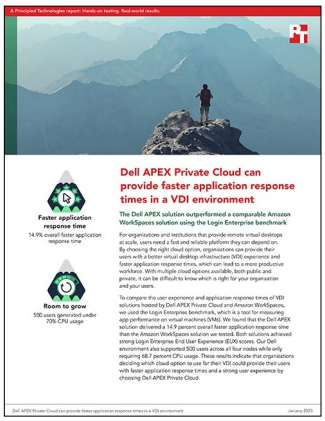

The science behind the report:

Dell APEX Private Cloud can provide faster application response times in a VDI environment

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 Dell APEX Private Cloud can provide faster application response times in a VDI environment.

We concluded our hands-on testing on November 24, 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 November 22, 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.

CPU utilization percentage for each run on each host during Dell APEX Private Cloud testing using Login Enterprise

Table 1: Maximum CPU utilization percentage for each run on each host.

Maximum CPU %	Host 1	Host 2	Host 3	Host 4
Run 1	71.7	75.0	75.6	72.0
Run 2	70.6	72.0	71.3	71.0
Run 3 (Median)	70.0	71.3	70.4	69.9

Table 2: Average CPU utilization percentage for each run on each host.

Average CPU %	Host 1	Host 2	Host 3	Host 4
Run 1	70.1	72.8	72.8	69.9
Run 2	68.5	69.8	68.6	68.3
Run 3 (Median)	68.4	69.7	68.6	68.1

Performance across all hosts during Dell APEX Private Cloud testing

Table 3: CPU utilization percentage, Login Enterprise EUX scores, and app errors across all hosts.

	Average CPU utilization%	Maximum CPU utilization %	Login Enterprise EUX score (higher is better)	App errors (determines median)
Run 1	71.4	75.6	7.9	99.9
Run 2	68.8	72.0	7.9	99.8
Run 3 (Median)	68.7	71.3	7.9	99.9

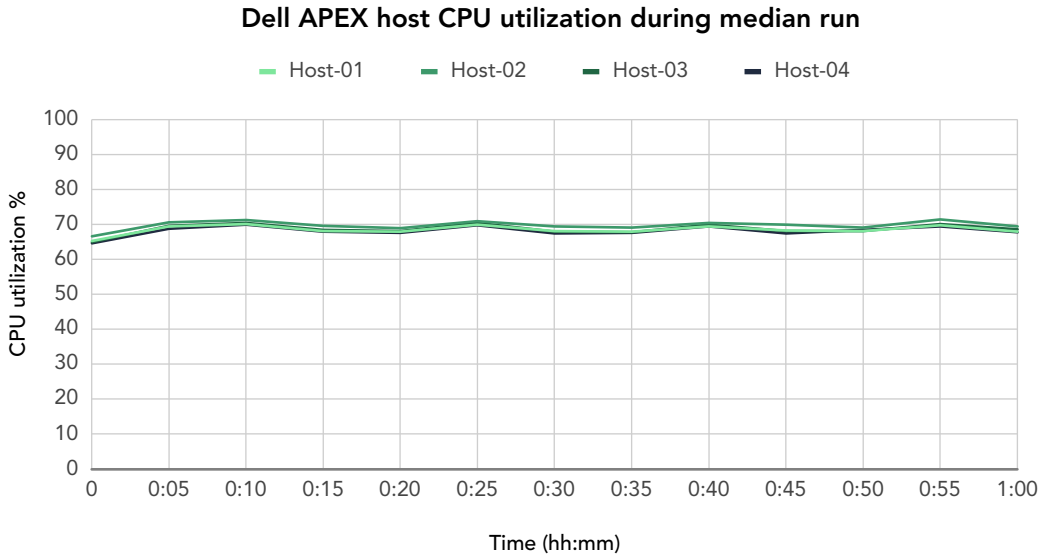

Figure 1: Dell APEX host CPU utilization percentage during the median run using Login Enterprise.

Login Enterprise EUX scores and application response times

Table 4: Login Enterprise EUX scores and application response times (in seconds) for the median runs of Dell Apex Private Cloud and Amazon WorkSpaces testing.

Login Enterprise results	Dell APC with VMware Horizon	AWS WorkSpaces
VSImax	> 500 Users	> 500 Users
EUX score	7.9	8.0
Microsoft Word		
Start	1.275	1.007
Open Window	0.518	0.481
Open Word document	1.191	1.233
Saving file	0.382	0.388
Total	**3.366**	**3.109**
Microsoft Excel		
Start	1.303	1.454
Saving file	0.494	0.538
Open Window	0.531	0.515
Open Excel document	1.269	1.187
Total	**3.597**	**3.694**
Microsoft PowerPoint		
Start	1.214	1.230
Open Window	0.468	0.423
Open PowerPoint document	1.735	2.220
Saving file	1.015	1.100
Total	**4.432**	**4.973**

Login Enterprise results	Dell APC with VMware Horizon	AWS WorkSpaces
Microsoft Outlook		
Start	2.821	4.990
Total	**2.821**	**4.990**
Microsoft Edge		
Logon	0.108	0.084
Total	**0.108**	**0.084**
Totals	**14.324**	**16.850**

System configuration information

Table 5: Detailed information on the systems we tested.

