



The science behind the report:

# Scale virtual desktops faster and provision virtual apps more easily with VMware Horizon and VMware App Volumes

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 [Scale virtual desktops faster and provision virtual apps more easily with VMware Horizon and VMware App Volumes](#).

We concluded our hands-on testing on July 14, 2022. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on July 8, 2022 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

## Our results

To learn more about how we have calculated the wins in this report, go to <http://facts.pt/calculating-and-highlighting-wins>. Unless we state otherwise, we have followed the rules and principles we outline in that document.

Table 1: Results of our testing.

	VMware Horizon 8	Citrix Virtual Apps and Desktops 7
<b>Deployment</b>		
Time to deploy VMs (h:mm:ss)		
50 VMs	0:01:55	0:05:46
100 VMs	0:01:57	0:08:07
200 VMs	0:04:34	0:15:17
Steps to deploy the initial 10 VMs		
Steps	19	27
Major tasks needed to deploy an app		
Tasks	14	27
<b>Average CPU node utilization during constant load at 25 users</b>		
CPU percent utilization	59.83%	60.85%

	VMware Horizon 8	Citrix Virtual Apps and Desktops 7
<b>Login Enterprise logon time</b>		
Login time (sec)		
Display protocol connection	7.8	6.1
Profile load	0.6	0.7
GPO processing	1.1	1
(Subtotal)	9.5	7.8
<b>Total login time</b>	<b>12</b>	<b>9.5</b>
<b>Login Enterprise EUX performance for 25 non-persistent optimized VMs</b>		
EUX score	6.9	6.8
<b>Login Enterprise application performance for Microsoft Office 2019</b>		
Microsoft Word (sec)		
Start	1.911	1.991
Open window	0.889	0.879
Open Word document	1.463	1.48
Save file	0.513	0.493
<b>Total</b>	<b>4.776</b>	<b>4.843</b>
Microsoft Excel (sec)		
Start	2.271	2.491
Save file	0.644	0.658
Open window	0.966	1.012
Open Excel document	1.57	1.667
<b>Total</b>	<b>5.451</b>	<b>5.828</b>
Microsoft PowerPoint (sec)		
Start	1.842	1.951
Open window	0.821	0.783
Open PowerPoint document	2.093	2.064
Save file	1.203	1.186
<b>Total</b>	<b>5.959</b>	<b>5.984</b>
Microsoft Outlook (sec)		
Start	8.17	6.391
<b>Total</b>	<b>8.17</b>	<b>6.391</b>
Microsoft Edge (sec)		
Logon	0.141	0.149
<b>Total</b>	<b>0.141</b>	<b>0.149</b>
<b>Total application response time</b>	<b>24.497</b>	<b>23.195</b>

## System configuration information

Table 2: Detailed information on the systems we tested.

System configuration information	4 x Dell EMC VxRail V470F
BIOS name and version	Dell 2.10.5
Operating system name and version/build number	VMware ESXi, 7.0.3, 19193900
Date of last OS updates/patches applied	4/22/22
Power management policy	High performance
<b>Processor</b>	
Number of processors	2
Vendor and model	Intel Xeon E5-2698 v4
Core count (per processor)	20
Core frequency (GHz)	2.20
Stepping	1
<b>Memory module(s)</b>	
Total memory in system (GB)	512
Number of memory modules	16
Vendor and model	Hynix Semiconductor HMA84GR7MFR4N-UH
Size (GB)	32
Type	DDR-4
Speed (MHz)	2,400
Speed running in the server (MHz)	2,400
<b>Storage controller</b>	
Vendor and model	Dell HBA330 Mini
Cache size (GB)	0 MB
Firmware version	16.17.00.05
Driver version	17.00.12.00-1vmw.703.0.20.19193900
<b>Local storage</b>	
Number of drives	9
Drive vendor and model	HGST HUSMM1680ASS204 x 3, HGST HUSMR1619ASS204 x 6
Drive size (GB)	745.21 x 3, 1788.50 x 6
Drive information (speed, interface, type)	12Gb SAS, SSD
<b>vSAN configuration</b>	
Configuration summary	3-node vSAN cluster
Disk groups per host	3
Capacity disks per group	2
Cache disks per group	1

