Technical Research Report

PROWESS

Reimagine the Employee Experience in Hybrid Work Environments

Prowess Consulting identified how an integrated workforce solution like VMware® Anywhere Workspace with Dell™ PowerEdge™ servers can help organizations succeed with hybrid work environments.

Executive Summary

Hybrid work is here to stay. 64% of executives are convinced that flexible work options motivate employees, and more than 70% of employees are working from home at least 2–3 days per week.[1] But hybrid work environments create a unique set of challenges for organizations. As employees use more devices, access more applications, and work from more locations, IT teams are scrambling to support them. Some organizations try to get by on legacy technologies and point solutions. However, traditional IT environments and management solutions are not designed to support a distributed workforce. Using traditional tools can lead to operational complexity, fragmented security, and poor user experiences.

Prowess Consulting evaluated VMware® Anywhere Workspace running on Dell™ PowerEdge™ servers as a potential solution for managing hybrid work environments. Anywhere Workspace integrates modern tools into a single platform to deliver IT services like onboarding employees, managing remote devices and virtual desktops, and monitoring for security threats. After reviewing components including VMware Workspace ONE®, VMware® Secure Access Server Edge (SASE), and VMware® Carbon Black, we determined that organizations that deploy the Anywhere Workspace platform can enhance user experiences and achieve consistent, secure performance across locations and devices for hybrid workers. For employers embracing hybrid work environments for their employees, this solution could be a significant win.

Hybrid Work Environments

Organizations are supporting hybrid work environments as executives conclude that flexible work options keep employees motivated.[1] In a hybrid work environment, some employees might work remotely, others might work on-premises, and others might split their time between the office and other locations, such as home or coffee shops. But designing and managing hybrid work environments is not easy.

Challenges of Hybrid Work Environments

Today's executives face a wide variety of challenges as the concept of the workplace evolves from being a physical space to a digital space. Organizations must maximize employee engagement and productivity when employees work from almost anywhere. To support digital workspaces, IT teams must support an increasing number of device types, applications across multiple clouds, and different networks. Processes are often manual, and organizations might be constrained by legacy on-premises computing systems. Multiple IT management tools are often needed to run different platforms and operating systems, and each needs specific skillsets and resources. Additionally, an increased number of endpoints expands the attack surface and increases security risks. To address these challenges, organizations need an integrated workforce solution that unifies IT management into a single platform.

The Platform Advantage

Prowess Consulting observed that Anywhere Workspace can be used to replace multiple IT tools, reducing the number of IT skillsets and resources needed. In our analysis, we noted that Anywhere Workspace consists of three components, as shown in Figure 1: VMware Workspace ONE, VMware SASE, and VMware Carbon Black.

Figure 1 | The VMware® Anywhere Workspace platform provides integrated tools to streamline IT

VMware Workspace ONE®

We started our evaluation by reviewing VMware Workspace ONE. Gartner has cited Workspace ONE as a leader in the unified endpoint management (UEM) category for the last five years.[2] In our analysis, we identified three key benefits of Workspace ONE UEM:

1. **Automated onboarding.** New employee devices can register over the air during the initial power-up. Admins can easily set up and customize an imageless configuration of work profiles such as emails, VPNs, and Wi-Fi.

Employees are
2.6x
as likely to be satisfied with their employer if onboarding is exceptional.[3]

61%
of organizations report that they wrestle with onboarding.[4]

2. **Management across endpoints.** Workspace ONE UEM manages and secures devices and apps by taking advantage of the native mobile device management (MDM) capabilities of iOS® and Android™ devices and mobile-cloud management efficiencies of Windows®, Apple® macOS®, and Google Chrome™ devices.
3. **Integrated single-sign-on (SSO).** Integrated SSO eliminates multiple logins for better security, speed, and ease of use.

Virtual Apps and Desktops

VMware Workspace ONE integrates UEM technology with virtual application delivery through VMware Horizon®. We identified the following key benefits:

- **Automatic software installation.** IT teams can create an automated workflow for installing software, applications, files, scripts, and commands, which can save time and reduce expenses.
- **Broad support.** Workspace ONE makes use of VMware Horizon, a virtualization software product, to deliver desktops and apps on Windows, macOS, Linux®, iOS, Chrome, and Android endpoints.
- **Secure virtual apps.** IT teams can secure sensitive and confidential information.