System configuration information	4 x Dell® VXRAIL™ V670F
BIOS name and version	Dell 1.5.4
Non-default BIOS settings	Unknown
Operating system name and version/build number	VMware® ESXi™, 7.0.3, 19898904
Date of last OS updates/patches applied	2022-09-21
Power management policy	Performance
Processor	
Number of processors	2
Vendor and model	Intel® Xeon® Gold 6338
Core count (per processor)	32
Core frequency (GHz)	2.00
Stepping	6
Memory module(s)	
Total memory in system (GB)	1,024
Number of memory modules	16
Vendor and model	Hynix® Semiconductor HMAA8GR7CJR4N-XN
Size (GB)	64
Type	DDR-4
Speed (MHz)	3,200
Speed running in the server (MHz)	3,200
Local (OS) storage controller	
Vendor and model	Dell BOSS-S2
Cache size (MB)	0
Firmware version	2.5.13.4008
VMware vSAN™ storage controller	
Vendor and model	Dell HBA355i
Cache size (MB)	0
Firmware version	17.15.08.00
Local (OS) storage	
Number of drives	2
Drive vendor and model	Micron® MTFDDAV480TDS
Drive size (GB)	447.13
Drive information (interface, type)	M.2, NVMe®

System configuration information	4 x Dell® VXRAIL™ V670F
vSAN storage	
Number of drives	6
Drive vendor and model	Samsung® MZ7L33T8HBLTAD3
Drive size (GB)	3576.98
Drive information (interface, type)	SATA, SSD
vSAN configuration	
Configuration summary	4-node vSAN cluster
Disk groups per host	2
Capacity disks per group	3
Cache disks per group	1
Storage Policy	vSAN Default Storage Policy
Space Efficiency	None
Data-at-rest encryption	Disabled
Data-in-transit encryption	Disabled
RDMA support	Disabled
Network adapter A	
Vendor and model	Broadcom® NetXtreme® E-Series Advanced Dual-port 25Gb SFP28 Ethernet OCP 3.0
Number and type of ports	2, 25Gb SFP28
Driver version	22.0.7.60
Network adapter B	
Vendor and model	Broadcom BCM57414 NetXtreme-E 10Gb/25Gb RDMA Ethernet
Number and type of ports	2, 10Gb/25Gb Ethernet
Driver version	UNK
Cooling fans	
Vendor and model	Dell Embedded
Number of cooling fans	12
Power supplies	
Vendor and model	Dell PWR SPLY, 2400W, RDNT, DELTA
Number of power supplies	2
Wattage of each (W)	2,400

Table 6: Version information for the software we used in testing.

Software version information	
Virtual desktop infrastructure (VDI) management	VMware Horizon® 8
VDI management build number	8.6.0 build – 20099816 Version 2206

Table 7: Detailed information on the cloud solutions we tested.

Cloud configuration information	Dell APEX Private Cloud	Amazon WorkSpaces
General information		
Date testing ended	2022-10-27	2022-11-23
Cloud service provider (CSP)	Dell APEX™ Private Cloud	AWS® WorkSpaces
Region	US South	us-east-1
Availability zones	N/A	us-east-1a & us-east-1c
Workload information		
Workload name and version	Login Enterprise® 4.9.4	Login Enterprise 4.9.4
Workload type	Standard Knowledge Worker	Standard Knowledge Worker
Connector customization	N/A	Provided by Login Enterprise (available at https://github.com/mkent-at-loginvsi/AWSWorkspacesClient)
Cloud VM or instance details		
Number of VMs	500	500
VM or instance size	vSphere 2vCPU, 4GiB RAM, 50GB drive	Standard Base, 2vCPU, 4GiB RAM, 80GB drive, 10GB user
BIOS name and version	VMware, Inc. VMW71.00V.18227214. B64.2106252220, 2.7	Xen 4.2.amazon, 2.7
vCPU	2	2
Memory (GB)	4	4
Underlying processor model	Intel Xeon Gold 6338 CPU @ 2.00GHz	Intel Xeon CPU E5-2676 v3 @ 2.40GHz
vNIC information/Underlying NIC speed (GB)	10	1
vNIC driver version	1.9.9.0	8.2.5.32
Other instance hardware or parameter details	Launchers located on Dell APEX Private Cloud infrastructure	Launchers located at PT data center
Operating system information		
Image or template name and UUID	"Win10VDI Template 4"	Custom based on "Standard with Windows 10 (Server 2019 based)" 2 vCPU, 4.0 GB Memory, 10 GB Storage
Operating system name	Microsoft Windows 10 Pro Version 10.0.19043	Microsoft Windows Server 2019 Datacenter Version 1809
Operating system build number	Build 19043	Build 17763.3650
Date patches last applied	2022-10-26	2022-11-10
Changes made from CSP image	No – custom image created (not provided by CSP)	Updated to latest patches, added Office 2019 (Word, Excel, PowerPoint, Outlook)

Cloud configuration information	Dell APEX Private Cloud	Amazon WorkSpaces
Instance storage (volume type 1)		
Number of volumes	1	2
Volume use in this test	OS	OS, data
CSP volume type	vSAN Datastore on Dell VXRAIL	WorkSpaces defined General Purpose SSD EBS volumes
OS volume size (GB)	50	80
Data volume size (GB)	N/A	10
Encryption type	None	None

How we tested

Overview

The following methodology outlines steps to compare Dell APEX Private Cloud and Amazon WorkSpaces utilizing the Knowledge Worker Workload from Login Enterprise (LE).

Our infrastructure for Dell APEX Private Cloud consisted of an environment with two four-node ESXi clusters running the following infrastructure: domain controller (DNS, DHCP, Active Directory, Certificate Authority), VMware Horizon 8 server, Login Enterprise appliance, and 20 Login Enterprise Launchers on one cluster and 500 virtual desktops on the other cluster. Dell hosted all servers in their private data center located in Texas.

