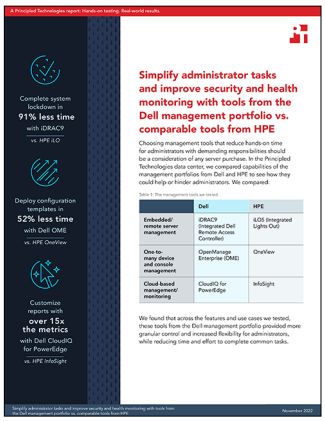

The science behind the report:

Simplify administrator tasks and improve security and health monitoring with tools from the Dell management portfolio vs. comparable tools from HPE

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 Simplify administrator tasks and improve security and health monitoring with tools from the Dell management portfolio vs. comparable tools from HPE.

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: Results of our Integrated Dell Remote Access Controller (iDRAC 9) and HPE Integrated Lights Out (iLO5) testing.

	Integrated Dell Remote Access Controller (iDRAC) 9 v 6.00	HPE Integrated Lights Out (iLO5) v 2.70
Management features comparison		
Number of remote HTML management features	10	4
Number of remote BIOS management features	52	4
System Lockdown use case		
Time to complete use case (m:ss)	0:18	3:40
Number of steps to complete	3	12
Dynamic USB use case		
Time to complete use case (m:ss)	0:37	2:49
Number of steps to complete	4	12

Table 2: Results of our Dell OpenManage Enterprise and HPE OneView testing.

	Dell OpenManage Enterprise v 3.9.0 (Build 55)	HPE OneView v 7.00.00-0460837
Deploying configuration templates		
Time to complete deployment (m:ss)	0:32	1:07
Number of steps to complete deployment	10	12
Built-in reporting comparison		
Number of built-in reports each solution offers	41	10

Table 3: Results of our Dell CloudIQ for PowerEdge and HPE InfoSight testing.

	Dell CloudIQ for PowerEdge	HPE InfoSight
Setting up a policy-based security view		
Number of steps	2	5
Customizable report metrics comparison		
Number of customizable report metrics each solution offers	66	4

System configuration information

Table 4: Detailed information on the systems we tested.

System configuration information	HPE ProLiant DL380 Gen10 Plus	HPE ProLiant DL385 Gen10 Plus V2	Dell™ PowerEdge™ R750	Dell PowerEdge R7525
BIOS name and version	U46 v1.58 (01/13/2022)	A42 v2.54 (12/03/2021)	Dell 1.6.5	Dell 2.5.6
Operating system name and version/build number	ESXi_7.0.2 build-17867351	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	09/15/22	09/15/22	09/15/22	09/15/22
Power management policy	Balanced	Balanced	Balanced	Balanced
Processor				
Number of processors	1	2	2	2
Vendor and model	Intel® Xeon® Gold 6334 CPU @ 3.60GHz	AMD EPYC 72F3 8-Core Processor	Intel Xeon Silver 4314 CPU @ 2.40GHz	AMD EPYC 7252 8-Core Processor
Core count (per processor)	8	8	16	8
Core frequency (GHz)	3.60	3.70	2.40	3.1
Memory module(s)				
Total memory in system (GB)	64	64	128	64
Number of memory modules	4	4	4	4
Vendor and model	Samsung® M393A2K43DB3-CWE	Hynix HMA82GR7DJR8N-XN	Hynix HMAA4GR7CJR8N-XN	Hynix HMA82GR7CJR8N-XN
Size (GB)	16	16	32	16
Type	PC4-25600	PC4-25600	PC4-25600	PC4-25600
Speed (MHz)	3,200	3,200	3,200	3,200
Speed running in the server (MHz)	3,200	3,200	2,666	3,200
Storage controller				
Vendor and model	HPE Smart Array E208i-a SR Gen10	HPE Smart Array E208i-a SR Gen10	Dell HBA355i	Dell PERC H345
Cache size	N/A	N/A	N/A	0
Firmware version	4.11	4.11	17.15.08.00	51.16.0-4076
Local storage				
Number of drives	2	2	2	2
Drive vendor and model	HPE MM1000GFJTE	HPE MM1000GFJTE	SKhynix HFS480G3H2X069N	SKhynix HFS480G3H2X069N
Drive size	1 TB	1 TB	447 GB	447 GB
Drive information (speed, interface, type)	7,200, 6Gb SATA, HDD	7,200, 6Gb SATA, HDD	6Gb SATA, SSD	6Gb SATA, SSD