Measuring VM Density with VMware Horizon®

To better evaluate Workspace ONE, we measured the virtual desktop infrastructure (VDI) density created using Workspace ONE with VMware Horizon. VMware Horizon enables IT departments to run remote desktops and applications in the data center and deliver these desktops and applications to employees. VDI density refers to the number of virtual desktops that can be efficiently and effectively hosted on a single cluster of servers in a VDI environment. The concept of VDI density is important for several reasons:

- **Resource utilization:** Efficient VDI density maximizes the use of hardware resources and can lead to improved performance.
- **Cost efficiency:** Increased VDI density reduces the number of physical servers required, which can lead to cost savings.
- **Simplified management:** With higher VDI density, the administrative overhead associated with server management, updates, and maintenance can be reduced.

Test Setup

We measured density for the following two persona types:

- **Knowledge workers:** These workers use the full Microsoft® Office suite and videoconferencing software, and they often have multiple applications and web tabs open simultaneously. A knowledge worker is allocated two vCPUs, 4 GB of memory, and an 80 GB disk.
- **Power workers:** These users have the same requirements as knowledge workers, but they also use high-resolution graphics and video editing software. A power worker is allocated four vCPUs, 8 GB of memory, and an 80 GB disk.

For our testing, we examined three configurations on a server cluster consisting of three PowerEdge R7625 servers (see Table A1 in the Appendix for configuration details):

- VMware Horizon 7 with VMware vSAN™ 7
- VMware Horizon 8 with vSAN 8
- VMware Horizon 8 with vSAN 8 and NVIDIA® A16 graphics processing units (GPUs)

One NVIDIA A16 GPU was included in each server in our third configuration to provide higher performance. This simulated the type of platform required by a power worker who needs to perform graphic-intensive tasks.

Testing Methodology

See the Test Methodology section in the Appendix for details on how to recreate our tests. Each server cluster consisted of three PowerEdge R7625 servers. For our third test scenario, we included one NVIDIA A16 GPU in each server, for a total of three GPUs in the server cluster.

VDI Density Testing Results

The VDI density results are shown in Table 1. Each number represents user density per cluster.

Table 1 | VDI virtual machine (VM) instances created

Persona	VMware vSAN™ 7 and VMware Horizon® 7 VDI	VMware vSAN™ 8 and VMware Horizon® 8 VDI	VMware vSAN™ 8 and VMware Horizon® 8 VDI with NVIDIA® A16 GPUs
Knowledge worker instances	211	307	330
Power worker instances	141	156	153

Dell Technologies recommends a user density of 160 VDI instances per server cluster for knowledge workers and 120 VDI instances per server cluster for power workers.[5] VMware Horizon surpassed these recommendations. We also found that Workspace ONE with VMware Horizon offered a streamlined process for creating these VMs.

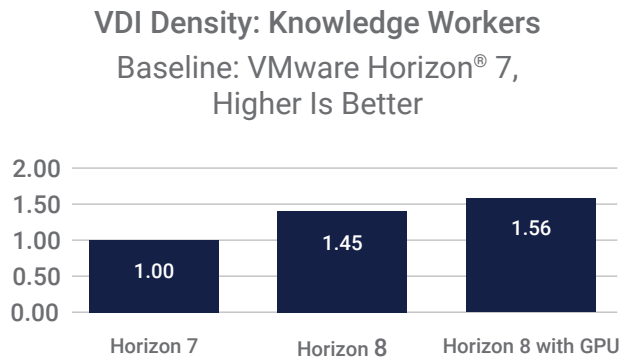

Figure 2 | Comparison of the VDI density of VMware Horizon® 8 to Horizon 7 for knowledge workers

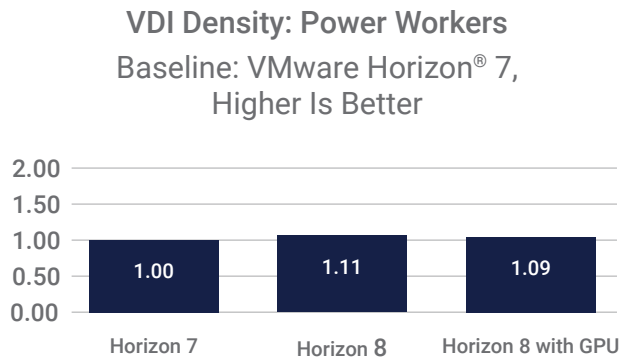

Figure 3 | Comparison of the VDI density of VMware Horizon® 8 to Horizon 7 for power workers

For knowledge workers, we found that Horizon 8 can create up to 45% more VDI instances/cluster, as compared to Horizon 7, while Horizon 8 with NVIDIA GPUs can create up to 56% more VDI instances/cluster, as compared to Horizon 7 (see Figure 2). For power workers, we found that Horizon 8 can create up to 11% more VDI instances/cluster, as compared to Horizon 7. Horizon 8 with NVIDIA GPUs can create up to 9% more VDI instances/cluster, as compared to Horizon 7 (see Figure 3).