We determined the number of 500 virtual desktops on our cluster by repeatedly running our Knowledge Worker workload until we reached our saturation point. We considered the cluster saturated when our workload reached our target of 65-75 sustained percent CPU utilization. We increased the number of VMs until performance measured consistently across the run as seen in Figure 1 (CPU utilization). We measured processor utilization using vRealize Operations.

After determining the optimal number of VMs for Dell APEX Private Cloud, we ran the same test with 500 users on Amazon WorkSpaces. We created a Virtual Private Cloud (VPC) and deployed a Directory Server and the required WorkSpaces VMs. We received custom code from Login Enterprise to run the LE Knowledge Worker workload on the AWS solution. Our Login Enterprise Server and launchers were located at the PT office in Durham, NC, while the WorkSpaces infrastructure was located on us-east-1. We created scripts to create our directory users and our individual WorkSpaces.

We conducted Login Enterprise Knowledge Worker workload testing using five applications:

- Microsoft Word
- Microsoft Excel
- Microsoft Outlook
- Microsoft PowerPoint
- Microsoft Edge

Between each test, we restarted all VMs and waited 30 minutes. Each test includes a 125-minute logon period, or 1 minute per system per host. Once our launchers finished initiating logins and detected that all users were ready, each user ran the Knowledge Worker workload. For a description of the Knowledge Worker workload, vist https://support.loginvsi.com/hc/en-us/articles/6964511176348-Knowledge-worker-default-workload-.

Dell APEX Private Cloud environment summary

Below is a summary of our Dell APEX Private Cloud Environment. Our four-node Dell APEX Cloud cluster hosted a VMware Horizon server running 500 virtual desktops.

Hardware

- Server model: 4 x Dell VXRAIL E670F
- Processors: Intel Xeon Gold 6330 CPU @ 2.00GHz
- Memory: 1 TB memory (pool total 4 TB)
- Local SSD storage: 448 GB
- Shared vSAN total: 85.46 TB
- Network adapters: 25 Gbit/s NICs

Virtual machines

- Infrastructure cluster
  - vCenter (pre-configured by Dell)
  - Domain Controller with four vCPUs, 16 GB of memory, and a120GB hard drive
  - VMware Horizon 8 Server with four vCPUs, 16 GB of memory, and a 120GB hard drive
  - Login Enterprise (LE) Appliance with two vCPUs, 4 GB of memory, and a 100GB hard drive
  - 20 x Windows Server 2022 LE Launchers, each with four vCPUs, 16 GB of memory, and a 120GB hard drive
- VDI cluster

- 500 x Windows 10 virtual desktops, each with two vCPUs, 4 GB of memory, and a 50GB hard drive

Amazon WorkSpaces environment summary

Our Amazon WorkSpaces environment used a WorkSpaces Directory on a virtual private cloud in us-east-1. As you configure the AWS environment, you'll see many available options, such as VPC Configuration, Directory Type, OS Version, and Primary/Secondary Availability Zones. Below we show the options that we chose for this settings section:

- Cloud Network Type: VPC
- Availability Zones:
- Customize AZs→Primary: us-east-1a, Secondary: us-east-1c
- NAT gateways: One per AZ
- Directory Service:
  - Directory Type: AWS Managed Microsoft AD
  - Microsoft AD Edition: Standard Edition for small to medium sized businesses
  - VPN and subnets: Select the VPC created for the test along with the private subnets it contains
- 500 WorkSpaces:
  - Bundle: "Standard with Windows 10 (Server 2019 based)" - two vCPUs, 4.0 GiB of Memory
  - Root volume: 80 GB
  - User volume: 10 GB
  - Protocol: PCoIP

Configuring the Dell APEX Private Cloud environment

Dell provided a stock Dell APEX Private Cloud environment for our team we describe in System configuration information. Dell preconfigured our SUT cluster as a typical customer would receive their private cloud solution. Therefore, Dell provided a login to the preconfigured vCenter environment with vRealize already deployed along with vSAN and Distribute Switch services.

Below are the steps we took to configure our environment including customizing our policies and deploying the server roles for AD, DNS, DHCP, and ADCS. We also deployed Horizon.

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 gold VM for virtual desktops ensure testing executed correctly.

Installing Active Directory Domain Services

1. Log into the vSphere client as administrator@vsphere.local.
2. On the infrastructure server, deploy a Windows Server 2022 VM named DC01, and log in as an administrator.
3. Launch Server Manager.
4. Change computer name, set static IP, and reboot.
5. Click Manage→Add Roles and Features.
6. At the Before you begin screen, click Next.
7. At the Select installation type screen, leave Role-based or feature-based installation selected, and click Next.
8. At the Server Selection Screen, select the server from the pool, and click Next.
9. At the Select Server Roles screen, select Active Directory Domain Services.
10. When prompted, click Add Features, and click Next.
11. At the Select Features screen, click Next.
12. At the Active Directory Domain Services screen, click Next.
13. At the Confirm installation selections screen, check Restart the destination server automatically if required, and click Install.

Configuring Active Directory and DNS services on DC01

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 `vdi.test`, and click Next.
5. At the Domain Controller Options screen, leave the default values, and enter a password twice.
6. To accept default settings for DNS, NetBIOS, and directory paths, click Next four times.
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 vdi\Administrator and the password you chose in step 5.
11. Open DNS Manager on your DNS.
12. Right-click your DNS FQDN, and choose Properties.
13. Click the Forwarders tab.
14. Click the Edit button.
15. Add the IP address of the primary DNS on the network, and click OK.
16. Click Apply / OK.

