Deploying Citrix Cloud on the Google Cloud Platform (GCP) provides agility in provisioning applications and desktops. GCP IaaS can supplement resources of on-premises datacenters, allowing IT to satisfy sudden demand and support rapid geo expansion. This document guides you through the process of configuring Citrix Cloud XenApp and XenDesktop Service with Google Cloud.

Introduction
Whether your organization is just beginning to adopt the cloud or has already achieved a cloud-first approach, Citrix Cloud meets you where you are in your cloud journey. Citrix Cloud services are available to help extend existing on-premises Citrix software deployments, to help create hybrid workspace services, and to provide simple approaches to consuming cloud-native technology. By deploying Citrix software as a service, Citrix Cloud simplifies management of Citrix technologies by unifying virtual apps, desktops, data, device management, and networking on any cloud or infrastructure. This integrated approach is the simplest way to securely create and deliver digital workspaces. This deployment guide describes GCP concepts, components, and basic GCP implementation with Citrix Cloud.

Google Cloud Platform (GCP) consists of services and resources, including Google Cloud Storage (GCS), and Google Compute Engine (GCE) virtual machines (VMs), hosted in Google’s data centers around the globe. Data centers are referenced by their global region, such as Central US, Western Europe, and East Asia. Regions include collections of zones, which are isolated from each other within the region. Zone identifiers include the region name, such as us-central1-a, europe-west3-b, and asia-east1-c.

The architecture presented here delivers Citrix application services and hosted shared desktop services to users via Citrix Cloud. It enables a hybrid approach in which organizations can simplify the running of Citrix management services from on-premises to Citrix Cloud and use GCP to deliver cloud-based XenApp services.

In the current Citrix Cloud release, when integrated with GCP, there are some limitations within Citrix Cloud that need to be considered. A few components including Machine Creation Services (MCS) and machine power management are not yet available inside Citrix Cloud.

The first part of this guide describes the GCP and Citrix Cloud components. The second part is a “runbook” that gives specific procedures for installing and configuring a proof-of-concept (POC) XenApp deployment on GCP from Citrix Cloud. Citrix XenApp scalability when hosted within specific GCP instances is also included.
# Table of Contents

- **Introduction**  
  1

- **Planning a Citrix XenApp Deployment: Design Choices**  
  3
  - Concepts and Terminology  
    3
  - Projects  
    4
  - GCE compute  
    4
  - GCE storage  
    4
  - XenApp infrastructure and application storage in GCP  
    4
  - GCP networking  
    4
  - Windows instance costs  
    5
  - Other infrastructure components  
    5

- **XenApp scalability testing on different GCP instance types**  
  5

- **Runbook: Configuring XenApp and NetScaler in GCP**  
  8

- **Step 1: Plan Your Deployment**  
  8
  - Sizing for Infrastructure Server Components  
    8
  - Sizing for Workload Servers  
    8
  - Sizing for XenApp HSD Servers  
    9

- **Step 2: Configure GCP Topology**  
  9
  - Create a GCP Virtual Network  
    10
  - Create a bastion machine  
    18
  - Configure GCE Active Directory  
    22

- **Step 3: Create Infrastructure Citrix Cloud VMs**  
  26

- **Step 4: Prepare the XenApp Golden Image VM**  
  34

- **Step 5: Create a Machine Catalog**  
  40

- **Step 6: Create a Delivery Group**  
  45

- **Step 7: Assigning access to users**  
  48

- **Step 8: Access GCE securely using NetScaler Gateway Service**  
  48

- **Learn More**  
  51
Planning a Citrix XenApp Deployment: Design Choices

Citrix Cloud is a new control-plane-hosted Software-as-a-Service (SaaS) offering that enables key pieces of the Citrix infrastructure — such as the Delivery Controller, Storefront and NetScaler Gateway Service — to be hosted separately from where the workload resides. By provisioning Citrix XenApp in GCP with Citrix Cloud, businesses can avoid the acquisition and maintenance costs associated with expanding on-premises infrastructure. Instead, they can use GCP Infrastructure-as-a-Service (IaaS) to supply the compute, storage, and networking resources needed to provision application sessions and desktops to meet demand.

To help customers with the use case for a single public cloud deployment in GCP, this guide presents a summary of GCP scalability test results and cost factors that impact deployment decisions. Figure 1 illustrates how Citrix components can be deployed on GCP and managed with Citrix Cloud.

Figure 1: Citrix Cloud infrastructure deployment with Google Cloud as a resource location
Concepts and Terminology

GCP services can vary according to geographic regions. At the time of writing this document, GCP is generally available in 13 regions, 39 zones, and over 100 points of presence around the world.

