



The science behind the report:

Boost end user productivity with Citrix Virtual Apps and Desktops on Google Cloud

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 [Boost end user productivity with Citrix Virtual Apps and Desktops on Google Cloud](#).

We concluded our hands-on testing on March 22, 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 February 15, 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, in seconds, of our testing.

	Google Cloud n2-standard-16	Amazon EC2 m5n.4xlarge	Microsoft Azure Standard_D16s_v4
Logon time			
Display protocol connection	11.500	11.200	11.600
Profile load	0.100	0.100	0.200
GPO processing	0.900	0.900	0.700
Total	13.900	13.300	13.900
Notepad			
Start	0.291	0.547	0.691
Total	0.291	0.547	0.691

	Google Cloud n2-standard-16	Amazon EC2 m5n.4xlarge	Microsoft Azure Standard_D16s_v4
Microsoft Word			
Start	1.306	1.673	1.653
Open window	0.607	0.779	0.829
Open Word document	1.136	1.286	1.495
Save file	0.432	0.591	0.712
Total	3.481	4.329	4.689
Microsoft Excel			
Start	1.212	1.492	1.475
Open window	0.518	0.67	0.804
Open Excel document	0.608	0.796	0.809
Save file	1.044	1.161	1.257
Total	3.382	4.119	4.345
Microsoft PowerPoint			
Start	1.021	1.257	1.274
Open window	0.587	0.723	0.845
Open PowerPoint document	2.397	2.645	2.263
Save file	1.267	1.572	1.594
Total	5.272	6.197	5.976
Microsoft Outlook			
Start	2.807	3.436	3.525
Total	2.807	3.436	3.525
Microsoft Edge			
Load web page	0.603	0.809	0.760
Total	0.603	0.809	0.760

System configuration information

Table 2: Detailed information on the instances we tested.

System configuration information	Google Cloud <i>n2-standard-16</i>	Amazon EC2 <i>m5n.4xlarge</i>	Microsoft Azure <i>Standard_D16s_v4</i>
Test date	2022-02-08	2022-03-04	2022-03-21
Region	US - Virginia	US - Virginia	US - Virginia
Workload and version	Login Enterprise 4.84	Login Enterprise 4.84	Login Enterprise 4.84
Workload type	Knowledge Worker	Knowledge Worker	Knowledge Worker
Compute			
Number of processors	1	1	1
Processor vendor and model	Intel Xeon CPU @ 2.8GHz	Intel Xeon Platinum 8259CL	Intel Xeon Platinum 8272CL
Processor generation	Cascade Lake	Cascade Lake	Cascade Lake
Core count (threads)	8 (16)	8 (16)	8 (16)
Hyperthreading	Yes	Yes	Yes
Core frequency (GHz)	2.8	2.5	2.6
Number of vCPU per VM	16	16	16
Memory module(s)			
Total memory in system (GB)	64	64	64
Local storage			
Storage	SSD persistent disk	General purpose SD (gp2)	Premium SSD P10-LRS
Disk size (GB)	128	128	128

How we tested

Each environment infrastructure creation process varied slightly, depending on the cloud provider's level of auto-configuration, which created different baseline Virtual Delivery Agent (VDA) host VMs. To ensure a uniform testing environment, we created our own gold image for the VDA VM on each cloud service using identical methodologies.

Deploying Login Enterprise

Deploying the 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 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.

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 click the Application(s) option.
11. Select all the applications to test. Click Save.

Running a test

1. Next to the test to run, click the white triangle in the green circle.
2. Validate the test parameters, and click Confirm.

Deploying and configuring the cloud environments

Deploying the Google Cloud solution

1. From the Google Cloud control panel, click the project drop-down at the top of the screen, and click New Project.
2. Enter the Project name, and select a Billing account and Organization. Click Create.
3. Click APIs and Services, and enable Compute Engine API and Cloud Deployment Manager v2 API.
4. In the IAM control panel, give the GDM service account (*@cloudservices.gserviceaccount.com) owner permissions in the project.
5. Create a bucket using the following command line:

```
gsutil mb gs://<bucketname>
```

6. Generate a credentials.json file with a Citrix Cloud API key.
(See <https://github.com/GoogleCloudPlatform/citrix-on-gcp/blob/exp2/README.md> for format and contents.)
7. Upload credentials.json into a bucket in the project.
8. Once uploaded, verify the file format and access permissions with the following command:

```
gsutil cat gs://<bucketname>/credentials.json
```