Configuring 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, 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 in the previous section (VDI\Administrator), and click Commit.
12. On the Summary page, click Close.
13. On the Add Roles and Features Wizard, click Close.
14. In Server Manager, click Tools→DHCP.
15. In the left pane, double-click your server, and click IPv4.
16. In the right pane, under IPv4, click More Actions, 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: `100.80.42.10`
    - End IP address: `100.80.43.254`
    - Length: `23`
    - Subnet mask: `255.255.254.0`
20. Click Next.
21. At the Add Exclusions and Delay page, leave defaults, and click Next.
22. Set the Lease Duration to four hours, 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. At the Specify IPv4 DNS Settings screen, for the parent domain, type `vdi.test`
26. Type the preferred DNS server, and 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 Certificate Services in Microsoft Active Directory on DC01

1. Log onto DC01 as administrator@vdi.test.
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 DC01.vdi.test, and click Next.
7. At the server roles menu, check Active Directory Certificate Services.
8. When prompted, click Add Features, and click Next.
9. Leave Select features at defaults, and click Next.
10. At the Active Directory Certificate Services introduction page, click Next.
11. Select Certification Authority and Certification Authority Web Enrollment.
12. When prompted, click Add Features, and click Next.
13. Click Next three times, click Install, and click close.
14. In server manager, click the yellow triangle titled Post-deployment configuration.
15. On the destination server, click Configure Active Directory Certificate Services.
16. Leave credentials as vdi\administrator, and click Next.
17. Select Certification Authority, Certificate Enrollment Web Service, and Certification Authority Web Enrollment, and click Next.
    - If one or more of these options are greyed out, continue through the process, and then go through it again to include the missing components.
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, and click Next.
25. Click Configure.
26. When the system is finished configuring, click Close.
27. Reboot.
28. Open a command prompt, and type `ldp`
29. Click Connection and connect.
30. For server, type `dc01.vdi.test`
31. Change the port to 636.
32. Check SSL, and click OK.

Configuring secure LDAP on DC01.vdi.test on DC01

1. Open administrative tools, and select Certification Authority.
2. Click vdi-DC01-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, and click Apply.
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 (certsrv).
11. In the right pane, right-click Certificate Templates→New→Certificate Template to Issue.
12. Select LDAPoverSSL, and click OK.

Configuring the Windows gold VM image for Dell APEX Private Cloud environment

We created a base image to deploy using VMware Horizon. For this gold image, we created a Microsoft Windows 10 Enterprise VM, then installed Microsoft Office Professional Plus 2019.

Creating the baseline Windows 10 VM

1. In vCenter, right-click the host, and select New Virtual Machine…
2. Select Create a New Virtual Machine, and click Next.
3. Enter a name for the VM, and select the location for the virtual machine, and click Next.
4. Select the host for the new VM, and click Next.
5. Select the datastore for the new VM, and click Next.
6. For the compatibility level, select ESXi 7.0 U2 and later, and click Next.
7. Select the Guest OS Family and Version: Windows/ Microsoft Windows 10 (64-bit), and click Next.
8. Adjust the virtual hardware settings to match the following:
   - CPU: 2
   - Memory: 4 GB, Reserve all guest memory (All locked)
   - Hard Disk: 50 GB (Thin Provision)
   - New SCSI controller: VMware Paravirtual
   - New Network: <Test network name>, Adapter type: VMXNET 3
9. To add a second CD/DVD drive, 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`, and set the Value to `false`.
17. Click Next.
18. Click Next, and click Finish.

Installing Windows 10 on the baseline VM

1. Start the VM, and click Launch Remote Console.
2. Select the region settings for Windows 10, and click Next.
3. Click Install now.
4. Select Windows 10 Enterprise, and click Next.
5. Accept the license agreement, and click Next.
6. Click Custom: Install Windows only (advanced).
7. In the vCenter UI, select the VM, click Install VMware Tools…, and select MOUNT.
8. In the VM remote console, click Load driver.
9. Click Browse, and on the VMware Tools drive, navigate to \Program Files\VMware\VMware Tools\Drivers\pvscsi\Win8\amd64.
10. Click OK.
11. Select the VMware PVSCSI Controller, and click Next.
12. To install on Drive 0, click Next.
13. When presented with the region dialog, press CTRL+SHIFT+F3 to enter Audit mode.

Configuring the baseline VM

1. If the VM is 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 the following:
   - Carbon Black Helper
   - Service Discovery
   - Volume Shadow Copy
6. Click Next.
7. Click Install.
8. Obtain and install the latest version of the VMware Horizon Agent.
9. Accept defaults until you reach Custom Setup.
10. At Custom Setup, disable all features except the following:
    - Core
    - VMware Horizon Instant Clone
    - VMware Audio
11. Click Next.
12. Enable the remote Desktop capability on this computer, and click Next.
13. Click Install.
14. To reboot the VM, click Finish, and click Yes.
15. To install .Net Framework 3.5, open an Administrator command prompt, and enter:

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

16. Run Windows Update.

Forcing Edge to update to the latest available version

1. Open Edge, and complete the initial setup. The prompt appears when you first open the application.
2. Browse to edge://settings/help, and let Edge complete the auto-update process.
3. Once the update is complete, exit the browser.
4. Open File Explorer, and browse to C:\Program Files (x86)\Microsoft\EdgeUpdate\.
5. Rename MicrosoftEdgeUpdate.exe to disable the auto-update feature:
   - Note: If you do not disable the auto-update feature, Edge will update to a new version (when available) each time you open the browser.
6. Reboot the VM.

Installing Office Professional Plus 2019 on the gold image VM

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.