Five critical types of GCP resources are needed for XenApp on GCP: IAM, projects, compute, storage, and networking. The following sections introduce fundamental GCP IaaS concepts as well as general project, compute, storage, and networking requirements in this architecture.

Projects

- A project is the core organizational component of Google Cloud Platform. Projects provide abstract groupings that you can use to associate resources with a department or functional team. All Cloud Platform resources belong to a project. All GCP projects are assigned a single user project creator role by default. Additional project members and IAM roles should be created to control access to Compute Engine services.

Identity Access Management

- Each project in GCP can be assigned granular permissions using IAM policies. By default, project owner is assigned the editor owner role which is being used in the deployment guide, however more granular access can be defined. Consult with your local security team to assess what level of access your account may have to the project.

GCE compute

- Compute Engine offers predefined virtual machine configurations for every need, from micro to instances with 96 vCPUs or 624 GB of memory, in standard, high-memory, and high-CPU configurations. The following compute resources are relevant to any XenApp deployment on GCP:
  - Predefined Machine Type. A predefined machine type has a preset number of vCPUs and amount of memory, and is charged at a set price, described in the pricing page.
  - Custom Machine Type. By configuring parameters such as vCPU and memory, you can tailor a Custom Machine Type for specific needs and significant savings.

GCE storage

- Persistent disks are durable network storage devices that your instances can access as though they were physical disks in a desktop or a server. GCE instances by default have a single root persistent disk with an operating system. Additional disks can be added later for instances where applications require more local storage. The choices for disk expansion are Standard persistent disks, SSD persistent disks, Local SSDs, and Cloud Storage buckets. In most cases, Local SSD is not a common practice for XenApp as the data that you store on a local SSD persists only until you stop or delete the instance. The data on each persistent disk is distributed across several physical disks. Compute Engine manages the physical disks and the data distribution to ensure redundancy and to optimize performance. Persistent disks are available as either standard hard disk drives (HDD) or solid-state drives (SSD).
  - Persistent disks are located independently from your virtual machine instances, so you can detach or move persistent disks to retain data even after you delete VM instances. Persistent disk performance scales automatically with size, so you can resize your existing persistent disks or add more persistent disks to an instance to meet your performance and storage space requirements.
  - Persistent Disk has no per-I/O cost, so there is no need to estimate monthly I/O to calculate budget for what you will spend on disks.
  - Standard persistent disks have a read IOPS of 3,000 and write of 15,000 per instance. SSD persistent disks have a read IOPS of 40,000 and write of 30,000 per instance.
  - Each persistent disk has a limit of 64TB in size. You can attach up to 16 independent persistent disks to most instances.

When estimating storage capacity, remember that XenApp and XenDesktop deployments have two storage needs: storage for XenApp infrastructure servers and applications, and storage for user profiles.

XenApp infrastructure and application storage in GCP

Approximately 50 GB of storage is needed for a XenApp server master image. This number can vary depending on the size of the application workload. The minimum OS Boot Disk size in GCE is 50 GB for Windows 2016 and 32 GB for Windows 2012R2. To simplify a XenApp image deployment, create a new XenApp server image to minimize required capacity instead of migrating an existing on-premise image.

GCP networking

GCP Virtual Private Cloud (VPC) networking enables flexible networking, with network options to support a variety of deployment scenarios. VPC networking offers automatic setup of your virtual topology with suggested prefix ranges and network policies. As your services become
more complex, you have the control to seamlessly customize your VPC’s size and connectivity rules to adapt to your needs. Using the Google Cloud Console, an administrator can configure custom IP address ranges if the defaults are not sufficient.

- VPC Ingress traffic is free.
- Egress traffic to the same zone, to a different GCP service in the same region, and to Google product are all free.
- Egress traffic between zones in the same region or regions within the US costs $0.01/GB.
- There are two types of VPCs. Auto and custom mode. Auto-mode VPC networks start with a single subnet in each region with pre-defined IP ranges. Custom mode VPC networks require all subnets to be created manually.
- A VPC can have a maximum of 7000 virtual machines per network. This is a set rule, not a quota number, and can’t be changed at this time.
- If there is a need for more than 7000 machines, then additional networks can be created.

Windows instance costs
All GCE instances run at a per-second billing rate. For premium instances such as Windows images, please refer to the Windows Server Pricing or the Google Cloud Pricing Calculator.