System configuration information	HPE ProLiant DL380 Gen10 Plus	HPE ProLiant DL385 Gen10 Plus V2	Dell™ PowerEdge™ R750	Dell PowerEdge R7525
Network adapter A				
Vendor and model	Intel Eth CNA X710-DA2	Intel Eth CNA X710-DA2	1x Broadcom® Gigabit Ethernet BCM5720	1x Broadcom Gigabit Ethernet BCM5720
Number and type of ports	2 x 10GbE	2 x 10GbE	2 x 1Gb	2 x 1Gb
Firmware version	1.2829.0	1.2829.0	1.2829.0	1.2829.0
Network adapter B				
Vendor and model	N/A	N/A	1x Intel® Ethernet 10G 4P X710-T4L-t OCP	Broadcom Adv. Dual 25Gb Ethernet
Number and type of ports	N/A	N/A	4 x 10GbE	2 x 25GbE
Firmware version	N/A	N/A	20.5.13	20.5.13
Cooling fans				
Vendor and model	HPE	HPE	Dell Gold	Dell Gold
Number of cooling fans	4	6	4	4
Power supplies				
Vendor and model	HPE P38995-B21	HPE P38995-B21	Dell 0CYHHJA02	Dell
Number of power supplies	1	1	2	2
Wattage of each (W)	800	800	1400	800

How we tested

Comparing Dell iDRAC vs HPE iLO

System lockdown (iDRAC)

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

System lockdown (iLO)

1. Open a web browser, and connect to the iLO login page. Enter username and password, and click Login.
2. In the lower left corner, click the Screen to launch the remote console.
3. At the far left of the screen, click the top-down menu→Power→Reset.
4. Wait for system to enter pre-boot. To enter System Utilities, press F9.
5. From the System Utilities screen, select System Configuration.
6. Select BIOS/Platform Configuration (RBSU).
7. Select Server Security.
8. Select Server Configuration Lock Options.
9. Click Setup Server Configuration Lock.
10. Click Generate Server Configuration Lock Digital Fingerprint.
11. Enter and confirm the passphrase used to enable the server configuration lock.
12. Click OK.
13. Press F12, or click Save and Exit.
14. Click OK.
15. Click Reboot.

Disabling USB Ports (iDRAC)

Initial configuration

1. Open a web browser, and connect to the iDRAC login page. Enter 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.

Enable or disable dynamically

1. Open a web browser, and connect to the iDRAC login page. Enter 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 (iLO)

1. Open a web browser and connect to the iLO login page. Enter username and password, and click Login.
2. In the lower left corner, click the screen to launch the remote console.
3. At the far left of the screen, click the top-down menu→Power→Reset.
4. Wait for the system to enter pre-boot. To enter System Utilities, press F9.
5. From the System Utilities screen, select System Configuration.
6. Select BIOS/Platform Configuration (RBSU).
7. Select System Options.
8. Select USB Options.
9. Beside USB Control, use the drop-down menu, and select one of the following settings:
10. All USB Ports Enabled—Enables all USB ports and embedded devices.
11. All USB Ports Disabled—Disables all USB ports and embedded devices.
12. External USB Ports Disabled—Disables external USB ports.
13. Internal USB Ports Disabled—Disables internal USB ports.
14. Press F12, or click Save and Exit.
15. Click Yes - Save Changes.
16. Click Reboot, or press Enter to reboot the system.

Comparing Dell OME vs HPE OneView

Creating an alert policy for 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 box beside Enable. 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(s) to which you want to apply the policy, 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.

Creating an alert (per alert) (OneView)

1. Log into OneView
2. On the dashboard, click Active Alerts.
3. Select a specific alert based on severity, and review the alert.
4. Click the resource with the problem.
5. On the Server Hardware screen, click Actions, and select the action to be performed.

Deploying a device template (OME)

1. Log into OME
2. Click Configuration→Templates.
3. Select the check box corresponding to the template you want to deploy, and click Deploy Template.
4. In the Job Target dialog box, select the device(s). Unselect Do not forcefully reboot the host OS option, and click Next.
5. Leave the Boot to Network ISO option unchecked, and click Next.
6. In the iDRAC Management IP screen, select Don't change IP settings to keep the iDRAC IP intact, and click Next.
7. Select all attributes to include in the template, unselect to exclude them, and click Next.
8. In the Schedule section, run the job immediately or schedule for a later time, and click Finish.
9. To deploy the template, click Yes.
10. Click OK.

Deploying a device template (OneView)

1. Log into OneView.
2. From the main menu, select Servers menu.
3. Select Server Profile Templates.
4. Select the template from existing templates.
5. Click Actions.
6. Click Create server profile.
7. Provide all required details.
8. Provide a Name for the profile to associate with a server.
9. Provide a description.
10. Select the server hardware to associate the profile.
11. For firmware baseline, select Managed manually.
12. Click Create.

Comparing Dell CloudIQ for PowerEdge vs HPE Infosight

Policy-based security view (CloudIQ)

1. Log into the CloudIQ console.
2. From the Cybersecurity menu, click Cybersecurity Issues.
3. Review the Active Cybersecurity issues that have been identified based on the template assigned to the system.

iLO-based security view (InfoSight)

InfoSight doesn't appear to have an option that uses policies to view all security issues. Instead, an administrator logs in to each iLO, and manually verifies each configuration setting:

1. Log into iLO.
2. Click Security.
3. Click through the different tabs to verify configuration settings.

Read the report at https://facts.pt/Lt5Q31q

This project was commissioned by Dell Technologies.

Principled Technologies®

Facts matter.®