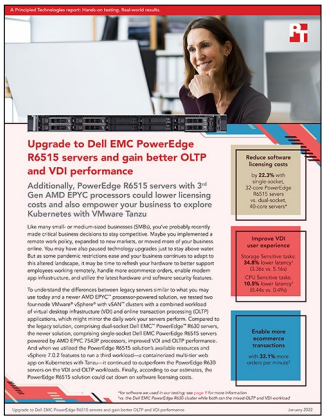

The science behind the report:

Upgrade to Dell EMC PowerEdge R6515 servers and gain better OLTP and VDI performance

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 Upgrade to Dell EMC PowerEdge R6515 servers and gain better OLTP and VDI performance.

We concluded our hands-on testing on November 8, 2021. 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 20, 2021 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: The results of our OLTP database testing. Higher is better.

	Total operations per minute (OPM)
Dell EMC™ PowerEdge™ R630 cluster simultaneously running the OLTP and VDI workload	129,571
Dell EMC PowerEdge cluster R6515 simultaneously running the OLTP and VDI workload	171,252
Percentage OPM increase vs. the Dell EMC PowerEdge R630 cluster	32.1%
Dell EMC PowerEdge R6515 cluster simultaneously running the OLTP, VDI, and Weathervane workloads	166,879
Percentage OPM increase vs. the Dell EMC PowerEdge R630 cluster	28.7%

Table 2: The results of our VDI testing with 100 VDI users. Lower latency is better.

	Operational latency while performing CPU Sensitive tasks (seconds)	Operational latency while performing Storage Sensitive tasks (seconds)
Dell EMC PowerEdge R630 cluster simultaneously running the OLTP and VDI workload	0.4988	5.1649
Dell EMC PowerEdge cluster R6515 simultaneously running the OLTP and VDI workload	0.4462	3.3624
Percentage latency decrease vs. the Dell EMC PowerEdge R630 cluster	10.5%	34.8%
Dell EMC PowerEdge R6515 cluster simultaneously running the OLTP, VDI, and Weathervane workloads	0.4703	3.5122
Percentage latency decrease vs. the Dell EMC PowerEdge R630 cluster	5.7%	31.9%

Table 3: Each cluster's average CPU utilization while running the workloads. Lower is better.

	Average CPU utilization while simultaneously running VDI and OLTP database workloads	Average CPU utilization while simultaneously running VDI, OLTP, and Weathervane workloads
Dell EMC PowerEdge R630 cluster	77.7%	N/A
Dell EMC PowerEdge R6515 cluster	74.5%	78.0%

CPU utilization charts

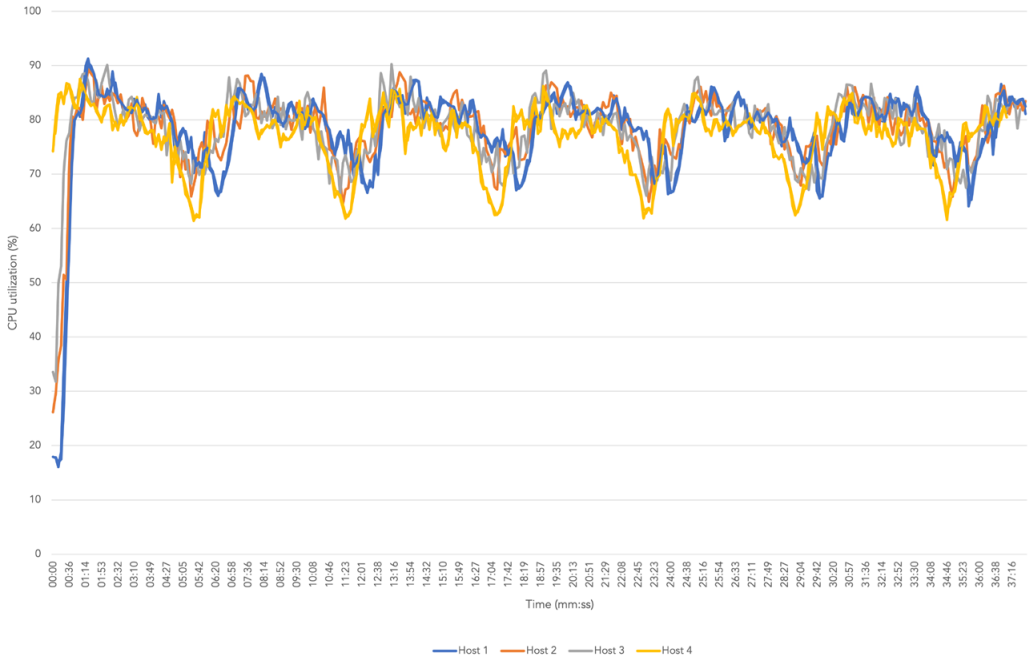

Figure 1: CPU usage for individual Dell EMC PowerEdge R630 servers while running the OLTP and VDI workloads simultaneously. Source: Principled Technologies.

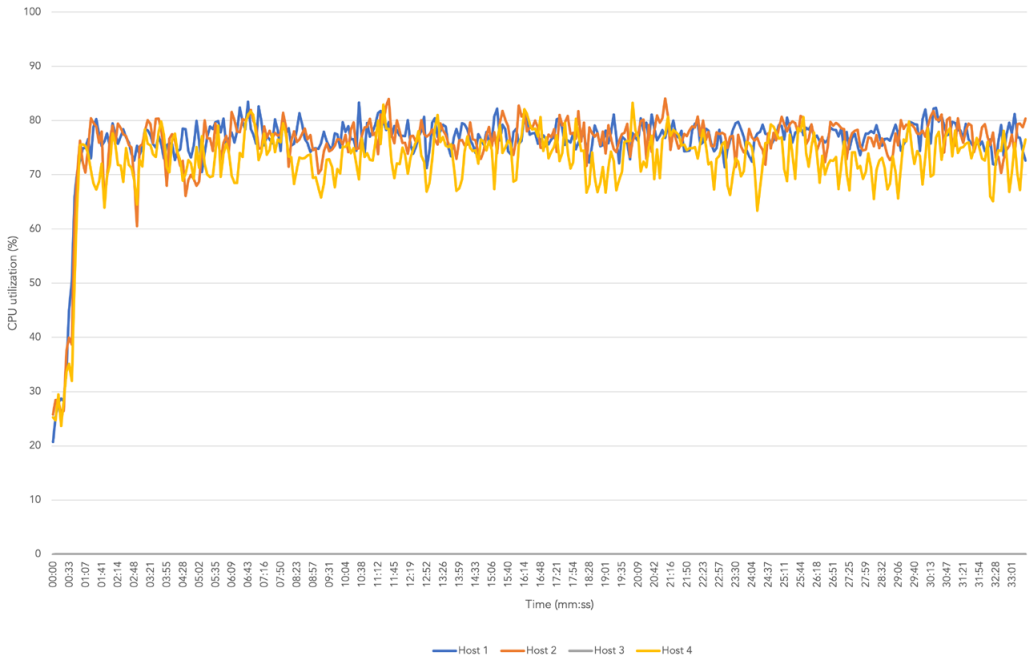

Figure 2: CPU usage for individual Dell EMC PowerEdge R6515 servers while running the OLTP and VDI workloads simultaneously. Source: Principled Technologies.

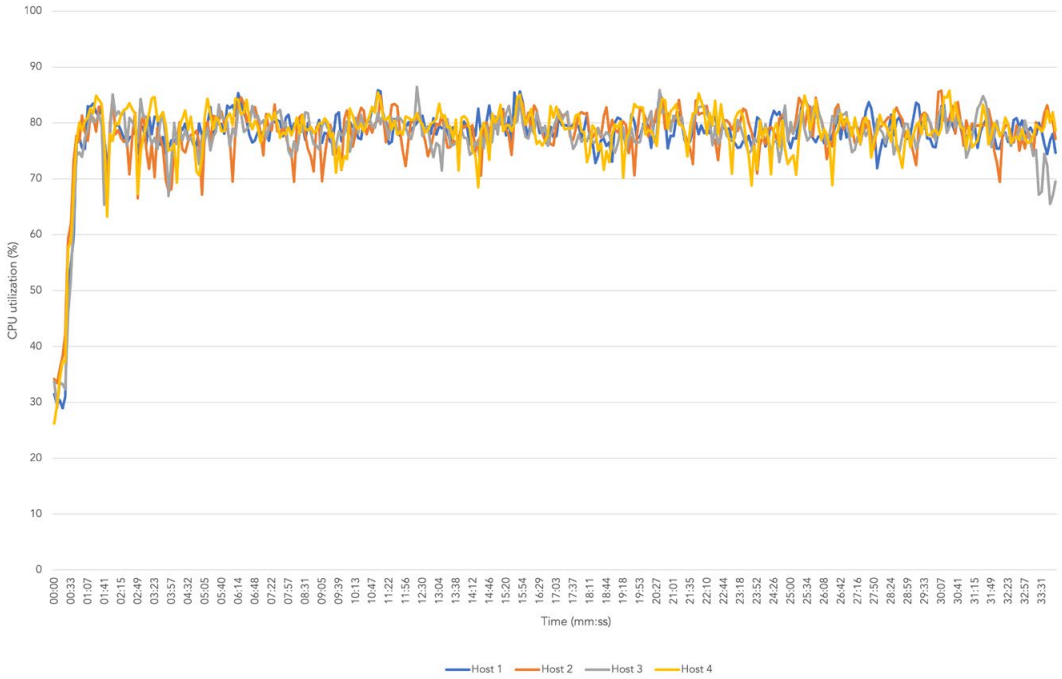

Figure 3: CPU usage for individual Dell EMC PowerEdge R6515 servers while running the OLTP, VDI, and Weathervane workloads simultaneously. Source: Principled Technologies

Licensing cost information

Table 4: Technical specifications relevant to our licensing cost comparison.

	Dell EMC PowerEdge R630 configuration	Dell EMC PowerEdge R6515 configuration
Number of servers in cluster	4	4
Number of CPUs per server	2	1
Number of cores per CPU	20	32
Total number of cores per server	40	32
Number of 2-core licenses per server	20	16

Table 5: A comparison of three-year licensing costs (including purchase cost plus three years of support) for a dual-socket, 40-core server and a single-socket, 32-core server such as the Dell EMC PowerEdge R6515 we tested. We researched this data on November 11, 2021 using publicly available sources. Amounts are in USD, do not include taxes, and do not include VDI software costs.

