The science behind the report:

Equip your Dell EMC PowerEdge R740xd servers with Intel Optane persistent memory to support more VDI users

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 *Equip your Dell EMC PowerEdge R740xd servers with Intel Optane persistent memory to support more VDI users*.

We concluded our hands-on testing on January 6, 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 November 8, 2020 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

Table 1: Results of our testing

	1.5TB Intel® Optane™ PMem + 384GB DRAM configuration	768GB DRAM configuration
3GB memory per desktop (1.5GB reserved)		
Number of desktops	266	256
CPU utilization (percentage)	100.00%	100.00%
Response time at max capacity (ms)	1,552	1,722
6GB memory per desktop (6GB reserved)		
Number of desktops	236	117
CPU utilization (percentage)	96.15%	46.30%
Response time at max capacity (ms)	1,308	779
12GB memory per desktop (12GB reserved)		
Number of desktops	118	58
CPU utilization (percentage)	47.68%	24.47%
Response time at max capacity (ms)	787	709

System configuration information

Table 2: Detailed information for the systems we tested.

System configuration information	Dell EMC™ PowerEdge™ R740xd	
BIOS name and version	Dell 2.8.2	
Non-default BIOS settings	N/A	
Operating system name and version/build number	VMware™ ESXi™ 7.0.1 (Build 16850804)	
Date of last OS updates/patches applied	9/1/2020	
Power management policy	Performance	
Processor		
Number of processors	2	
Vendor and model	Intel Xeon® Gold 6248R	
Core count (per processor)	24	
Core frequency (GHz)	3.0	
Stepping	N/A	
Memory module(s)	DRAM-only configuration	Intel Optane persistent memory + DRAM configuration
Memory type 1: Intel Optane persistent memory		
Total memory in system (GB)	N/A	1,536
Number of memory modules	N/A	12
Vendor and model	N/A	Intel NMA1XXD128GPS
Size (GB)	N/A	128
Type	N/A	Optane PMem
Memory type 2: DRAM		
Total memory in system (GB)	768	384
Number of memory modules	24	12
Vendor and model	Samsung® M393A4K40BB1-CRC0Q	Samsung M393A4K40BB1-CRC0Q
Size (GB)	32	32
Type	DDR4 DRAM	DDR4 DRAM
Speed	2,667	2,667
Storage controller		
Vendor and model	Dell HBA330 Adp	
Cache size	0 MB	
Firmware version	16.17.03.05	
Driver version	N/A	

System configuration information	Dell EMC™ PowerEdge™ R740xd
Local storage (type A)	
Number of drives	2
Drive vendor and model	Intel Optane SSD DC P4800X Series SSDPE21K375GAT
Drive size	375 GB
Drive information	NVMe™
Local storage (type B)	
Number of drives	6
Drive vendor and model	Intel SSD D3 Series SSDSC2KB038T8R
Drive size	3.84 TB
Drive information	SATA SSD
Network adapter	
Vendor and model	Intel x710 10 GbE SFP+
Number and type of ports	2 x 10GbE
Driver version	I40en
Cooling fans	
Vendor and model	UltraFlo V60E12BS10M3-07A02
Number of cooling fans	6
Power supplies	
Vendor and model	Dell L1100E-S1
Number of power supplies	2
Wattage of each (W)	1,100

Login VSI results charts

Figure 1: Login VSI results, 3GB memory per desktop/1.5GB reserved, for the 1.5 TB Intel Optane PMem + 384GB DRAM configuration.

Figure 2: Login VSI results, 3GB memory per desktop/1.5GB reserved, for the 768GB DRAM configuration.

Figure 3: Login VSI results, 6GB memory per desktop/6GB reserved, for the 1.5 TB Intel Optane PMem + 384GB DRAM configuration.

Figure 4: Login VSI results, 6GB memory per desktop/6GB reserved, for the 768GB DRAM configuration.
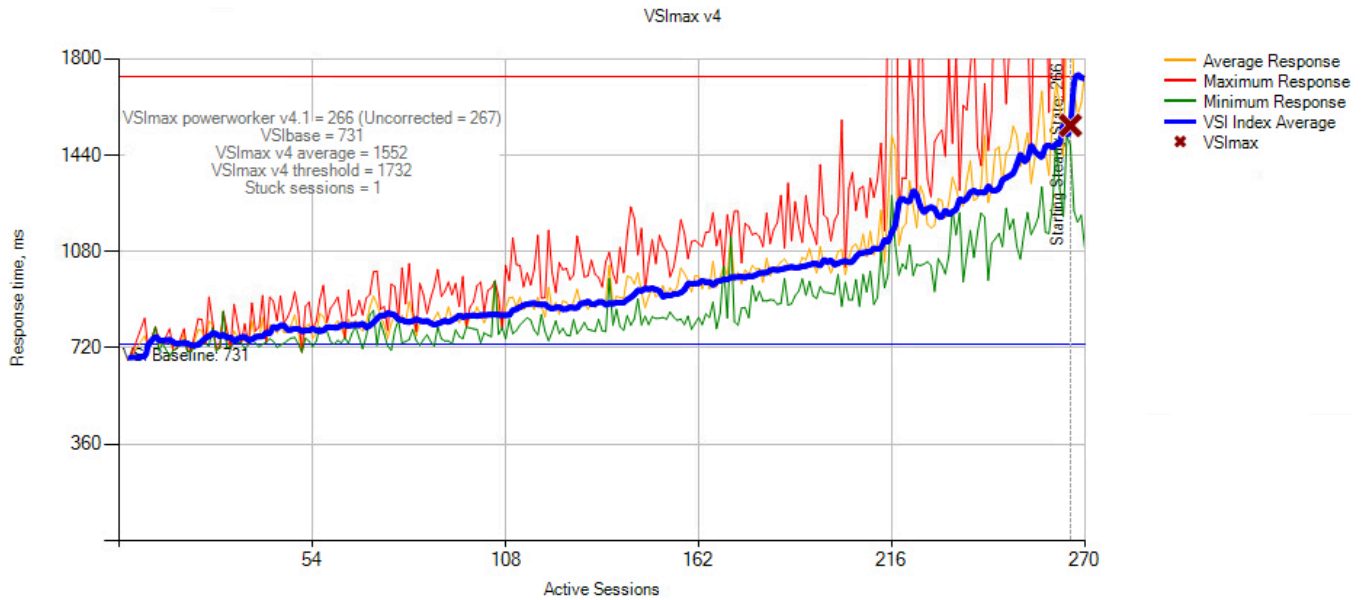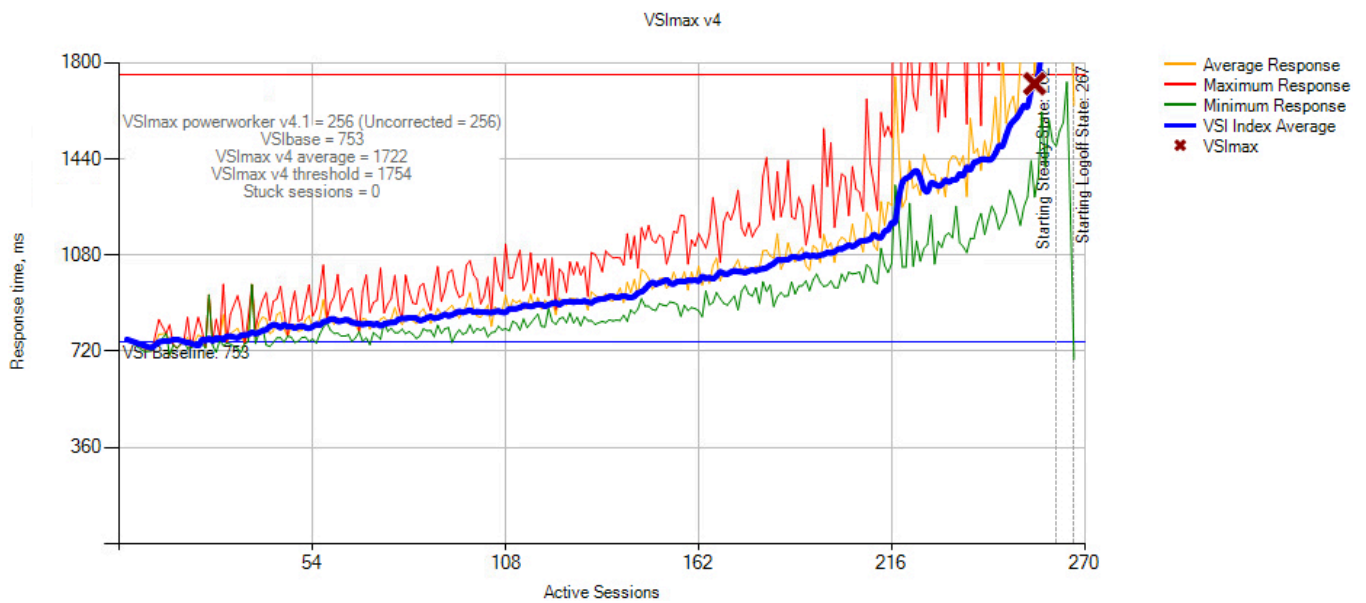
Figure 5: Login VSI results, 12GB memory per desktop/12GB reserved, for the 1.5 TB Intel Optane PMem + 384GB DRAM configuration.