System configuration information		4 x Dell EMC VxRail V470F
Storage policy		vSAN Default Storage Policy
Space efficiency		None
Data-at-rest encryption		Disabled
Data-in-transit encryption		Disabled
RDMA support		Disabled
Network adapter		
Vendor and model		Intel Ethernet 10G 4P X520/I350 rNDC,
Number and type of ports		4x10GbE
Driver version		19.0.12
Cooling fans		
Vendor and model		Dell Embedded
Number of cooling fans		6
Power supplies		
Vendor and model		09TMRFA01
Number of power supplies		2
Wattage of each (W)		1100

Table 3: Version information for the software we used in testing

Software version information	VMware	Citrix
Virtual Desktop Infrastructure management	VMware Horizon 8	Citrix Virtual Apps and Desktops 7
VDI management build number	2203	2203
Application management	VMware App Volumes 4	Citrix App Layering
Application management build number	2203	2206

# How we tested

## Configuring the Active Directory VM

We installed and configured a VM to host Active Directory services, DNS, DHCP, NTP, and to be a certificate authority. In addition, we created a golden VM for virtual desktops and applied registry edits to ensure testing executed correctly. All these functions are necessary to run our testing.

### Installing Active Directory Domain Services

1. Log into the vSphere client as administrator@vsphere.local.
2. On the infrastructure server, deploy a Windows Server 2019 VM 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 DC1

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

### Configuring the Windows time service on DC1

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

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

## Setting up DHCP services on DC1

1. Open Server Manager.
2. Select Manage, and click Add Roles and Features.
3. Click Next twice.
4. At the Select server roles screen, elect 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 set up previously (TEST\Administrator), and click Commit.
12. On the Summary page, click Close.
13. Click Close on the Add Roles and Features Wizard.
14. In Server Manager, click Tools→DHCP.
15. In the left pane, double-click your server, and click IPv4.
16. In the right pane, click More Actions (under IPv4), and select New Scope.
17. Click Next.
18. Enter a Name and Description for the scope, and click Next.
19. Enter the following values for the IP Address Range:
  - Start IP address: 172.16.10.1
  - End IP address: 172.16.100.254
  - Length: 16
  - Subnet mask: 255.255.0.0
20. Click Next.
21. At the Add Exclusions and Delay page, leave defaults and click Next.
22. Set the Lease Duration to 30 days, and click Next.
23. At the Configure DHCP Options page, leave Yes selected, and click Next.
24. At the Router (Default Gateway) page, enter the gateway IP address, and click Next.
25. For the parent domain. at the Specify IPv4 DNS Settings screen, type `test.local`.
26. Type the preferred DNS server, IPv4 address, and click Next.
27. At the WINS Server page, leave the fields empty, and click Next.
28. At the Activate Scope page, leave Yes checked, and click Next.
29. Click Finish.

## Installing and configuring SSL Certificate in Microsoft Active Directory on DC1

1. Log onto DC1 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 DC1.test.local, and click Next.
7. At the server roles menu, expand Active Directory Certificate Services.
8. Select Certification Authority, Certificate Enrollment Web Service, and Certification Authority Web Enrollment.
9. When prompted, click Add Features, and click Next.
10. Leave Select features at defaults, and click Next.
11. At the Active Directory Certificate Services introduction page, click Next.
12. Select Certificate Authority and Certificate Authority Web Enrollment.
13. When prompted, click Add Features, and click Next.
14. Click Next two times, click Install, and close.
15. In server manager, click the yellow triangle titled Post-deployment configuration.
16. On the destination server, click Configure Active Directory Certificate Services.
17. Leave credentials as test\administrator, and click Next.
18. Select Certification Authority, Certificate Enrollment Web Service, Certification Authority Web Enrollment, and click Next.
19. Select Enterprise CA, and click Next.

20. Select Root CA, and click Next.
21. Select Create a new private key, and click Next.
22. Select SHA256 with a 2048 Key length, and click Next.
23. Leave the names fields and defaults, and click Next.
24. Change expiration to 10 years, and click Next.
25. Leave Certificate database locations as default, and click Next.
26. Click Configure.
27. When finished configuring, click Close.
28. Open a command prompt, and type `ldp`.
29. Click Connection, and connect.
30. For server, type `dc1.test.local`.
31. Change the port to 636.
32. Check SSL, and click OK.

