The science behind the report:

Protect data at rest with negligible impact on NVMe disk performance metrics

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 Protect data at rest with negligible impact on NVMe disk performance metrics.

We concluded our hands-on testing on June 23, 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 May, 25, 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: HCIBench performance metrics on an HCI cluster consisting of three Dell™ PowerEdge™ R7525 servers.

	Dell PowerEdge server-based HCI cluster with OpenManage™ SEKM enabled	Dell PowerEdge server-based HCI cluster without OpenManage SEKM enabled
Random read test		
IOPS		
Two-NVMe® disk group	656,939	660,638
Three-NVMe disk group	913,346	916,451
Latency (milliseconds)		
Two-NVMe disk group	0.59	0.58
Three-NVMe disk group	0.42	0.42
Throughput (MB/s)		
Two-NVMe disk group	2,566.17	2,580.61
Three-NVMe disk group	3,567.80	3,579.89

	Dell PowerEdge server-based HCI cluster with OpenManage™ SEKM enabled	Dell PowerEdge server-based HCI cluster without OpenManage SEKM enabled
Random read/write test		
IOPS		
Two-NVMe disk group	218,156	223,558
Three-NVMe disk group	297,198	305,016
Latency (Milliseconds)		
Two-NVMe disk group	1.76	1.72
Three-NVMe disk group	1.30	1.26
Throughput (MB/s)		
Two-NVMe disk group	852.17	873.29
Three-NVMe disk group	1,160.90	1,191.46

System configuration information

Table 2: Detailed information on the servers we used in testing the HCI cluster.

System configuration information	Dell PowerEdge R7525 x3
BIOS name and version	Dell 2.6.6
Non-default BIOS settings	VMware® ESXi™ 7.0.3 19482537 U3 P35
Operating system name and version/build number	05/25/22
Date of last OS updates/patches applied	5.10.10.00
Power management policy	Balanced
Processor	
Number of processors	2
Vendor and model	AMD™ EPYC™ 7763 64-Core processor
Core count (per processor)	64
Core frequency (GHz)	2.45
Memory module(s)	
Total memory in system (GB)	512
Number of memory modules	16
Vendor and model	Hynix Semiconductor HMA84GR7CJR4N-XN
Size (GB)	32
Type	PC4-25600
Speed (MHz)	3,200
Speed running in the server (MHz)	3,200
Storage controller	
Vendor and model	Dell PCIe SSD Backplane
Firmware version	3.56
Local storage	
Number of drives	Up to 6 tested per server
Drive vendor and model	Kioxia - Dell Ent NVMe FIPS CM6 MU 3.2TB
Drive size (TB)	3.2
Drive type	PCIe SSD (NVMe)
Network adapter	
Vendor and model	Broadcom Gigabit Ethernet BCM5720
Number and type of ports	2 x 1 GbE
Network adapter	
Vendor and model	Broadcom Adv Dual 25Gb Ethernet
Number and type of ports	2 x 25 GbE

System configuration information	Dell PowerEdge R7525 x3
Cooling fans	
Vendor and model	Dell High Performance (Gold Grade)
Number of cooling fans	12
Power supplies	
Vendor and model	Dell 0CYHHJA01
Number of power supplies	2
Wattage of each (W)	1,400

Table 3: Detailed information on the server we used in testing the IT benefits of the SEKM feature.

System configuration information	Dell PowerEdge R750xs
BIOS name and version	Dell 1.5.4
Non-default BIOS settings	Intel Turbo Boost enabled, Virtualization enabled
Operating system name and version/build number	Windows Server 2019
Date of last OS updates/patches applied	03/15/22
Power management policy	Balanced
Processor	
Number of processors	2
Vendor and model	Intel® Xeon® Gold 6330 CPU
Core count (per processor)	28
Core frequency (GHz)	2.00
Stepping	6
Memory module(s)	
Total memory in system (GB)	256
Number of memory modules	16
Vendor and model	Samsung® M393A2K43DB3-CWE
Size (GB)	16
Type	PC4-25600-R
Speed (MHz)	3,200
Speed running in the server (MHz)	2,933
Storage controller	
Vendor and model	Dell PERC H755
Cache size (GB)	8
Firmware version	52.16.1-4158
Driver version	7.716.03.00

System configuration information	Dell PowerEdge R750xs		
Local storage (type A)			
Number of drives	2	2	4
Drive vendor and model	Toshiba® THNSF8120CCSE	Toshiba PX05SVB096Y	Seagate® ST91000640NS
Drive size (GB)	111.25	893.75	931
Drive information (speed, interface, type)	SATA SSD 6 Gbps	SAS SSD 12Gbps	3 Gbps
Network adapter			
Vendor and model	Broadcom® Gigabit Ethernet BCM5720		
Number and type of ports	2 x 1 GbE		
Cooling fans			
Vendor and model	Dell HPR SLVR		
Number of cooling fans	5		
Power supplies			
Vendor and model	Dell 01CW9GA03		
Number of power supplies	2		
Wattage of each (W)	1,400		

How we tested

The procedures below assume you have a functional KMS with all profiles, certificates, users, and tokens correctly configured on the KMS for iDRAC registration. Instructions for how to complete these tasks appear on pages 32 to 51 of the Setup and Deployment Guide: https://www.delltechnologies.com/en-us/collaterals/unauth/white-papers/products/servers/sekm-setup-and-deployment-guide-white-paper.pdf.