Figure 6: Login VSI results, 12GB memory per desktop/12GB reserved, for the 768GB DRAM configuration.
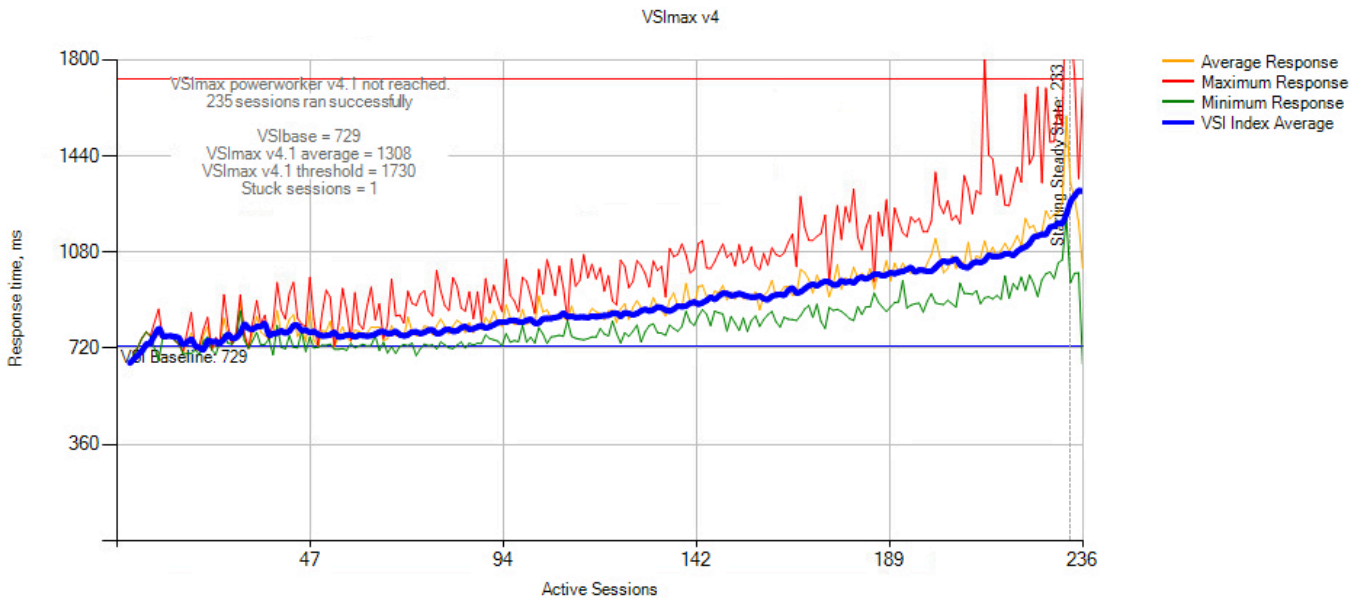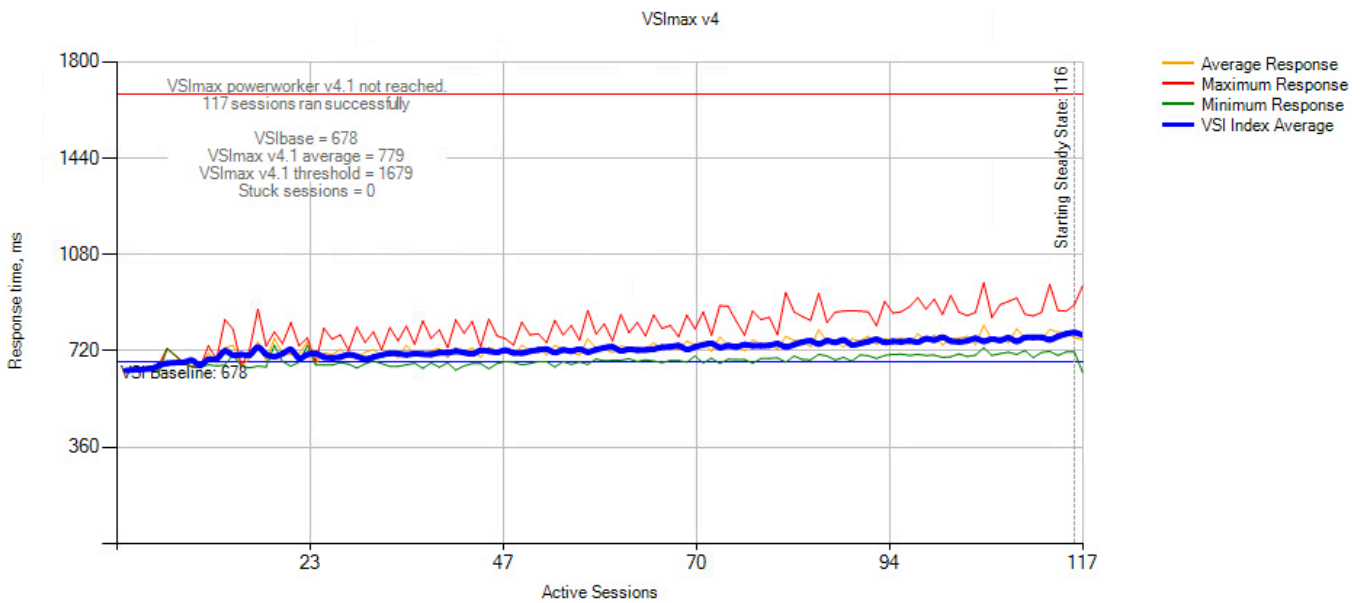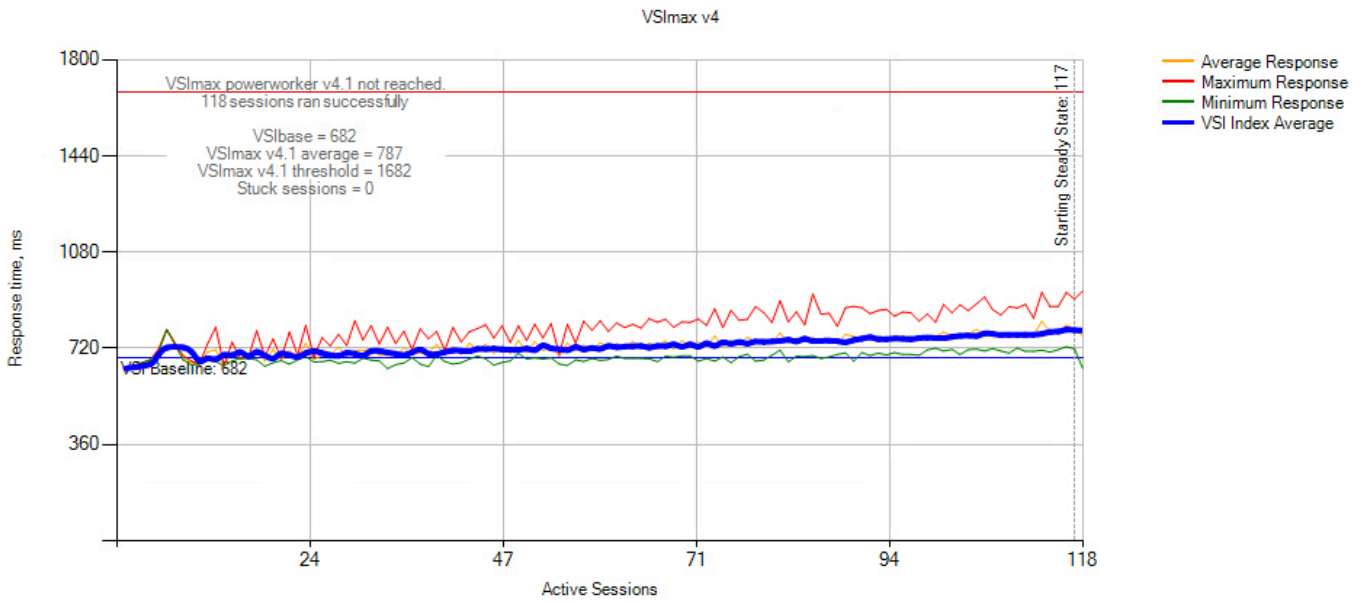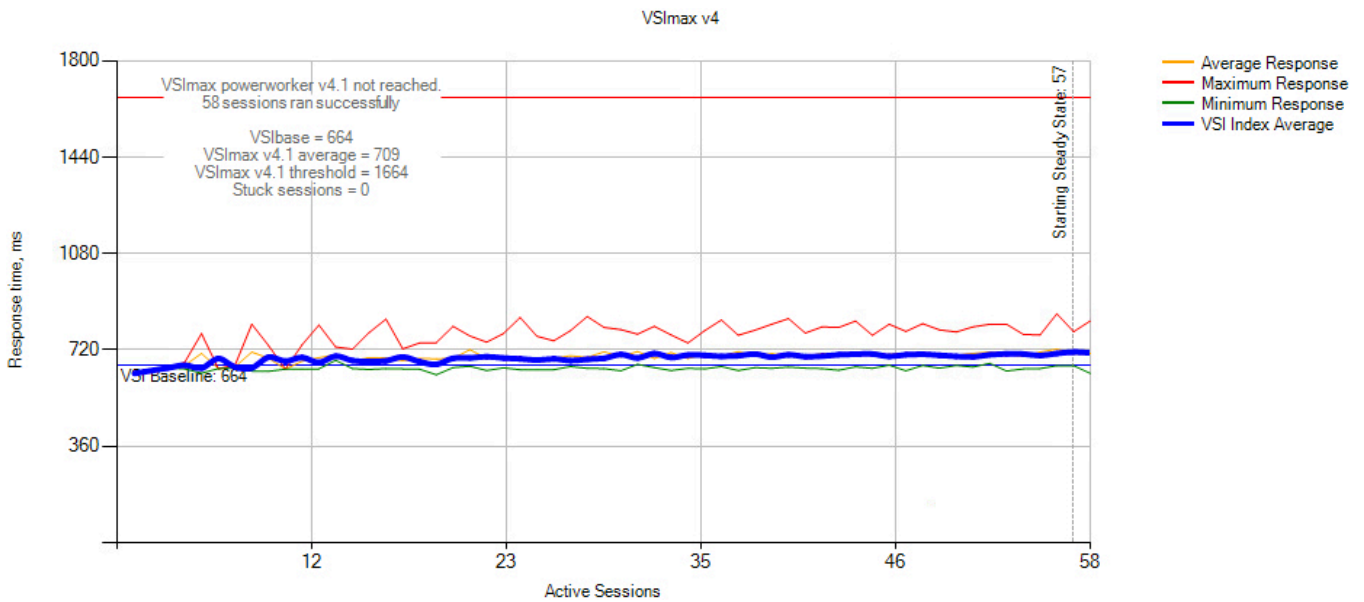
How we tested