## Configuring secure LDAP on DC1.test.local on DC1

1. Open administrative tools, Certification Authority
2. Click test-DC1-CA→Certificate Templates
3. Right-click Manage.
4. Right-click Kerberos Authentication, and select Duplicate Template.
5. Click General.
6. Rename the template and its display name.
7. Click Request Handling.
8. Check the box for Allow private key to be exported, and click OK.
9. Right-click the new template, and rename it LDAPoverSSL
10. Return to the Certificates console.
11. In the right pane, right-click New Certificate Template to Issue.
12. Select LDAPoverSSL, and click OK.

## Joining VMware® vCenter® to Active Directory

1. In the vSphere client, click the Menu dropdown, and select Administration.
2. Under Single Sign On, select Configuration.
3. In the Identity Provider tab, select Active Directory Domain.
4. Select the vCenter, and click Join AD.
5. Enter the AD administrator credentials, and click OK.

## Deploying Login Enterprise

### Deploying Login Enterprise appliance to the on-premises test environment

1. In the on-premises vCenter environment, select the test client host, and right-click Deploy OVF Template....
2. In the deploy OVF Template wizard, select local file, and click Browse....
3. Select the LoginEnterprise OVA, click Open, and click Next.
4. Select a datacenter, and click Next.
5. Review the details, and click Next.
6. Accept the license agreements, and click Next.
7. Select the infrastructure datastore, and click Next.
8. Select the network with internet access, and click Next.
9. To deploy the appliance, click Next, and click Finish.
10. After deployment completes, power on the VM, and note the IP address.

## Configuring Login Component for Logon Enterprise

1. In the Login Enterprise appliance web interface, click Accounts.
2. Scroll to the bottom of the page, and click to download the Logon Executable.
3. Extract LoginPI.Logon.exe from the zip, and copy it to the sysvol share on the domain controller.
4. Edit the properties on the user group for the test users, and type the following into the login script field:

```
LoginPI.Logon.exe <URL of the LoginVSI appliance>
```

5. In the Virtual User Accounts pane, click the +, and click Bulk Accounts.
6. Enter the base Username, Password, Domain, Number of digits for the user sequence, and Number of accounts to be created. Click Save.
7. In the Windows Active Directory Users and Computers control panel, create a security group called Citrix Users.
8. Create an OU in Active Directory named Citrix Users, and create accounts to match those in Login Enterprise.
9. Open the Citrix Users security group, and add the newly created users to the group.

## Deploying launchers

1. In the Login Enterprise appliance web interface, click Launchers.
2. Scroll to the bottom of the page, and click to download the Windows x64 launcher.
3. Extract the launcher to the desktop, and run Setup.msi.
4. Click Next, and proceed through the installer. To close the installation once it completes, click Finish.
5. To start the launcher, double-click the Login Enterprise Launcher icon on the desktop.
6. Complete steps 1 through 5 on as many launchers as needed for the environment.

## Creating Application test profiles

1. Download application testing scripts from <https://github.com/LoginVSI/ApplicationScriptsLE/>.
2. In the Login Enterprise appliance web interface, click Applications.
3. Click Add new application.
4. Enter the Application name, type, and target. Click Save.
5. In the application list, click the pencil to edit the newly created application profile.
6. Click Upload Script, and upload the matching script from the GitHub repository. Click Save.
7. Complete steps 1 through 6 for each application to test.

## Configuring test parameters

1. In the Login Enterprise appliance web interface, click Manage Tests.
2. Click Create a new Load Test +
3. Enter a name for the test, and select Citrix StoreFront.
4. Enter the Server URL and Resource to be used.
5. In the Accounts field, select All users.
6. In the Launchers field, select All Launchers.
7. Click Save.
8. Enter the number of users to log in within the same number of minutes to the desired level.
9. Set the test duration to 60 minutes.
10. In the Actions pane, click Add action(s), and then the Application(s) option.
11. Select all the applications to test. Click Save.

## Running a test

1. Click the "Play" icon next to the test.
2. Validate the test parameters, and click Confirm.



## Configuring the Windows gold image VM

We created a Microsoft Windows 10 Enterprise VM, then installed Microsoft Office Professional Plus 2019.