9. Clone the GDM template from the GitHub repository code branch into the Google Cloud console file system with the following command:

```
git clone https://github.com/GoogleCloudPlatform/citrix-on-gcp.git
```

10. Change to the cloned project folder with the following command:

```
cd citrix-on-gcp
```

11. Checkout the exp2 branch with the following command:

```
git checkout exp2
```

12. Initiate the deployment manager job with the following command:

```
gcloud deployment-manager deployments create <mygdm-name> --template templates/citrix-on-gcp.jinja --properties citrix-creds:gs://<bucketname>/credentials.json
```

Deploying the AWS solution

1. Log into the AWS Console.
2. To create a secure client connection with Citrix, use the following steps:
 - a. Log into the Citrix cloud management console, and go to the API access menu at <https://us.cloud.com/identity/api-access>.
 - b. Copy the customer ID for future use.
 - c. Name the client, and click Create Client.
 - d. Save the Secure Client ID and Secure Client Secret locally.
3. Launch the Citrix Virtual Apps and Desktops quick start by navigating to <https://fwd.aws/Yqarw>.
4. In the upper right corner of the navigation bar, select the Region.
5. Keep the default settings for the template and URL, and click Next.
6. On the Specify Details page, change the Stack name to match your environment.
7. Enter the following parameters for the deployment:
 - a. **Citrix Cloud Configuration:**
Enter the Citrix Customer Cloud ID, Citrix Cloud Secure Client ID, and Citrix Cloud Secure Client Secret.
 - b. **Active Directory Configuration:**
Change the Domain DNS and NetBIOS names if necessary, and enter a domain admin password.
 - c. **Amazon EC2 Configuration:**
Select the existing EC2 key pair, RD Gateway, and VDA instance type.
Enter a public URL to download the VDA server setup file.
 - d. **Network Configuration:**
Select the Availability Zone, and enter the allowed CIDR for clients accessing the gateway.
8. Click Next.
9. On the Configure stack options page, add tags for the environment, and click Next.
10. On the Review page, validate the configuration options displayed, and click Create Stack.

Deploying the Azure solution

1. Sign into the Azure control panel.
2. To create an Azure Active Directory for authentication, use the following steps:
 - a. Click + Create a Resource, and select Azure Active Directory.
 - b. Click Create.
 - c. Enter the Organization name and Initial domain name.
3. To create a gold image with Windows 10 Enterprise multi-session, use the following steps:
 - a. Click + Create a resource, search for Microsoft Windows 10, and select the Microsoft-issued resource.
 - b. For plan, select Windows 10 Enterprise multi-session, version 21H2.
 - c. Select the subscription and resource group to use for the environment.
 - d. Enter a name for the gold VM image.
 - e. Select the Region and Size for the VM.
 - f. Enter credentials for the Administrator account, and adjust inbound port rules if necessary.
 - g. Click to confirm the Licensing validation.
 - h. Click Next: Disks.
 - i. Select OS disk type: Standard SSD.
 - j. Click Next: Networking.
 - k. Select the Virtual network for the VM.
 - l. Click Review + create.
4. To create a Cloud Connector in the environment, use the following steps:
 - a. Click + Create a resource, search for Windows Server, and select the Microsoft-issued resource.
 - b. Select the plan Windows 2016 Datacenter.
 - c. Select the subscription and resource group to use for the environment.
 - d. Enter a name for the VM.
 - e. Select the Region and Size for the VM.
 - f. Enter credentials for the Administrator account, and adjust inbound port rules if necessary.
 - g. Click to confirm the Licensing validation.
 - h. Click Next: Disks.
 - i. Select OS disk type>Premium SSD.
 - j. Click Next>Networking.