We concluded that an upgrade to Horizon 8 from Horizon 7 can help improve VDI density. However, we noted a slight drop in density for the power worker when testing Horizon 8 without and with a GPU (see Figure 3). This decrease occurs because GPU memory cannot be overcommitted and is allocated in quantized chunks.

Digital Employee Experience

Workspace ONE has a digital employee experience (DEX) solution that can provide insights and automation to remediate issues before those issues reach the end-user experience. Proactive detection and remediation become the first line of defense, helping avoid unnecessary help-desk tickets and offering a revolutionary way to manage end-user experiences.

80%

of surveyed executives want to improve employee productivity regardless of location.[6]

62%

of surveyed executives want to improve the IT support resolution time of digital experience issues.[6]

VMware® SASE

VMware SASE converges cloud networking with security. Regardless of the location of users and applications, SASE allows IT teams to provide employees secure access from a single management platform. We learned that VMware SASE customers experience a 50% reduction in time to manage IT network and security operations.[7] In addition, the solution provides several benefits for organizations with remote and hybrid workforces:

- **Zero trust network access:** VMware SASE uses Zero Trust Network Access (ZTNA), an identity-, location-, and context-based approach that "trusts no one," granting authorized resources on demand.
- **Cloud web security:** We discovered that components such as remote browser isolation (RBI) move web browsing to a remote location, not the user's device, so malware and viruses can't enter the device or network.
- **Network performance management:** We learned components such as VMware® SD-WAN Client provide IT teams with a secure remote access solution that can help optimize hybrid workers' connections for speed and reliability.

VMware® Carbon Black

VMware Carbon Black is a software-as-a-service (SaaS) solution that combines the intelligent system hardening and behavioral prevention needed to keep emerging threats at bay. It provides next-generation antivirus, endpoint detection and response, managed detection, and audit and remediation capabilities using one agent integrated into Workspace ONE.

Carbon Black can help organizations successfully manage hybrid environments in multiple ways:

- **Support for a multimodal employee experience:** No matter where an employee is working, with what devices, or on which networks, their user experience remains the same.
- **Automation:** Through integration with Workspace ONE, IT teams can set up automatic actions to mitigate threats to managed devices.
- **Edge security:** Protect apps and data from wherever they are accessed, including at the distributed edge, through intrinsic security that delivers secure digital workspaces.

Innovate Business Processes with Anywhere Workspace

As employees use more devices, access more applications, and work from more locations, organizations must scramble to scale remote services while maintaining tight security and delivering great customer service. Business leaders can take this opportunity to implement new, innovative ways of doing work by adopting an integrated workforce solution. Prowess Consulting explored how this can be accomplished by researching the features of VMware Anywhere Workspace.

We found that Anywhere Workspace promotes business agility with over-the-air onboarding, and it helps remove the friction between technology and employees with integrated SSO and automatic software installation. Anywhere Workspace with VMware Horizon offers a streamlined process for delivering virtual desktops and applications. VMware SASE customers experience a 50% reduction in time to manage IT network and security operations.[7]

Our conclusion is that VMware Anywhere Workspace running on Dell PowerEdge servers is a potential solution for managing hybrid work environments. Anywhere Workspace integrates modern tools into a single platform to deliver IT services that can help organizations deliver well-orchestrated and seamless employee experiences.

Appendix

Prowess Consulting used the configurations shown in Table A1 to evaluate VDI density.

Table A1 | Three-node Dell™ PowerEdge™ server cluster VDI density testing configurations