### Installing the Microsoft Edge driver on the Login Enterprise appliance

1. Find the Microsoft Edge driver matching your current version of Edge at [developer.microsoft.com/en-us/microsoft-edge/tools/webdriver/](https://developer.microsoft.com/en-us/microsoft-edge/tools/webdriver/).
2. Connect to the Login Enterprise appliance via SSH.
3. Run the following command:

```
chmod 707 /loginvsi/content/selenium
```

4. Create a folder named `EdgeChromium[Major Version #]` inside `/loginvsi/content/selenium`.
5. Extract `msedgedriver.exe` from the downloaded zip file, and copy it to the created folder.

### Creating the baseline Windows 10 VM

1. In vCenter, right-click on the host, and select **New Virtual Machine...**
2. Select **Create a New Virtual Machine**, click **NEXT**.
3. Enter a name for the VM, and select the location for the virtual machine. Click **NEXT**.
4. Select the host for the new VM, click **NEXT**.
5. Select the datastore for the new VM, click **NEXT**.
6. Select the compatibility level, "ESXi 7.0 U2 and later". Click **NEXT**.
7. Select the Guest OS Family and Version: **Windows/ Microsoft Windows 10 (64-bit)**. Click **NEXT**.
8. Adjust the virtual hardware settings to match:
  - CPU: 2
  - Memory: 4GB, Reserve all guest memory (All locked)
  - New SCSI controller: VMware Paravirtual
  - New Network: <Test network name>, Adapter type: `VMXNET 3`.
9. Click **ADD NEW DEVICE**, and select **CD/DVD Drive**.
10. For the first CD/DVD Drive, browse to the Windows ISO file on the datastore.
11. Delete the **New USB Controller**.
12. Expand the **Video Card** dropdown, and select 8 MB of total video memory.
13. Click the **VM Options** tab, and expand the **Advanced** drop-down.
14. Click **EDIT CONFIGURATION**.
15. Click **ADD CONFIGURATION PARAMS**.
16. In the **Name** field, enter `devices.hotplug`, set the **Value** to `false`.
17. Click **OK**.
18. Click **NEXT**, then **FINISH**.
19. Start the VM, then click **Launch Remote Console**.
20. Select the region settings for Windows 10, click **Next**.
21. Click **Install now**.
22. Select **Windows 10 Enterprise**, click **Next**.
23. Accept the license agreement, click **Next**.
24. Click **Custom: Install Windows only (advanced)**.
25. In the vCenter UI, select the VM and click **Install VMware Tools...**, and select **MOUNT**.
26. In the VM remote console, click **Load driver**.
27. Click **Browse**, and navigate on the VMware Tools drive to `\Program Files\VMware\VMware Tools\Drivers\pvscsi\Win8\amd64`
28. Click **OK**.
29. Select the **VMware PVSCSI Controller**, click **Next**.
30. Click **Next** to install on Drive 0.
31. When presented with the region dialog, press **CTRL+SHIFT+F3** to enter Audit mode.

## Configuring the baseline VM

1. If not already mounted, in the vCenter console, select the VM, and click Install VMware tools..., and select MOUNT.
2. On the VM, click the VMware tools AutoPlay popup, and select Run setup64.exe.
3. On the VMware Tools installer, click Next.
4. Select Custom, click Next.
5. Deselect:
  - Carbon Black Helper
  - Service Discovery
  - Volume Shadow Copy
6. Click Next.
7. Click Install.
8. Install .Net Framework 3.5: Open an Administrator command prompt, and enter:

```
DISM /Online /Enable-Feature /FeatureName:NetFx3 /All /LimitAccess /Source:D:\sources\sxs
```

9. Run Windows Update, and reboot the VM.

## Installing Office Professional Plus 2019 on the gold image VM

1. Install the Microsoft Office Professional Plus 2019 Volume using the offline installer, and install a pre-generated xml configuration file to install Word, Excel, PowerPoint, and Outlook only.
2. Open Windows Update, and click Advanced options.
3. Enable Receive updates for other Microsoft products, and click back.
4. Click Check for updates, and reboot if necessary.
5. Shut down the VM.
6. From the vCenter interface, right-click the VM and select Snapshot→Take snapshot...
7. Right-click the base VM, select Clone→Clone to Virtual Machine...
8. Enter the Virtual machine name for the Horizon environment and select a location. Click NEXT.
9. Select the host for test, click NEXT.
10. Select the storage for the test, click NEXT.
11. On the Select clone options page, click NEXT.
12. Click FINISH.
13. Repeat steps 7-12 to create a second clone for the Citrix environment.