Other infrastructure components
To support a XenApp deployment on GCP, the following additional components are required:
- Active Directory (AD). For client authentication, VDA registration, and access management, the architecture requires an AD domain controller (see "Setting up Active Directory on Google Compute Engine").
- DNS. Although name resolution can be provided by GCP or an external DNS server, this architecture requires an internal DNS server. A single VM can host both the AD services and a DNS server.
- DHCP and IP address configuration. GCE provides DHCP services that assign private IP addresses to VMs using a specified IP address range in a VPC network.
- NAT gateway instances for internet access

Sustained Use Discounts
GCP enables VM instances to leverage using sustained use discounts. Sustained use discounts offering an automatic cost savings when a VM instance is running for a significant duration in a month. When an instance is run more than 25% of a month, GCE will enable a discount savings for each incremental minute that VM instance is active. The discount will increase as VM instance usage rises and can go up to 30% for an instance that runs the entire month. Refer to the sustained use discounts link in the Learn More portion of this document.

<table>
<thead>
<tr>
<th>Usage Level (% of month)</th>
<th>% at which incremental is charged</th>
<th>Example incremental rate (USD/hour) for an n1-standard-1 instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>n1-standard-2</td>
<td>2</td>
<td>7.5</td>
</tr>
<tr>
<td>0%-25%</td>
<td>100% of base rate</td>
<td>$0.0475</td>
</tr>
<tr>
<td>25%-50%</td>
<td>80% of base rate</td>
<td>$0.0380</td>
</tr>
<tr>
<td>50%-75%</td>
<td>60% of base rate</td>
<td>$0.0285</td>
</tr>
<tr>
<td>75%-100%</td>
<td>40% of base rate</td>
<td>$0.0190</td>
</tr>
</tbody>
</table>

Table 1: Sustained use discounts example for GCE instances

XenApp scalability testing on different GCP instance types
Google Cloud Platform instance types vary according to infrastructure resources provided. Pricing for GCP VMs varies by region and includes Windows licensing (see "Google Cloud Platform Pricing Calculator").

Citrix engineers conducted single-server scalability testing to determine optimal user densities. Login VSI was used to generate user connections to XenApp VDA workers, simulating typical user workloads running on GCP instances. Login VSI uses the concept of Task Workers or Knowledge Workers for user simulation purposes.
When choosing the n1-standard series machine types, you can select a newer CPU platform to take advantage of faster processing. There might also be a difference in pricing when you select the new Skylake CPU instead of Broadwell or Sandy Bridge.

Table 2: GCP n1-standard-2 VM instance-type configuration and pricing

<table>
<thead>
<tr>
<th>Instance</th>
<th>Virtual CPUs</th>
<th>RAM (GB)</th>
<th>Storage (GB)</th>
<th>Storage Type</th>
<th>Price per hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>n1-standard-2</td>
<td>2</td>
<td>7.5</td>
<td>50</td>
<td>Persistent/Persistent SSD</td>
<td>$0.0200</td>
</tr>
</tbody>
</table>

Create an instance

- Name: citrix
- Zone: us-central1-a

Machine type

- CPUs: 2 vCPU
- Memory: 7.5 GB

CPU platform

- Intel Skylake or later

Figure 2: CPU platform options in GCP

The following tables show side-by-side comparisons of the maximum number of XenApp user sessions supported by the n1-standard-2 and n1-standard-4 series VM instance machine types in single-server scalability tests. A series of Login VSI tests was performed and then evaluated. The VSImax score calculates what Login VSI states are the maximum number of users or sessions an instance can handle. Note that it is normal for the Task Worker workload tests to generate a higher VSImax number than the Knowledge Worker workload tests due to the differences in applications. (See the workload testing blog for more information on workload differences.) Windows Defender Antivirus was installed with the proper Citrix Anti-virus exclusions set in place, and the new Citrix Optimizer was used to optimize Windows Server 2016. The testing results below reference the Intel Broadwell CPU chipset. Choosing a newer chipset such as the Intel Skylake processors, can also increase performance which also increases XenApp user session density. It is important to verify that the zone you are deploying to provides the newer Intel platforms.

Table 3: User Sessions comparison by GCP Instance type using Login VSI Task Worker user profile on n1-Standard-2.