Testing overview

We used a pair of dual-socket servers equipped with Intel Xeon Gold 6142M processors to host infrastructure and connected them to a 10 Gbps TOR (top-of-rack) switch. In the same way, we also connected our four Dell EMC R740xd servers to the TOR switch via 2 x 10 Gbps connections per server. We installed VMware ESXi 7.0 u1 on both infrastructure servers and the Dell EMC R740xd servers (see Table 3). We configured each server network so that all management, vMotion, and data traffic defaulted to NIC0 and all vSAN traffic defaulted to NIC1. In addition, we separated traffic by vLAN – management, data, vMotion, and vSAN.

We configured a vSAN cluster with the four Dell EMC servers with and created VMs (see Table 4) to create an enterprise environment consisting of a Windows Active Directory, DNS, and DHCP services as well as a Citrix® Apps and Desktops™ 7 and cloned out desktops via Citrix MCS (Machine Creation Services). For testing, we ran the VDI benchmark Login VSI 4.1 Power user workload. We set up three virtual desktop testing scenarios – virtual desktops with 12 GB of memory (all 12 GB reserved), 6 GB of memory (all 6 GB reserved) and 3 GB of memory (1.5 GB reserved). We first performed testing on a server node with 768 GB of DRAM and again on the same server node with 1.5 TB of Intel Optane persistent memory with 384 GB of DRAM used as memory cache. We recorded the maximum number of supported desktops, processor utilization, active memory, and total memory used along with average desktop response time. In each of the three scenarios we compared the output for the DRAM only node vs the node with Intel Optane persistent memory. We performed all testing with Windows 10 desktops using 4vCPUs. During testing, we also monitored the system under test to ensure no storage or networking bottlenecks were present.