	VMware Horizon® 7 with VMware vSAN™ 7 and VMware® Anywhere Workspace Configuration	VMware Horizon® 8 with VMware vSAN™ 8 with VMware® Anywhere Workspace Configuration	VMware Horizon® 8 with VMware vSAN™ 8 with VMware® Anywhere Workspace Configuration and NVIDIA® A16 GPUs
Server	3 x Dell™ PowerEdge™ R7625 or similar servers		
Configuration	VMware® Original Storage Architecture (OSA) AF-6 configuration		
Processor	AMD EPYC™ 9334 processor		
Core threads/CPU	32 cores/64 threads		
Frequency (Base/SCT/MCT)	2.7 GHz (max 4.4 GHz)		
Memory	512 GB RAM		
Memory DIMM	16 x Micron® MTC20F2085S1RC48BA1		
Memory speed	4,800 megatransfers per second (MT/s)		
Storage controller 01	AMD FCH Serial ATA (SATA) controller (Advanced Host Controller Interface [AHCI] mode)		
Storage controller 02	8-slot backplane 1		
Disk	6.4 TB Samsung® Dell™ NVM Express® (NVMe®) v2 aGN MU U.2		
Number of disks	8		
Network	2 x 1 Gb Broadcom® NetXtreme® BCM5720 2 x 100 Gb Broadcom® NetXtreme® E-Series P2100D BCM57508 QSFP		
Operating system (OS)	VMware ESXi™		
BIOS version	1.3.11		
iDRAC version	7.00.30.00		
VMware vSphere® version	88.0.1.00000		
VMware ESXi™ version	8.0.1 build 21495797		
VMware Horizon® 8 version	8.8 build 21073894		
GPU, host grid driver	Not applicable (N/A)	N/A	NVIDIA GRID® VMware vSphere® 8.0-535.54.06-535.54.03-536.25
GPU, make and model	N/A	N/A	NVIDIA® A16/NVIDIA® A2
GPU, VMware vCenter® version	N/A	N/A	8.0.1 build 21860503

We used the configurations shown in Table A2 for knowledge workers and power workers.

Table A2 | VDI VM configuration

Host	Knowledge Worker	Power Worker
Number of vCPUs	2	4
Memory	4 GB	8 GB
Disk	80 GB	80 GB

Test Methodology

Our engineers tested PowerEdge servers with vSAN 8 running with VMware Anywhere Workspace to demonstrate how the solution can help lower IT organizations' burdens, improve their employees' experiences, and improve security. This testing examined VDI density on three configurations:

- VMware vSAN 7 running Anywhere Workspace on a three-node cluster
- VMware vSAN 8 running Anywhere Workspace on a three-node cluster
- VMware vSAN 8 running Anywhere Workspace on a three-node cluster with one NVIDIA A16 GPU per server

The hypothesis behind our testing was that vSAN 8 with Anywhere Workspace features can improve the scalability of a VDI environment when compared to vSAN 7 with Anywhere Workspace. We also added NVIDIA GPUs to the VMware vSAN 8 with Anywhere Workspace VDI instances to offload graphic needs from the VMware vSphere® host CPUs and see how they improve the experience for users with the most intense graphics computing needs.

Test Procedure

An infrastructure host running VMware ESXi™ 7 was provided to Prowess Consulting by the test lab to host services outside of the scope of the vSAN cluster. This server hosted an Active Directory® Domain Services controller dedicated to the test environment (for details, see the installation and configuration documentation), in addition to VMware vCenter Server® for the three-node test vSAN cluster and the VMware Horizon virtualization manager.

VMware vSAN™ Cluster Installation and Configuration

The following instructions outline the steps we took to configure the VMware vSAN cluster.

Installing VMware ESXi™ and VMware vCenter Server®

1. Install ESXi on all three hosts following the VMware documentation.
    a. After installing ESXi, log in to the ESXi host user interface (UI).
    b. In the left-hand pane, navigate to the **Storage** page.
        i. Delete the default **datastore1**.
    c. Click the **New Datastore** button.
        i. In the **Select Creation Type** window, click **Next**.
        ii. In the **Select Device** window, in the **Name** field, enter **store1**.
        iii. In the **Select Device** window, select the first available NVM Express® (NVMe®) disk, and then click **Next**.
        iv. In the **Select Partitioning Options** window, select **Use Full Disk** and **VMFS 6** from the two drop-down menus, and then click **Next**.
        v. In the **Ready to Complete** window, review the details, and then click **Finish**.
    d. Repeat steps 1a–1c for all three ESXi hosts.
2. Download the VMware vCenter Server installer from the VMware website.
3. On your local client, run the installer.
4. At the **Welcome** screen, click **Next**.
    a. On the **End User License Agreement** page, accept the agreement, and then click **Next**.
    b. On the **vCenter Server Deployment Target** page, provide the IP of the infrastructure ESXi host, along with a username and password, and then click **Next**.
    c. On the **SSL Certificate Warning** page, click **Yes**.
    d. On the **Set Up vCenter Server VM** page, provide a name and password for vCenter Server, and then click **Next**.
    e. From the **Select Deployment Size** page, set **Deployment Size** to **Small**, set the **Storage Size** to **Default**, and then click **Next**.
    f. From the **Select Datastore** page, leave the default datastore, enable **Think Disk Mode**, and then click **Next**.
    g. From the **Configure Network Settings** page, change from **Static** to **DHCP IP Address** assignment.
    h. On the **Deployment Details** page, review the summary of settings, and then click **Finish**.