<table>
<thead>
<tr>
<th>XenApp</th>
<th>GCP Instance</th>
<th>Windows Server</th>
<th>Office</th>
<th>Antivirus</th>
<th>VSI</th>
<th>Load</th>
<th>VSImax</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.16 VDA</td>
<td>n1-Standard-2, 2vCPU, 7.5GB RAM, Broadwell CPU</td>
<td>2016</td>
<td>2016</td>
<td>Windows Defender</td>
<td>4.125.6</td>
<td>Task</td>
<td>9</td>
</tr>
</tbody>
</table>
### Table 4: User Sessions comparison by GCP Instance type using Login VSI Knowledge Worker user profile. n1-Standard-2

<table>
<thead>
<tr>
<th>XenApp</th>
<th>GCP Instance</th>
<th>Windows Server</th>
<th>Office</th>
<th>Antivirus</th>
<th>VSI</th>
<th>Load</th>
<th>VSI max</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.16 VDA</td>
<td>n1-Standard-2&lt;br&gt;2vCPU, 7.5GB RAM, Broadwell CPU</td>
<td>2016</td>
<td>2016</td>
<td>Windows Defender</td>
<td>4.1.25.6</td>
<td>Knowledge</td>
<td>7</td>
</tr>
</tbody>
</table>

### Table 5: User Sessions comparison by GCP Instance type using Login VSI Task Worker user profile on N1-Standard-2.

<table>
<thead>
<tr>
<th>XenApp</th>
<th>GCP Instance</th>
<th>Windows Server</th>
<th>Office</th>
<th>Antivirus</th>
<th>VSI</th>
<th>Load</th>
<th>VSI max</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.16 VDA</td>
<td>N1-Standard-4, 4vCPU, 15GB RAM, Broadwell CPU</td>
<td>2016</td>
<td>2016</td>
<td>Windows Defender</td>
<td>4.1.25.6</td>
<td>Task</td>
<td>14</td>
</tr>
</tbody>
</table>

### Table 6: User Sessions comparison by GCP Instance type using Login VSI Knowledge Worker user profile on N1-Standard-4.

<table>
<thead>
<tr>
<th>XenApp</th>
<th>GCP Instance</th>
<th>Windows Server</th>
<th>Office</th>
<th>Antivirus</th>
<th>VSI</th>
<th>Load</th>
<th>VSI MAX</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.16 VDA</td>
<td>N1-Standard-4, 4vCPU, 15GB RAM, Broadwell CPU</td>
<td>2016</td>
<td>2016</td>
<td>Windows Defender</td>
<td>4.1.25.6</td>
<td>Knowledge</td>
<td>12</td>
</tr>
</tbody>
</table>
Runbook: Configuring XenApp and NetScaler in GCP

The remainder of this document focuses on the step-by-step process of setting up and deploying the system. The major steps are:

- Step 1: Plan Your Deployment
- Step 2: Configure GCP Topology
- Step 3: Create Infrastructure Citrix Cloud VMs
- Step 4: Prepare the XenApp Golden Image VM
- Step 5: Create a Machine Catalog
- Step 6: Create a Delivery Group
- Step 7: Assigning access to users

Step 1: Plan Your Deployment

The first step in a GCP implementation is to create a sizing plan based on specific requirements, including licensing, functions, and appropriate sizing of infrastructure servers and XenApp workload servers.

Microsoft licensing in GCP

A key aspect for running Microsoft products in Google Cloud Platform is licensing. Leveraging Microsoft License Mobility enables the deployment of Windows Server applications, such as RDS, in GCP while using your existing Microsoft licenses. All Microsoft software applications that are migrated to GCP must also be covered by Microsoft Software Assurance (SA). The full list of entitled Windows Server application products can be found in the Microsoft Product User Rights (PUR). It is recommended that you review your Microsoft licensing agreements with Microsoft prior to starting a Proof-of-Concept.

Windows Server instances require an internet network connection to activate with the GCP KMS host: kms.windows.googleapis.com. The standard grace period for Windows server instances to register with the KMS host is 30 days. After 30 days, the instances will cease functioning. Currently, each Windows instance in GCP requires a public IP address to activate against a GCP public KMS. Alternatively, you can also bring your own Windows KMS licensing into GCP and host the required licenses. Refer to the Learn More section of this document for information on assigning public IP addresses for activation.

Sizing for Infrastructure Server Components

For most deployments, a single GCP Project can host the infrastructure server components, including the Cloud Connectors, Active Directory, Bastion, and File Services. To enhance availability, deploy pairs of infrastructure instances in different zones within a region. As shown in Table 7, the result includes a total of seven infrastructure VMs. Note: Active Directory Domain Controllers should also be deployed according to GCP documentation, with two writeable domain controllers in a new forest deployment. This document, however, begins with only one domain controller; additional domain controllers can be built later.