Installing Office 2019

1. Download the Office Deployment Tool from https://go.microsoft.com/fwlink/p/?LinkID=626065.
2. Save and run the following the prompts throughout the installer.
3. Create a new folder at the root of C: called O365 (should look like C:\O365\), and press OK.
4. Open a text editor, and save the following as C:\O365\configuration-Office2019Enterprise-mod.xml:

```
<Configuration>
  <Add OfficeClientEdition="64" Channel="PerpetualVL2019">
    <Product ID="ProPlus2019Volume">
      <Language ID="en-us" />
      <ExcludeApp ID="Access" />
      <ExcludeApp ID="Groove" />
      <ExcludeApp ID="Lync" />
      <ExcludeApp ID="OneDrive" />
      <ExcludeApp ID="OneNote" />
      <ExcludeApp ID="Publisher" />
      <ExcludeApp ID="Teams" />
    </Product>
  </Add>
  <RemoveMSI All="True" />
  <!--  <Display Level="None" AcceptEULA="TRUE" />  -->
  <!--  <Property Name="AUTOACTIVATE" Value="1" />  -->
</Configuration>
```

5. To begin the installation of Office 2019, open a command prompt, navigate to C:\O365\, and execute:

```
setup.exe /configure configuration-Office2019Enterprise-mod.xml
```

6. Once the installation completes, open Windows Update, and click Advanced options.
7. Enable Receive updates for other Microsoft products, and click Back.
8. Click Check for updates, and reboot if necessary.
9. Clean up any downloads, and empty the recycling bin.

Optimizing the base image using the VMware OS Optimizer Tool

1. Obtain and install the latest version of VMware OS Optimizer Tool (OSOT).
2. When the tool opens, click the Analyze button to start.
3. Click Common Options.
4. Click Security.
5. Select Disable Firewall, Disable Antivirus, and Disable Security Center, and click OK.
6. Keep the default selections, and click Optimize.
7. At the top, click Generalize.
8. Verify Time Zone, Input, and System Locale, and check the box for Automatic Restart. At the bottom, click Generalize. Once the process is complete, the VM will automatically reboot.
9. Download LGPO from https://www.microsoft.com/en-us/download/details.aspx?id=55319.
10. Download Secure Delete from https://download.sysinternals.com/files/SDelete.zip.
11. Extract to the same folder as OSOT (you may need to obtain this again after Generalizing the image).
12. To check whether you need to unblock the executables, right-click, and choose Properties.
13. Open OSOT, and at the top, click the Finalize tab.
14. At the bottom, click Finalize. Note: You will receive a prompt once complete.
15. Open the run box or command prompt, and execute the following command:

```
shutdown /s /t 0 /c "Image Ready"
```

Cleaning up the base image VM settings

Before capturing our gold image, we optimized the VM hardware by removing unnecessary options.

1. Right-click the gold image, and select Edit Settings.
2. Remove the CD/DVD drives.
3. Remove the SATA Controller, and click OK.
4. Right-click the gold image→Template→Export OVF Template.
5. Name the template, check the Advanced checkbox and Include extra configuration, and click OK. Note: This can take some time.
6. Delete the gold image VM from disk, and confirm.
7. Deploy the OVF Template you exported in step 5.
8. Right-click SUT, and click Deploy OVF Template.
9. Select local file, and upload files. When prompted, select the four files you previously created in step 5, and click OK.
10. Click Next.
11. Name the virtual machine, choose a location for it, and click Next.
12. Select a compute resource, and click Next.
13. Review the details, and click Next.
14. On the Select storage page, select the storage, change the virtual disk format to Thin Provision, and click Next.
15. Verify the desired network is selected, and click Next.

Preparing the image for deployment

To clone the VM in VMware Horizon, we needed to convert the gold VM to a VM template.

1. Right-click the imported OVF→Clone→Clone to Template.
2. Name the template, and complete the wizard with the remaining default options.

Deploying the virtual desktop pool on Dell APEX Private Cloud

Creating customization specifications (required for Horizon pool creation)

1. Open vCenter, and in the upper left, click the hamburger menu.
2. Click Policies and Profiles.
3. Select VM Customization Specification.
4. Click + New...
5. On page 1, specify a name for the Customization, set the appropriate vCenter Server, target OS, and ensure the checkbox next to Generate a new security identity (SID) is checked.
6. On page 2, specify an Owner name and Owner organization, which will be reflected in the OS of the virtual desktops.
7. On page 3, next to Use the virtual machine name, select the radio button.
8. On page 4, enter a product key for the appropriate OS, and do not check the box for Include server license information.
9. On page 5, enter and confirm a password for the Administrator account on the virtual desktops but do not check the box for Automatically logon as Administrator. This allows our Login Enterprise launchers to log in as the corresponding user without having a conflict with the existing local account.
10. On page 6, set the time zone.
11. Skip page 7.
12. On page 8, next to Use standard network settings for the guest operating system…, ensure the radio button is selected.
13. On page 9, enter your Windows Server domain and your domain administrator username and password.
14. On page 10, verify the accuracy of the information you entered, and click Finish.

Configuring a desktop pool and authorizing users/groups on the Horizon01 VM

1. Connect to the Horizon01 VM admin portal.
2. In the left pane, navigate to Inventory→Desktops, and click the Add button.
3. Ignore the More Information prompt about enabling View Storage Accelerator.
4. Select Automated Desktop Pool, and click Next.
5. Ignore the More Information prompt about enabling View Storage Accelerator.
6. Select Full Virtual Machines, and ensure the <vCenter FQDN> server is selected, and click Next.
7. Select Dedicated, check Enable Automatic Assignment, and click Next.
8. Click Next on Storage Policy Management if no vSAN is configured. Note: Use vSAN in Dell environment as it's available.
9. Enter `VDITest` for both the ID and Display Name, and click Next.
10. Make the following adjustments:

- Use a Naming Pattern.
- Specify the naming pattern. We used Win10VDI-{n:fixed=3}
- All Machines Up-Front.
- Maximum Machines: 500.