5. Wait for the installation to complete before proceeding.
6. At the **Appliance Configuration** page, select **Sync Time with NTP**, and then provide either a local ntp server or **pool.ntp.org**.
7. Select the **Enable SSH** checkbox, and then click **Next**.
8. On the **SSO Configuration** page, provide the following parameters:
    a. **SSO domain name:** Enter the name of a dedicated test domain.
    b. **Username:** Enter the name of the desired vCenter administrator user.
9. Clear the **Join the VMware CEIP** checkbox.
10. Wait for the installation to complete.

Creating and Deploying a vSAN Cluster

1. In the vSphere client for the newly created vCenter Server, right-click the vCenter Server in the left-hand panel, and then select **New Datacenter**.
    a. Provide a name for the data center, and then click **OK**.
2. Right-click the data center, and then select **New Cluster**.
    a. Provide a name for the cluster.
    b. Toggle **vSAN** to **On**.
    c. Click **Next**, review the details, and then click **Finish**.
3. Select the new cluster, and then, under the **Configure** tab, scroll down to **Configuration > Quickstart**.
4. On the **Cluster Quickstart** page, under **2. Add Hosts**, click **Add**.
5. On the **Add New And Existing Hosts to Your Cluster** page, enter the **IP Address**, **Username**, and **Password** for the three ESXi servers.
6. Click **Next**.
7. On the **Security Alert** page, select all three hosts, and then click **OK**.
8. On the **Host Summary** page, click **Next**.
9. On the **Review** page, click **Finish**.
10. Back on the **vSAN Cluster Quickstart** page, under **2. Add Hosts**, click **Re-Validate**.
11. Once validated, under **3. Configure Cluster**, click **Configure**.
    a. On the **Distributed Switches** page, select **Dswitch**, and then click **Next**.
    b. On the **vSAN Network** page, select the name of the Dswitch.
    c. For the **Physical Adapters** (uplink) section, select the interface of the 100 gigabit Ethernet (GbE) network interface controller (NIC), and then click **Next**.
    d. On the **Storage Traffic** page, select **Static IPs**, provide the desired IP configuration for the vSAN network, and then click **Next**.
    e. On the **Advanced Options** page, leave the default settings, and then click **Next**.
    f. On the **Claim Disks** page, set one disk from each host to **Cache** tier, set the remaining disks to **Capacity** tier, and then click **Next**.
    g. On the **Review** page, look over the vSAN configuration, and then click **Finish**.

VMware Horizon 7 Installation and Configuration

For this test, we set up two VMs on the infrastructure host:

- A VMware Horizon connector server (4 CPUs, 8 GB RAM, 60 GB storage)
- A VMware View composer server (4 CPUs, 8 GB RAM, 80 GB storage)

VMware Horizon Connector Installation and Configuration

1. On the **Horizon Connector** VM, download and launch the **Connector Installer**.
2. On the **Welcome** page, click **Next**.
3. On the **License Agreement** page, **Accept** the license agreement, and then click **Next**.
4. On the **Destination Folder** page, leave the default settings, and then click **Next**.
5. On the **Installation Options** page, select **Horizon 7 Standard Server**.
6. In the **IP Protocol** drop-down menu, select **IPv4**.
7. Select the **Install HTML Access** checkbox, and then click **Next**.
8. From the **Data Recovery** page, enter a data recovery password.
9. From the **Firewall Configuration** page, select **Configure Windows Firewall Automatically**, and then click **Next**.
10. From the **Initial Horizon 7 Administrator** page, provide the new Horizon 7 administrator credentials, and then click **Next**.
11. Wait until the installation is completed, and then log in to the Horizon 7 connector server.
12. Join the Horizon 7 connector server to the test Active Directory domain using steps specified by Microsoft.
13. Reboot the server and reconnect.
14. On the desktop, double-click the **Horizon 7 Administrator Console** shortcut.
15. Log in using the credentials you provided in step 10.
16. In the left-hand pane, navigate to **Settings > Servers**.
17. Under the **vCenter Servers** tab, click **Add**.
18. Under **vCenter Information**, provide the vCenter Server address, username, and password, and then click **Next**. The wizard will verify the server is accessible with those credentials.
19. On the **View Composer Settings** page, select **Standalone View Composer Server**, and then click **Next**.
20. From the **Storage Settings** page, make sure all ESXi hosts appear, and then click **Next**.
21. Click **Submit** to add the server to Horizon 7.