<table>
<thead>
<tr>
<th>Infrastructure Server</th>
<th># VMs required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Cloud Connectors</td>
<td>2</td>
</tr>
<tr>
<td>Active Directory/DHCP/DNS</td>
<td>2</td>
</tr>
<tr>
<td>File Services</td>
<td>2</td>
</tr>
<tr>
<td>Bastion</td>
<td>1</td>
</tr>
<tr>
<td>NAT Gateway</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>9</td>
</tr>
</tbody>
</table>

Sizing for Workload Servers

When planning a GCP deployment, you should evaluate requirements and classify user types such as:

- XenApp hosted, shared desktop (HSD) users
- Server virtual desktop (VDI) users
It is recommended that you perform some initial proof-of-concept workload testing to collect performance data to be used in deployment sizing, and complete the Workload Characteristics table below for each category of user. You might need to expand or condense columns in the table depending on how many types of users you anticipate. Include the expected number of XenApp hosted shared desktop (HSD) users.

When choosing a GCE instance type for your workloads, note that GCE offers different machine types such as n1-standard, n1-highmem, and n1-highcpu. Based on scalability testing, GCE instances within a series tend to scale in a linear fashion. For larger user populations, deploying a larger instance type in an n-series might be preferable to deploying many smaller instances because managing many smaller instances tends to increase the complexity of VM administration and management. For small user populations, it might also be desirable to use smaller instance types to achieve more effective power management: a greater number of smaller instances provides more granularity when it comes to powering down unused servers.

**Table 8: Workload Characteristics**

<table>
<thead>
<tr>
<th>Resource</th>
<th>User Type #1</th>
<th>User Type #2</th>
<th>User Type #3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workload description (such as Task Worker, Office Worker, Knowledge Worker)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workload classification (SVDI or HSD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expected number of users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expected IOPS per user</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expected outgoing network bandwidth per user</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expected CPU utilization (in cores) per user</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expected memory requirement per user</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instance series used (such as n1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage consumption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expected storage type</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Sizing for XenApp HSD Servers**

The results of POC testing will suggest the number of XenApp workload VMs. It is recommended that you conduct single VM scalability tests in which you execute a typical application workload using each different GCE instance type. Based on the user density achieved and the IOPS consumed, you can determine the total number of XenApp server VMs and Storage Accounts that are required.

Based on POC testing, decide which instance type offers the optimal user density, taking into account factors such as price and management complexity. Divide the total number of XenApp users in the deployment by the user density observed in testing to estimate the required number of XenApp workload VMs.

For example, recent testing performed shows a GCE n1-standard-2 instance supports a density of nine XenApp users under the default Login VSI Task Worker workload. In order to calculate for a total population of 400 XenApp users, approximately 44 VMs would be needed (400 users/9 XenApp users per VM = 44 VMs). Using the example of nine XenApp users on an n1-standard-2 instance, suppose each user consumes 11 to 15 IOPS. The total XenApp server consumption would average approximately 99 to 135 IOPS. Complete the gray areas in Table 9 to summarize GCP requirements for each workload type.

**Table 9: Defining GCP Resources According to Workload Requirements**

<table>
<thead>
<tr>
<th>GCP component</th>
<th>Guidelines</th>
<th>Infrastructure requirements</th>
<th>User Type #1 workload requirements</th>
<th>User Type #2 workload requirements</th>
<th>User Type #3 workload requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of VMs</td>
<td>Assign pairs of infrastructure VMs to the same Project</td>
<td>Typically, 4 VMs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2: Configure GCP Topology**

In this step, you create the required GCP IaaS topology, including project and VPC that will be used with XenApp infrastructure components.
It is assumed that you have a basic understanding of a GCP, and have some general experience creating VMs in GCP. To configure the IaaS topology in GCP for a XenApp deployment, you must first establish these three prerequisites:

- Configure GCP billing
- Configure a GCP project
- Configure a GCP VPC network

**Create GCE Billing**

Billing accounts are a prerequisite for creating GCE instances. In a GCP environment, billing accounts are tied to projects which are aligned to an organization. It is important to ensure that the proper billing structure is in place in your organization before proceeding forward.

*Figure 4: Google Cloud billing account linkage*

In figure 4, the organization has ownership over Projects A, B, and C, meaning that it is the Cloud IAM permissions parent of the three projects. The billing account is linked to Projects A, B, and C, meaning that it pays for expenses incurred by the three projects.

<table>
<thead>
<tr>
<th>Instructions</th>
<th>Visual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to the GCP Console. Under the _ and click <strong>Enable billing</strong> for your particular project.</td>
<td><img src="image" alt="Google Cloud Platform" /> <strong>You can use Compute Engine after you enable billing</strong> Pay only for what you use. Learn more about Compute Engine pricing. <strong>Enable billing</strong></td>
</tr>
</tbody>
</table>
Set the correct billing account for your specific project then click Set Account.

The enable billing process starts.