- k. Select the Virtual network for the VM.
 - l. Select a Public IP for the VM.
 - m. Click Review + Create.
 - n. Once the VM is created, RDP into the newly created VM.
 - o. Connect to Citrix Cloud to download the Cloud Connector by using the following steps:
 - i. Log into <https://us.cloud.com/locations>.
 - ii. Click + Resource Location.
 - iii. Name the location, and click Save.
 - iv. Under the new resource location, click + Cloud Connectors.
 - v. Click Download, and save the installation file locally.
 - p. Run the downloaded file, and wait for the connectivity test to complete successfully.
 - q. Click Sign In, and enter Citrix Cloud Credentials.
 - r. From the drop down menus, select the Customer and Resource location.
 - s. When the installation completes, click Close.
5. Configuring the hosting connection
 - a. Navigate to <https://xenapp.cloud.com/manage/webstudio>.
 - b. In the left panel, click Hosting.
 - c. Click Add Connection and Resources.
 - d. Select Create a new connection, and click the dropdown for Microsoft Azure.
 - e. Select Azure Global, and select the Zone name. Click Next.
 - f. Enter the Azure Subscription ID in the field, and enter a connection name.
 - g. Click Create new....
 - h. Sign into the Azure account, and accept the requested Permissions prompt.
 - i. On the Region page, select the region for the environment, and click Next.
 - j. On the Network page, enter a name for the resource, and select the Virtual network and Subnet.
 6. Creating a Citrix Cloud Machine Catalog
 - a. Navigate to <https://xenapp.cloud.com/manage/webstudio>.
 - b. In the left panel, click Machine Catalogs.
 - c. Click Create Machine Catalog.
 - d. On the Introduction page, click Next.
 - e. On the Machine Type page, select Multi-session OS.
 - f. On the Machine Management page, select Machines that are power managed.
 - g. Select Citrix Machine Creation Services (MCS), and from the dropdown, select the correct Resources. Click Next.
 - h. Select the Master Image from the list, and click Next.
 - i. On the Storage and License Types page, click Next.
 - j. On the Virtual Machines page, select 1 VM, and the machine size. Click Next.
 - k. On the Write Back Cache page, click Next.
 - l. On the Resources Groups page, click Next.
 - m. On the Network Interface Cards page, click Next.
 - n. On the Active Directory Computer Accounts page, select the OU for the VM computer account. Click Next.
 - o. On the Domain Credentials page, enter administrative account credentials for the Active Directory domain.
 - p. On the Summary page, enter a name for the Machine Catalog, and click Finish.
 7. Creating a Citrix Cloud Delivery Group
 - a. In the left panel, click Delivery Groups.
 - b. Click Create Delivery Group.
 - c. Click Next.
 - d. On the Machines page, select the Machine Catalog, and select 1 virtual machine. Click Next.
 - e. On the Users page, select Restrict use of this delivery group.
 - f. Click Add, and select the Windows AD security group for Citrix users. Click Next.
 - g. On the Desktops page, click Add.
 - h. Enter a Display name and Description for the desktop resource. Click OK, and click Next.
 - i. On the Summary page, enter a Delivery Group name. Click Finish.

Configuring the Windows gold image VM

We created a Microsoft Windows Server 2019 VM for Google Cloud and AWS, and a Windows 10 Enterprise multi-session VM as part of the Azure creation process. Then we installed Microsoft Office Professional Plus 2019 on the VMs

Creating the Amazon VM

1. In the AWS EC2 dashboard, click Launch Instances.
2. Search for Windows Server, and select Microsoft Windows Server 2019 Base.
3. Select m5n.4xlarge, and click Next: Configure Instance Details.
4. Select the correct Network and Subnet for the Citrix environment.
5. Do not Auto-assign Public IP.
6. Select Domain join directory, and select the Citrix-created AD.
7. Click Review and Launch.

Creating the Google Cloud VM

1. In the Google Cloud Platform control panel, select the VM Instances menu.
2. Click Create Instance.
3. Name the instance, and select the Region and Zone for the Citrix Environment.
4. Select Series N2 and Machine type n2-standard-16.
5. For Boot disk, click change, and select Windows Server, with Version Windows Server 2019 Datacenter.
6. Change the Boot disk type to SSD persistent disk, and the size to 128GB.
7. For the Service accounts, select the Citrix-created service account.
8. Apply the network tags rdp and vda.
9. Click Create.

Installing the Microsoft Edge driver for the gold image VM

1. Find the Microsoft Edge driver matching your current version of Edge at <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 msedge.exe from the downloaded zip file, and copy it to the created folder.

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.

Configuring a new VDA VM

1. To download and configure the Virtual Delivery Agent on the gold VM, use the following steps:
 - a. Go to <https://xenapp.cloud.com/downloads>, and download the Virtual Delivery Agent (VDA).
 - b. Run the downloaded file, and 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, additionally 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.

Read the report at <https://facts.pt/Yo7wmGv>

This project was commissioned by Google.



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.