## Configuring a new VDA VM

1. Download and configure the Virtual Delivery Agent on the gold VM.
  - a. Go to <https://xenapp.cloud.com/downloads>, and download the VDA.
  - b. Run the downloaded file, select Create a master MCS image, and click Next.
  - c. On the Core Components page, select Citrix Workspace App, and click Next.
  - d. On the Additional Components page, select Citrix VDA Upgrade Agent, and click Next.
  - e. On the Delivery Controller page, select Do it Manually, enter the public controller address, and click Next.
  - f. On the Features page, click Next.
  - g. On the Firewall page, click Next.
  - h. On the Summary page, Click Install.
  - i. On completion of the install, click Finish.

## Configuring VMware Horizon® 8 Connection Server

1. On the infrastructure server, deploy a Windows Server 2019 VM with 8 vCPUs and 16 GB of memory named view, and log in as an administrator.
2. Join the VM to the test.local domain, reboot, and log back in as a domain administrator.
3. Browse to VMware View installation media, and run the installation executable file.
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 or not to participate in the customer experience improvement program, and click Next.
12. To finish installing View Connection Server, complete the installation wizard.
13. Click Finish.
14. Reboot server.

## Configuring the VMware Horizon 8 Connection Server on the View 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 Instant Clone Engine provisioning operations: 20
```

7. Click Next.
8. Enter full domain name and user credentials.
9. Do not use Reclaim VM disk space or Enable View Storage Accelerator.
10. At the ready to complete screen, click Finish.
11. Open Horizon 8 View Administrator.
12. Log in as an administrator.
13. Select Settings→Domains.
14. Under Instant Clone Engine Domain Accounts, click Add.
15. Enter the Domain Name, Username, and Password for the domain administrator.
16. Click OK.

## Configuring Citrix Virtual Applications and Desktops (VAAD)

1. On a Windows Server 2019 VM, open the Virtual Apps and Desktops ISO, and next to Virtual Apps and Desktops, click Start.
2. Select Delivery Controller.
3. Accept the EULA, click Next.
4. Click Next to install all available components.
5. Enable all Features, click Next.
6. Leave Automatically checked, click Next.
7. Review the Summary, click Install.
8. On the Diagnostics page, choose whether to collect diagnostic information, and click Next.
9. Click Finish, reboot if prompted.
10. Open Citrix Studio, proceed through the wizard to create a site.
11. Select Application and desktop delivery Site.
12. Enter a name for the site, click to accept.
13. Configure licensing with licensing vendor.
14. Go to the Hosting page, select Add Connection and Resources.
15. Click Create a new Connection, select VMware vSphere.
16. Enter the Connection address, User name, Password, and name for the connection.
17. Select Citrix provisioning tools, click Next.
18. If using self-signed certificates, click Trust certificate, click OK.
19. Click Browse, and select the cluster for the virtual desktop deployment. Click OK.
20. Select Use storage shared by hypervisors, click Next.
21. Select the storage to use, click Next.
22. Name the network resources to use, then select the test network, and click Next.
23. Click Finish.

## Deploying virtual desktops using VMWare Horizon 8 Connection Server

1. Click Inventory→Desktops, click Add.
2. Leave Automated Desktop Pool selected, click Next.
3. Leave Instant Clone selected, click Next.
4. Leave Dedicated and Automatic Assignment selected, click Next.
5. Select Use VMware Virtual SAN, click Next.
6. Enter a pool ID and Display Name, click Next.
7. Enter a naming pattern and maximum number of machines, then click Next.
8. Browse to the Golden Image in vCenter, click Submit.
9. Browse to the Snapshot, click Submit.
10. Browse to the VM folder Location, click Submit.
11. Browse to the Cluster, click Submit.
12. Browse to the Resource Pool, click Submit.
13. Browse to the Datastore, click Submit, then click Next.
14. On the Desktop Pool Settings page, click Next.
15. On the Remote Display Protocol page, click Next.
16. On the Guest Customization page, browse to the AD Container, click Submit, then click Next.
17. On the Ready to Complete page, click Submit.
18. Click the Entitlements drop-down, then Add Entitlements.
19. On the Add Entitlements page, click Add, enter the group name, click Find, check the box next to the group, click OK, and then OK again.

## Adding machines and users to existing pools

1. In the Desktops panel, click the pool name, then click Edit.