Software	Licensing cost model	Estimated 3-year cost per license	A new 2-CPU, 40-core configuration	Dell EMC PowerEdge R6515 configuration	Difference
Microsoft Windows Server Datacenter[1]	2-core	$1,346.41	$26,928.13	$21,542.50	$5,385.63
Microsoft SQL Server 2019 Enterprise[2]	2-core	$24,059.00	$481,180.00	$384,944.00	$96,236.00
VMware® vSphere® Enterprise Plus, with basic support for 1 CPU[3]	Max 32 cores/ CPU socket	$5,588.20	$11,176.40	$5,588.20	$5,588.20
VMware vSAN™ 7 Enterprise, with basic support for 1 CPU[4]	Max 32 cores/ CPU socket	$13,100.00	$26,200.00	$13,100.00	$13,100.00
VMware Tanzu basic (3-year term) for 1 CPU[5]	Max 32 cores/ CPU socket	$2,985.00	$5,970.00	$2,985.00	$2,985.00
Total for individual server	-	-	**$551,454.53**	**$428,159.70**	**$123,294.83**
Total for four-server cluster	-	-	**$2,205,818.10**	**$1,712,638.80**	**$493,179.30**

1. Based on data from "Pricing and licensing for Windows Server 2022," accessed November 11, 2021, https://www.microsoft.com/en-us/windows-server/pricing.
2. Based on data from "SQL Server 2019 Pricing," accessed November 11, 2021, https://www.microsoft.com/en-us/sql-server/sql-server-2019-pricing.
3. Based on data from "VMware vSphere Enterprise Plus," accessed November 11, 2021, https://store-us.vmware.com/vmware-vsphere-enterprise-plus-284281000.html.
4. Based on data from "Dell Price List," accessed November 11, 2021, https://itprice.com/dell-price-list/vmware%20vsan%207%20enterprise,.html.
5. Based on data from "VMware Tanzu Basic - Per CPU," accessed November 11, 2021, https://store-us.vmware.com/vmware-tanzu-basic-per-cpu-5471172000.html.

System configuration information

Table 6: Detailed information on the systems we tested.

System configuration information	4 x Dell EMC PowerEdge R6515	4 x Dell EMC PowerEdge R630
BIOS name and version	2.2.4	2.13.0
Operating system name and version/build number	Dell ESXi version 7.0 update 2 build 18426014	VMware ESXi version 6.7 update 3 build 14320388
Date of last OS updates/patches applied	9/14/21	9/15/21
Power management policy	Performance	Performance
Processor		
Number of processors	1	2
Vendor and model	AMD EPYC™ 7543P	Intel® Xeon® E5-2698 v4
Core count (per processor)	32	20
Core frequency (GHz)	2.8	2.2
Stepping	1	1
Memory module(s)		
Total memory in system (GB)	256	256
Number of memory modules	16	16
Vendor and model	Hynix® HMA82GR7CJR8N-XN	Hynix HMA42GR7AFR4N-TF
Size (GB)	16	16
Type	PC4-3200AA	PC4-2133P
Speed (MHz)	3,200	2,133
Speed running in the server (MHz)	2,933	2,133
Storage controller		
Vendor and model	PERC H740P Mini	PERC H730 Mini Controller
Cache size (GB)	N/A	1,024
Firmware version	51.14.0-3900	25.5.7.0005
Driver version	7.716.03.00	7.710.07.00
Local storage (OS)		
Number of drives	2	2
Drive vendor and model	Intel SSDSCKKB240G8R	Intel S3710 SSDSC2BA400G4R
Drive size (GB)	240	400
Drive information (speed, interface, type)	6Gbps, SATA, M.2	6Gbps, SATA, SSD
Local storage (capacity)		
Number of drives	4	4
Drive vendor and model	Samsung® MZ-7LH11T9C	Intel S3610 SSDSC2BX016T4P
Drive size (GB)	1,920	1,600
Drive information (speed, interface, type)	6Gbps, SATA, SSD	6Gbps, SATA, SSD

System configuration information	4 x Dell EMC PowerEdge R6515	4 x Dell EMC PowerEdge R630
Local storage (cache)		
Number of drives	2	2
Drive vendor and model	Western Digital® WUSTR6480ASS200	Toshiba® THNSF8800CCSE
Drive size (GB)	800	400
Drive information (speed, interface, type)	12Gbps, SAS, SSD	6Gbps, SATA, SSD
Network adapter 1		
Vendor and model	Broadcom® Gigabit Ethernet BCM5720	QLogic 1Gb BCM57800
Number and type of ports	4x 1Gb Ethernet	2x 1Gb Ethernet
Firmware version	20.16.31	15.15.08
Network adapter 2		
Vendor and model	Broadcom Adv. Dual 25Gb Ethernet	QLogic 10Gb BCM57800
Number and type of ports	2x 25GbE SFP	2x 10GbE SFP
Firmware version	21.80.16.95	15.15.08
Cooling fans		
Vendor and model	Sunon PG40561BX	Dell TGC4J
Number of cooling fans	6	7
Power supplies		
Vendor and model	Delta Electronics D550E-S1	Dell 05RHVVA00
Number of power supplies	2	2
Wattage of each (W)	550	750

How we tested

Overview

For our testing, we deployed two on-premises VMware vSphere with vSAN clusters comprising four nodes and one supporting infrastructure server for each environment. Our legacy environment used four dual-socket Dell EMC PowerEdge R630 servers and VMware vSphere 6.7 Update 3, while our newer-generation environment used four single-socket Dell EMC PowerEdge R6515 servers and VMware vSphere 7.0 Update 2. For each environment, we deployed a PowerEdge R730 infrastructure server to support our infrastructure VMs: domain controller, VMware Horizon, VMware View Planner, and workload clients. For all testing, we isolated network traffic to a private network, supported by one Dell EMC Networking S5048F-ON switch for each environment. On each cluster, we ran the following workloads:

- An OLTP workload driven by DVD Store 3 (DS3)
  - For more information about DVD Store 3, visit https://github.com/dvdstore/ds3.
- A VDI environment of 100 active users using VMware View Planner 4.6
  - For more information about VMware View Planner 4.6 visit https://docs.vmware.com/en/VMware-View-Planner/4.6/user-guide/GUID-0B57E9DF-B79B-40FC-A37B-1CBF1A8F8AEC.html.

In addition to the two workloads, we also deployed the following workload on our newer-generation environment:

- A multi-tier web application supported by VMware vSphere with Tanzu Kubernetes using VMware Weathervane 2.1.
  - For more information about Weathervane 2.1, view the development blog at https://blogs.vmware.com/performance/2020/02/weathervane2-kubernetes.html and GitHub repository at https://github.com/vmware/weathervane.

To support our testing, we deployed the following infrastructure VMs on both environments:

- Active Directory Domain Controllers deployed on Windows Server
- Router VM deployed on Window Server
- VMware Horizon Server deployed on Windows Server
- VMware vCenter Server 7.0 Update 2 (newer-generation)/ 6.7 Update 3 (legacy)

For our legacy environment, we deployed an additional Horizon Composer VM to support our Horizon 7 environment. For our newer-generation environment, we also deployed an auxiliary VM to support our VMware Weathervane workload.

For more information on our VM configurations, see the table below.

Table 7: Specifications for the VMs we used in our testing.

VM name	Workload	Cluster	Newer-generation environment OS	Legacy environment OS	VM quantity per environment	vCPU	Memory (GB)	Disk 1 (GB)	Disk 2 (GB)	Disk 3 (GB)
DVD Store Database Host	DVD Store 3	Cluster under test	Windows Server 2022	Windows Server 2016	12	8	32	100	100	30
DVD Store Driver	DVD Store 3	Infrastructure	Windows Server 2022	Windows Server 2016	12	2	4	40	N/A	N/A
Windows 10 Clients	Viewplanner	Cluster under test	Windows 10	Windows 10	100	2	4	90	N/A	N/A
Horizon Server	Viewplanner	Infrastructure	Windows Server 2022	Windows Server 2016	1	8	32	300	N/A	N/A
Horizon Composer	Viewplanner	Infrastructure	N/A	Windows Server 2016	1	4	16	60	100	N/A
Driver Control Nodes	Weathervane	Cluster under test	VMware Photon OS	N/A	3	2	8	16	N/A	N/A
Driver Worker Nodes	Weathervane	Cluster under test	VMware Photon OS	N/A	4	2	8	16	N/A	N/A
Application Control Nodes	Weathervane	Cluster under test	VMware Photon OS	N/A	3	2	8	16	N/A	N/A
Application Worker Nodes	Weathervane	Cluster under test	VMware Photon OS	N/A	4	2	8	16	N/A	N/A

Running the tests

On the legacy PowerEdge R630 environment and the newer-generation PowerEdge R6515 environment, we completed the steps below for our tests with OLTP and VDI workloads.

1. Restart the DS3 database VMs.
2. Once the DS3 database VMs are responding again, start the created workload on the View Planner test harness. Wait 10 minutes.
3. After 10 minutes have passed, start the DS3 workload.

On the newer-generation PowerEdge R6515 environment, we completed the steps below for our tests with VDI, OLTP, and Weathervane workloads.

1. Start the Weathervane workload. This will load all necessary containers. Wait until the Weathervane workload is running and returns the passed check for the first QoS period.
2. Restart the DS3 database VMs.
3. Once the DS3 database VMs are responding again, start the created workload on the View Planner test harness. Wait 10 minutes.
4. After 10 minutes have passed, start the DS3 workload.
5. Once the View Planner and DS3 workloads have finished, stop the Weathervane workload.

For each solution, we ran each workload three times. We used the combined total OPM from our DS3 servers to determine our median run. We reported metrics using that median run.

See the sections below for more details on how we prepared and ran each of the three workload components.

Preparing the test environment

Setting up the infrastructure and the vSphere test clusters

Installing VMware vSphere 7.0 Update 2 (Newer-generation only)

We used the following steps to install vSphere on each server under test in the newer-generation environment as well as the infrastructure server.

