



The science behind the report:

Streamline operations with new and updated VMware vSphere 8.0 features on 16th Generation Dell PowerEdge servers

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 operations with new and updated VMware vSphere 8.0 features on 16th Generation Dell PowerEdge servers](#).

We concluded our hands-on testing on March 1, 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 February 28, 2023 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	2x Dell PowerEdge R6625
BIOS name and version	Dell 1.1.3
Non-default BIOS settings	N/A
Operating system name and version/build number	VMware ESXi, 8.0.0, 21203435
Date of last OS updates/patches applied	02/28/2023
Power management policy	Performance
Processor	
Number of processors	2
Vendor and model	AMD EPYC 9554 64-Core Processor
Core count (per processor)	64
Core frequency (GHz)	3.1
Stepping	Model 17 Stepping 1

System configuration information		2x Dell PowerEdge R6625
Memory module(s)		
Total memory in system (GB)	128	
Number of memory modules	8	
Vendor and model	Hynix HMCG78MEBRA107N	
Size (GB)	16	
Type	PC5-38400	
Speed (MHz)	4,800	
Speed running in the server (MHz)	4,800	
Storage controller		
Vendor and model	PERC H755 Front	
Cache size (GB)	8	
Firmware version	52.14.0-3901	
Driver version	7.722.02.00	
Local storage (vSAN)		
Number of drives	4	
Drive vendor and model	Dell Ent NVMe v2 AGN MU U.2	
Drive size (GB)	6,400	
Drive information (speed, interface, type)	NVMe Gen4, SSD, 2.5	
Local storage (OS)		
Number of drives	2	
Drive vendor and model	Toshiba AL15SEB060NY	
Drive size (GB)	600	
Drive information (speed, interface, type)	12Gbps, SAS, HDD, 2.5	
Network adapter		
Vendor and model	2x Intel Ethernet 25G 2P E810-XXV	
Number and type of ports	4x 25Gb	
Driver version	21.5.9	
Cooling fans		
Vendor and model	Dell Gold	
Number of cooling fans	16	
Power supplies		
Vendor and model	Dell, 1400W, RDNT, ARTESYN	
Number of power supplies	2	
Wattage of each (W)	1,400	

How we tested

Setting up the VMware vCenter environment

We started with two Dell PowerEdge R6625 servers and enabled the TPM 2.0 modules in each. We installed the initial VMware vSphere 8.0 release of the Dell-customized VMware ESXi image on each server. We deployed the latest version of VMware vCenter and an Active Directory VM on a separate infrastructure server. We added all the servers to the vCenter and added the vCenter FQDN to the domain with a DNS record. We created a cluster of the two Dell PowerEdge R6625 servers.

In vCenter, we created a host image of the first host and applied the image to both servers in the cluster, and we then added a native key provider. We updated the host images to the latest release as well as the Dell vendor add-on via vCenter. On the first host in the cluster, we created a Microsoft Windows 11 VM and enabled virtual TPM (vTPM) for it, updated the OS, and created a template of the finished VM. Finally, we cloned the template and deployed the cloned VM to the second host in the cluster.

Performing the use cases

Detecting issues

1. In the vCenter vSphere client, select the target cluster.
2. Select Updates.
3. On the Image screen, select Run Pre-Check.
4. Select the target server, and review the details for Pre-check.

Staging cluster image updates in advance of remediation

1. In the vCenter vSphere client, select the target cluster.
2. Select Updates.
3. On the Image screen, select Stage All.

Remediating the cluster

1. In the vCenter vSphere client, select the target cluster.
2. Select Updates.
3. On the Image screen, select Stage All.
4. Click Remediate All.
5. On the Review Remediation Impact, click Start Remediation.

Provisioning the vTPM

Adding a native key provider

1. In the vCenter vSphere client, select the vCenter.
2. Select Configure.
3. Under Security, click Key Providers.
4. Click Add, and click Add Native Key Provider.
5. Enter a name, and check the box next to Use key provider only with TPM protected ESXi hosts (Recommended).
6. Click Add Key Provider.
7. Select the Native Key Provider you created, and click Back-Up.
8. In the popup box, click Back Up Key Provider.
9. Save the native key file to a secure location.

Creating the Windows 11 VM

1. In the vCenter vSphere client, select the first host in the cluster.
2. Click Actions, and click New Virtual Machine....
3. At Select a creation type, click Next.
4. Enter a name for the VM, and click Next.
5. Select the first host of the cluster, and click Next.
6. Select a datastore, and click Next.
7. At the Select compatibility screen, click Next.
8. Select Microsoft Windows 11 (64-bit), check the box next to Enable Windows Virtualization Based Security, and click Next.
9. Click Add New Device, click Trusted Platform Module, and click Next.
10. At the Ready to complete screen, click Finish.

Installing Windows 11

1. In the vCenter vSphere client, select the Windows 11 VM.
2. Click Launch Remote Console.
3. Click the green play button to power on the VM.
4. Click VMRC, hover over Removable Devices, hover over CD/DVD drive 1, and click Connect to Disk Image File (iso)...
5. Select the Windows 11 ISO Image, and click Open.
6. In the VM console, select Boot Normally, and press any button when prompted.
7. At the Windows Setup screen, click Next.
8. Click Install now.
9. Select Windows 11 Pro, and click Next.
10. Accept the license agreement, and click Next.
11. Click Custom: Install Windows only (Advanced).
12. Click Next.
13. Select the country, and click Yes.
14. Select the keyboard layout, and click Yes.
15. Click Skip.
16. Enter a name for the VM, and click Next.
17. Click Set up for work or school, and click Next.
18. Click Sign-in options, and click Domain join instead.
19. Enter a username, and click Next.
20. Enter a password, and click Next.
21. Enter the password again, and click Next.
22. Answer the three security questions, and click next between each.
23. Click Next twice, and click Accept.
24. Once the desktop appears, click the power button, and click Shut down.
25. Close the remote console.

Cloning the Windows 11 VM to template

1. In the vCenter vSphere client, select the Windows 11 VM.
2. Click Actions, click Clone, and click Clone to Template....
3. Enter a name for the template, and click Next.
4. Select the first host, and click Next.
5. At the Select TPM provisioning policy, select Replace, and click Next.
6. Select a datastore, and click Next.
7. Click Finish.

Deploying the template

1. In the vCenter vSphere client, select the second host in the cluster.
2. Click Actions, and click New Virtual Machine....
3. At Select a creation type, select Deploy from template, and click Next.
4. Select Data Center, select the template that you previously created, and click Next.
5. Enter a name for the VM, and click Next.
6. Select the second host, and click Next.
7. At the Select TPM provisioning policy, select Replace, and click Next.
8. Select a datastore, and click Next.
9. Click Next.
10. Click Finish.

Read the report at <https://facts.pt/jrP8jaA>



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.