Physical servers

Table 3: Server configuration information.

Server	OS	Role(s)
Infra1 and 2	VMware ESXi 7.0 U1	Infrastructure cluster
SUT 1-4	VMware ESXi 7.0 U1	vSAN – Node Under Test

Virtual machines

Table 4: VM configuration information.

VM name	OS / Role	vCPU count	Memory size (GB)	Disk size (GB)	Server host / cluster
DC1	Windows Server 2019 / Domain controller, DNS, DHCP	4	8	C:\40	infra
vCenter	VMware vCenter Server Virtual Appliance ver 7 U1	4	20	Appliance determined	infra
XD1	Windows Server 2019 / Citrix Desktop Delivery controllers	4	8	C:\40 D:\50	infra
CIFS1	Windows Server 2019 / Roaming profiles and redirected folders	2	8	C:\40 D:\200	infra
CIFS2	Windows Server 2019 /LoginVSI content share	2	8	C:\40 D:\200	infra
VSI-MGMT	Windows Server 2019/ LoginVSI management server	2	8	C:\40 D:\200	infra
L01-32	Windows 10 x64 Enterprise/ Login VSI launcher	4	8	C:\40	infra
Win10-gold	Windows 10 x64	4	8	C:\50	vSAN Node under test

Installing VMware ESXi 7.0 U1

1. First, install ESXi 7.0 U1 on the infrastructure servers. Then, complete the same steps to install ESXi 7.0 U1 on the Dell EMC PowerEdge R740xd servers.
2. Attach the installation media.
3. Boot the server.
4. Select the installation media.
5. At the VMware Installer screen, press Enter.
6. At the EULA screen, press F11 to Accept and Continue.
7. Under Storage Devices, select the appropriate virtual disk, and press Enter.
8. Select US as the keyboard layout, and press Enter.
9. Enter the root password twice, and press Enter.
10. Press F11 to start the installation.
11. After the server reboots, press F2, and enter root credentials.
12. Select Configure Management Network, and press Enter.
13. Select the appropriate network adapter, and click OK.
14. Select IPv4 settings and enter the desired IP address, subnet mask, and gateway for the server.
15. Select OK and restart the management network.

Deploying VMware vCenter 7.0 U1

We deployed the VMware vCenter 7.0 U1 virtual appliance onto an infrastructure server, created our infrastructure VMs, and configured our four Dell PowerEdge R740xd servers into a vSAN cluster.

1. On a Windows machine 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 the vCenter Server Appliance will be deployed.
9. Provide the servers credentials, and click Next.
10. At the Configure Network Settings page, configure the network settings for your environment, and click Next.
11. Review your settings, and click Finish.
12. When the deployment completes, click Next.
13. At the Introduction page, click Next.
14. At the Appliance configuration page, select the time synchronization mode and SSH access settings, and click Next. We used a local NTP server and enabled SSH.
15. Select Create a new SSO domain.
16. Provide a password and confirm it.
17. Provide an SSO Domain name and SSO Site name, and click Next.
18. At the CEIP page, click Next.
19. At the Ready to complete page, click Finish.
20. When the installation completes, click Close.
21. Using the vSphere web client, log into the vCenter server using the credentials previously provided.

Creating a data center in VMware vCenter and adding hosts

We created two clusters 1) infra, to host infrastructure VMs necessary for testing, and 2) SUT (server under test), to host all virtual desktops. We configured a vSAN for the SUT cluster consisting of two disk groups – one cache disk and four capacity drives each, for a total of eight NVMe SSDs per compute node.

Creating the data center
1. Once logged into the vCenter, navigate to Hosts and Clusters.
2. Select the primary site management vCenter.
3. Right-click the vCenter object, and select New Datacenter…
4. Enter a name for the new data center, and click OK.
5. Right-click the new data center, and click New Cluster…
6. Enter SUT as the name for the new cluster.
7. Click OK.
8. Repeat steps 1 through 7 to create an Infra cluster.

Adding the hosts
1. Once the cluster has been created, right-click the cluster, and click Add Host.
2. Enter the FQDN or IP address of the first host, and click Next.
3. Enter the root credentials for the server, and click Next.
4. To accept the server's certificate, click Yes.
5. Review the server details, and click Next.
6. Assign the desired license, and click Next.
7. Disable Lockdown mode, and click Next.
8. Click Finish.
9. Repeat steps 1 through 8 for the remaining SUTs and the client host.

Creating a vSAN for testing on the SUT cluster

We created a vSAN with the disks available in each compute node in the cluster under test. We used a separate vLAN for vSAN traffic and a dedicated 10 Gbps physical adaptor for each node. Our vSAN was composed of two disk groups - using the Intel 375GB P4800X disks for cache and Intel 3.48TB S4510s for capacity.

1. In the Hosts and Clusters pane, select the newly created cluster.
2. Click the Configure tab, and under Configuration, select Quickstart.
3. Under Cluster basics, click Edit.
4. Enable vSAN, and click OK.
5. Under Add Hosts, click Add.
6. Enter the IP and credentials for each of the hosts you wish to add to the cluster, and click Next.
7. Under Configure hosts, click Configure.
8. Under Physical adapters, click the drop-down next to the adapters you wish to use for vSAN traffic, and select DSwitch. Leave the Distributed switches and Port groups options as default. Click Next.
9. Enter the value of the VLAN you wish to use for vSAN.
10. If you wish, change IP type to static and type in IP addresses for the hosts. Otherwise, leave the IP type as DHCP. Click Next.
11. On the Advanced options screen, click Next.
12. On the Claim disks screen, select the disks you wish to use for capacity and cache, and click Next.
13. Click Next, and click Finish.

Creating the VM template for Windows Server 2019

We created a simple VM template to create all infrastructure VMs.

Deploying a template VM

1. Launch the VMware vCenter HTML5 client.
2. Right-click the infrastructure host, and choose New Virtual Machine…
3. Choose Create a new virtual machine, and click Next.
4. Name the virtual machine, and click Next.
5. Choose the correct host, and click Next.
6. Choose the correct datastore, and click Next.
7. Choose ESXi 7.0 and later, and click Next.
8. Choose Windows for the Guest OS Family, and Microsoft Windows Server 2019 (64-bit) for Guest OS Version. Click Next.
9. Set the vCPU count to 4, memory to 4GB, New Hard Disk capacity to 40GB, change the network adaptor to VMXnet3.
10. Click Finish.

Installing and configuring Windows Server 2019 Enterprise on the template VM

Install a base OS on the template VM.

1. In the VMware vCenter HTML5 client, click on the VM you created, and click Launch Remote Console.
2. Attach the Windows Server 2019 Enterprise ISO to the VM, and turn the VM on.
3. When prompted to boot from DVD, press any key.
4. When the installation screen appears, leave language, time/currency format, and input method as default, and click Next.
5. Click Install now.
6. When prompted, enter the product key.
7. Select Windows Server 2019 Datacenter Edition (Server with a GUI), and click Next.
8. Check I accept the license terms, and click Next.
9. Click Custom: Install Windows only (advanced).
10. Select Drive 0 Unallocated space, and click Next. This will start the install automatically, and Windows will restart automatically after completing the install.
11. When the Settings page appears, fill in the Password and Reenter Password fields with the password of your choice.
12. Log in with the password you set.
13. In the VMware Remote Console, attach VMware Tools to the VM.
14. In Windows, the VMware Tools should show up in the CD drive. Double-click to start the install.
15. Choose Typical as the install type, and reboot the VM when the install is finished.
16. Log back into Windows and in Server Manager, set the time zone, enable RDP if desired, and disable the firewall.
17. Run Windows updates until you have no new updates to install.
18. Power off the template VM, which you will use for all Windows Server 2019 infra VMs (see Table 2).