1. Boot to the VMware vSphere 7.0 Update 2 installation media using USB installer.
2. To continue, press Enter.
3. To accept and continue, press F11.
4. Under Storage Device, select the installation drive, and press Enter to continue.
5. For keyboard layout, select US Default, and press Enter to continue.
6. Enter the root password twice, and press Enter to continue.
7. At the Confirm Install window, press F11 to install.
8. At the Installation Complete window, press Enter to reboot.
9. After reboot, press F2 to configure system.
10. Log in with root user/password and press Enter for OK.
11. Scroll to Configure Management Network, and press Enter.
12. Scroll to IPv4 Configuration, and press Enter.
13. Scroll to Static IPv4, and use spacebar to select it.
14. Set the IPv4 address, Subnet Mask, and Default gateway.
15. To continue, press Enter for OK.
16. Scroll to IPv6 Configuration, and press Enter.
17. Scroll to Disable IPv6, and use spacebar to select it.
18. To continue, press Enter for OK.
19. Scroll to DNS Configuration, and press Enter.
20. Scroll to manually configure DNS, and use spacebar to select it.
21. Add Primary DNS Server, Alternate DNS Server, and provide the hostname for the system.
22. Scroll to Custom DNS Suffixes, and press Enter.
23. Add the suffix that is required for testing, and press Enter for OK.
24. To accept the changes, press Esc.
25. To confirm changes, press Y. The system will reboot.
26. After reboot, press F2 to configure system.
27. Log in with root user/password, and press Enter for OK.
28. Scroll to Troubleshooting Options, and press Enter.

29. Select Enable ESXi Shell, and press Enter to enable it.
30. Select Enable SSH, and press Enter to enable it.
31. Scroll to Restart Management Agents, and press Enter.
32. To confirm, press F11 for OK.
33. To exit, press Esc.
34. To log out, press Esc.

Installing the VMware vCenter Server Appliance 7.0 Update 2 (Newer-generation environment only)

We deployed the VMware vCenter Appliance on our newer-generation infrastructure server.

1. Download the VMware vCenter installation ISO from the VMware support portal at https://my.vmware.com.
2. Mount the image on your local system, and browse to the vcsa-ui-installer folder. Expand the folder for your OS, and launch the installer if it doesn't automatically begin.
3. Once the vCenter Server Installer wizard opens, click install.
4. To begin installation of the new vCenter server appliance, click Next.
5. To accept the license agreement, check the box, and click Next.
6. Enter the IP address of a temporary ESXi host. Provide the root password, and click Next.
7. To accept the SHA1 thumbprint of the server's certificate, click Yes.
8. Accept the VM name, and provide and confirm the root password for the VCSA. Click Next.
9. Set the size for environment you're planning to deploy, check Thin Disk, and click Next.
10. Select the datastore to install on, accept the datastore defaults, and click Next.
11. Enter the FQDN, IP address information, and DNS servers you want to use for the vCenter server appliance. Click Next.
12. To begin deployment, click Finish.
13. When Stage 1 has completed, click Close. To confirm, click Yes.
14. Open a browser window, and connect to https://[vcenter.fqdn]:5480/.
15. On the Getting Started - vCenter Server page, click Set up.
16. Enter the root password, and click Log in.
17. Click Next.
18. Enable SSH access, and click Next.
19. To confirm the changes, click OK.
20. Enter `vsphere.local` for the Single Sign-On domain name, enter a password for the administrator account, confirm it, and click Next.
21. Click Next.
22. Click Finish.

Installing VMware vSphere 6.7 Update 3 (Legacy environment only)

We used the following steps to install vSphere on each server under test in the legacy environment as well as the infrastructure server.

1. Attach the installation media to the test server.
2. Boot the server.
3. At the VMware Installer screen, press Enter.
4. At the EULA screen, to Accept and Continue, press F11.
5. Under Storage Devices, select the appropriate virtual disk, and press Enter.
6. For the keyboard layout, select US, and press Enter.
7. Enter the root password twice, and press Enter.
8. To start the installation, press F11.
9. After the server reboots, press F2, and enter root credentials.
10. Select Configure Management Network, and press Enter.
11. Select the appropriate network adapter, and select OK.
12. Select IPv4 settings, and enter the desired IP address, subnet mask, and gateway for the server.
13. Select OK, and restart the management network.
14. Repeat steps 1 through 13 on the rest of the legacy test servers.

Deploying the VMware vCenter Server 6.7 Update 3 Appliance (Legacy environment only)

We deployed the VMware vCenter Appliance on our legacy infrastructure server.

1. On a Windows server or VM, locate the VMware-VCSA installer image.
2. Mount the image, navigate to the vcsa-ui-installer folder, and double-click win32.
3. Double-click installer.exe.
4. Click Install.
5. Click Next.
6. Accept the terms of the license agreement, and click Next.
7. Leave the default vCenter Server with an Embedded Platform Services Controller selected, and click Next.
8. Enter the FQDN or IP address of the host onto which you will deploy the vCenter Server Appliance.
9. Provide the server's username and password, and click Next.
10. To accept the certificate of the host to which you chose to connect, click Yes.
11. Provide a name and password for the vCenter Appliance, and click Next.
12. Set an appropriate Appliance Size, and click Next.
13. Select the appropriate datastore, and click Next.
14. At the Configure Network Settings screen, configure the network settings as appropriate for your environment, and click Next.
15. Review your settings, and click Finish.
16. When the deployment completes, click Next.
17. At the Introduction screen, click Next.
18. At the Appliance configuration screen, select the time synchronization mode and SSH access settings, click Next.
19. Select Create a new SSO domain.
20. Provide a password, and confirm it.
21. Provide an SSO Domain name and SSO Site name, and click Next.
22. At the CEIP screen, click Next.
23. At the Ready to complete screen, click Finish.
24. When installation completes, click Close.
25. Using the vSphere web client, log into the vCenter server using the credentials previously provided.

Creating a cluster in VMware vSphere

We created two test clusters with vSAN enabled: one using the Dell EMC PowerEdge R630 servers and one using the Dell EMC PowerEdge R6515 servers.

1. Open a browser, and enter the address of the vCenter server you deployed (https://[vcenter.FQDN]/ui).
2. Select the vCenter server in the left panel, right-click, and select New Datacenter.
3. Provide a name for the new data center, and click OK.
4. Select the data center you just created, right-click, and select New Cluster.
5. Give a name to the cluster, click OK.
6. In the cluster configuration panel, under Add hosts, click Add.
7. Check the box for Use the same credentials for all hosts. Enter the IP Address and root credentials for the first host, and the IP addresses of all remaining hosts. Click Next.
8. Check the box beside Hostname/IP Address to select all hosts, and click Ok.
9. Click Next.
10. Click Finish.

Configuring the virtual network

We used a private network for the infrastructure and test server clusters management network. The Horizon VMs must be able to access each server on a private IP. VMware vCenter and the vSphere hosts will also need to have private IPs connected to this network. Additionally, we created separate networks for vSAN traffic and vMotion traffic. We configured our physical switch ports with the required VLANs (10,11,12,20,21,22) and MTU settings (9216).

Creating a Distributed vSwitch and workload port group

1. From the vSphere client, click Home→Networking.
2. Select your data center, and in the Actions pull-down menu on the right panel, select Distributed vSwitch→New Distributed vSwitch.
3. Either enter a name for your vSwitch or accept the default. Click Next.
4. Select the appropriate version for your environment.
   - For the newer-generation environment, select 7.0.2 - ESXi 7.0.2 and later.
   - For the legacy environment, select 6.6.0 - ESXi 6.7 and later
5. Click Next.
6. Select the number of uplinks you'll give the Distributed Virtual Switch. We selected two. Click Next.
7. Click Finish.
8. Right-click the new Distributed Virtual Switch, and click Edit Settings…
9. Click Advanced.
10. Enter `9000` for the MTU setting, and click OK.
11. Right-click the new Distributed vSwitch, and select Add and Manage Hosts.
12. Leave Add hosts selected, and click Next.
13. To add new hosts, click the plus sign. To select all the hosts in your target cluster, check the box beside Host Click OK, and click Next.
14. Select the NICs for this Distributed vSwitch, and click Assign Uplink. We selected the two 10Gb connections on each host.
15. At the top of the panel, accept the defaults, and check "Apply this uplink assignment to the rest of the hosts."
16. Click OK, and click Next.
17. Do not assign VMkernel adapters at this time. Click Next.
18. Do not migrate any VM networking at this time. Click Next.
19. Click Finish.
20. Right-click the Distributed vSwitch, and select Distributed Port Group→New Distributed Port Group.
21. Type the name for the port group, and click Next.
22. Change the VLAN type to VLAN, and set the VLAN ID to the desired VLAN. Click Next.
23. Click Finish.

We completed the steps for creating a new port group three times using the following parameters in each environment:

- Legacy environment
  - Name: Private
    - VLAN: 20
  - Name: vMotion
    - VLAN: 21
  - Name: vSAN
    - VLAN: 22
- Newer-generation environment
  - Name: Private
    - VLAN: 10
  - Name: vMotion
    - VLAN: 11
  - Name: vSAN
    - VLAN: 12

Create a VMkernel Network Adapter

1. From the vCenter UI in the Hosts and Clusters view, right-click a host, and click Add Networking…
2. Select VMkernel Network Adapter, and click Next.
3. Click Browse… under Select an existing network.
4. Select the desired Distributed Port Group you created in the previous section.
5. If necessary, assign a different Network label.
6. Select the desired service or services for the VMkernel, and click Next.
7. Select Use static IPv4 settings, and enter the desired IPv4 address, subnet mask, and default gateway.
8. Click Next.
9. Click Finish.

We completed these steps on each server under test for the private network, vSAN network, and vMotion network using the appropriate IPv4 settings for each network and enabling the corresponding service for each VMkernel network adapter. We enabled the management service on the private network VMkernel and re-added the hosts to vCenter Server using the private IP.

Adding private management IP to vCenter

To add a private management IP to the vCenter, perform the following steps.

1. Navigate to https://[vcenter ip]:5480.
2. Log into with vCenter as administrator@vsphere.local.
3. Click Networking.
4. In the top right corner of the Network Settings page, click Edit.
5. Select your preferred NIC. We used NIC 1, as a public management IP was already using NIC 0.
6. Under Hostname and DNS, leave Obtain DNS settings automatically selected.
7. Under NIC settings, leave IPv4 enabled and disable IPv6. Enter a static IP address and prefix for vCenter management on the private network. You can leave the gateway blank.
8. Click Next, and click Finish.

Configuring VMware vSAN on the clusters

1. In the Hosts and Clusters pane, select the newly created test server cluster.
2. Click the Configure tab, and under vSAN, select Services.
3. Click Configure...
4. Select Single Site Cluster, and click Next.
5. Leave the default services, and click Next.
6. On the Claim disks page, select the disks which you wish to use for Capacity and Cache, and click Next.
7. Click Next, and click Finish.

Configuring the domain

Installing the Active Directory Server VM

We installed and configured a VM with 2 vCPUs, 8GB of RAM, and a 90GB VMDK on the private network to host Active Directory, DNS, DHCP, and NTP and to be a certificate authority. In addition, we configured a Microsoft Windows Server 2022 VM, installed updates, and created a template for use throughout the configuration process to quickly deploy the required infrastructure. We created a gold Windows 10 Clients VM for virtual desktops and applied registry edits to ensure testing executed correctly. All these functions were necessary for our testing.

