The science behind the report:

Dell PowerEdge R660xs: Maximize VDI density while delivering a strong user experience and minimize power consumption

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 PowerEdge R660xs: Maximize VDI density while delivering a strong user experience and minimize power consumption.

We concluded our hands-on testing on May 25, 2023. 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 May 23, 2023 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 2: The results of our Login Enterprise 2022 Knowledge Worker workload benchmark testing results.

	Dell™ PowerEdge™ R660xs
Login Enterprise 2022 Knowledge Worker EUX metrics	
Login Enterprise VSIMax	290
Login Enterprise EUX Score	6.2
Average application response time (seconds)	1.509
Application response times (seconds)	
Prepare Microsoft Office 365	3.097
Launch Microsoft Outlook	5.081
Launch Microsoft Edge	2.631
Log onto Microsoft Edge	0.136
Launch Microsoft Excel	1.529
Save Microsoft Excel file	0.496
Open Microsoft Excel window	0.741

	Dell™ PowerEdge™ R660xs
Open Microsoft Excel document	1.378
Launch Microsoft PowerPoint	1.396
Open Microsoft PowerPoint window	0.613
Open Microsoft PowerPoint document	1.864
Save Microsoft PowerPoint file	1.198
Launch Microsoft Word	1.451
Open Microsoft Word window	0.674
Open Microsoft Word document	1.456
Save Microsoft Word file	0.401
iDRAC power consumption results	
Average watts under full load	714
Average watts per VDI session while under full load	2.46

System configuration information

Table 3: Detailed information on the system we tested.

System configuration information	Dell PowerEdge R660xs
BIOS name and version	Dell 1.1.2
Non-default BIOS settings	System Profile: Performance Workload Profile: Virtualization Optimized Performance Profile
Operating system name and version/build number	Dell-VMware® ESXi™ 8.0 GA Build-21203435 (A03)
Date of last OS updates/patches applied	5/18/23
Power management policy	Performance
Processor	
Number of processors	2
Vendor and model	Intel® Xeon® Gold 6448Y
Core count (per processor)	32
Core frequency (GHz)	2.10
Stepping	Model 143 Stepping 7
Memory module(s)	
Total memory in system (GB)	1,024
Number of memory modules	16
Vendor and model	Hynix® HMCG94AEBRA109N
Size (GB)	64
Type	DDR5 DRAM
Speed (MHz)	4,800
Speed running in the server (MHz)	4,800
Storage controller	
Vendor and model	Marvell BOSS-N1 Modular
Cache size (MB)	0
Firmware version	2.1.13.2017
Local storage (OS)	
Number of drives	2
Drive vendor and model	Dell EC NVMe™ ISE 7400 RI M.2
Drive size (GB)	447.13
Drive information (speed, interface, type)	8 GT/s, M.2, NVMe
Local storage (data)	
Number of drives	2
Drive vendor and model	Dell Ent NVMe CM6 MU
Drive size (GB)	2,980.82
Drive information (speed, interface, type)	16 GT/s, PCIe, NVMe

System configuration information	Dell PowerEdge R660xs
Network adapter	
Vendor and model	Broadcom® Adv Dual 25Gb Ethernet
Number and type of ports	2 x 25Gb
Driver version	22.31.13.70 (family version)
Cooling fans	
Number of cooling fans	7
Power supplies	
Vendor and model	Dell 07DWXYA01
Number of power supplies	2
Wattage of each (W)	1,400

How we tested

Overview

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

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

Each test includes a 300-minute log-on period, or 1 minute per system. Once a launcher completed the login process and detected that the session was ready, it would initiate the knowledge worker workload for that session. For a description of the knowledge worker workload see here: https://support.loginvsi.com/hc/en-us/articles/360001046100-Login-VSI-Workloads-Default-workloads-information.

Environment summary

Below is a summary of our environment. Our single-node Dell PowerEdge R660xs hosted 300 virtual desktops to push beyond the capabilities of the server, and determine the maximum session count for good performance.

Hardware

- Server model: 1 x Dell PowerEdge R660xs
- Processors: Intel Xeon Gold 6448Y
- Memory: 1TB
- Local SSD storage: 2 x 3.2 TB PCIe SSD
- Network adapters: Dual 25GbE

Virtual machines

- Infrastructure host (additional hardware)
- vCenter, deployment size Small
- Domain Controller with four vCPUs, 16 GB of memory, and a 120GB hard drive
- VMware Horizon 8 Server with four vCPUs, 16 GB of memory, and a 90GB hard drive
- Login Enterprise (LE) Appliance with two vCPUs, 4 GB of memory, and a 100GB hard drive
- Launcher host (additional hardware)
- 13 x Windows Server 2022 Login Enterprise Launchers, each with eight vCPUs, 32 GB of memory, and a 50GB hard drive
- VDI host (SUT)
- 300 x Windows 10 virtual desktops, each with two vCPUs, 3 GB of memory, and a 50GB hard drive

To build our environment and complete our testing, we completed the steps detailed below to complete the following high-level tasks.