Installing and configuring Microsoft Windows Active Directory Domain Controller and supporting services

We installed and configured a VM to host Microsoft Active Directory services, DNS, DHCP, and NTP. Later, Login VSI creates several OUs for virtual desktops, launchers, and users and then apply group policies to each; this directory is necessary for testing to execute correctly.

Installing the Domain Controller VM

1. Log into the vSphere client as administrator@vsphere.local.
2. On the infra server, deploy a Windows Server 2019 VM from the template named DC1, 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 Domain Controller VM

1. After the installation completes, a screen should pop up with configuration options. If a screen does not appear, click the Tasks flag in the upper-right section of Server Manager.
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 the Domain Controller VM

1. To ensure reliable time, we pointed our Active Directory server to a physical NTP server.
2. Open a command prompt.
3. Type the following:

```
W32tm /config /syncfromflags:manual /manualpeerlist:"us.pool.ntp.org"
W32tm /config /reliable:yes
W32tm /config /update
W32tm /resync
Net stop w32time
Net start w32time
```

Setting up DHCP services on the Domain Controller VM

1. Open Server Manager.
2. Select Manage, and click Add Roles and Features.
3. Click Next twice.
4. Select DHCP Server, and click Next.
5. At the Introduction to DHCP Server screen, click Next.
6. At the Specify IPv4 DNS Settings screen, type test.local for the parent domain.
7. Type the preferred DNS server IPv4 address, and click Next.
8. At the Specify IPv4 WINS Server Settings screen, select WINS is not required for applications on the network, and click Next.
9. At the Add or Edit DHCP Scopes screen, click Add.
10. At the Add Scope screen, enter the Name DHCP Scope name.
11. Set the following values, and click OK.
    a. Start IP address = 172.16.10.1
    b. End IP address = 172.16.100.254
    c. Subnet mask = 255.255.0.0
    d. Check the Activate This Scope box.
12. At the Add or Edit DHCP Scopes screen, click Next.
13. Click the Enable DHCP v6 Stateless Mode radio button, and click Next.
14. Leave the default IPv6 DNS Settings, and click Next.
15. At the Authorize DHCP server dialog box, select Use current credentials.
16. At the Confirm Installation Selections screen, click Next. If the installation is set up correctly, a screen displays saying that DHCP server install succeeded.
17. Click Close

Installing the Login VSI 4.1 benchmark

The Login VSI 4.1 installation has several parts, the Active directory setup, a CIFS media share and a management console and target agent setup. We deployed each according to the Login VSI 4.1 documentation at **https://www.loginvsi.com/documents/documentation/Login-VSI-Installation-Guide.pdf.**

Installing and setting up the Login VSI 4.1 management VM

To create users and coordinate testing we first setup a VM named VSI-MGMT and ran the LoginVSI Dataserver install media on it. This installed the Login VSI management console/

1. On the infra server cluster, deploy a Windows Server 2019 VM from the template named VSI-MGMT, and log in as test\administrator.
2. Create a folder named D:\share.
3. Right-click the D:\share folder, and click Properties.
4. Click the Sharing tab, and click Share…
5. Add everyone, system, and administrators to the Read/Write group, and click Share.
6. Unpack the Login VSI install media.
7. Open Datacenter setup\setup.exe.
8. At the welcome screen, click Next.
9. Select the share named \\vsi-mgmt\share, and click Next.
10. Check the Start Login VSI Management Console checkbox to start the Management Console when the setup is completed, and click Finish.
11. At the management console, enter the path to your Login VSI license file, and click Save.

Configuring Login VSI: AD setup, creating users and default GPOs (Group Policy Objects)

Login VSI management console creates a powershell script that automates the creation of users and GPOs to ensure successful testing. We used this functionality to create a .ps1 file and then copy and execute it on our Domain controller "DC1."

1. On the VM named VSI-MGMT, open the VSI management console, and click 1. AD setup.
2. Enter the following:
   a. Base OU: DC=test,DC=local
   b. Username: LoginVSI
   c. Password1: *********
   d. Domain: (auto detect checked)
   e. Number of users: 1000
   f. Formatting length: 4
   g. Launcher user: Launcher-v4
   h. Launcher password: **********
3. Click Save to .sp1.
4. Copy the VSIADSetup.ps1 file to \\DC1\c$.
5. Log into DC1 as administrator and execute the c:\VSIADSetup.ps1 from step 2 in Windows PowerShell™.

Setting up the Active Directory roaming profiles and folder redirection

For testing, we chose to use Microsoft Windows Active directory roaming profiles and folder redirection. This way all virtual desktop users would keep their profile information regardless of which desktop VM the were assigned at logon.

Deploying a VM for roaming profiles and folder redirection

1. Log into the vSphere client as administrator@vsphere.local.
2. On the infra server cluster, deploy a Windows Server 2019 VM from the template named CIFS1, 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.

Setting up Microsoft Active Directory roaming profiles CIFS shares on CIFS1

1. Log onto the VM named CIFS1, open Windows Explorer, and create the following folders: D:\user_profiles, and D:\user_folders and add permissions of read/write to the test.local/everyone group.
2. Right-click the D:\user_profiles, and D:\user_folders folder, and select Properties, for each:
3. Click the Sharing tab, and select Share…
4. Add everyone, system, and administrators to the read/write group, and click Share.
5. Click OK, Apply, OK, and Close.

Assigning Login VSI user profiles to the user_profiles share

1. Log onto the VM named DC1 as test\administrator.
2. Open Active Directory Users and Computers.
3. Browse to test.local→Login_VSI→Users→Target.
4. Select all Login VSI users, and right-click Properties.
5. Click Profile, and enter profile path \\cifs1\user_profiles\%username%.

Configuring folder redirection for Login VSI users

1. Log onto the VM named DC1 as test\administrator.
2. Open the Group Policy Editor.
3. Open Forest→Domains→test.local, right-click Group Policy Objects, and select New.
4. Type folder_redirection, leave source starter GPO as None, and click OK.
5. Right-click the folder redirection GPO, and click Edit.
6. Browse User Configuration→Policies→Windows Settings→Folder Redirection, and right-click AppData (roaming).
7. In the AppData (roaming) Properties, target-tab select the following:
8. Setting: Basic (redirect everyone's folders to the same location)
9. Target folder location: Create a folder for each user under the root path
10. Root path: \\CIFS1\user_folders
11. In the AppData (roaming) Properties→Setting tab, remove the checkbox for Grant the user exclusive right to AppData (roaming), and click OK.
12. Repeat steps 6 through 8 for all subfolders in the folder redirection tree.
13. Close the Folder Redirection group policy.
14. In the Group Policy Editor, right-click the folder redirection policy, and select GPO Status→Computer Configuration Settings Disabled.
15. In the Group Policy Editor, drag the folder redirection GPO to Forest→Domains→test.local→Login_VSI→Users→Target.