1. Log into the vSphere client as administrator@vsphere.local.
2. On the infra server, deploy a Windows Server VM from the template using the appropriate specs from Table 7, and log in as an administrator.
3. Launch Server Manager.
4. Click Manage→Add Roles and Features.
5. At the Before you begin screen, click Next.
6. At the Select installation type screen, leave Role-based or feature-based installation selected, and click Next.
7. At the Server Selection screen, select the server from the pool, and click Next.
8. At the Select Server Roles screen, select Active Directory Domain Services.
9. When prompted, click Add Features, and click Next.
10. At the Select Features screen, click Next.
11. At the Active Directory Domain Services screen, click Next.
12. At the Confirm installation selections screen, check Restart the destination server automatically if required, and click Install.

Configuring Active Directory and DNS services on the Active Directory server

1. After the installation completes, a screen should pop up with configuration options. If a screen does not appear, in the upper-right section of Server Manager, click the Tasks flag.
2. Click Promote this server to a Domain Controller.
3. At the Deployment Configuration screen, select Add a new forest.
4. In the Root domain name field, type `test.local` and click Next.
5. At the Domain Controller Options screen, leave the default values, and enter a password twice.
6. Click Next four times to accept default settings for DNS, NetBIOS, and directory paths.
7. At the Review Options screen, click Next.
8. At the Prerequisites Check dialog, allow the check to complete.
9. If there are no relevant errors, check Restart the destination server automatically if required, and click Install.
10. When the server restarts, log on using test\Administrator and the password you chose in step 5.

Configuring the Windows time service on Active Directory server

To ensure reliable time, point your Active Directory server to a physical NTP server.

1. Open a command prompt.
2. Type the following:

```
W32tm /config /syncfromflags:manual /manualpeerlist:"<ip address of a NTP server>"
W32tm /config /reliable:yes
W32tm /config /update
W32tm /resync
Net stop w32time
Net start w32time
```

Setting up DHCP services on the Active Directory server

1. Open Server Manager.
2. Select Manage, and click Add Roles and Features.
3. Click Next twice.
4. At the Select server roles screen, select DHCP Server.
5. When prompted, click Add Features, and click Next.
6. At the Select Features screen, click Next.
7. Click Next.
8. Review your installation selections, and click Install.
9. Once the installation completes, click Complete DHCP configuration.
10. On the Description page, click Next.
11. On the Authorization page, use the Domain Controller credentials you set up previously (TEST\Administrator). Click Commit.
12. On the Summary page, click Close, and click Close on the Add Roles and Features Wizard.
13. In Server Manager, click Tools→DHCP.
14. In the left pane, double-click your server, and click IPv4.
15. In the right pane, under IPv4, click More Actions, and select New Scope.
16. Click Next.
17. Enter a Name and Description for the scope and click Next.
18. Enter the following values for the IP Address Range, then click Next.
    - Start IP address = `172.16.10.1`
    - End IP address = `172.16.100.254`
    - Length = `16`
    - Subnet mask = `255.255.0.0`
19. At the Add Exclusions and Delay page, leave defaults, and click Next.
20. Set the Lease Duration, and click Next. We used 30 days.
21. At the Configure DHCP Options page, leave Yes selected, and click Next.
22. At the Router (Default Gateway) page, leave the fields blank, and click Next.
23. At the Specify IPv4 DNS Settings screen, type `test.local` for the parent domain.
24. Type the preferred DNS server IPv4 address, and click Next.
25. At the WINS Server page, leave the fields empty, and click Next.
26. At the Activate Scope page, leave Yes checked, and click Next.
27. Click Finish.

Installing and configuring SSL Certificate in Microsoft Active Directory on the Active Directory server

1. Log onto the Active Directory server as administrator@test.local.
2. Open Server Manager.
3. Select Manage, and click Add Roles and Features.
4. When the Add Roles and Features Wizard begins, click Next.
5. Select Role-based or feature-based installation, and click Next.
6. Select the Active Directory FDQN, and click Next.
7. At the server rolls menu, select Active Directory Certificate Services.
8. When prompted, click Add Features, and click Next.
9. Leave Select features as is, click Next.
10. At the Active Directory Certificate Services introduction page, click Next.
11. Select Certificate Authority and Certificate Authority Web Enrollment.
12. When prompted, click Add Features, and click Next.
13. Click Next two more times, click Install, and click Close.
14. In Server Manager, click the yellow triangle icon for Post-deployment configuration.
15. On the destination server, click Configure Active Directory Certificate Services.
16. Leave credentials as test\administrator, and click Next.
17. Select Certificate Authority and Certificate Authority Web Enrollment, and click Next.
18. Select Enterprise CA, and click Next.
19. Select Root CA, and click Next.
20. Select Create a new private key, and click Next.
21. Select SHA256 with a 2048 Key length, and click Next.
22. Leave the names fields and defaults, and click Next.
23. Change expiration to 10 years, and click Next.
24. Leave Certificate database locations as default. Click Next.
25. Click Configure.
26. When the configuration finishes, click Close.
27. Open a command prompt, and type `ldp`
28. Click Connection, connect.
29. Type the Active Directory FDQN for server.
30. Change the port to `636`
31. Check SSL, and click OK.

Configuring secure LDAP on the Active Directory Server

1. Open administrative tools→Certification Authority.
2. Under the Active Directory server FQDN, right-click Certificate Templates, and select Manage. Right-click Kerberos Authentication, and select Duplicate Template.
3. Click Request Handling.
4. Check the box for Allow private key to be exported, and click OK.
5. Right-click the new template, and rename it to `LDAPoverSSL`
6. Return to the Certificates console. In the right pane, right-click New→Certificate Template to issue.
7. Select LDAPoverSSL, and click OK.

Setting up VMware Horizon 7 Composer on the composer VM (legacy environment only)

We completed the steps in this section on the legacy environment only. For the legacy environment, we deployed two templates: a Horizon View server and a SQL server. We gave our legacy SQL server an additional 90GB hard disk for the SQL installation, and then we initialized and mounted the drive as an OS volume.

Installing SQL 2019 Enterprise and Microsoft SQL Server Management Studio

1. On the infra server, deploy a Windows Server VM from the template using the appropriate specs from Table 7 for composer, and log in as an administrator.
2. Download en_sql_server_2019_enterprise_x64_dvd_5e1ecc6b, and open Setup.exe.
3. Select installation, and click New SQL Server stand-alone installation or add features to an existing installation.
4. In the SQL Server 2019 Setup, select Use Microsoft Update to check for updates, and click Next.
5. Enter a product key, and click Next.
6. Accept the License terms, and click Next.

7. For Feature Selection, select Database Engine Services, Full-Text and Semantic Extractions for key phrases, Client Tools Connectivity. Click the link to Download Reporting Services.
8. Click download for Microsoft SQL Server Reporting Services 2017.
9. Click SQLServerREportingServices.exe.
10. Click Install Reporting Services.
11. Leave the default free edition, and click Next.
12. Accept the license terms, and click Next.
13. Select Install Reporting Services only, and click Next.
14. Leave the defaults for Install location, and click Install.
15. Once the process completes, click Close.
16. Return to the SQL Server 2019 Setup wizard, and click Next.
17. On the Instance Configuration screen, leave the default instance, and click Next.
18. On the Server Configuration screen, change the Startup Types to Automatic. Click Next.
19. On the Server Configuration screen, select Mixed Mode, add the current user, and enter a password for the sa account. Click Data Directories.
20. Change the Data root directory to the additional drive. Click Next.
21. Click Install. Once complete, click Close.

Installing SQL Management Tools

1. In the SQL Server Installation Center, click Install SQL Server Management Tools.
2. Click Download SQL Server Management Studio 18.9.2.
3. Run SSMS-Setup-ENU.
4. Click Install.
5. Once complete, click restart.

Configuring SQL Server

1. Open SQL Server 2019 Configuration Manager.
2. Click SQL Server services→SQL Server Browser, right-click, and click Properties.
3. In the service tab, change the start mode to automatic, and click OK.
4. Right-click SQL Server Browser, click Start, and close SQL Server Configuration Manager.

Creating a SQL Express Database for composer and an ODBC connection on the composer VM (Legacy environment only)

1. Open SQL Server Management Studio.
2. Select windows authentication, and click Login.
3. In the Object Explorer, right-click the SQL Server, and click Properties.
4. Click Security.
5. Under Server authentication, select SQL Server and Windows Authentication mode.
6. Click OK.
7. In the Object Explorer, right-click SQL Server, and click Restart.
8. In the security tab login, right-click, create a user named composer, click server roles, select sysadmin, and click OK.
9. Right-click the databases folder, and click New database.
10. Name the database `composer` and select the composer user as owner.
11. Click OK, and close SQL Server Management Studio.
12. Select Run, and type `odbcad64.exe`
13. Press Enter.
14. Click the system DSN tab.
15. Click Add.
16. Click SQL Server Native Client 11, and click Finish.
17. In the Create a New Data Source to SQL Server text box, type the connection name composer
18. For Server, select composer\sqlexpress, and click Next.
19. Change authentication to With SQL Server authentication using the composer login and password, and click Next.
20. Type `composer` for the Login ID, and type the appropriate password.
21. Click Next.
22. Click Finish.
23. Click Test Data Source…
24. To create the Composer ODBC connection, click OK.

Configuring the VMware Horizon environment

The following steps are required for both the legacy and newer-generation VMware Horizon environments.

Installing the VMware Horizon Connection Server on the Horizon Server VM

1. On the infra server, deploy a Windows Server VM from the template using the appropriate specs for the Horizon Server from Table 7 for view, and log in as an administrator.
2. Browse to the relevant VMware View installation media.
3. Click Run.
4. At the Welcome screen, click Next.
5. Agree to the End User License Agreement, and click Next.
6. Keep the default installation directory, and click Next.
7. Select View Standard Server, and click Next.
8. At the Data Recovery screen, enter a backup password, and click Next.
9. Allow View Server to configure the Windows firewall automatically, and click Next.
10. Authorize the local administrator to administer View, and click Next.
11. Choose whether to participate in the customer experience improvement program, and click Next.
12. On the Ready to Install the Program screen, leave General, and click Install.
13. To finish installing View Connection Server, complete the installation wizard.
14. Click Finish.
15. Reboot server.
16. Join the VM to the test.local domain.