Configuring the environment

The sections below detail 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 to 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 `vdi16g.local`, 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 4.
11. Open DNS Manager on your DNS.
12. Right-click your DNS FQDN, and choose Properties.
13. Click the Forwarders tab.
14. Click Edit.
15. Add the IP address of the primary DNS on the network, and click OK.
16. Click OK.

Configuring DHCP services on DC01

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 set up previously (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, 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: `172.16.0.2`
    - End IP address = `172.16.3.254`
    - Length = `22`
    - Subnet mask = `255.255.252.0`
20. Click Next.
21. At the Add Exclusions and Delay page, leave defaults, and click Next.
22. Set the Lease Duration to 4 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 `vdi16g.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 Certificate Services in Microsoft Active Directory on DC01

1. Log onto DC01 as administrator@vdi16g.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 DC01.vdi16g.local, 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 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, Certification Authority Web Enrollment, and click Next:
    - If one or more of these options are grayed 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 finished configuring, click Close.
27. Reboot.
28. Open a command prompt, and type `ldp`
29. Click Connection, and connect.

30. For server, type `dc01.vdi16g.local`
31. Change the port to 636.
32. Check SSL, and click OK.

Configuring secure LDAP on DC01.vdi16g.local 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

We created a base image to deploy using VMware Horizon. For this gold image, we created a Microsoft Windows 10 Enterprise VM, and 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, 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 8.0 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: 3 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 drop-down, and select 8 MB of total video memory.
13. Click the Advanced Parameters tab.
14. In the Attribute field, enter `devices.hotplug`, and set the Value to `false`.
15. Click Add, then click Next.
16. Click Next, then 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, and click Install VMware Tools…, and select MOUNT.
8. In the VM remote console, click Load driver.

9. Click Browse.
10. On the VMware Tools drive, navigate to \Program Files\VMware\VMware Tools\Drivers\pvscsi\Win8\amd64.
11. Click OK.
12. Select the VMware PVSCSI Controller, and click Next.
13. To install on Drive 0, click Next.
14. When presented with the region dialog, to enter Audit mode, press CTRL+SHIFT+F3.

Configuring the baseline VM

1. If not already mounted, in the vCenter console, select the VM, click Install VMware tools…, and select MOUNT.
2. On the VM, click the VMware tools AutoPlay pop-up, and select Run setup64.exe.
3. On the VMware Tools installer, click Next.
4. Select Custom, and click Next.
5. Deselect:
   - 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. Disabling automatic updates ensures consistency during testing.
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: https://go.microsoft.com/fwlink/p/?LinkID=626065
2. Save, and then run, following the prompts throughout the installer.
3. Create a new folder at the root of C: called O365 (should look like C:\O365\), and click 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, and 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. Cleanup 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 Analyze.
3. Click Common Options.
4. Click Security.
5. Select Disable Firewall, Disable Antivirus, 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, System Locale, and check the box for Automatic Restart. At the bottom, click Generalize.
9. Once the process is complete, the VM will automatically reboot.
10. Download LGPO from https://www.microsoft.com/en-us/download/details.aspx?id=55319.
11. Download Secure Delete from https://download.sysinternals.com/files/SDelete.zip.
12. Extract to the same folder as OSOT (you may need to obtain this again after Generalizing the image).
13. Check to see if the executables need to be unblocked by right-clicking, and choosing Properties.
14. Open OSOT, at the top, click Finalize.
15. At the bottom, click Finalize. Note: You will receive a prompt once complete.
16. Open the run box or command prompt, and execute the 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 check box, 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 previously created in step, 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

Creating customization specifications (required for Horizon pool creation)

1. Open vCenter, and, in the upper-left corner, 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 select Generate a new security identity (SID).
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, click Use the virtual machine name.
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 allowed our Login Enterprise launchers to login 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, select Use standard network settings for the guest operating system....
13. On page 9, enter your Windows Server domain, your domain administrator username, and password.
14. On page 10, verify the accuracy of the information 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 Add.
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, select the <vCenter FQDN> server, and click Next.
7. Select Dedicated, check Enable Automatic Assignment, and click Next.
8. If no vSAN is configured, on Storage Policy Management, click Next. Note: VSAN was not available in our environment.
9. Enter `VDI_Pool` for the ID and `VDI Pool` for the Display Name, and click Next.