11. Click Next.
12. Make selections for vCenter Settings, and click Next.
13. Keep defaults for Desktop Pool Settings, and click Next.
14. Change Maximum number of monitors to 1, and click Next.
15. Keep defaults for Advanced Storage Options, and click Next.
16. Select desired customization specification for the Guest OS, and click Next.
17. Check box for Entitle Users After Adding Pool, and click Submit.
18. Click Add.
19. Enter a Name/User Name starts with: `vdi`

    - Note: This should identify the VDI users group.

20. Click Find.
21. Check box to select all, and click OK.
22. Click OK.

Deploying Login Enterprise

We used the following steps to deploy our Login Enterprise Appliance on both the Dell APEX Private Cloud environment and the Amazon WorkSpaces environment.

Deploying the Login Enterprise appliance

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 Login Enterprise OVA, click Open, and click Next.
4. Select a data center, 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.
11. Log into the Login Enterprise VM, and follow the prompts.
12. Set the new IP and admin password, and when prompted, allow the VM to reboot. This can take up to 10 minutes. Log back into the Login Enterprise VM with new password.
13. In the Login Enterprise console, generate new encryption key, and record the key.

Configuring the login component for Login 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. From the zip, extract LoginPI.Logon.exe, and copy it to {domain}/scripts directory on the sysvol share of the domain controller.
4. In the Virtual User Accounts pane, click the +, and click Bulk Accounts.
5. Enter the base Username, Password, Domain, Number of digits for the user sequence, and Number of accounts to create. Click Save.

    - Example: vsiuser_ , <Password> , vdi , 3 , 500

6. Once the bulk accounts have been created, create an Account Group by clicking the + to Add new account group→Filter.
7. Enter a name for your group and a description, and click Next.
8. Enter * to select all the users, and click Save.
9. Log into DC01 as a domain administrator.
10. In the Windows Active Directory Users and Computers control panel, create a group called VDI Users of:

    - Group scope: Global
    - Group type: Security

11. Use the following PowerShell code to create bulk users and add them to the intended security group (created above):

```
$start = 1
$end = 500
$count = $start..$end
$path = "CN=Users,DC=vdi,DC=test"
$userName = "vsiuser_"

foreach ($i in $count) {

Write $i $number
$number = ($start++).ToString(("0").PadLeft(3,'0'))

New-AdUser -Name $userName$number -Path $path -Enabled $True -ChangePasswordAtLogon $false `
     -AccountPassword (ConvertTo-SecureString "<Password>" -AsPlainText -force) -passThru `
     -ScriptPath "LoginPI.Logon.exe https://<IP of LE appliance>"
Get-ADUser -Identity $UserName$Number | Add-ADPrincipalGroupMembership -MemberOf "VDI Users"
}
```

Installing the Microsoft Edge driver on the Login Enterprise appliance

1. Find the Microsoft Edge (x64) driver matching the current version of Edge installed on your Windows 10 VM at https://developer.microsoft.com/en-us/microsoft-edge/tools/webdriver/.
2. Connect to the Login Enterprise appliance via SSH. A menu will appear.
3. Navigate to Troubleshooting→Open Bash Shell.
4. To set permissions, execute command:

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

5. Change directory to `/loginvsi/content/selenium`
6. In `/loginvsi/content/selenium`, create a folder named `EdgeChromium<Major Version #>`
   - Example: `/loginvsi/content/selenium/EdgeChromium105`
7. To download the Edge browser, execute command:

```
wget <URL to x64 version of Edge from step 1>
```

   - Example: `wget https://msedgedriver.azureedge.net/105.0.1343.33/edgedriver_win64.zip`
8. Extract msedgedriver.exe from the downloaded zip file by executing the command:

```
unzip edgedriver_64.zip
```

9. Copy the .zip file to the folder you created in step 6 by executing the command:

```
cp msedgedriver.exe EdgeChromium<Major Version#>
```

Configuring the Amazon WorkSpaces environment

We followed the linked documentation throughout this section to configure our Amazon WorkSpaces environment: https://docs.aws.amazon.com/workspaces/latest/adminguide/launch-workspace-microsoft-ad.html

Creating the VPC

1. From the VPC console, click Create VPC.
2. Create the following resources:
   - VPC and more (default)
   - Check auto-generate for name-tagging and specify name
3. Set the number of Availability Zones (AZs) to 2 (default).
4. Next to Customize AZs, configure your Availability Zones according to the following:
   - Number of public subnets: 2 (default)
   - Number of private subnets: 2 (default)
5. Set NAT gateways to 1 per AZ.
6. Click Create VPC.

Creating the directory

1. Click Create Directory.
2. Select AWS Managed Microsoft AD (default), and click Next.
3. Make the following selections:
   - Edition: Standard Edition
   - Organization name: <Your company name>
   - Directory DNS name: <Your company FQDN>
4. Create and confirm an admin password.
5. Click Next.
6. Choose the VPC you created in the previous section.
7. Choose the 2 private subnets you created for the selected VPC.
8. Click Next.
9. Click Create.