Create a GCP VPC Network
GCP Virtual Private Cloud (VPC) is a global feature that spans all services in the cloud using private RFC 1918 address spaces. Auto-mode VPC network contains subnets, each with a defined IP range, and each capable of holding multiple VM instances and other resources. Instances and other resources draw their internal IP addresses from their respective subnets, making subnets the logical isolation partitions for the VPC network. Every project is provided with a default VPC network with preset configurations and firewall rules. You can choose to customize the default VPC network by adding or removing rules, or you can create new VPC networks in your project.

Instructions
Connect to the GCP Cloud Console, and click VPC Network.

The default VPC and regions assigned to the VPC will appear.
In this configuration we will deploy a new Auto VPC for Citrix workloads.

Click on Create VPC Network.

Enter a name in field for the VPC and a description. Note that the name of the VPC must be lowercase.

In the Subnet creation mode section, click on Automatic. This will enable the ability to modify the default ingress and egress firewall rules. Note that the default IP address range are the same as in the default VPC.
In the Firewall rules section, the default set of rules appear. RDP and other rules are required for Windows VM instances such as infrastructure, Cloud Connectors, and XenApp machines to communicate. The default firewall rules follow a more permissive approach than a restrictive one. In this deployment guide, the permissive approach will be followed to ensure all necessary ports and protocols can communicate inside and outside the VPC. Select all the required firewall rules such as:
Citrix-allow-icmp
Citrix-allow-internal
Citrix-allow-rdp

Note: It is important to review these rules with the appropriate security teams and modify as necessary. Restrictive firewall rules can be applied as well as VM instance tags to increase security.

Click Create.

Alternatively, Google Cloud Shell can also be used to automate the creation of the VPC and permissive firewall rules by copying the script in the right column and changing the project name if necessary.

The new VPC will appear in the console with the appropriate firewall rules applied.

Create Firewall rules
GCP firewall rules provide secure approved connections to virtual machines via combinations of IP address, ports, and protocols. These rules will append access for virtual machines either via inbound (ingress) or outbound (egress) communication. For the bastion machine, management, and Citrix XenApp virtual machines, the necessary firewall rules will be applied as well as tags assigned to the machines to link the firewall rules to. Additional information regarding firewall rules can be found in the Learn More section of this document.
**Instructions**

Connect to Firewall rules, Create Firewall Rule

**Visual**

![VPC network](image)

1. In the Create a firewall rule enter the following information:
   - **Name**: citrix-allow-rdp-external
   - **Description**: External RDP remote management for bastion virtual machines
   - **Network**: Citrix
   - **Priority**: 65534
   - **Direction of traffic**: Ingress
   - **Action on match**: Allow

2. **Targets**: Specified target tags
   - **Target tags**: bastion,
   - **Source filter**: IP ranges
   - **Source IP ranges**: 0.0.0.0/0
   - **Second source filter**: none
   - **Protocols and ports**: Specified protocols and ports
     - **tcp**: 3389

3. Click Create.

The new firewall rule is created and bound to the Citrix VPC network. In this firewall rule, RDP is open from the internet using an ANY IP source address range. To increase security, it is recommended that...
Create NAT Gateway

By default, inside GCP, instances without a public IP cannot make external connections to services such as the internet. In order to enable instances such as the Citrix Connector to access the internet, NAT gateway instances need to be created with the appropriate firewall rules in place to provide access to the internet. A NAT gateway machine can route traffic on behalf of all instances in a network. For higher resiliency, each gateway is placed in a separate managed instance group with size 1 and a simple health check attached to ensure they’ll automatically restart if they fail. The gateways are placed in separate instance groups so they’ll have a static external IP attached to the instance templates. Two n1-standard-2 NAT Debian-9 gateways will be leveraged in this portion of the guide; however, you can use any other number or size of gateway instances. n1-standard-2 instances are capped at 4Gbps of network traffic and if more bandwidth is needed choose n1-standard-8s which is capped at 8Gbps. In this architecture only two NAT gateway instances and public IP addresses will be configured.

<table>
<thead>
<tr>
<th>Instructions</th>
<th>Visual</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connect to Google Cloud Shell.</strong></td>
<td><img src="https://via.placeholder.com/150" alt="Cloud Shell" /></td>
</tr>
<tr>
<td>Reserve a static public IP to the first NAT Gateway in your local region copying the command below into Google Cloud Shell. gcloud compute addresses create nat-1 --region us-central1 Press Enter. Next store the public IP address to the first NAT gateway using the command below. Copy and paste the command for NAT1 into Cloud Shell. nat_1_ip=$(gcloud compute addresses describe nat-1 --region us-central1 --format='value(address)') Press Enter. Repeat the process above and change the value from nat-1 to nat-2 to create the second NAT public IP. gcloud compute addresses create nat-2 --region us-central1 Press Enter. Next store the public IP address to the second NAT gateway using the command below. Copy and paste the command for NAT2 into Cloud Shell.</td>
<td><img src="https://via.placeholder.com/150" alt="Cloud Shell" /></td>
</tr>
</tbody>
</table>
nat_2_ip=$(gcloud compute addresses describe nat-2 --region us-central1 --format='value(address)')
Press Enter.