Distributing Login VSI media content and downloading the Login VSI Pro Library

Login VSI recommends creating a dedicated content share separate from the management console server. We created a VM named CIFS2 and copied the _VSI_Websites directory and the _VSI_Content folder it. Because we ran the Power user workload, we also downloaded the Login VSI Pro Library and added it to the CIFS 2 share. Download the Login_VSI_Pro_Lib.exe library from **https://www.loginvsi.com/downloads/login-vsi**.

Deploying a VM for Login VSI Pro library

1. Log into the vSphere client as administrator@vsphere.local.
2. On the infra server, deploy a Windows Server 2019 VM from the template named CIFS2, 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.

Copying the Login VSI media to from the management server to CIFS2

1. Log into the VM named CIFS2 as test\administrator.
2. Open Windows Explorer, and create a folder called d:\vsishare.
3. Add permissions of read/write to the test.local/everyone group.
4. Right-click the d:\share, and select Properties.
5. Click the Sharing tab, and select Share…
6. Add everyone, system, and administrators to the read/write group, and click Share.
7. Click OK, Apply, OK, and Close.
8. Copy \\vsi-mgmt\vsishare_VSIwebsites_ to D:\vsishare..
9. Copy \\vsi-mgmt\vsi_VSI_Content to D:\vsishare.

Installing the Login VSI Pro media library

1. Log into the VM named CIFS2 as test\administrator.
2. Click on the downloaded library named Login_VSI_Pro_Lib.exe.
3. To start the installation, click Next.
4. Specify the path as //CIFS2/vsishare, and click Next.
5. Click Finish.

Creating the Windows 10 Enterprise (x64) Login VSI Launcher image

We created a Microsoft Windows 10 Enterprise (x64) template VM named Launcher and cloned out launcher VMs. Each Launcher can launch up to 25 virtual desktop sessions.

Deploying a Launcher 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. Choose Custom, and click Next.
5. Assign the name launcher, and click Next.
6. Select the infrastructure cluster, and click Next.
7. Select the local DAS.
8. Choose compatible with ESXi 7.0, and click Next.
9. Choose Windows, choose Microsoft Windows 10 (64-bit), and click Next.
10. For CPUs, select 4 CPUs, 8 GB RAM 50 GB Disk, and click Next.
11. Click Finish.
12. Click the Hardware tab.
13. Click CD/DVD Drive.
14. Select Connect the VM virtual CD-ROM to the Microsoft Windows 10 x64 installation disk.
15. Click OK.
16. Power on the Microsoft Windows 10 VM.

Installing Windows 10 Enterprise (x64) on the Launcher VM

1. When the installation prompts you, press any key to begin setup.
2. Enter your language preferences, and click Next.
3. Click Install.
4. Accept the license terms, and click Next.
5. Select Custom, and select the drive that will contain the OS.
6. Click Install.
7. Type user for the username, and click Next.
8. Enter no password, and click Next.
9. At the system protection screen, select Use recommended settings, and click Next.
10. Enter your time zone, and click Next.
11. Select the Work Network setting, and click Next.
12. Install VMware Tools, and select Complete Installation. For more information, visit ***http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=340***.
13. Reboot the server.
14. Connect the machine to the Internet, and install all available Windows updates. Restart as necessary.
15. Join the domain, and restart the VM.

Installing the Citrix Workspace client on Launcher VM

1. Log into the launcher VM as test\administrator.
2. Mount the Citrix install media (ver 2009.0.0.27084).
3. Open Windows Explorer, and browse to and run /Citrix Receiver and Plug-ins/Windows/Receiver/CitrixWorkspaceApp.exe.
4. Click Start.
5. Agree to the license agreement, and click Next.
6. Do not select Enable single sign-on, and click Next.
7. Do not click Enable App protection, and click Install.
8. Click Finish, and power off the Launcher VM. It is now ready to be cloned.

Creating the Windows 10 Enterprise (x64) gold image VM

We created a Microsoft Windows 10 Enterprise (x64) template VM named Win10-gold and added applications for testing.

Creating Win10-gold 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. Choose Custom, and click Next.
5. Assign the name win10-gold, and click Next.
6. Select the Cluster Under test, and click Next.
7. Select the vSAN datastore.
8. Choose compatible with ESXi 7.0, and click Next.
9. Choose Windows, select Microsoft Windows 10 (64-bit), and click Next.
10. For CPUs, select 4 CPUs, 8 GB RAM (8 GB Reserved), 50 GB Disk, and click Next.
11. Click Finish.
12. Click the Hardware tab.
13. Click CD/DVD Drive.
14. Select Connect the VM virtual CD-ROM to the Microsoft Windows 10 x64 installation disk.
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. Enter your language preferences, and click Next.
3. Click Install.
4. Accept the license terms, and click Next.
5. Select Custom, and select the drive that will contain the OS.
6. Click Install.
7. Type user for the username, and click Next.
8. Enter no password, and click Next.
9. At the system protection screen, select Use recommended settings, and click Next.
10. Enter your time zone, and click Next.
11. Select the Work Network setting, and click Next.
12. Install VMware Tools, and select Complete Installation. For more information, visit ***http://kb.vmware.com/selfservice/microsites/ search.do?language=en_US&cmd=displayKC&externalId=340***.
13. Reboot the server.
14. Connect the machine to the Internet, and install all available Windows updates. Restart as necessary.
15. Join the domain, and restart the VM.

Installing Microsoft Office Professional Plus 2019 on the gold image VM

1. Log onto win10-gold as test\administrator.
2. Mount the Microsoft Office 2019 media to d:\.
3. Open to d:\office\setup64.exe.
4. Wait for Office 2019 Professional Pro to install.

Installing the Citrix Virtual Desktop Agent on the gold image VM

1. Log onto win10-gold as test\administrator.
2. Mount the Citrix install media (ver 2009.0.0.27084).
3. Click AutoSelect.exe.
4. Next to Virtual Apps and Desktops, click Start.
5. Click Prepare Machines and images.
6. Click Create a master MCS image, and click Next.
7. Leave core components as default, and click Next.
8. Leave Additional components as default, and click Next.
9. Change the Delivery Controller configuration to let Machine Creation Services do it automatically, and click Next.
10. Leave features as default, and click Next.
11. Leave firewall as automatic, and click Next.
12. Review the summary, and click Install.
13. Deselect the Collect diagnostic information checkbox, and click Next.
14. To restart the VM, click Finish.

Installing the Login VSI 4.1 agent on the Windows 10 gold image VM

1. Log onto win10-gold as test\administrator.
2. Mount the LoginVSI media, and run \LoginVSI4140\2.Targert Setup\Target setup.exe.
3. Click Next.
4. Keep all defaults, and click Next.
5. Click Finish.

Disabling Windows Defender A/V scanning on the Windows 10 gold image VM

To ensure the fastest possible testing, we disabled A/V scanning. If this setting is not disabled, there is a considerable amount of I/O that will occur for several hours after system reboots.

1. Log onto win10-gold as test\administrator.
2. Click the Windows start icon→Settings.
3. In Windows settings, click Updates and Security.
4. Click Windows Security.
5. Click Open Windows Security.
6. Click Virus & Threat Protection.
7. Click Virus & Threat Protection Settings.
8. Click the sidebar on Real-time protection.
9. Close Settings.