Additionally, these procedures assume you have created a VMware vSphere cluster containing three Dell PowerEdge R7525 servers, and populated the cluster with six direct-attached NVMe drives. PERC-attached drives are necessary for the Securing PERC-attached drives and performing rebootless updates sections below. You must download files, such as the HCIBench OVA file, in advance.

Configuring vSAN disk groups

1. Open a browser page, and enter the IP address of FQDN of your vCenter server.
2. Log in with administrative credentials.
3. In the vSphere Client, select the vSAN cluster you want to configure.
4. At the top of the right panel, click the Configure menu item.
5. Using the scroll bar in the left of the vSAN cluster panel, scroll down to vSAN.
6. Click Disk Management.
7. Click Claim Unused Disks.
8. Expand the collapsed list for NVMe Dell ENT NVMe…
9. Select a disk on the first host.
10. To Claim For Cache Tier, use the pull-down menu.
11. Ensure at least one drive is left as Claim for Capacity Tier.
12. Repeat claiming procedures for each disk group. Each disk group must contain one cache and one capacity drive.
13. Repeat the claiming procedure for each host. Ensure that each host contains the same number of disk groups, and that each disk group contains only one cache and one capacity drive.
14. All unused drives must be claimed as Do not claim. Note: In our testing, we used two-disk groups or three-disk groups per host. In the two-disk group test, we marked two drives as Do not claim per host.
15. Click Create.
16. The vSAN build process begins.

Setting HCIBench test parameters and launching a test

1. Open a browser page, and enter https://[HCIBench_IP_Address]:8443
2. When prompted, provide the root credentials you entered at deployment, and press enter.
3. Under vSphere Environment Information, set the following parameters:
    a. vCenter Hostname/IP
    b. vCenter Datacenter name
    c. Datastore(s) Name - we used “vsanDatastore”
    d. vCenter Username
    e. Cluster Name – we used “vSAN”
    f. Network Name – we used “10G Data”
    g. vCenter Password
    h. Toggle the switch for Reuse VMs if Possible
4. Under Benchmarking Tool, select VDBENCH.
5. Under Guest VM Configuration, set the following parameters:
    a. VM Name Prefix – we used hci-vdb
    b. Number of VMs = 6
    c. Number of Data Disk = 8
    d. Number of CPU = 4
    e. Size of Data Disk in GiB = 25
    f. Size of RAM in GB = 8
6. Under Testing Configuration, set the following parameters:
    a. Test Name
    b. Prepare Virtual Disk Before Testing = None
    c. Testing Duration (Seconds) = 900

d. Click the Add button for Select a Workload Parameter File.

   i. For 70 percent read / 30 percent write testing, set the following parameters:

      1. Number of Disks to Test = 8
      2. Working-Set Percentage = 100
      3. Number of Threads Per Disk = 8
      4. Block Size = 4K
      5. Read Percentage = 70
      6. Random Percentage = 100
      7. Test Time = 900
      8. Click Submit.

   ii. For 100 percent read testing, set the following parameters:

      1. Number of Disks to Test = 8
      2. Working-Set Percentage = 100
      3. Number of Threads Per Disk = 8
      4. Block Size = 4K
      5. Read Percentage = 100
      6. Random Percentage = 100
      7. Test Time = 900
      8. Click Submit.

   iii. Click Close.

e. For Select a Workload Parameter File, click Refresh.
f. To select one of the tests you just created, use the pull-down menu.

7. Click Save Config.
8. Validate parameters, and click Validate Config. If you made edits, click Save Config before continuing.
9. Once a validation passes with no errors, click Start Test.

Resetting between HCIBench test runs

1. Open a browser page, and enter https://[HCIBench_IP_Address]:8443
2. When prompted, provide the root credentials, and press enter.
3. Scroll to the bottom of the page, and click Delete Guest VMS.
4. Upon completion, you'll receive a message indicating Unable to find guest VMs with prefix: 'hci-vdb'.
5. Click Close Window.
6. Close the browser page.
7. Open a browser, and enter the IP address of your vCenter.
8. Log in with administrative credentials.
9. In the vSphere client, locate the HCIBench_2.6.1 VM, and select it.
10. Right-click, and select Power→Shut Down Guest OS.
11. To confirm guest OS shutdown, click Yes.
12. In vCenter, select the vSAN cluster.
13. In the right panel, from the top-menu bar, select Configure.
14. Use the scroll bar in the left of the vSAN cluster panel, and scroll down to vSAN.
15. Select Disk Management.
16. Under Disk Management, click View Disks. The first cluster member is pre-selected.
17. To the left of the first disk group listed, click the three-dot ellipsis, and select Remove.
18. Use the pull-down menu for vSAN data migration, select No data migration, and click Remove.
19. Repeat the removal action for each disk group on your host.
20. To select the second host, use the pull-down menu near the top of the Disk Management panel.
21. Repeat the removal action for each disk group on your host.
22. To select the third host, use the pull-down menu near the top of the Disk Management panel.
23. Repeat the removal action for each disk group on your host.
24. In the vSphere client main menu tree on the left of the screen, select the first host.
25. Right-click the first host, and select Maintenance Mode→Enter Maintenance Mode.
26. Use the pull-down menu for vSAN migration, select No data migration, and click OK.