Download the startup config into Google Cloud Shell for the NAT instances. Instances will use the startup.sh later on.
gsutil cp gs://nat-gw-template/startup.sh .
Press Enter.

Create the first NAT instance using a template by copying the command into Google Cloud Shell.
gcloud compute instance-templates create nat-1 --network=ctrix --machine-type n1-standard-2 --can-ip-forward --tags natgw --metadata-from-file=startup-script=startup.sh --address $Nat_1_ip
Press Enter.
Repeat the process for the second NAT instance by copying the command into Google Cloud Shell.
gcloud compute instance-templates create nat-2 --network=ctrix --machine-type n1-standard-2 --can-ip-forward --tags natgw --metadata-from-file=startup-script=startup.sh --address $Nat_2_ip
Press Enter.

Health checks monitor an instance responsiveness in GCP. If traffic such as HTTP fails, then the health check will restart the instances to resolve the service. Copy and paste the commands below into Google Cloud Shell.
gcloud compute health-checks create http-nat-health-check --check-interval 30 --healthy-threshold 1 --unhealthy-threshold 5 --request-path /health-check
Press Enter.

Health check monitoring services in GCP require firewall rules to permit traffic from the Health Check public IP addresses that are associated to the NAT services. Copy the command and paste it into Google Cloud Shell then hit Enter.
gcloud compute firewall-rules create "natfirewall-health" --network=ctrix --allow tcp:80 --target-tags natgw --source-ranges "130.211.0.0/22", "35.191.0.0/16"
Note: Additional information regarding Health Checks and the public IP addresses, can be found in the Learn More section of the document.
GCP Instance Groups simplify management by grouping similar machines together to streamline management across instances. The NAT gateway templates created earlier will be applied and instances will be created in separate zones for high availability.

Copy and paste the commands below into Google Cloud Shell.

gcloud compute instance-groups managed create nat-1 --size=1 --template=nat-1 --zone=us-central1-c
Press Enter.
Repeat the process for the nat-2 instance group by copying and pasting the command below into Google Cloud Shell.

gcloud compute instance-groups managed create nat-2 --size=1 --template=nat-2 --zone=us-central1-f
Press Enter.

Auto healing ensure that any unhealthy NAT gateway can be automatically restarted via a health check. Copy and paste the commands below into Google Cloud Shell to enable Auto healing for the first NAT gateway instance group.
Copy and paste the commands below into Google Cloud Shell.

gcloud beta compute instance-groups managed set-autohealing nat-1 --health-check nat-health-check --initial-delay 120 --zone=us-central1-c
Press Enter.

Repeat the process for the nat-2 instance group by copying and pasting the command below into Google Cloud Shell.

gcloud beta compute instance-groups managed set-autohealing nat-2 --health-check nat-health-check --initial-delay 120 --zone=us-central1-f
Press Enter.

Enter the commands to gather instance information into Google Cloud Shell.

```
awk '$1 ~ /^nat-1/ { print $1 }'
```
Press Enter.
Repeat the process for nat-2.
Press Enter.

Adding routes to the NAT gateways with the instance tags internet-nat to specific instances will ensure that NAT is applied and internet access is permitted.

Copy and paste the commands below into Google Cloud Shell.

```plaintext
gcloud compute routes create natroute1 --network=citrix --destination-range 0.0.0.0/0 --tags internet-nat --priority 800 --next-hop-instance-zone us-central1-c --next-hop-instance $nat_1_instance
```

Press Enter.

Repeat the process for the nat-2 instance by copying and pasting the command below into Google Cloud Shell.

```plaintext
gcloud compute routes create natroute2 --network=citrix --destination-range 0.0.0.0/0 --tags internet-nat --priority 800 --next-hop-instance-zone us-central1-f --next-hop-instance $nat_2_instance
```

Press Enter.

Create a bastion machine

Connecting to non-public GCE instances requires a remote management or bastion instance. This instance requires a public IP address for RDP access. This machine can be more carefully controlled, shut down or have the public IP address removed later to secure the environment.