Optimizing the Windows 10 gold image VM

1. Log onto win10-gold as test\administrator.
2. Download the Windows optimization tool from VMware.
3. Extract the zip file, and run VMwareOSOptimizationTool_b1170_16669532.exe.
4. Click Template, and select VMWare\Windows 10.
5. Click Analyze.
6. Select all suggestions, and click Optimize.
7. When settings finish applying, reboot the VM.

Finalizing the Windows 10 gold image VM and taking a snapshot

Citrix Virtual Desktops and Apps 7 requires a VM snapshot to create a Machine Catalog.

1. In vCenter, shut down the Windows 10 gold image.
2. Right-click the VM named win10-gold, and select Take a snapshot.
3. Name each snapshot, and click OK.

Setting up a Citrix Virtual Apps and Desktops 7 infrastructure

We installed a Microsoft Windows 2019 VM named XD1 from the template, and installed Citrix Virtual Apps and Desktops on it. We configured the Citrix Store and licenses required.

Deploying Citrix Delivery Controller

1. On the infra server, deploy a Windows Server 2019 VM from the template named XD1, and log in as test\administrator.
2. Mount the Citrix Install media Launch AutoSelect.exe.
3. Click Start Virtual Apps and Desktops.
4. Click Getting Started for Delivery Controller.
5. Accept the license agreement, and click Next.
6. Keep all four components checked (delivery Controller, Studio, Director, License server), and click Next.
7. Keep both features checked (Install Microsoft SQL Server 2017 Express CU16 and Windows remote assistance), and click Next.
8. Leave firewall ports as default, and click Next.
9. Click Install.
10. To reboot, click Close.
11. Log in and allow the installation to complete.
12. Deselect Collect diagnostic information, and click Next.
13. To launch Studio, click Finish.

Installing and configuring Citrix Desktops and Apps on the XD1 VM

1. On the Citrix Studio welcome screen, click Deliver applications and desktops to your users.
2. Name the site XD1, and click Next.
3. In the Database menu, leave the default values, and click Next.
4. In the Licensing menu, click Use existing license, browse to the licensing file, and click Next.
5. In the Connection menu, select VMware vSphere, type `https://<ipaddress of the vcenter>/sdk` and use the appropriate credentials, and click Next.
6. Select Trust certificate, and click OK.
7. Select the vDT vSAN cluster, local storage, and click Next.
8. Select the vSAN storage and check boxes for OS, person vDisk and temporary, and click Next.
9. Name the Network Resources network, and click Next.
10. Leave additional features unchecked, and click Next.
11. At the summary menu, click Finish.

Configuring the Citrix Storefront

1. Open the Citrix Studio →Storefront, right-click, and select Create Storefront.
2. At the Getting Started menu, click Next.
3. Name the store the same as the Desktop Delivery Controller (example XD1 = XD1), and click Next.
4. To add a Desktop Delivery Controller, click Add, and enter the following:
5. Display name (Example - XD1)
6. Add the local delivery controller (example XD1 = XD1)
7. Transport type: Select HTTP
8. Click OK, and click Next.
9. For remote access, leave defaults, and click Next.
10. Select User name and password for authentication methods, and click Next.
11. Select the Make this the default Store for PNAgent checkbox, click Create, and click Finish.

Deploying virtual desktops with Citrix Virtual Desktops and Apps 7

Using the Citrix Studio on the VM XD1, we used Citrix Machine Creation Services to create a Machine Catalog. We created and configured a Delivery Group, and added machines from the Machine Catalog to the new Delivery Group.

Creating a Citrix Machine Catalog
1. Log onto XD1 as test/administrator.
2. Open Citrix Studio.
3. Click Machine Catalog, and in the right pane, click Create Machine Catalog.
4. On the introduction screen, click Next.
5. For Operating system, select single-session OS, and click Next.
6. For Machine Management, leave the default (machines that are power managed and Citrix MCS), and click Next.
7. Select the gold master image created above and the snapshot, select 2003 for minimum functional level for this catalog, and click Next.
8. Select the appropriate number of VMs, and click Next.
9. Select the LoginVSI→Computers→Target OU and name the VMs, and click Next.
10. Name the catalog.
11. Click Finish.

Creating a Citrix Delivery Group
1. Log onto XD1 as test/administrator.
2. Open Citrix Studio.
3. Right-click Delivery Group, and select Create new Delivery Group.
4. Click Next.
5. Select the catalog you just created, add the appropriate number of machines, and click Next.
6. Select restrict use to this delivery group, add the test\LoginVSI group, and click Next.
7. Do not add any applications, and click Next.
8. Add the desktop by clicking Add, selecting a name, selecting restrict to group add test\LoginVSI group to the desktop assignments, click OK, and click Next.
9. Name the Delivery Group, and click Finish.
10. By default, Citrix automatically powers on desktops as needed and powers them off to be as power-efficient as possible. Teo ensure all desktops powered on and were idle, we opened a powershell command window and ran the following (where 'name' is the group name from step 9):
    - Set-BrokerDesktopGroup -Name "name" -AutomaticPowerOnForAssigned $False
    - Set-BrokerDesktopGroup -Name "name" -AutomaticPowerOnForAssignedDuringPeak $False
    - Set-BrokerDesktopGroup -Name "name" -OffPeakBufferSizePercent 100
    - Set-BrokerDesktopGroup -Name "name" -PeakBufferSizePercent 100
    - Set-BrokerDesktopGroup -Name "name" -ShutdownDesktopsAfterUse $False

Cloning VSI Launcher VMs and configuring the Login VSI 4.1 management console for testing

We cloned out our Launchers and configured the management console.

Converting the Launcher VM to a template and cloning the template
1. In vSphere Client, right-click the launcher VM, and select Template→Convert to Template.
2. Right-click the launcher template to deploy a virtual machine from the template.
3. Type launcher_1 as the new VM name, and click Next.
4. Click Datacenter, and click Next.
5. Click the launcher server, and click Next.
6. Select the appropriate storage, and click Next.
7. Select Customization using existing customization specifications, select the appropriate file, and click Next.
8. To deploy the new VM, click Finish.
9. Repeat steps 2 through 8 to deploy all the launchers.

Configuring the Login VSI console for testing

1. Log onto the VSI-MGMT VM as test\administrator.
2. Open the Login VSI management console.
3. Click Infrastructure→Data servers.
4. Right-click, select Add server, and enter UNC path **\\CIFS2\vsishare_VSI_Content.**
5. Click Infrastructure →Web Servers.
6. Right-click, select Add server, and enter UNC path **\\CIFS2\vsishare_VSI_Content.**
7. Click Add Launchers.
8. At the Add launchers wizard, click Next.
9. Click Batch entry, and enter the following:

> ◆ Name=L
> ◆ Start number=1
> ◆ Increment=1
> ◆ Count= 32
> ◆ Maximum capacity=25
> ◆ Formatting length=2

10. Click Next, and click Finish.

Running the Login VSI benchmark

We created a run profile by creating files outlined in Appendix A. Then, we created a profile by copying the files to the vsi-mgmt VM. Each scenario required us to change the number of users.