Configuring the VMware Horizon Connection Server on the Horizon Server VM

1. Open a web browser, and navigate to http://<view connection1 FQDN>/admin.
2. Log in as administrator.
3. Under Settings→Product Licensing and Usage, click Edit License…
4. Enter a valid license serial number, and click OK.
5. Under Settings→Servers, in the vCenter Servers tab, click Add…
6. Enter vCenter server credentials, and edit the following settings:
   - Max concurrent vCenter provisioning operations: 20
   - Max concurrent power operations: 50
   - Max concurrent View Composer maintenance operations: 20
   - Max concurrent View Composer provisioning operations: 20
   - Max concurrent Instant Clone Engine provisioning operations: 20
7. Click Next.
8. At the Storage screen, deselect Reclaim VM disk space and Enable View Storage Accelerator. Click Next.
9. **On the legacy environment only:** At the View Composer screen, select Standalone View Composer Server. Enter the server address and credentials, and click Next.
10. At the ready to complete screen, click Finish.

Testing transactional database performance with DVD Store 3

We used the following steps to configure the test VMs for DVD Store 3. We deployed eight VMs in each environment with the following settings:

- 8 vCPUs
- 32 GB of RAM
- 1 x 100GB VMDK for the OS
- 1 x 100GB VMDK for SQL Data on a separate VMware Paravirtual SCSI controller
- 1 x 30GB VMDK for SQL Log on a separate VMware Paravirtual SCSI controller
- 1 VMXNET adapter on the private network

Installing Microsoft Windows Server 2022 Datacenter Edition (Newer-generation environment only)

1. Boot the VM to a Microsoft Windows Server 2022 installation ISO.
2. Click Install.
3. When prompted to Activate Windows, indicate that you don't have a product key.
4. Select Windows Server Datacenter (Desktop Experience), and click Next.
5. Click the box to accept the license terms, and click Next.
6. Select Custom: Install Windows only (advanced), and click Next.
7. After the server reboots, enter a password for the Administrator account, and click Finish.
8. Log into the Administrator account.
9. For the networks question, click Yes.
10. In the Server Manager application, click Local Server.
11. Click Computer Name, and change it to the desired name.
12. When Server Manager starts, on the toolbar, select Manage, and select Server Manager Properties.
13. Check the box to not start Server Manager automatically at logon, and click OK.
14. On the Server Manager application, click Local Server.
15. On the Windows Firewall line, click Domain: Off.
16. In the Control Panel window, click Turn Windows Firewall on or off, turn the firewall off for all three networks, and click OK. Close the Control Panel window.
17. On the Remote Desktop line, click Disabled, and on the pop-up, click Allow remote connections. Click OK twice.
18. On the Feedback & Diagnostics line, click Settings, set the Feedback drop-down to Never, set the Diagnostics drop-down to Full, and close the Settings window.
19. On the IE Enhanced Security Configuration line, click On, turn it off for both Administrators and Users, and click OK.
20. Select your desired Time Zone.
21. On the Windows Defender line, click Real-Time Protection: On, turn all options off, and close the Settings window.
22. Close the Server Manager application.
23. Open the Settings window, and select Update & Security.
24. Click Check for updates. The VM will download and apply patches. This will likely be a long process.
25. Restart if necessary, and continue applying patches until there are no more available.
26. Navigate to the Services application, set the Windows Update service to Disabled, and turn it off.

Installing SQL Server 2019 (Newer-generation environment only)

1. Attach the installation media ISO for SQL Server 2019 to the VM.
2. Click Run SETUP.EXE. If Autoplay does not begin the installation, navigate to the SQL Server 2019 DVD, and double-click it.
3. In the left pane, click Installation.
4. Click New SQL Server stand-alone installation or add features to an existing installation.
5. Specify Evaluation as the edition you are installing, and click Next.
6. To accept the license terms, click the checkbox, and click Next.
7. Click Use Microsoft Update to check for updates, and click Next.
8. At the Feature Selection screen, select Database Engine Services, Full-Text and Semantic Extractions for Search, Client Tools Connectivity, and Client Tools Backwards Compatibility.
9. Click Next.
10. At the Instance configuration screen, leave the default selection of default instance, and click Next.
11. At the Server Configuration screen, accept defaults, and click Next.
12. At the Database Engine Configuration screen, select the authentication method you prefer. For our testing purposes, we selected Mixed Mode.
13. Enter and confirm a password for the system administrator account.
14. Click Add Current user. This may take several seconds.
15. Click Next.
16. At the Ready to Install screen, click Install.
17. Close the installation window.
18. In the SQL Server Installation Center, click on Install SQL Server Management Tools.
19. Click Download SQL Server Management Studio.
20. Click Run.
21. When the Microsoft SQL Server Management Studio screen appears, click Install.
22. When the installation completes, click Close.

Installing Windows Server 2016 (Legacy environment only)

1. Boot the VM to a Microsoft Windows Server 2016 installation ISO.
2. When prompted to boot from DVD, press any key.
3. When the installation screen appears, leave language, time/currency format, and input method as default, and click Next.
4. Click Install now.
5. When the installation prompts you, enter the product key.
6. Select Windows Server 2016 Datacenter Edition (Server with a GUI), and click Next.
7. Check I accept the license terms, and click Next.
8. Click Custom: Install Windows only (advanced).
9. Select Drive 0 Unallocated Space, and click Next. Windows will begin and restart automatically.
10. When the Settings page appears, fill in the Password and Reenter Password fields with the same password.
11. Log in with the password you set up in the previous step.
12. Enable RDP, disable the firewall, and run Windows Updates.

Installing SQL Server 2012 (Legacy environment only)

1. Boot the VM to the installation ISO for SQL Server 2012.
2. Click Run SETUP.EXE. If Autoplay does not begin the installation, navigate to the SQL Server 2012 ISO, and double-click it.
3. In the left pane, click Installation.
4. Click New SQL Server stand-alone installation or add features to an existing installation.
5. Select Enter the product key, and enter the product key. Click Next.
6. To accept the license terms, click the checkbox, and click Next.
7. To check for updates, click Use Microsoft Update, and click Next.
8. To install the setup support files, click Install.
9. If no failures display, click Next.
10. At the Setup Role screen, choose SQL Server Feature Installation, and click Next.
11. At the Feature Selection screen, select Database Engine Services, Full-Text and Semantic Extractions for Search, Client Tools Connectivity, Client Tools Backwards Compatibility, Management Tools – Basic, and Management Tools – Complete.
12. Click Next.
13. At the Installation Rules screen, after the check completes, click Next.
14. At the Instance configuration screen, leave the default selection of Default instance, and click Next.
15. At the Server Configuration screen, choose NT Service\SQLSERVERAGENT for SQL Server Agent, and choose NT Service\MSSQLSERVER for SQL Server Database Engine. Change the Startup Type to Automatic. Click Next.
16. At the Database Engine Configuration screen, select the authentication method you prefer. For our testing purposes, we selected Mixed Mode.
17. Enter and confirm a password for the system administrator account.
18. Click Add Current user. This may take several seconds.
19. Click the Data Directories tab to relocate the system, user, and temp db files.
20. Change the location of the root directory to the D:\volume.
21. Click Next.
22. At the Error and usage reporting screen, click Next.
23. At the Installation Configuration Rules screen, check that there are no failures or relevant warnings, and click Next.
24. At the Ready to Install screen, click Install.
25. After installation completes, click Close.
26. Close the installation window.
27. Open SQL Server 2012 Configuration Manager, and expand Protocols for MSSQLSERVER.
28. Right-click Named Pipes, and choose Enabled.
29. Click OK, and restart the SQL service.
30. Add SQL server management studio v18.1.
31. Download and open SSMS-Setup-ENU.exe.
32. At the welcome screen, select the default install location, and click Install.
33. To complete the Microsoft SQL Management Studio setup, click Restart.

Configuring and running DVD Store 3

We generated the data using the Install.pl script included with DS3, providing the parameters for our 40GB database size and the database platform we used. We ran the Install.pl script on a utility system running Windows Server 2016 to generate the database schema. After processing the data generation, we built the 40GB database in Microsoft SQL Server and performed a full backup, storing the backup file locally on each test VM. We used that backup file to restore the database when necessary. The only modification we made to the schema creation scripts were the specified file sizes for our database. We explicitly set the file sizes higher than necessary to ensure that no file-growth activity would affect the outputs of the test. Other than this file size modification, we created and loaded the database in accordance with DVD Store documentation.

1. Generate the data and create the database and file structure using database creation scripts in the DS3 download. Make size modifications specific to our 40GB database, and make the appropriate changes to drive letters.
2. Create database tables, stored procedures, and objects using the provided DVD Store scripts.
3. Set the database recovery model to bulk-logged to prevent excess logging.
4. Load the data we generated into the database. For data loading, use the import wizard in SQL Server Management Studio. Where necessary, retain options from the original scripts, such as Enable Identity Insert.
5. Create indices, full-text catalogs, primary keys, and foreign keys using the database-creation scripts.
6. Update statistics on each table according to database-creation scripts, which sample 18 percent of the table data.
7. On the SQL Server instance, create a ds3user SQL Server login using the following Transact SQL (TSQL) script:

```
USE [master]
GO
CREATE LOGIN [ds3user] WITH PASSWORD=N'',
DEFAULT_DATABASE=[master],
DEFAULT_LANGUAGE=[us_english],
CHECK_EXPIRATION=OFF,
CHECK_POLICY=OFF
GO
EXEC master..sp_addsrvrolemember @loginame = N'ds3user',
@rolename = N'sysadmin'
USE [DS3]
CREATE USER [ds3DS3user] FOR LOGIN [ds3user]
EXEC sp_addrolemember N'db_owner', N'ds3DS3user'
USE [master]
CREATE USER [ds3masteruser] FOR LOGIN [ds3user]
EXEC sp_addrolemember N'db_owner', N'ds3masteruser'
```

8. Set the database recovery model back to full.
9. Create the necessary full text index using SQL Server Management Studio.
10. Create a database user, and map this user to the SQL Server login.
11. Perform a full backup of the database. This backup allows you to restore the databases to a pristine state.

Running the DVD Store 3 tests

We created a series of batch files, SQL scripts, and shell scripts to automate the complete test cycle from a controller Windows Server VM on our infrastructure server. Additionally, we used eight Windows Server VMs on our infrastructure sever as clients to run the DVD Store 3 driver remotely. DVD Store outputs an orders-per-minute metric, which is a running average calculated through the test. In this report, we report the last OPM that each target reported.

