the date defaults, click Next.
11. Check the box for Critical, and click Next.
12. Check the box for Power Control, and select Graceful Shutdown. Click Next.
13. To create and apply the policy, click Finish.

Scheduling power action jobs in APEX AIOps Infrastructure Observability (formerly CloudIQ)

1. Log into CloudIQ.
2. Expand Monitor, and click Systems.
3. Click Server.
4. Select a server to open the system details page.
5. At the top left of the Details page, click Actions, and select a power job.
6. Click Ok to confirm job submission.

Scheduling firmware updates in APEX AIOps Infrastructure Observability (formerly CloudIQ)

1. Log into CloudIQ.
2. Expand Manage, and click System Updates.
3. Click Server.
4. Select any compliance reports.
5. Select the systems or components you want to update, and click Update.
6. Select Schedule Update.
7. Click the date, and choose the date and time you want to set the update schedule. Click Next.
8. Choose either Reset iDRAC or Clear Job Queue. Click Next.
9. Review the summary, and click Finish.

[Read the report ▶](#)

This project was commissioned by Dell Technologies.



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.