1. Log into the VSI-MGMT VM as test/administrator.
2. Create a folder called //vsi-mgmt/vsishare/_VSI_Configuration/testing_profile.
3. Create a folder called //vsi-mgmt/vsishare/_VSI_Configuration/testing_profile/_CurrentTest.
4. Copy the launchers file to //vsi-mgmt/vsishare/_VSI_Configuration/testing_profile.
5. Copy the DataLocations, Global, and VSIlauncher files to //vsi-mgmt/vsishare/_VSI_Configuration/testing_profile/_CurrentTest.
6. Open the management console, and begin a test.

Note: As a one-time task, you must create desktop user profiles for each desktop user before testing can begin. Do this by running a test and selecting the "enable profile create mode" in the Basic test configuration screen. Windows also defaults .pdf files to open in the Edge browser. We needed to run the profile create job twice, once to create the profile and again with a script using the setuserfta.exe (from **https://kolbi.cz/SetUserFTA.zip**). You can use the following steps to change the pdf file association to Adobe Reader.

7. Log onto the VSI MGMT VM.
8. Create the directory **\\vsi-mgmt\vsishare_VSI_tools**.
9. Extract setuserfta to **\\vsi-mgmt\vsishare_VSI_tools**.
10. Open **\\DC1\sysvol\test.local\scripts\V4-VSI_Login.bat**.
11. Add the following to the first line of V4-VSI_Login.bat: Call|\\vsi-mgmt\vsishare_VSI_tools\setuserfta.exe| |\\vsi-mgmt\vsishare_VSI_tools\setuserfta\loginvsiconfig, and save the new file .
12. Create a file named **\\vsi-mgmt\vsishare_VSI_tools\LoginVSIConfig** with the following text: .pdf, AcroExch.Document.11.

Once the profiles are created and the pdf association has been changed, remove the line in **\\DC1\sysvol\test.local\scripts\V4-VSI_Login.bat** from step 5.

Appendix A – Login VSI config files

Each of these files (Launchers, DataLocations, Global and VSIlauncher) were created in notepad and saved without file extensions. Please note that we shortened some redundancies in these files with […], this requires duplication of the session for the file to work correctly. Edit the NumberOfSessions in VSIlauncher to reflect the testing scenario desired.

Launchers

```
[l01]
Capacity=25
Disabled=0
CMLaunch=0
Notes=
[l02]
Capacity=25
Disabled=0
CMLaunch=0
Notes=
[…]
[l32]
Capacity=25
Disabled=0
CMLaunch=0
Notes=
```

DataLocations

```
[Dataservers]
Server1=\\CIFS2\vsishare\_VSI_Content
[Server1]
name=Default
enabled=1
[WebServers]
WebServer1=\\CIFS2\vsishare\_VSI_Websites
[WebServer1]
name=Default
enabled=1
[Server2]
[WebServer2]
[Library]
doc=1000
docx=1000
jpg=1000
mm=1000
pdf=1000
ppt=1000
pptx=1000
pst=1000
txt=1
xlsx=1
[Websites]
BBC=20
ENGADGET=20
PINTEREST=20
Player=20
THEVERGE=20
```

Global

```
[Settings]
Use_SessionM=1
LauncherHeartbeat=10
UserHome=H:
Groupdrive=M:
LauncherPollInterval=5
EngineWorkloadIndexPollInterval=5
EngineProcessPollInterval=5
TimerInterval=360
PublishedAppsLogFileShare=
RelaunchAppsOnSubsequentLoops=1
WorkloadIndexDebug=0
LogoffAt=segment
Logoff_Action=shutdown /l /f
logout_on_fatal_error=0
EsxtopEnabled=0
EsxtopServer=
EsxtopUsername=
EsxtopPassword=
EsxtopIntervalRecording=30
EsxtopAmountRecording=120
EsxtopFileKeepDuration=never
Pause={Pause}
MashupBehavior=Calculated
Workload_Loops=99999
SegmentBehavior=Calculated
SBC_timer_detect=0
PDFPrinting=1
ZIPLocation=%TEMP%\VSI\Zip
Verify_runtime_files=1
RandomInitialWait=5
DisableVideoViewing=0
IEVideoOption=Auto
Workload_Language=English
IEVersion=11
Office_code=2019
Office_version=16
Office_Language=English
office_print_sequence={altdown}fppp{altup}
log_category_AppStart=True
log_category_ShellExecuteWait=True
log_category_WebStart=False
log_category_LoopTimer=False
log_category_RandomCopy=False
log_category_SegmentTimer=False
SegmentsPerFile=20
Engine_Debug=0
Workload_Debug=0
winwait_timeout=120
winwaitactive_timeout=120
timer_timeout=60
ShellExecuteWaitTimeout=0
Workload=powerworker
[GUI]
AgentRunLoop=1
Fancy=1
CheckShareWritable=1
Mode=Normal
[Logon]
MapUserHome=1
MapGroupDrive=1
ImportOfficeReg=1
CopyPST=1
SetFreemindFTA=1
EngineStartup=Shell
```

VSIlauncher

```
[Scenario]
CPUEnabled=disabled
NumberOfCPU=0
CoresEnabled=disabled
NumberOfCores=0
HyperThreadingEnabled=disabled
HostsEnabled=disabled
NumberOfHosts=0
[Launcher]
BaseLinePhase=0
Servername=
Username=
Password=enc:BD177557C81239CED1:enc
ShowPassword=C04033148B4E
Domain=
useCSV=1
MultipleResources=0
CCL={VSISHARE}\_VSI_Binaries\Connectors\SFConnect.exe /url http://%CSV_DDC%/Citrix/%CSV_DDC% /user
test.local\%CSV_UserName% /password Password1 /resource "%CSV_resource%" /desktopviewer true /display
absolute /displayabsolute 1920x1080
CSV=\\vsi-mgmt\vsishare\ccv.csv
AgentRunLoop=1
PhasesCount=1
NumberOfSessions= {number of sessions desired}
NumberOfWindows=3600
SequentialInterval=30
AutoLogoff=1
LogoffTimeOut=120
CreateProfile=0
TSDiscon=0
PreTestScript=
PostTestScript=
[Launcher_FD]
Servername=
Username=
Password=
ShowPassword=
Domain=
useCSV=1
MultipleResources=0
CCL={VSISHARE}\_VSI_Binaries\Connectors\SFConnect.exe /url http://%CSV_DDC%/Citrix/%CSV_DDC% /user
test.local\%CSV_UserName% /password Password1 /resource "%CSV_resource%" /desktopviewer true /display
absolute /displayabsolute 1920x1080
CSV=\\vsi-mgmt\vsishare\singleserver.csv
AgentRunLoop=1
[VSI]
SkipAddLaunchersScreen=0
SkipCommandLineScreen=0
Increment=0
TestNamePattern=
SkipStartTestScreen=0
SkipAllWelcomeScreens=1
[Phase1]
Name=Phase 1
Sessions=
PhaseTime=3600
Pause=False
[LauncherWorkload]
launcherUsername=launcher
launcherDomain=test
launcherPassword=
launcherWorkflow=0
limitConcurrent=25
launcherResolution=1920x1080
launcherDisconnectAfterLaunch=0
```

Custom CCV-

```
UserName,DDC,resource
loginvsi001,XD1,p1
loginvsi002,XD1,p1
loginvsi003,XD1,p1
loginvsi004,XD1,p1
loginvsi005,XD1,p1
[…]
```

Read the report at http://facts.pt/7oiWGCO ▶

This project was commissioned by Dell Technologies.

PT Principled Technologies®

Facts matter.®