Adding user to the WorkSpaces directory

After creating the target Directory, we deployed a domain-joined EC2 VM with the following configuration, which we used to manage user credentials for our 500 users:

- Instance type: t2.xlarge (4 vCPU, 16 GiB memory, 30 GiB disk)
- Availability Zone: us-east-1a

Configuring the gold VM image for Amazon WorkSpaces environment

Creating the WorkSpace gold VM Image

1. Click Create WorkSpaces.
2. Select the directory you created in the Creating the directory section, and click Next.
3. Create required user(s) (if not already present in Active Directory), and click Next.
4. Select the Bundle Standard with Windows 10 (Server 2019 based) with the client protocol PCoIP, and click Next.
5. Set AutoStop to 2-3 hours (ensure they stay online long enough to complete a full test).
6. Under Customization, next to User volume, click the down arrow, select a root/user combination of 80/10, and click Next.
7. At the bottom of the Review page, click Create Workspaces.
8. Launch the WorkSpace.
9. Download the WorkSpaces client software to access to the WorkSpace at https://clients.amazonworkspaces.com/.
10. Enter the registration code from the WorkSpace summary page into the WorkSpaces client software.
11. Enter the username and password into the WorkSpaces client software to access the WorkSpace.
12. Download the Edge browser, and capture current version.
13. Ensure the version of Edge is loaded into the LE appliance per earlier instructions in the Installing the Microsoft Edge driver on the Login Enterprise appliance section.
14. Disable update of Edge per earlier instructions in the Forcing Edge to update to the latest available version section.
15. Install Office 2019 per the instructions in the Installing Office Professional Plus 2019 on the gold image VM section.
16. Launch Windows Update to ensure the latest updates are applied to the VM.
17. Shut down the VM.

Creating the WorkSpaces image and bundle

1. If you are still connected to the WorkSpace, disconnect by choosing Amazon WorkSpaces, and Disconnect in the WorkSpaces client application.
2. In the WorkSpaces console, in the navigation pane, choose WorkSpaces.
3. To open the WorkSpace's details page, select the WorkSpace. Click Create image.
4. When prompted, reboot (restart) your WorkSpace. Rebooting your WorkSpace will update it to the latest version. Once the system shows as available with no modifications, continue to the next step.
5. Enter an image name. Choose Create Image. Once the system has created the image, continue to the next step.
6. In the navigation pane, choose Images.
7. Select the newly created image, and choose Actions and Create bundle. It may take 45 minutes to show as available.
8. Enter a bundle name and a description, and then select the following:
   - For Bundle hardware type: Standard Base
   - For Storage settings: 80 GB Root volume size, 10 GB User volume size
9. Select Create bundle. Check back in a few minutes to see if it completed.
10. To create 500 WorkSpaces, we used AWS CLI to initiate. Here is an example command:

```
aws workspaces create-workspaces --profile=<profile> --workspaces DirectoryId=<DirectoryID>,UserName=<
UserName>,BundleId=<BundleID>,Tags=[{Key=<KeyName>,Value=<Value>}] --region us-east-1
```

Configuring the PT environment for Amazon WorkSpaces

There were several occurrences where our test environment required a different configuration from the SUT environment. We outline many of those occurrences below.

We hosted 20 launchers to push the workload for our AWS testing. We setup an isolated network, a router with public access, and jumpboxes to help drive this effort.

Deploying the launchers

Note: The launcher software must be open on the launcher for it to be detected and available within Login Enterprise.

We handled our launcher virtual machines differently for each test scenario. For our Dell testing, we hosted our launcher VMs on the Infrastructure Cluster. For AWS, we hosted the launcher VMs in our labs, on a PT hosted cluster. We configured them as follows.

Creating the baseline launcher VM

1. In vCenter, right-click an infrastructure cluster host, and select New Virtual Machine…
2. Select Create a New Virtual Machine, and click Next.
3. Enter a name for the VM, and select the location for the virtual machine, and click Next.
4. Select the host for the new VM, and click Next.
5. Select the datastore for the new VM, and click Next.
6. Select the compatibility level ESXi 7.0 U2 and later, and click Next.
7. Select the Guest OS Family and Version: Windows/ Microsoft Windows Server 2022 (64-bit), and click Next.
8. Adjust the virtual hardware settings to match the following:
   - CPU: 4
   - Memory: 16 GB
   - Hard Disk: 50 GB (Thin Provision)
   - New SCSI controller: LSI Logic SAS
   - (Dell APEX Private Cloud) New Network: <Private network name>, Adapter type: VMXNET 3
   - (AWS) New Network: <Public network name>, Adapter type: VMXNET 3
   - CD/DVD drive 1: Content Library ISO File (browse to the location where Windows Server 2022 ISO is stored)
9. Click Next, then click Finish.

Installing Windows Server 2022 on the baseline launcher VM

1. Start the VM, and click Launch Remote Console.
2. To start booting from the mounted ISO, press any key.
3. Select the region settings for Windows Server 2022, and click Next.
4. Click Install now.
5. Enter the product key for Windows Server 2022, and click Next.
6. Select Windows Server 2022 Standard (Desktop Experience), and click Next.
7. Accept the license agreement, and click Next.
8. Click Custom: Install Microsoft Sever Operating System only (advanced).
9. Click Next to install on Drive 0.
10. When presented with the region dialog, press CTRL+SHIFT+F3 to enter Audit mode.

Modifying Windows to allow necessary traffic for testing

1. Disable firewalls for all three zones (public / domain / private).
2. Enable Remote Desktop with minimal security.
3. From the Server Setup menu, disable IE security features.
4. Edit hosts file for IP and DNS of the Login Enterprise appliance.

Installing the launcher setup

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, and run Setup.msi.
4. Click Next, and proceed through the installer.
5. Click Finish to close the installation once it completes.

Installing the VMware Horizon View client

Note: This step is for Dell APEX Private Cloud only.