Each complete test cycle consisted of these general steps:

1. Clean up prior outputs from the target system.
2. Drop the database from the target.
3. Restore the database on the target.
4. Reboot the target.
5. Wait for a ping response from the server under test and the client system.
6. Let the test server idle for 10 minutes.
7. Start the DVD Store driver on the clients.

We used the following DVD Store 3 parameters for testing:

```
ds3sqlserverdriver.exe --target=<target _ IP> --ramp_rate=10 --run_time=30 --n_threads=32
    --db_size=40GB --think_time=0.00 --detailed_view=Y --warmup_time=15 --report_rate=1 --pct_
    newcustomers=20 --csv_output=<drivepath>
```

Testing VDI performance with VMware View Planner 4.6

We ran the VMware View Planner 4.6 benchmark standard workload to determine the maximum number of virtual desktop users a platform could support. We needed to install and set up a VMware Horizon 7 environment and supporting infrastructure. We deployed 100 virtual desktops on the system under test (SUT). We then ran the VMware View Planner 4.6 benchmark against it.

Deploying the VMware View Planner 4.6 test harness

1. Download the viewplanner-harness-4.6.0.0-16995088_OVF10.ova file from VMware.
2. From the vCenter client, select the infra host, and right-click Deploy OVF Template…
3. In the Deploy OVF Template wizard, select local file, and click Browse…
4. Select viewplanner-harness-4.6.0.0-16995088_OVF10.ova, click Open, and click Next.
5. Select a DataCenter, and click Next.
6. Select the Infra host, and click Next.
7. Review details, and click Next.
8. Accept the license agreements, and click Next.
9. Select the local DAS datastore, and click Next.
10. Select the private network, and click Next.
11. On the customize template screen, enter the initial root password, and either accept the defaults to use DHCP or configure the Networking Properties. We used DHCP.
12. Click Next, and click Finish to deploy the harness.
13. Power on the new VM, and note the IP address.

Configuring the VMware View Planner 4.6 test harness

Our steps only include adding the vCenter server and not the Horizon server, as we found that View Planner provided a more reliable experience with only one selected.

1. Open a browser, and navigate to http://<ip address of the harness>:3307/vp-ui/
2. Log in as follows:
   - Username: `vmware`
   - Password: `viewplanner`
3. Click Log in.
4. Click servers
5. Select infra, and click Add New.
6. Enter the following information:
   - Name = `vCenter`
   - IP = IP of vCenter
   - Type = `vcenter`
   - DataCenter = `Datacenter`
   - Domain = `vsphere.local`
   - Username = `administrator`
   - Password = SSO password for vCenter
7. Click Save.
8. Click Identity server.
9. Click Add new.
10. Enter the following information:
    - Name = `test.local`
    - IP = IP of the Active Directory server
    - Type = `microsoft_ad`
    - Username = `administrator`
    - Password = password for administrator@test.local
11. Click Save.

Deploying the Windows 10 Enterprise (x64) gold image VM

We created a Microsoft Windows 10 Enterprise VM; installed Microsoft Office 2016 Pro plus, Google Chrome, and Adobe® Reader DC (32-bit); and prepared the VM for cloning to create our 100 Windows 10 Client VMs. We deployed the VM on the cluster where we would later deploy the Horizon Pool, avoiding the need to reactivate Office on each VM.

1. Log into vCenter via the VMware web client.
2. Right-click the Virtual Machines tab, and select New Virtual Machine.
3. Select Create a new virtual machine.
4. Assign the name `view-gold`, and click Next.
5. Select the SUT cluster, and click Next.
6. Select the local DAS datastore.
7. Choose compatible with ESXi 7.0 U2 and later, and click Next.
8. Choose Windows, choose Microsoft Windows 10 (64-bit), and click Next.
9. For CPUs, select 2 CPUs, 4 GB RAM, 90 GB Disk, and click Next.
10. Click Finish.
11. Right-click the VM, and select Edit Settings.
12. Click the CD/DVD Drive drop-down, and select Datastore ISO file.
13. Browse to the Microsoft Windows 10 x64 installation disk ISO.
14. Click Connect...
15. Click OK.
16. Power on the Microsoft Windows 10 VM.

Installing Windows 10 Enterprise (x64) on the gold image VM

1. When the installation prompts you, press any key to begin setup.
2. Click Install now.
3. Select Windows 10 Enterprise, and click Next.
4. Accept the license terms, and click Next.
5. Select Custom, and select the drive that will contain the OS.
6. Click Next.
7. Select the keyboard layout, and click Yes.
8. Click Skip a second keyboard layout.
9. Click Domain join instead.
10. Type `user` for the username, and click Next.
11. Do not enter a password, and click Next.
12. At the privacy settings screen, click Accept.
13. To decline Cortana, click Not now.
14. Using vCenter, connect the media and Install VMware Tools. During installation, select Complete Installation. For more information, visit http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=340.
15. Reboot the server.
16. Right-click the Start button, and click System.
17. Click Rename this PC, and enter a new name for the VM.
18. Click Next, and click Restart now.
19. Connect the machine to the internet, and install all available Windows updates. Restart as necessary.
20. Join the domain, and shutdown the VM.

Editing the VMX file

1. Browse to the VMX file location for the Windows 10 golden VM.
2. Download the VMX file, and open it using a text editor.
3. After the final line, add "`monitor_control.pseudo_perfctr="1".`
4. `Save the file, and overwrite the current VMX file on the datastore.`

Installing the VMware Horizon agent on the gold image VM

1. Start the Windows 10 gold image VM.
2. Navigate to the VMware Horizon View media, and run the VMware Horizon Agent file.
3. Click Run.
4. At the Welcome screen, click Next.
5. Accept the VMware end user license agreement, and click Next.
6. Select defaults, and click Next.
7. Click Install.
8. Click Yes to reboot.

Installing VMware View Planner agent on the gold image VM

1. Double-click viewplanner-agent-4.6.0.0-16995088.exe.
2. Click Next.
3. Accept the end user license agreement.
4. Click Next.
5. Enter the IP address of the View Planner harness, and click Next.
6. Wait for the installer to complete, and click Finish.
7. Reboot the VM.

Installing Google Chrome version 92.0.4515.107 on the gold image VM

1. Download the newest version of Chrome.
2. Double-click the installer executable, and click Run.
3. Close Chrome.
4. Find the Selenium driver matching your current version of Chrome at chromedriver.chromium.org/downloads. We used v94.0.4606.41.
5. Create a folder named [baseVersion_fullVersion] inside C:\viewplanner\lib\chrome_driver.
6. Extract chromedriver from the downloaded zip, and copy it to the newly created folder.

Installing Office Professional Plus 2019 on the gold image VM

1. Run the Microsoft Office Professional Plus 2019 media en_office_professional_plus_2019_x86_x64_dnd_7ea28c99.iso.
2. Complete the installation using all defaults.
3. Open Windows Update, and click Advanced options.
4. Enable Receive updates for other Microsoft products, and click the back button.
5. Click Check for updates, and reboot if necessary.
6. Run Word, accept the EULA and activate Office by entering your license.

Installing Adobe Reader DC version 2020.012.20043 on the gold image VM

1. Download and install Adobe Reader from http://acrobat.adobe.com. Use the "Do you have a different language or operating system?" option, and select the following:
   - Step 1: Windows 10
   - Step 2: English
   - Step 3: Reader DC: Reader DC 2021.007.20091 English for Windows.
     - Do not select the 64-bit version, as View Planner requires the 32-bit version.
2. Disable any McAfee add-ons, and click Download Acrobat Reader.

Setting Windows Media Player as default Video Player on the gold image VM

1. Click Start, and select Settings.
2. Click Apps, and in the left pane, click Default Apps.
3. Under Video player, select Windows Media Player.

Disabling Windows Updates on the gold image VM

1. Click Start, and type `Services`
2. Scroll down to Windows Update, right-click it, and select Properties.
3. Under Startup type, select Disabled.
4. Under Service status, click Stop. Click OK.

Disabling Windows Firewall on the gold image VM

1. Click Start, and type `Firewall`
2. Select Firewall & network protection.
3. Turn off Microsoft Defender Firewall for Domain, Private, and Public networks.

Configuring Regedit to Skip License Activation on the gold image VM

1. Click Start→Run, and type `regedit`
2. Browse to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmware-viewcomposer-ga.
3. Right-click Skip License Activation, and click Modify…
4. Change the value from 0 to 1. Click OK.

Configuring Regedit for autologin on the gold image VM

1. Click Start→Run, and type `regedit`
2. Browse to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
3. Double-click the DefaultDomainName entry, type your domain, and click OK.
4. Double-click the DefaultUserName entry, type your username (Administrator), and click OK.
5. Double-click the DefaultPassword entry, type your password, and click OK. If it doesn't exist, complete the following procedure
    a. On the Edit menu, click New→String Value.
    b. Type `DefaultPassword`, and press Enter.
    c. Double-click DefaultPassword.
    d. In the Edit String dialog, type your password, and click OK.
6. Double-click AutoAdminLogon.
7. In the Edit String dialog box, type `1`, and click OK.

Configuring Regedit to disable lock screen on the gold image VM

1. Click Start→Run, and type `regedit`
2. Browse to HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
3. Right-click Windows.
4. Click New→Key.
5. Name the new key `Personalization` and click Enter.
6. In the Personalization folder, in the right pane of the Registry Editor, right-click, and select New→DWORD (32-bit) Value.
7. Name the value `NoLockScreen` and click Enter.
8. Double-click NoLockScreen.
9. In the Edit DWORD dialog box, type `1`. Click OK.

Configuring Regedit to suppress MS Office 2019 First Things First message on the gold image VM

1. Click Start→Run, and type `regedit`
2. Browse to HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\General.
3. Double-click shownfirstrunoptin.
4. In the Edit DWORD dialog box, type `0`. Click OK.
5. Browse to HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\FirstRun.
6. On the Edit menu, click New→DWORD (32-bit) Value.
7. Name the value BootedRTM and click Enter.
8. Double-click BootedRTM.
9. In the Edit DWORD dialog box, type `1`. Click OK.
10. Create a new key at HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Registration.
11. On the Edit menu, click New→DWORD (32-bit) Value.
12. Name the value AcceptAllEulas and click Enter.
13. Double-click AcceptAllEulas.
14. In the Edit DWORD dialog box, type `1`. Click OK.

Optimizing the Windows 10 gold image VM

1. Download the Windows optimization tool from VMware at https://flings.vmware.com/vmware-os-optimization-tool.
2. Extract the zip file, and run VMwareHorizonOSOPtimizationTool-x86_64-2107.exe as administrator.
3. Click Template, and select VMWare\Windows 10.
4. Click Analyze.
5. Select all suggestions, and click Optimize.
6. When settings finish applying, reboot the VM.