2. Select the Provisioning Settings tab, and change the Maximum Machines to 50. Click OK.

## Deploying VAAD virtual desktops

1. Select Machine Catalogs, then right-click and select Create Machine Catalog.
2. On the Introduction page, click Next.
3. On the Operating System page, select Single-session OS, click Next.
4. On the Machine Management page, under Citrix Machine Creation Services (MCS), select the resource in the dropdown. Click Next.
5. On the Desktop Experience page, select No, discard all changes and clear virtual desktops when the user logs off, click Next.
6. On the Master Image page, select the master image and snapshot, and set the minimum functional level to 2106 (or newer). Click Next.
7. On the Virtual Machines page, enter 10 for the number of virtual machines, click Next
8. On the Computer accounts page, select the Active Directory location for the new computer accounts, and a naming schema. Click Next.
9. On the Summary page, enter the Machine Catalog name, click Finish.

## Creating machine catalog

1. Right-click Delivery Groups, then select Create Delivery Group.
2. On the Introduction page, click Next.
3. On the Machines page, change the number of machines to 10, click Next.
4. On the Delivery Type page, select Desktops. Click Next.
5. On the Users page, select Restrict use of this Delivery Group to the following users, and select the allowed user group. Click Next.
6. On the Desktop Assignment Rules page, click Add, enter a Display name, and click OK. Click Finish.
7. On the Summary page, enter the Delivery Group name, click Finish.
8. Right-click the new delivery group, select Edit delivery group.
9. Select the Machine allocation page, then click Import list. Browse to a previously-generated list, click Open. Click Apply, then OK.

## Adding machines to existing groups

1. In the Machine Catalogs section, right click the machine catalog, and select Add Machines.
2. Enter the number of machines to add, click Next.
3. On the Computer Accounts page, click Next, and then Finish on the Summary page.
4. Machine deployment time.
5. In the Delivery Groups section, right-click the delivery group, and select Add Machines.
6. On the Machines page, change the number of machines for the delivery group to the desired number, click Next.
7. On the Machine allocation page, select Import list, and browse to the previously-generated list, click Open. Click Next, then Finish.
8. Double-click the delivery group to go to the Search section, and select the new VMs by shift-clicking.
9. Right-click the VMs, and select Start.
10. When prompted, Are you sure you want to start 40 VMs?, click Yes.

## Configuring Citrix App Layers

### Deploying App Layering appliance

1. In vSphere, browse to VMs and Templates.
2. Right-click the infrastructure host, and select Deploy OVF Template.
3. In Select source, select Local file, and click Upload Files.
4. Browse to the Citrix App Layers OVA, and click Open, then Next.
5. Name the VM to be deploy, and select the folder for deployment. Click Next.
6. Select the infrastructure host to run the VM, and click Next.
7. Select Thick Provision Lazy Zeroed, specify a storage location, and click Next.
8. Select the private test network, and click Next.
9. Review the settings, and click Finish.

### Configuring App Layering appliance

1. Browse to the IP address of the appliance and log in with the default credentials.
2. Agree to the Citrix License Agreement.
3. Change default account passwords when prompted.
4. On the Get Started page, click Connect to configure a network file share.
5. On the file share page, click Edit.
6. Enter the path to an SMB file share, and enter a user name and password with access.
7. Click Confirm and Complete to connect to the file share.

8. Click System→Directory Services.
9. Click Add Directory Junction.
10. Enter the Server Address, Bind DN, Bind Password, Base DN, and a Friendly name for the connection. Click Confirm and Complete.
11. On the Get Started page, click Create a connector configuration.
12. Click Add Connector Configuration.
13. Select Machine Creation for vSphere. Click New.
14. Enter a name for the configuration, the vCenter Server address and credentials, click Check Credentials.
15. Select the Datacenter, Virtual Machine Template, ESX Host name, Datastore, Network, and Virtual Machine folder for the VMs.
16. Ensure Offload Compositing is checked, click Test.
17. Once confirmed, click Save.

## Configuring VMware App Volumes

1. On a Windows Server 2019 VM, run the App Volumes Manager setup.msi installer.
2. Accept the EULA, click Next.