27. To confirm, click OK.
28. When the host is in Maintenance Mode, right-click the host, and select Power→Reboot.
29. Provide a reboot reason, and click OK. The server will reboot and in vCenter show as Not Responding.
30. Repeat the Maintenance Mode and reboot processes for each host in the cluster.
31. When all servers appear in vCenter as responding in Maintenance Mode, right-click each server and select Maintenance Mode→Exit Maintenance Mode.
32. Power on the HCIBench_2.6.6 VM.

Securing PERC-attached drives

1. Apply the SEKM configuration to the iDRAC.
2. To verify that SEKM is enabled for the controller, click Storage-SEKM.
3. Click Overview, and select Controllers.
4. Locate the PERC you want to configure.
5. Under Actions, use the pull-down menu, and select Edit.
6. Click Next.
7. Under Security, select Secure Enterprise Key Manager.
8. Click Add to Pending.
9. Click At Next Reboot
10. To view the status of the job, click Job Queue.
11. Verify the job is marked as scheduled.
12. Reboot the server.
13. View Job Queue to verify completion.
14. To verify the controller is secured with SEKM, expand the PERC details in Storage-Overview, and scroll down to Security Status and Encryption Mode.

Securing direct-attached drives

1. Open a web browser, enter the address for your target iDRAC, and log in with administrative credentials (we used root / calvin).
2. Click iDRAC Settings→Services
3. Expand iDRAC Key Management, and change the Key Management Service from iLKM to SEKM.
4. Check the box for Auto Secure Security Capable Drives.
5. Enter the KMS IP address.
6. Enter the designated KMS user ID and password used for managing this iDRAC.
7. Click Generate a CSR, open the file, and copy the contents to your clipboard.
8. On the Key Management System, sign the CSR by pasting the contents from the CSR file into the appropriate field on the KMS Certificate Authority.
9. Click Upload Signed CSR, browse to the location of the saved .PEM file you downloaded from the KSM Certificate Authority, and click Open.
10. Download the KMS CA Certificate.
11. Click Upload the KMS CA Certificate, browse to the location of the saved CA Certificate .PEM file you downloaded from the KSM Certificate Authority, and click Open.
12. Click Test Network Connection to verify connectivity, and click OK to confirm or re-enter KMS iDRAC account password.
13. Click Apply.

Converting from iDRAC LKM to OpenManage SEKM

This procedure assumes you have configured LKM within the iDRAC and are using iDRAC LKM encryption.

1. Open a web browser, enter the address for your target iDRAC, and log in with administrative credentials (we used root / calvin).
2. Click iDRAC Settings→Services.
3. Expand iDRAC Key Management, and change the Key Management Service from iLKM to SEKM.
4. Check the box for Auto Secure Security Capable Drives.
5. Enter the iLKM key security key passphrase.
6. Enter the KMS IP address.
7. Enter the designated KMS user ID and password for managing this iDRAC.
8. Click Generate a CSR, open the file, and copy the contents to your clipboard.
9. On the key management system, sign the CSR by pasting the contents from the CSR file into the appropriate field on the KMS Certificate Authority.

10. Click Upload Signed CSR, browse to the location .of the saved .PEM file you downloaded from the KSM Certificate Authority, and click Open.
11. Download the KMS CA Certificate.
12. Click Upload the KMS CA Certificate, browse to the location of the saved CA Certificate .PEM file you downloaded from the KSM Certificate Authority, and click Open.
13. Click Test Network Connection to verify connectivity, and click OK to confirm or re-enter KMS iDRAC account password.
14. Click Apply.

Performing rebootless updates

This procedure assumes you have already downloaded the firmware appropriate for your target disks. We downloaded Express-Flash-PCIe-SSD_Firmware_6N6C0_WN64_1.1.0_A01.EXE from support.dell.com.

1. Open a web browser, enter the address for the target iDRAC, and log in with administrative credentials (we used root / calvin).
2. From the top menu bar, select Maintenance→System Update.
3. In the Manual update section, click Browse, locate the firmware you just downloaded, and click OK.
4. Click Upload.
5. Make sure the update is complete.
6. Under update details, check the box next to the firmware item, and click Install.

This project was commissioned by Dell Technologies.