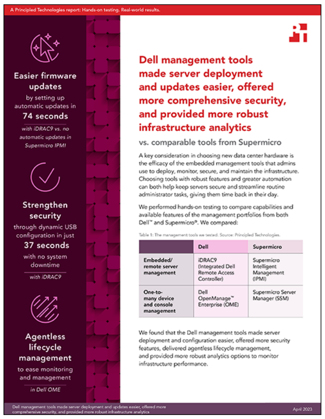
A Principled Technologies report: Hands-on testing. Real-world results.



A Principled Technologies report: Hands-on testing. Real-world results.

Easier firmware updates

by setting up automatic updates in

74 seconds

with iDRAC9 vs. no automatic updates in Supermicro IPMI

Strengthen security

through dynamic USB configuration in just

37 seconds

with no system downtime

with iDRAC9

Agentless lifecycle management

to ease monitoring and management

in Dell OME

Dell management tools made server deployment and updates easier, offered more comprehensive security, and provided more robust infrastructure analytics

vs. comparable tools from Supermicro

A key consideration in choosing new data center hardware is the efficacy of the embedded management tools that admins use to deploy, monitor, secure, and maintain the infrastructure. Choosing tools with robust features and greater automation can both help keep servers secure and streamline routine administrator tasks, giving them time back in their day.

We performed hands-on testing to compare capabilities and available features of the management portfolios from both Dell™ and Supermicro®. We compared:

Table 1: The management tools we tested. Source: Principled Technologies.

	Dell	Supermicro
Embedded/ remote server management	iDRAC9 (Integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
One-to-many device and console management	Dell OpenManage™ Enterprise (OME)	Supermicro Server Manager (SSM)

We found that the Dell management tools made server deployment and configuration easier, offered more security features, delivered agentless lifecycle management, and provided more robust analytics options to monitor infrastructure performance.

Dell management tools made server deployment and updates easier, offered more comprehensive security, and provided more robust infrastructure analytics

April 2023

The science behind the report:

Dell management tools made server deployment and updates easier, offered more comprehensive security, and provided more robust infrastructure analytics

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 management tools made server deployment and updates easier, offered more comprehensive security, and provided more robust infrastructure analytics.

We concluded our hands-on testing on March 10, 2023. 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 January 17, 2023 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 testing with Integrated Dell™ Remote Access Controller (iDRAC9), Dell OpenManage™ Enterprise (OME), Supermicro® Intelligent Management (IPMI), and Supermicro Server Manager (SSM).

Use case	Dell iDRAC9 and OME		Supermicro IPMI and SSM		
	Time (s)	Steps	Available?	Time (s)	Steps
Security					
Multi-factor authentication (MFA)	62	7 or 12	No	N/A	N/A
Dynamic USB	37	4	Manual	170	6
Ease of use					
Automatic updates	74	7	No	N/A	N/A
Server profile configuration	91 + 51	12	Mixed	N/A	N/A
BIOS configuration	N/A	N/A	No	N/A	N/A
Telemetry streaming	N/A	N/A	No	N/A	N/A

Table 2: Continued results of our testing with iDRAC9, Dell OME, Supermicro IPMI, and SSM.

Use case	**Dell OpenManage Enterprise**		**Supermicro Intelligent Management**		
	Time (s)	**Steps**	**Available?**	**Time (s)**	**Steps**
Analytics					
Sending telemetry data	N/A	N/A	No	N/A	N/A
Reporting	N/A	N/A	Yes	N/A	N/A
Ease of use					
HTML 5 based console	N/A	N/A	No	N/A	N/A
Third-party device monitoring	N/A	N/A	No	N/A	N/A
Deployment	32	10	Yes	26	6
View power utilization/carbon emission data	N/A	N/A	Mixed	N/A	N/A
Agent-free lifecycle management	N/A	N/A	No	N/A	N/A
Automatic component firmware updates	N/A	N/A	Mixed	N/A	N/A
Mobile monitoring/management	N/A	N/A	No	N/A	N/A

System configuration information

Table 3: Detailed information on the systems we tested.