3. Select Install App Volumes Manager, click Next.
4. Select Local installation of SQL Server Express, and Windows Integrated Authentication.
5. Select Choose a new database, and Overwrite existing database (if any).
6. Disable SQL Server certificate validation.
7. Change the listening port from 443 to 80.
8. Check the box to Allow Connections of HTTP (insecure), click Next.
9. Leave the default installation path, click Install.
10. Browse to the App Volumes Manager IP address, and log in.
11. Click Configuration→AD Domains, then click Register Domain.
12. Enter the Active Directory Domain Name, Domain Controller Host, LDAP Base, Username, and Password.
13. Click Disable certificate validation, click Register.
14. Go to the Admin Roles tab, and click Assign Role.
15. Enter the AD group for the Administrators group, click Assign.
16. Go to the Machine Managers tab, click Register Machine Manager.
17. Set the type to vCenter Server, enter the Hostname, Username, Password.
18. Select to Issue mount operations to ESXi servers, and enter the ESXi Username and Password.
19. Leave Mount Local unchecked, and Queue, Async, and Throttle checked. Click Save.
20. Go to the Storage tab, click Upload Templates.
21. Select all the templates, click Upload.

## Deploying App Layer VMs (Generalized steps for comparison)

1. Create base a BIOS-based Windows 10 Enterprise OS image, and matching template VM with no disks attached.
2. Install Windows updates.
3. Install Citrix App Layering OS Machine Tools.
4. Install .Net Framework 3.5 and Configure OS settings for Citrix layering.
5. Do not domain join the VM, do not snapshot.
6. Clone VM to create a baseline for deployed VMs.
7. Run App Layering services setup.
8. Run additional Citrix App Layering-specific scripts and optimization commands.
9. Run App Layering Machine Tools PowerShell script to import the OS layer.
10. Create a Platform Layer from the OS layer in the Appliance interface.
11. Copy the VMDK files from the SMB share to the datastore location for the template without disks from step 1, and attach them to the template VM.
12. Connect to the VM console, install Citrix Virtual Apps and Desktops agent and reboot.
13. Recompile .Net runtimes with ngen utility in 32 and 64 bit mode.
14. Run the application shortcut on the desktop to shut down and finalize the image.
15. Shutdown, and copy the VMDK files back to the SMB file share under the Finalize Disks folder.
16. Finalize the Platform Layer in the console.
17. Create an Application Layer from the OS layer in the App Layering console.
18. Copy the VMDK files from the SMB share to the datastore location for the template without disks from step 1, and attach them to the template VM.

19. Connect to the VM console, install Office 2019, and reboot the VM.
20. Recompile .Net runtimes with ngen utility in 32 and 64 bit mode.
21. Run the App Layer tools shortcut on the desktop to shut down and finalize the image.
22. Shutdown, and copy the VMDK files back to the SMB file share under the Finalize Disks folder.
23. Finalize the Application Layer in the console.
24. Create an Image template in the console.
25. Select the OS, Platform, and Application layers.
26. Deploy the template.
27. Deploy VMs via Citrix Virtual Apps and Desktops.

## Deploying App Volumes VMs (Generalized steps for comparison)

1. Create base a Windows 10 Enterprise VM image for packaging VM.
2. Install Windows updates.
3. Install the VMware App Volumes agent.
4. Clone the VM to create a baseline for deployed VMs.
5. Domain join the packaging VM.
6. Take a Snapshot of the packaging VM.
7. In App Volumes console, Create a new Application for Office 2019.
8. Configure the Package settings for Office 2019.
9. Connect to the VM, install Office 2019, and reboot the VM.
10. Use the App Volumes shortcut on the desktop to finalize and shut down the VM.
11. Finalize the package in the App Volumes console.
12. In vCenter, revert packaging VM to the snapshot created in step 6 to package another application.
13. In the App Volumes console, mark the application as active.
14. In the App Volumes console, assign the application to existing VMs/Users.

Read the report at <https://facts.pt/1fQOJG3>

This project was commissioned by VMware.



Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc. All other product names are the trademarks of their respective owners.

#### DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:

Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.'s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.'s testing. Customer's sole and exclusive remedies are as set forth herein.