VMware Horizon View Composer Installation and Configuration

1. On the **View Composer** VM, download and launch the Microsoft® SQL Server® 2019 Express edition installer.
2. Select the **Basic** installation method.
3. On the **Microsoft SQL Server License Terms** page, click **Accept**.
4. On the **Specify SQL Server Install Location** page, leave the default settings, and then click **Install**.
5. Once installation completes, click **Install SSMS** to open the download page for SQL Server Management Studio (SSMS).
6. Download the SSMS installer from the download page, and then begin the installation.
7. On the **Welcome** page, click **Install**.
8. Restart the Horizon View composer VM.
9. Reconnect to the Horizon View composer VM and launch SSMS.
10. Connect to SQL Server using the default settings.
11. In the left-side explorer, right-click the **SQL Server** name, and then select **Properties**.
    a. Under **Properties**, navigate to the **Security** page, select **SQL Server and Windows Authentication Mode**, and then click **OK**.
12. In the left-side explorer, right click **Database**, and then select **New Database**.
    a. On the **New Database** page, enter **ViewComposer** as the database name.
    b. Under the **Options** tab, ensure that **Recovery Model** is set to **Simple**, and then click **OK**.
13. In the left-side explorer, right-click **Login**, and then select **Create New Login**.
14. On the **Login** page, provide a username.
    a. Select **SQL Server Authentication**, and then provide a password.
    b. Disable **Enforce Password Policy**.
    c. Change the default database to **ViewComposer**.
    d. Navigate to the **User Mapping** tab, and then select the **View Composer** database.
        i. At the bottom of the wizard, select **db_owner**, and then click **OK**.

15. From the **Start** menu, search for and launch **OBDC Data Sources (64-bit)**.
    a. Navigate to the **System DSN** tab, and then click **Add**.
    b. From the **Create New Data Source** window, select **SQL Server Native Client 11.0**, and then click **Finish**.
    c. From the **Create a New Data Source to SQL Server** window, provide a name and the address for the SQL Server instance.
    d. From the **How Should SQL Server Verify the Authenticity of the Login ID?** page, select **With SQL Server Authentication Using a Login ID and Password Entered by the User**, and then provide the login credentials created in step 14.
    e. Select **Change the Default Database To**, update to the **ViewComposer** database, and then click **Next**.
    f. Click **Finish**.
    g. Review and test the data source. A popup should indicate that the test was successful.
16. On the **View Composer** VM, launch the **View Composer** installer.
    a. On the **Welcome** page, click **Next**.
    b. When prompted to **Accept the license terms**, click **Next**.
    c. On the **Destination Folder** page, leave the default folder, and then click **Next**.
    d. On the **Database Information** page, provide the following information:
        i. **OBDC Connection Name:** Enter the name provided in step 15c.
        ii. **Username for ODBC Data Source:** Use the credentials created in step 14.
        iii. **Password for the database connection:** Use the credentials created in step 14.
    e. Click **Next**.
17. Log in to the **Horizon Connection Server** VM.
18. In the left pane, navigate to **Settings > Servers**.
19. Click the **vCenter Server**, and then go to the **View Composer** tab.
20. Provide the following details for the Horizon View composer server:
    a. **Server Address:** Enter the IP or FQDN of the Horizon View composer VM.
    b. **Username:** Enter the Horizon View composer username.
    c. **Password:** Enter the Horizon View composer password.
21. Verify **Port** is set to **18443**, and then click **OK**.

Horizon 8 Installation and Configuration

For this test, we created a single VM on the infrastructure server:

- Horizon connector server (4 CPU, 8 GB RAM, 60 GB storage)

Horizon Connector Installation and Configuration

1. On the Horizon connector VM, launch the Horizon installer.
2. At the **Welcome to the Installer** page, click **Next**.
3. At the **License Agreement** page, accept the license agreement, and then click **Next**.
4. At the **Destination Folder** page, leave the default settings, and then click **Next**.
5. At the **Installation Options** page, select **Horizon Standard Server**.
    a. When asked to specify **IP Protocol**, select **IPv4**.
    b. Select **Install HTML Access**, and then click **Next**.
6. From the **Data Recovery** page, enter the data recovery password, and then click **Next**.
7. From the **Firewall Configuration** page, select **Configure Windows Firewall automatically**, and then click **Next**.
8. From the **Initial Horizon Administrator** page, select **Authorize a specific domain user or domain group**, provide the domain username, and then click **Next**.
9. On the **User Experience Improvement Program**, clear the **Join the VMware Customer Experience Improvement Program** checkbox, and then click **Next**.
10. On the **Ready to Install the Program** page, verify the installation path and that it is set for **General installation type**, and then click **Install**.
11. Follow steps 14–21 under Horizon 7 Connector Installation and Configuration to add the test vCenter server to the Horizon 8 connector.