Finalizing the Windows 10 gold image VM

1. In vCenter, shut down the Windows 10 gold image.
2. Right-click the VM, and select Take a snapshot.
3. Name the snapshot `Gold Image` and click OK.

Deploying virtual desktops using VMware Horizon Connection Server

1. Open the Horizon View Administrator.
2. Log in as an administrator.
3. Under Setting→Domains, click Add.
4. Add the domain administrator account and credentials, and click OK.
5. Under Inventory, click Desktops, and click Add.
6. If you see a More Information popup, click Ignore.
7. Select Automated Desktop Pool, and click Next.
8. Select Instant Clone, and click Next.
9. Select Dedicated, and leave Enable Automatic Assignment checked.
10. On the Storage Policy Management page, leave defaults, and click Next.
11. Type `pool` for the pool ID and display name, and click Next.
12. Under Naming Pattern, enter an appropriate name pattern for the pool. Note this for the View Planner testing settings in the next section.
13. Select All Machines Up-Front.
14. Under Pool Sizing, type the max number of desktops and the number of spare (power on) desktops, and click Next.
15. Under vCenter Settings, select the following depending on where you are deploying virtual machines, and click Next:
    - Golden Image in vCenter
    - Snapshot
    - VM folder location
    - Cluster
    - Resource pool
    - DataStore
16. On the Desktop Pool Settings page, leave defaults, and click Next.
17. On the Remote Display Protocol page, leave defaults, and click Next.
18. On the Advanced Storage Options page, leave defaults, and click Next.
19. Under Guest customization, accept the following defaults:
    - Domain: test.local
    - AD container: CN=Computers)
    - Use Clone Prep
20. Click Next.
21. Click Submit. (Note: Because this testing is local, you do not need to specify any entitlements.)

Creating the VMware View Planner benchmark run profiles

1. Log into the View Planner run harness GUI: [runharness IP]/admin.
2. Log in with the following credentials:
   - Username: `vmware`
   - Password: `viewplanner`
3. In the left pane, click Run Profile.
4. In the top right of the window, click Add New.
5. Add a name for the profile.
6. Select local as the Run Mode.
7. Enter the desired number of VMs for VM/Session Count.
8. Leave Iteration Count at 5.
9. Leave Rampup Time blank, and leave Think Time at 5. Click Next.
10. Enter a name for the workgroup. Note that it cannot start with a number.
11. Select the Workprofile you wish to test with. We selected (Standard)***
12. Leave Percent VM at 100%.
13. Next to Desktop VM, click the plus sign.
14. Enter a prefix name that matches the prefix you used in the pool above.
15. From the Infraserver dropdown, select your vCenter server.
16. Leave Vdiserver Name unfilled, and click the green check. Click Next.
17. Review your profile, and click Finish.

Running the VMware View Planner benchmark

1. Open a browser to http:/<viewplanner IP address>/admin, and log in as vmware.
2. Click Run, and click NEW RUN.
3. Select the Run Profile and Run Name, and click Start.

Testing Kubernetes performance with Weathervane 2.1 (newer-generation environment only)

Our newer-generation environment uses two Tanzu Kubernetes Grid (TKG) clusters to run Weathervane 2.1: an application cluster and a workload driver cluster. Weathervane is an application-level performance benchmark which runs a number of simulated users (WvUsers) while verifying that the built-in Weathervane quality-of-service (QoS) requirements remain unbroken. One cluster hosts the Weathervane benchmark application instances and the other hosts the Weathervane workload drivers. We deployed a run-harness auxiliary VM to a separate infrastructure host to run the benchmark and manage the testbed. We have listed the details of our workload driver control and worker nodes, as well as our application control and worker nodes in the VM specifications table at the beginning of this document.

We deployed Weathervane on the newer-generation cluster only. To support our Kubernetes cluster, we configured vSphere with Tanzu and deployed an Ubuntu VM. We managed vSphere with Tanzu using the Workload Management screen on the vSphere client. We've provided the details below.

Configuring our environment for vSphere with Tanzu

Enabling DRS on the target cluster

1. From the vSphere Client, navigate to the SUT cluster, and click Configure.
2. Under vSphere DRS, click Edit.
3. In the Edit Cluster Settings screen, click the toggle to enable vSphere DRS.
4. For the Automation Level, ensure that the setting is Fully Automated, and click OK.

To ensure even distribution of VMs with DRS enabled, we created VM/Host Groups, VM/Host Rules, and VM Overrides. You can complete this in the Configure menu for the cluster under test. We assigned three SQL Server VMs and 25 Horizon client VMs to each host.

Enabling HA on the target cluster

1. From the vSphere Client, navigate to the SUT cluster, and click Configure.
2. Under vSphere HA, click Edit.
3. In the Edit Cluster Settings screen, click the toggle to enable vSphere HA. Leave all defaults, and do not enable Proactive HA.

Creating a Distributed vSwitch and Port Group

1. From the vSphere Client, click Home→Networking.
2. Right-click the DvSwitch, and select Distributed Port Group→New Distributed Port Group.
3. Name it `Workload Network` and click Next.
4. Change the VLAN type to VLAN, and set the VLAN ID to VLAN 2. Click Next.
5. Click Finish.

Creating a DevOps user

1. From vSphere client, click Home→Administration.
2. In the left panel, click Users and Groups.
3. In the right panel, click Users, select the vsphere.local domain, and click Add.
4. Provide a username and password, and click Add.
5. For simplicity, we added the DevOps user to a group with Administrator privileges. Click Groups, and select the Administrators group. Click Edit.
6. Under Add Members, search for the user you just created, and add them to the Administrators group. Click Save.

Creating the HAProxy content library

1. Download the vSphere compatible HAproxy OVF (v0.2.0): https://github.com/haproxytech/vmware-haproxy.
2. From vSphere client, click Content Libraries in left menu pane.
3. In the Content Libraries panel on the right, click Create.
4. Name the content library `HAproxy-cl` and click Next.
5. Accept the default, and click Next.
6. Choose the storage location for the content library, and click Next.
7. Review, and click Finish.
8. Click on the newly created HAproxy-cl content library.
9. In the upper portion of the right panel for HAproxy-cl, click the actions pull-down menu, and select Import Item.
10. Change the selection to local file, and click the upload files button.
11. Browse to the location of the OVF file you downloaded in step 1, and click Open.
12. Click Import.

Creating the TKG content library

1. From vSphere client, in the left menu pane, click Content Libraries.
2. In the Content Libraries panel on the right, click Create.
3. Name the content library `TKG-cl` and click next
4. Select Subscribed content library, and use https://wp-content.vmware.com/v2/latest/lib.json for the subscription URL. Click Next.
5. Click Yes to verify.
6. Choose the storage location for the content library, and click Next.
7. Review, and click Finish.

Creating the storage tag

1. From the vSphere client, select Menu→Storage.
2. From the left pane, select the vSAN storage.
3. Under the Summary tab, locate the Tags panel, and click Assign.
4. Click Add Tag.
5. Name the tag `Tanzu`. Click Create New Category.
6. Give the category name `Tanzu Storage`. Clear all object types except Datastore, and click Create.
7. Use the Category pull-down menu to select Tanzu Storage, and click Create.
8. Check the box beside the newly created tag, and click Assign.

Creating VM storage policy

1. From the vSphere client, click Menu→Policies and Profiles.
2. In the left panel, click VM Storage Policies.
3. Click Create.
4. Create a new VM Storage policy named `tkg-clusters` and click Next.
5. Check the box for Enable tag based placement rules, and click Next.
6. Use the Tag Category pull-down menu to select the Tanzu Storage policy you created. Click Browse Tags.
7. Click the Tanzu checkbox, and click OK.
8. Click Next.
9. Review the compatible storage to make sure your storage target is marked as compatible, and click Next.
10. Click Finish.

Deploying HAProxy

We completed the steps below to host the HAProxy Content Library on the infrastructure server and storage.

1. From the vSphere client, click Menu→Content Libraries.
2. Click the HAproxy-cl library.
3. In the left panel, click OVF & OVA Templates, and in the panel below, right-click on haproxy template. Select New VM from This Template…
4. Provide a simple name–we used `HAProxy`–and select the Datacenter and/or folder you want to deploy to. Click Next.
5. Select the cluster or compute resource where you want to deploy the HAProxy VM, and click Next.
6. Review details, and click Next.
7. Check the box to accept all license agreements, and click Next.
8. Accept the default configuration, and click Next.
9. Select the target storage for the VM, and click Next. We selected the infrastructure storage.
10. Select VM Network for the private network, and choose a network for the workload network. Choose the workload network for the Frontend network, and click Next.
11. Complete the template using the following settings:

    - Appliance Configuration Section
        - Root Password: `Password1!`
        - Check the box for Permit Root Login.
        - Leave the TLS CA blank.
    - Network Configuration Section
        - Leave the default "haproxy.local"
        - Local DNS server: `192.168.0.10`
        - Management IP: `192.168.0.70/16`
        - Management Gateway: `192.168.0.1`
            - NOTE: The description asks for the workload network gateway address. You should enter the management gateway address instead.
        - Workload IP: `172.16.0.10/16`
        - Workload gateway: `172.16.0.1`
    - Load Balancing Section:
        - Load balancer IP ranges: `172.16.10.1/24`
        - Accept the default management port.
        - HAProxy User ID: `admin`
        - HAProxy password: `Password1!`
12. Click Next.
13. Review the summary, and click Finish. The deployment will take a few minutes to completely deploy and configure.
14. Power on the HAProxy VM.

Getting the certificate hash for the HAProxy server

1. Open an SSH session to the HAProxy management address and connect using root and Password1!
2. Type the following: `cat /etc/haproxy/ca.crt`
3. Copy the entire output (including the first and last lines). You will need this for step 7 in the next section.
4. Close the SSH session.