System configuration information	Dell PowerEdge™ R750	Supermicro SYS-220U-TNR
BIOS name and version	Dell 1.8.2	Supermicro 1.4
Operating system name and version/ build number	Intel® Turbo Boost enabled, Virtualization enabled	Intel Turbo Boost enabled, Virtualization enabled
Date of last OS updates/patches applied	02/17/2023	02/17/2023
Power management policy	Balanced	Balanced
Processor		
Number of processors	2	2
Vendor and model	Intel Xeon® Silver 4314 CPU @2.40GHz	Intel Xeon Silver 4314 CPU @2.40GHz
Core count (per processor)	16	16
Core frequency (GHz)	2.40	2.4
Stepping	6	6
Memory module(s)		
Total memory in system (GB)	128	128
Number of memory modules	4	4
Vendor and model	Hynix HMAA4GR7CJR8N-XN	Samsung® M393A4K40DB3-CWE
Size (GB)	32	32
Type	PC4-25600R	PC4-25600
Speed (MHz)	3,200	3,200
Speed running in the server (MHz)	2,666	2,666
Storage controller		
Vendor and model	Dell HBA355i Fnt (Embedded)	Supermicro SAS 3408
Cache size	N/A	2 GB
Firmware version	17.15.08.00	5.130.01-3211
BIOS version	N/A	7.13.00.0
Local storage		
Number of drives	2	2
Drive vendor and model	SK hynix HFS480G3H2X069N	INTEL SSDPEL1K20
Drive size (GB)	480	185
Drive information (speed, interface, type)	6 Gbps, SATA, SSD	8Gb SAS, NVMe SSD
Network adapter		
Vendor and model	Broadcom® BCM5720, Intel Ethernet10G 4P X710-T4L-tOCP	Supermicro AOC-2UR68GF-i2XT
Number and type of ports	2 x 1GbE, 4 x 10GbE	2 x 10GbE
Firmware version	22.00.6, 20.5.13	8.50

System configuration information	Dell PowerEdge™ R750	Supermicro SYS-220U-TNR
Cooling fans		
Vendor and model	Dell Gold	Supermicro FAN-0209L4
Number of cooling fans	12	4
Power supplies		
Vendor and model	Dell 0CYHHJA02	Supermicro PWS-1K62A-1R
Number of power supplies	2	1
Wattage of each (W)	1,400	1,600

How we tested

Disabling USB ports (iDRAC)

Initial configuration

1. Open a web browser, 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. To enable or disable the ports, use the drop-down menu. Click Apply.

Disabling USB ports (Supermicro IPMI)

1. Open a web browser, and connect to the Supermicro IPMI management page. Enter a username and password, and click Login.
2. Click the remote console preview to launch the remote console.
3. On the right-hand sidebar menu, click the Power button, select Power Reset, and click Apply.
4. To enter Setup, press Del.
5. Navigate to Advanced→Chipset Configuration→South Bridge→Legacy USB Support (Enabled/Disabled/Auto).
6. Select a setting, and press F4 to Save & Exit. Te reboot, click Yes.

Enabling multi-factor authentication (iDRAC)

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 to the bottom of the page. If SecurID is not already configured, perform the following:
    a. Click the link for the SecurID configuration.
    b. If it has not already been installed, upload the RSA Server Certificate.
5. Enter the RSA SecurID Authentication Server URL, the Client ID, and the Access Key, and click Test Network Connection.
6. Click Configure.
7. Click OK.
8. Beside RSA SecurID State, use the drop-down menu to select Enabled. Click Save.
9. 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 to the bottom of the page. If an SMTP server is not already configured, perform the following:
    a. Click the link for Configure SMTP.
    b. Enter the IP address or FQDN of the SMPT server, and click Configure.
    c. Click OK.
5. Beside the Easy 2FA State, use the drop-down menu to select Enabled. Enter the IP address for the user, and click Test Connection.
6. Click OK.
7. Click Save.
8. 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`.
7. From the Location Type drop-down menu, select HTTPS.
8. Under HTTPS Server settings, enter `downloads.dell.com`.
9. 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).
10. 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.

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 at https://facts.pt/V5fDf06 ▶

This project was commissioned by Dell Technologies.

Principled Technologies®

Facts matter.®

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.