NVIDIA GRID® vGPU Installation and Configuration

We used the following instructions to install and configure the NVIDIA GPUs on the VMware ESXi hosts.

VMware ESXi Host Configuration

1. Download the NVIDIA GRID® driver archive appropriate for your GPU model from the NVIDIA Enterprise Application Hub.
2. After extracting the archive, log in to vCenter server and select the ESXi host from the left-hand pane.
    a. On the host's **Datastores** tab, click the **store1** datastore.
    b. On the **Files** tab, click **Upload Files**.
    c. Upload the .VIB file from the **host_drivers** folder in the extracted directory.
3. In the vSphere UI, right-click the ESXi host, and then select **Maintenance Mode > Enter Maintenance Mode**.
4. Use Secure Shell (SSH) to connect to the ESXi host and navigate to **/vmfs/volumes/*<name of datastore>***. Verify that the .VIB file has been uploaded to the host.
5. Install the .VIB via the following ESXi command-line interface (CLI) command:

```
esxcli software vib install -v /vmfs/volumes/<datastore name>/<NVIDIA driver vib file>
```

6. Reboot the ESXi server.
7. From the **VMware vCenter** web client, right-click on the host, and then select **Maintenance Mode** > **Exit Maintenance Mode**.
8. Run the following command in the ESXi shell to verify if the driver is loaded; if the results are empty, check **dmesg** for any load-time errors with the driver:

```
vmkload_mod -l | grep nvidia
```

9. The **nvidia-smi** command will display a list of the GPUs installed on your system.
10. Log in to the **vSphere** client, and then navigate to **Configure > Graphics > Host Graphics**.
    a. On the **Host Graphics** tab, click **Edit**.
    b. In the **Edit Host Graphics Settings** window, select **Shared Direct**, and then click **OK**.
    c. Reboot the host to apply the new setting.

Creating a vGPU Virtual Desktop

1. On your chosen vGPU machine, select **Actions > Edit Settings**.
2. Select **Add New Device**, and then select **PCI Device** from the drop-down menu.
3. The new PCI device will register as an NVIDIA_GRID_vGPU. Expand the **PCI Device 0** details to select the specific vGPU profile desired for testing. For documented vGPU profile options and use cases, see the NVIDIA documentation.
4. Boot the VM, and then download the NVIDIA display driver for Windows from "NVIDIA virtual GPU Software (Quadro vDWS, GRID vPC, GRID vApps)."
5. Locate the downloaded driver, and then launch the installer.
6. In the **Extraction** window, leave the default file path, and then click **OK**.
    a. On the **License Agreement** page, click **Agree and Continue**.
    b. On the **Installation Options** page, select **Custom**, and then click **Next**.
    c. On the **Custom Installation Options** page, select to perform a clean installation, and then click **Next**.
    d. Once installation has completed, reboot the VM.

Testing the VM Creation and Testing Loop

We created two VM profiles for this test:

- Knowledge worker (2 vCPUs, 4 GB RAM, 80 GB storage)
- Power user (4 vCPUs, 8 GB RAM, 80 GB storage)

VM Creation

1. Create either a Windows 10 (Horizon 7 testing) or Windows 11 (Horizon 8 testing) VM matching either of the two configurations above.
2. After the operating system (OS) is installed, mount and install VMware tools on the VM.

3. For the vGPU testing only, modify the system configuration as documented in the Creating vGPU Virtual Desktop procedure above.
4. Download and install the VMware Horizon agent appropriate for the version of Horizon being tested.
    a. On the **Welcome** page of the installer, click **Next**.
    b. On the **License Agreement** page, click to accept, and then click **Next**.
    c. On the **Network Protocol Configuration** page, select **IPv4**, and then click **Next**.
    d. On the **Custom Setup** page, leave the default values, and then click **Next**.
    e. Review the installation path on the **Ready to Install** page, and then click **Install**.
5. Download **Cinebench R23** from the Cinebench website.
    a. Extract the archive file.
6. Open **Notepad.exe** and copy the following code into the Notepad window. Replace the section enclosed in carets with the full file path of the Cinebench folder.

```
@ECHO OFF
cd <path to extracted CinebenchR23 directory>
for /L %%i IN (1,1,5) do (
.\Cinebench.exe g_CinebenchCpuXTest=true g_CinebenchCpu1Test=false g_CinebenchMinimumTestDuration=1
)
```

    a. Save the file as **Cinebench.bat** on the local desktop.
7. Create a shortcut for Cinebench.bat, and then copy it to **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp**.
8. Restart the machine and ensure Cinebench boots and begins to run the benchmark.
9. Once successful, power down the VM, and then, under **Actions**, select **Template > Convert to Template**.