1. Download the VMware Horizon View client from the homepage of the Horizon Server or from https://www.vmware.com/go/viewclients#win64.
2. Upon opening, click Customize Installation.
3. Enter the default connection server (as FQDN).
4. Leaving all other options unchanged, click Agree & Install.
5. Upon completing the installation, accept the prompt to reboot.

Installing the Amazon WorkSpaces client and performing the initial login

Note: This step is for Amazon WorkSpaces only.

1. At the Welcome screen, click Next.
2. At Installation Scope, select Install for all users of this machine, and click Next.
3. At Destination Folder, keep the default, and click Next.
4. At the Ready to Install page, click Install.
5. Upon completion, click the Finish button, and open the Amazon WorkSpaces application.
6. Enter your registration code for Amazon WorkSpaces, and click Register.
7. Download the Custom Connector files for testing Login Enterprise on AWS. Note: Login Enterprise provided us with custom code for running the AWS testing for Login Enterprise.
8. Place the Login Enterprise custom connector files at C:\Program Files\Login VSI\Login PI 3 Launcher\AWS\.
9. Ensure each of the custom connector files is unblocked (right-click→Properties→look for unblock checkbox).

Importing the root CA for your local domain

1. Visit http://< IPofDC >/certsrv.
2. Log in as the administrator account.
3. Click Download a CA certificate.
4. Select the root CA of your domain controller (if not already selected), and click Install CA certificate.
5. If prompted, keep the file, and open it.
6. Click Install Certificate.
7. Navigate to Local Machine→Next.
8. Place the certificate in the Trust Root Certification Authorities certificate store, select Next, and click Finish.

Creating the VM template for the launcher

1. To shut down the VM and leave a comment in the logs saying image ready, once the Launcher template VM has been prepared according to the steps above, open the run box or command prompt and execute the command:

```
shutdown /s /t 0 /c "Image Ready"
```

2. Right-click the Launcher Gold image you just created, select Template→Convert to Template, and click Yes.
3. To clone the required number of Launchers from the Launcher template, right-click the Infrastructure cluster, and select New Virtual Machine…
4. Select Deploy from template, and click Next.
5. Click the Data Center tab, select the Launcher Gold image, and click Next.
6. Enter a name for the new Launcher clone, and click Next.
7. Select an Infrastructure host, and click Next.
8. Select the storage location, and click Next.
9. Click Next, and click Finish.
10. On each clone, do the following:

    - Change the computer name in Windows Sever 2022.
    - Use AutoLogon from SysInternals to automate the login process.
    - Open startup directory for the Administrator account, and place a shortcut to the Login Enterprise launcher in it.
    - Reboot to test login and launching of the launcher application.
    - Verify the Login Enterprise appliance detects the launcher.

Creating the LE test applications

Note: Login Enterprise provided us with custom code for running the AWS testing for Login Enterprise.

1. In the Login Enterprise appliance web interface, click Applications.
2. Click the + to Add or import new application→Import Application.
3. Select the desired test script, click Open, and click Save. Note: Since testing, Login Enterprise has updated their product to make the Knowledge Work workflow available out-of-the-box. See this article for additional information: Knowledge Worker: Out-of-the-box – Login VSI.
4. Complete steps 2 and 3 for each application to test.
5. Next to application groups, click the + to Add new application group.
6. Enter a group name and optionally a description, and click Next.
7. Click the + to Add action(s) →Application(s).
8. Check the box next to the following applications, and click Save:

    - KW_PrepareOffice2019_Default_Script
    - KW_PrepareOffice365_Default_Script
    - KW_Outlook_Default_Script
    - KW_Edge_Default_Script
    - KW_Excel_Default_Script
    - KW_PowerPoint_Default_Script
    - KW_Word_Default_Script
    - Close Excel_Default_Script
    - Close_Word_Default_Script
    - Close PowerPoint_Default_Script

9. Click the pencil next to each of the following, and click the box next to Run Once, and click Save:

    - KW_PrepareOffice2019_Default_Script
    - KW_PrepareOffice365_Default_Script

10. Click the pencil next to each of the following, click the box next to Leave Application Running, and click Save:

    - KW_Outlook_Default_Script
    - KW_Excel_Default_Script
    - KW_PowerPoint_Default_Script
    - KW_Word_Default_Script

11. Click Done to save the Application Group.

Configuring the LE test parameters

1. In the Login Enterprise appliance web interface, click Manage Tests.
2. Click + to Create a new Load Test.
3. Enter a name for the test, and select VMware Horizon View for the Connector (Dell APEX Private Cloud only).
4. For Amazon Workspaces, select Custom connector, and enter the following information:
   - Host: <External IP address of the LE appliance>
   - Connection command line: `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File "C:\Program Files\Login VSI\Login PI 3 Launcher\AWS\AWSWorkspacesClient.ps1" -UserName {username} -Password {password}`
5. Verify the Connection command line accurately points to the install location for the VMware Horizon View or Amazon WorkSpaces Client on the Launcher(s). Edit the path as needed.
6. In the Accounts field, select the group you created that contains all users.
7. In the Launchers field, select the group you created that contains all launchers.
8. Click Save.
9. For Login, enter 500 for users and 125 for minutes. To reach this number, we divided the number of VMs by the number of hosts. This results in a login time of one minute per user per host.
10. Set the test duration to 60 minutes.
11. In the Actions pane, click Add action(s), and click the Application(s) option.
12. Select all the applications to test, and click Save.

Launching the tests

1. In the Login Enterprise appliance, next to the test to run, click the Play icon.
2. Validate the test parameters, and click Confirm.

Read the report at https://facts.pt/oX4aL61 ▶

This project was commissioned by Dell Technologies.

Principled Technologies®

Facts matter.®