10. Make the following adjustments:
    - Use a Naming Pattern
    - Specify the naming pattern. We used `vDesktop{n:fixed=3}`
    - All Machines Up-Front
    - Maximum Machines: 300
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. Name/User Name starts with: `vdi`
    - Note: This should identify the VDI users group.
20. Click Find.
21. To select all, check the box, and click OK.
22. Click OK.

Deploying Login Enterprise

We used the following steps to deploy our Login Enterprise Appliance.

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. To download the Logon Executable, scroll to the bottom of the page, and click Logon Executable.
3. Extract LoginPI.Logon.exe from the zip, and copy it to {domain}/scripts directory on the sysvol share of the domain controller.
4. In the Virtual User Accounts pane, click +, and click Bulk Accounts.
5. Enter the base Username, Password, Domain, Number of digits for the user sequence, and Number of accounts to be created, and click Save.
    - Example: `vdiuser_ , <Password> , vdi16g.local , 3 , 300`
6. Once the bulk accounts have been created, create an Account Group by clicking + to Add new account group→Filter.
7. Enter a name for your group, add a description, and click Next.
8. To select all the users, enter the wildcard character `*`, 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. To create bulk users and add them to the intended security group (created above), use the following PowerShell code:

```
$start = 1
$end = 300
$count = $start..$end
$path = "CN=Users,DC=vdi16g,DC=local"
$userName = "vdiuser_"

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"
}
```

Deploying the launchers

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

We configured the Windows Server 2022 Launchers 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, 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 8.0 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: 8
    - Memory: 32 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 Windows Server 2022 ISO is stored)
9. Click Next, and 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. To install on Drive 0, click Next.
10. To enter Audit mode, when presented with the region dialog, press CTRL+SHIFT+F3.

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.

Installing the launcher setup

1. In the Login Enterprise appliance web interface, click Launchers.
2. To download the Windows x64 launcher, scroll to the bottom of the page, and click Windows x64 launcher.
3. Extract the launcher, and run Setup.msi.
4. Click Next, and proceed through the installer.
5. To close the installation once it completes, click Finish.

Installing the VMware Horizon View client

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

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. Local Machine→Next.
8. Place the certificate in the Trust Root Certification Authorities certificate store→Next→Finish.

Creating the VM template for the launcher

1. 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→Template→Convert to Template, and click Yes.
3. To clone the required number of Launchers from the Launcher template, right-click the Infrastructure cluster→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 launcher is detected in the Login Enterprise appliance.

Creating the Login Enterprise test applications

1. In the Login Enterprise appliance web interface, click Applications.
2. Click + to Add or import new application→Import Application.
3. Select the desired test script, click Open, and click Save. Note: After we completed testing, Login Enterprise 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. Once all applications have been imported, create an Application Group.
6. Next to application groups, click + to Add new application group.
7. Enter a group name, [optionally] a description, and click Next.
8. Click + to Add action(s)→Application(s).
9. Check the box next to the following applications, and click Save:
   - (KW) Prepare for Microsoft Office 365
   - (KW) Microsoft Outlook
   - (KW) Microsoft Edge (browsing + multimedia)
   - (KW) Microsoft Excel
   - (KW) Microsoft PowerPoint
   - (KW) Microsoft Word
   - (KW) Close Microsoft Excel
   - (KW) Close Microsoft Word
   - (KW) Close Microsoft PowerPoint
10. Click the pencil next to each of the following, click the box next to Run Once, and click Save:
    - (KW) Prepare for Microsoft Office 365
11. Click the pencil next to each of the following, click the box next to Leave Application Running, and click Save:
    - (KW) Microsoft Outlook
    - (KW) Microsoft Excel
    - (KW) Microsoft PowerPoint
    - (KW) Microsoft Word
12. To save the Application Group, click Done.

Configuring the Login Enterprise 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.
4. Verify the Connection command line accurately points to the install location for the VMware Horizon View on the Launcher(s). Edit the path as needed.
5. In the Accounts field, select the group you created which contains all users.
6. In the Launchers field, select the group you created which contains all Launchers.
7. Click Save.
8. For Login, enter 300 for users and 300 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.
9. Set the test duration to 60 minutes.
10. In the Actions pane, click Add action(s), and click the Application(s) option.
11. 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 Play.
2. Validate the test parameters, and click Confirm.

Read the report at https://fact.pt/g9z7oRk

This project was commissioned by Dell Technologies.