Desktop Pool Configuration and Testing Loop

1. Log in to the Horizon connector server.
2. On the left pane, navigate to **Inventory,** and then click **Desktops**.
3. From the **Desktop Pools** page, click **Add**.
4. From the **Add Pool** window, select **Automated Desktop Pool**, and then click **Next**.
5. From the **vCenter Server** window, select **Full Virtual Machines**, and then click **Next**.
6. From the **User Assignment** window, select **Floating**, and then click **Next**.
7. From the **Storage Optimization** window, select **Use VMware Virtual SAN**, select the **vSAN datastore**, and then click **Next**.
8. From the **Desktop Pool ID** window, provide a unique name for the pool, and then click **Next**.
9. From the **Provisioning Settings** window, select **Enable Provisioning and Stop Provisioning on Error**.
    a. Provide a naming pattern with the format of ***<identifying string>*-{n}**.
    b. Under **Desktop Pool Sizing**, select **All Machines Up Front**, and then set **Max Number of Machines** to **500**.
        i. Also set **Number of Powered On Machines** to **500**.
10. On the **vCenter Settings** page, provide the following parameters:
    a. **Template:** Name of the template from step 8 under VM creation
    b. **Virtual Machine Location: *<Test data center/VM/VMfolder>***
    c. **Host or Cluster: vSAN cluster**
    d. **Resource Pool: vSAN cluster**
    e. **Datastores: vSAN datastore**
11. Click **Next**.
12. On the **Desktop Pool** settings page, confirm the following parameters:
    a. **State: Enabled**
    b. **Session Type: Desktop**
    c. **Remote Machine Power Policy: Always Powered On**
    d. **Automatically Log Off after Disconnect: Never**
    e. **Allow User to Restart/Reset Their Machine: Yes**
    f. **Allow User to Initiate Separate Desktop Sessions: No**
    g. **Delete Machine on Logoff: No**

13. On the **Remote Display Settings** page, confirm the following:
    a. **Default Display Protocol: VMware Blast**
    b. **Allow Users to Choose Protocol: Yes**
    c. **3D Renderer: Manage using vSphere Client**
    d. **HTML Access: Enabled**
    e. **Allow Session Collaboration: Enabled**
14. Click **Next**.
15. On the **Advanced Storage Options** page, select **Use View Storage Accelerator**, and then click **Next**.
16. On the **Guest Customization** page, select **None – Customization will be done manually**, and then click **Next**.
17. On the **Review** page, select **Entitle users after adding pool**, and then click **Submit**.
18. When prompted to entitle users, search for the **Domain Users** group, and then select the resulting entry.
19. Click **Add**, and then click **Submit**.
20. Monitor the vSphere client page for the vSAN cluster until resource utilization alerts for all three VMware ESXi hosts appear.
    a. Under the **Cluster > VM** tab, take the total count of deployed VMs (subtracting the three vCLS machines created as part of cluster deployment).
    b. Filter the VM results by the phrase **Powered On**, and then take a new count, again subtracting three.
    c. These two numbers are the results for the test.
21. In the **Horizon Administration** console, navigate to the created desktop pool, and then click **Delete**.
    a. When prompted, select to **Delete the VMs from Disk**, and then click **Submit**.
22. Once the VMs show as deleted in the vSphere client, repeat steps 1–21 twice more for a total of three runs.

[1] EY. "Workplace of the Future Index 2.0." November 2022.
[2] VMware. "VMware Named a Leader in the 2022 Gartner® Magic Quadrant™ for Unified Endpoint Management for Fifth Year in a Row." August 2022.
[3] Gallup. "The Relationship Between Engagement at Work and Organizational Outcomes." October 2020.
[4] Tolly. "VMware Work From Home Test Report by Tolly." Commissioned by VMware. January 2021.
[5] TechTarget. "Work-from-home infrastructure HCI tips for VDI, remote desktops." July 2020.
[6] Forester Consulting. "Optimizing Digital Employee Experience For Anywhere Work." Commissioned by VMware. April 2022.
[7] VMware. "VMware Secure Access Receives 2022 TMCnet Zero Trust Security Excellence Award." February 2023.

0923/220228