Configuring Workload Management

1. From the vSphere client, click Menu→Workload Management
2. Click Get Started.
3. Review the messages and warnings regarding supported configurations. Click Next.
4. Select the Cluster you want to enable workload management on, and click Next.
5. Choose the capacity for the control plane VMs. We chose Small. Click Next.
6. Choose the storage policy to be used for the control plane nodes. We chose tkg-clusters. Click Next.
7. Configure the Load Balancer section with the following:
   - Name: `haproxy`
   - Type: `HA proxy`
   - Data plane API Addresses: `192.168.0.70`
   - User name: `admin`
   - Password: `Password1!`
   - IP Address Ranges for Virtual Servers: `172.16.10.1 - 172.16.10.254`
   - Server Certificate Authority: Paste from step 3 in the previous section.
8. Click Next.
9. Configure the Management Network with the following:
   - Network: `VM Network`
   - Starting IP Address: `192.168.85.1`
   - Subnet Mask: `255.255.0.0`
   - Gateway: `192.168.0.1`
   - DNS Server: `192.168.0.10`
   - NTP Server: `192.168.0.10`
10. Click Next.
11. Configure Workload Network with the following:
    - Leave the default for Services addresses.
    - DNS Servers: `10.41.0.10`
12. Under Workload Network, click Add.
13. Accept default for network-1.
    - Port Group: `Workload Network`
    - Gateway: `192.168.0.1`
    - Subnet: `255.255.0.0`
    - IP Address Ranges: `192.168.1.65-192.168.1.126`
14. Click Save.
15. For TKG Configuration, use the following:
    - Click Add beside Add Content Library. Select the TKG-cl library and click OK.
16. Click Next.
17. Click Finish. The workload management cluster will deploy and configure. You may see apparent errors during configuration–these will resolve upon successful completion.

Configuring Kubernetes namespace for service deployment

1. In Workload Management, click Namespaces.
2. Click Create Namespace.
3. Select the target cluster, and provide a name. We used `tanzu-ns`. Click Create.
4. The new namespace is created. Click the Permissions tab and click Add.
5. Choose vSphere.local for the identity source. Search for the DevOps user you created. Select the "can edit" role. Click OK.
6. Click the Storage tab.
7. In the Storage Policies section, click Edit.
8. Select the tkg-clusters policy, and click OK. The environment is ready for connection and container deployment.

Installing and configuring Ubuntu VM for Tanzu Kubernetes Grid CLI

1. Log into vCenter, and from the Menu dropdown, click Storage.
2. Select datastore1, and click Files.
3. Click Upload Files, and upload the Ubuntu 18.04.5 ISO image.
4. Right-click the cluster, and click New Virtual Machine.
5. Click Next.
6. Enter a name for the VM, and click next.
7. Click Next.
8. Select datastore1, and click Next.
9. Click Next.
10. Select Linux from the Guest OS Family dropdown, select Ubuntu Linux (64 bit) from the guest OS version dropdown, and click Next.
11. Assign the VM two vCPUs, 8 GB of memory, and a 40 GB hard disk.
12. From the New CD/DVD Drive dropdown, select Datastore ISO File, and select the Ubuntu ISO you previously uploaded to the datastore. Ensure Connect At Power On is checked, and click Next.
13. Click Finish.
14. Power on the VM, and click Launch Remote Console.
15. Click Install Ubuntu.
16. Click Continue.
17. Select Minimal installation, and click Continue.
18. Click Install now.
19. Click Continue twice.
20. Enter your desired full name, computer name, username, and password, and click Continue.
21. Click Restart Now.

Creating the auxiliary Ubuntu VM

Installing the auxiliary Ubuntu VM

1. Install Ubuntu 18.04 LTS on an auxiliary VM running on the additional infrastructure server in the vSphere environment. The VM should have sufficient space on its root files system (100 GB suffices) to hold several Docker images.
2. Configure the Ubuntu VM so that it has two virtual network adapters: one in the management network and the other in the workload network.
3. Configure settings for networking on the Ubuntu VM, and verify that both adapters can reach their respective gateway addresses.

Installing Tanzu Kubernetes Grid Standalone version 1.3.1

1. Log onto the VM as the local user.
2. Install Docker 20 on Ubuntu following the instructions at https://docs.docker.com/engine/install/ubuntu/

```
sudo apt-get remove docker docker-engine docker.io containerd runc
    sudo apt-get update
    sudo apt-get install apt-transport-https ca-certificates curl gnupg lsb-release
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | \
      sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
echo "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] \
      https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | \
      sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update
    sudo apt-get install docker-ce docker-ce-cli containerd.io
```

3. Add root to the Docker group:

```
sudo usermod -a -G docker root
```

4. Log out and log back in as `root`.
5. Start Docker:

```
sudo service docker start
```

6. Create SSH keys:

```
ssh-keygen -t rsa -b 4096 -C root@auxbox
```

Installing Kubectl Plugin for vSphere

1. Open a browser on the VM, and navigate to the IP of one of the three SupervisorControlPlane VMs. In our environment, the first control plane VM is at 10.218.201.201.
2. Click Advanced, and click Accept the Risk and Continue to bypass the certificate warning.
3. Click Download CLI Plugin Linux.
4. Select Save File, and click OK.
5. Open the Files app, and navigate to the Downloads folder.
6. Copy the file onto the auxiliary Ubuntu VM.
7. Right-click vsphere-plugin.zip, and select Extract Here.
8. Open a terminal, and navigate to the vsphere-plugin binary within the extracted folder:

```
cd Downloads/vsphere-plugin/bin
```

9. Make the vsphere-plugin binary executable, and add it to PATH:

```
  sudo mv kubectl-vsphere /usr/local/bin/
  sudo mv kubectl /usr/local/bin/
```

Creating the TKG clusters

1. Log out, and change the context:

```
kubectl vsphere logout
kubectl vsphere login --insecure-skip-tls-verify --server=https://192.168.85.1 --vsphere-
    username=administrator@vsphere.local --tanzu-kubernetes-cluster-name=tkg-appcluster-01 --tanzu-
    kubernetes-cluster-namespace=tanzu-ns
```

2. Create the application and driver clusters. You may review the corresponding configuration at the end of this document.

```
kubectl -f apply appcluster.yaml
kubectl -f apply dricluster.yaml
```

3. Log into the app cluster, and configure the permissions using the following commands. You may review the tkc-psp.yaml file at the end of this document.

```
Kubectl vsphere logout
kubectl vsphere login --insecure-skip-tls-verify --server=https://192.168.85.1 --vsphere-
    username=administrator@vsphere.local --tanzu-kubernetes-cluster-name=tkg-appcluster-01 --tanzu-
    kubernetes-cluster-namespace=tanzu-ns
kubectl vsphere login --insecure-skip-tls-verify --server=https://192.168.85.1 --vsphere-
    username=administrator@vsphere.local --tanzu-kubernetes-cluster-name=tkg-dricluster-01 --tanzu-
    kubernetes-cluster-namespace=tanzu-ns
kubectl config use-context tkg-appcluster-01
kubectl -f apply tkc-psp.yaml
kubectl config use-context tkg-dricluster-01
kubectl -f apply tkc-psp.yaml
```

Running the Weathervane tests

In this section, we list the steps to run the VMware Weathervane benchmark on the system under test. We used the continuous run option with 2,500 users.

Running the tests

1. Log into the run-harness instance.
2. Download Weathervane using the following command:

```
git clone https://github.com/vmware/weathervane
```

3. Navigate to the Weathervane folder.
4. Open the run configuration file with the following command:

```
vim weathervane.config.k8s.quickstart
```

5. Edit the file with the parameters we described in the weathervane.config.k8s.2500users file in the Appendix of this document. For additional information on the configuration parameters, visit https://github.com/vmware/weathervane/blob/master/doc/userDocs/usersGuide.md#quickstart-guide
6. Save, and exit the text editor.
7. Run the test with the following command:

```
sudo ./runWeathervane.pl -configFile=weathervane.config.k8s.2500users
```

Appendix: Files we used in our testing

We used the following configuration files to run Weathervane:

- appcluster.yaml
- dricluster.yaml
- tkc-psp.yaml
- weathervane.config.k8s.2500users

appcluster.yaml

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TanzuKubernetesCluster
metadata:
  name: tkg-appcluster-01
  namespace: tanzu-ns
spec:
  distribution:
    version: 1.19.7+vmware.1-tkg.1.fc82c41
  topology:
    controlPlane:
      count: 3
      class: guaranteed-medium
      storageClass: tkg-clusters
    workers:
      count: 4
      class: best-effort-medium
      storageClass: tkg-clusters
  settings:
    storage:
      defaultClass: tkg-clusters
    network:
      cni:
        name: antrea
      services:
        cidrBlocks: ["172.19.0.0/16"]
      pods:
        cidrBlocks: ["172.18.0.0/16"]
```

dricluster.yaml

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TanzuKubernetesCluster
metadata:
  name: tkg-dricluster-01
  namespace: tanzu-ns
spec:
  distribution:
    version: 1.19.7+vmware.1-tkg.1.fc82c41
    #version: 1.21.2+vmware.1-tkg.1.ee25d55
  topology:
    controlPlane:
      count: 3
      class: guaranteed-medium
      storageClass: tkg-clusters
    workers:
      count: 4
      class: best-effort-medium
      storageClass: tkg-clusters
  settings:
    storage:
      defaultClass: tkg-clusters
    network:
      cni:
        name: antrea
      services:
        cidrBlocks: ["172.21.0.0/16"]
      pods:
        cidrBlocks: ["172.20.0.0/16"]
```

tkc-psp.yaml

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: psp:privileged
rules:
- apiGroups: [‘policy']
  resources: [‘podsecuritypolicies']
  verbs:     [‘use']
  resourceNames:
  - vmware-system-privileged
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: all:psp:privileged
roleRef:
  kind: ClusterRole
  name: psp:privileged
  apiGroup: rbac.authorization.k8s.io
subjects:
- kind: Group
  name: system:serviceaccounts
  apiGroup: rbac.authorization.k8s.io
```

weathervane.config.k8s.2500users

```
{
  "description" : "small",
  "configurationSize": "xsmall",
  "runStrategy" : "fixed",
  "users" : 2500,
  "runForever" : true,
  "numAppInstances" : 1,
  "dockerNamespace" : "[dockeruser]",
  "createNamespaces" : true,
  "prepareConcurrency" : 4,
  "reloadOnFailure" : true,
  "kubernetesClusters" : [
    {
      "name" : "appCluster",
      "kubeconfigFile" : "/root/.kube/config",
      "kubeconfigContext" : "tkg-appcluster-01",
    },
    {
      "name" : "driverCluster",
      "kubeconfigFile" : "/root/.kube/config",
      "kubeconfigContext" : "tkg-dricluster-01",
    },
  ],
  "driverCluster" : "driverCluster",
  "appInstanceCluster" : "appCluster",
  "appIngressMethod" : "nodeport-internal",
  "cassandraDataStorageClass" : "tkg-clusters",
  "postgresqlStorageClass" : "tkg-clusters",
  "nginxCacheStorageClass" : "tkg-clusters",
}
```

Read the report at https://facts.pt/CF42nPk ▶

This project was commissioned by Dell Technologies.