The science behind the report:

Improve security, sustainability, and administrator efficiency with the Dell server 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 Improve security, sustainability, and administrator efficiency with the Dell server management portfolio.

We concluded our hands-on testing on May 3, 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 April 1, 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	HPE ProLiant DL380 Gen11
BIOS name and version	Dell 1.8.2	U54 v1.44
Non-default BIOS settings	Intel® Turbo Boost enabled, Virtualization enabled	Intel Turbo Boost enabled, Virtualization enabled
Date of last OS updates/patches applied	024/29/2024	03/22/2024
Power management policy	Balanced (initial) / Performance (post-test)	Balanced (initial) / Performance (post-test)
Processor		
Number of processors	2	2
Vendor and model	2x Intel Xeon® Gold 6454S CPU @2.20GHz	Intel Xeon Gold 6454S CPU @2.2GHz
Core count (per processor)	32	32
Core frequency (GHz)	2.20	2.2
Stepping	8	8

System configuration information	Dell™ PowerEdge™ R760	HPE ProLiant DL380 Gen11
Memory module(s)		
Total memory in system (GB)	256	256
Number of memory modules	16	16
Vendor and model	Hynix SYS-221H-TNR	Samsung M321R2GA3BB6-CQKVS
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)	HPE MR416i-p Gen11
Cache size (GB)	N/A	8
Firmware version	17.15.08.00	52.22.3-4650
Local storage		
Number of drives	6	6
Drive vendor and model	Samsung MZILG1T6HCJRAD3	HPE MO001600PZWSH
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 BASE-T OCP Adptr Broadcom P210tep 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
Firmware 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	HPE
Number of cooling fans	6	6
Power supplies		
Vendor and model	Dell 06C11WA02	HPE P03178-B21
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 HPE Integrated Lights-Out (iLO 6) and Dell Technologies OpenManage Enterprise (OME) to HPE OneView.

Disabling USB ports with iLO 6

1. Log into iLO 6.
2. Click to launch the remote console. Click the far-left menu, and click Power→Reset.
3. When prompted during POST, press F9 to enter System Utilities.
4. From the System Utilities screen, select System Configuration→BIOS/Platform Configuration (RBSU)→System Options→USB Options→USB Control.
5. Select External USB Ports Disabled. Press F12 to save the settings and reboot.
6. To confirm settings changes, click Yes.
7. Click Reboot.

Disabling front USB ports with iDRAC9

1. Log into iDRAC9.
2. Browse to Configuration→System Settings.
3. Expand Hardware Settings→Front Ports. Select Disabled, and click Apply.
4. To confirm, click Yes.

Completing system lockdown with iLO 6

1. Log into iLO 6.
2. Click to launch the remote console.
3. Click the far-left menu, and click→Power→Reset.
4. When prompted during POST, press F9 to enter System Utilities.
5. From the System Utilities screen, select System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Server Configuration Lock Settings.
6. Click Setup Server Configuration Lock.
7. Enter a server configuration lock password, and press Enter. Re-enter the password to confirm.
8. Re-enter the security section, and submit the password.
9. Change the following options:
    a. Server Configuration Lock Challenge required: Select Enabled or Disabled.
    b. Prepare system for Transport: Select Enabled or Disabled.
    c. Halt on Server Configuration Lock failure detection: Select Enabled or Disabled.
10. Press F12 or click the button at the bottom right to save the settings and reboot.
11. To confirm setting changes, click Yes.
12. To confirm exit and reboot, click Reboot.

Completing system lockdown with 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 in turned on.

Changing a BIOS configuration item with iLO 6

1. Log into iLO 6.
2. Click to launch the remote console.
3. Click the far-left menu, and click→Power→Reset.
4. When prompted during POST, press F9 to enter System Utilities.
5. From the System Utilities screen, select System Configuration→BIOS/Platform Configuration (RBSU)→Power and Performance Options.
6. Change Energy/Performance Bias to Maximum Performance. Press F12 or click the button at the bottom right to save the settings and reboot.
7. To confirm setting changes, click Yes.
8. To confirm exit and reboot, click Reboot.

Deploying a server template with OME

1. Log into OME Console.
2. From the main menu, select Configuration→Templates.
3. Check the box beside the template you want to deploy, and click Deploy Template.
4. To choose the target servers, click Select.
5. Check the box(es) to select the device(s) or group of devices you want to deploy, and click OK. We selected a group containing all of the servers under test.
6. Click Next.
7. Leave the Boot to Network ISO fields clear, and click Next.
8. Accept the default Don't change IP settings, and click Next.
9. Select or clear any configuration settings you want modified/unmodified, and click Next.
10. Click Finish to Run immediately, and confirm.

Deploying a server template with OneView

1. Log into OneView Console.
2. From the main menu, select Server's menu→Server Profile Templates.
3. Select one of the existing templates listed, and click Actions→Create Server Profile.
4. Provide all required details :
    a. Provide Name for the profile to associate with a server.
    b. Provide description in description field.
    c. Select the server hardware to be associated with (only one server can be selected).
    d. For the firmware baseline, select managed manually.
5. Click Create.

Creating alert-based actions in OneView

1. Log into OneView.
2. On the dashboard, click the Active Alerts widget.
3. Click a specific alert to review the alert, and click the affected resource to take an action.
4. Within the Server Hardware section, click the action button in the upper right menu, and select an action from the menu.
5. To confirm the action you selected, click Yes.

Creating alert-based actions in 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.

Read the report at https://facts.pt/w9zEpwk ▶

This project was commissioned by Dell Technologies.

Principled Technologies®

Facts matter.®