<table>
<thead>
<tr>
<th>Instructions</th>
<th>Visual</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Google Cloud Platform Console, click Compute Engine, then click Create.</td>
<td>Compute Engine VM instances</td>
</tr>
</tbody>
</table>

Compute Engine lets you use virtual machines that run on Google’s infrastructure. You can choose from micro-VMs to large instances running Debian, Windows, or other standard images. Create your first VM instance, import it by CloudEndure migration service or try the quickstart to build a sample app.
In the Instance Name, enter the following information:
Name: cx-mmgt
(all names in GCP must be lower case)
Zone: us-central1-c
(or closest zone to your location)
Machine Type: 2 vCPUs 7.5 GB memory

Under Boot Disk, click Change, and select the following:
Boot Disk: Windows Server 2016
Boot Disk type: Standard persistent disk
Size: 50 GB
Click Select.

In the Identity and API access field, accept the default for Compute Engine default service account.

Scroll down and click Management, disks, networking, SSH keys.

Click on the Networking tab. In the Network tags field enter the tag name bastion.

In Network interfaces click the edit pencil icon.
Change the **network** to your created Citrix VPC network. Make sure that **External IP** is set to **Ephemeral**. Click **Done**.

![Network Interface](image)

Scroll to the bottom where it says **command line**.

Copy the entire contents of the `gcloud` command line file to use later for automation of additional instances. Click **close**.

Alternatively, the `gcloud` code in the right column can be used to create a bastion machine. Simply copy the code and replace the `XXXXXXXXXXXX` with your service account number.

Equivalent **REST** on **command line**

```bash
```

There are a few methods to create the VM. Either click **Create** or use the **Google Cloud Shell** and paste the code into the shell window. We will use Google Cloud Shell to create the VM.

Activate the Google Cloud Shell VM serial console to use the script from the previous step. Click on the `> _ ` icon.

Paste the script inside the Google Cloud Shell window then hit **Enter**. The Google Cloud Shell machine creation status appears. Although the Status says running, the instance is not immediately ready: it takes some time for setup and activation.

In the Google Cloud Shell type `gcloud compute instances get-serial-port-output ctx-mgmt`. This will display the VM deployment status.
The VM creation process takes between 5 to 10 minutes for an instance to be ready. When the instance is complete, the status displays as ready to use.

Navigate back to Compute Engine in the Cloud Console and locate the cbx-mgmt VM in the Connect column click on the drop-down menu and select Set Windows Password.

Create a new username such as ctxadmin then click Set. Note that the username administrator is disabled in Windows instances in GCP.

Copy the local admin credentials to a safe location. This will be used to RDP into the management machine.

There are a few ways remotely connect to the bastion VM using RDP. If you are using a Windows PC simply open Remote Desktop Connection (mstsc.exe). If you are using Google Chrome, install the Chrome Remote Desktop.

In the GCP console, click on RDP in cbx-mgmt machine or in the drop-down menu click download the RDP file. Connect to cbx-mgmt machine using either RDP tool.
If you are using the Google Chrome RDP app, the remote certificate message will be displayed. Click continue. If you are using Windows RDP, click Connect.

Enter in the username clixadmin with the password created previously. Click Ok.

A connection to the clix-mgmt machine is established. This bastion machine will be the primary method for remoting into the remaining Windows machines in GCP.

Configure GCE Active Directory
Citrix Cloud requires Microsoft Active Directory (AD) to authenticate users and to integrate with the Citrix Cloud Connector and XenApp instances. Before a XenApp VM or Citrix Cloud Connector can be accessed in a GCE subscription for XenApp, it must successfully authenticate against the GCE AD domain controller. See "AD controllers in GCE" for details. For high availability, place each domain controller in separate zone.

The following procedure shows how to create a new instance in GCE for Microsoft Active Directory.
In the GCP console, open the Google Cloud Shell console.

Verify what Windows images you have in your region, by entering the following command:
gcloud compute images list --project windows-cloud --no-standard-images

To create the first domain controller using Google Cloud Shell, copy the script from the right side into a text editor like notepad. In the command, replace the "project_name" and service-account "number" with the project name and number with your account. Copy and paste the script into Cloud Shell and hit Enter.


The VM is created in GCE.

Although the status says running, the instance is not immediately ready; it takes some time for setup and activation.

To view the creation status, use the serial console for the instance in Google Cloud Shell, and enter the command below.
gcloud compute instances get-serial-port-output ctx-dc

The VM creation process takes between 5 to 10 minutes for an instance to be ready. When the instance is complete, the status displays as ready to use.

From the GCP console click on ctx-dc and choose Set Windows password.
From the GCP console enter the username `domain_svc` or similar to create the new administrator account and obtain a temporary password (this password should be changed at first log in).

Copy the password to use in the next step.

*Note: It is important to save these credentials for the administrator account in a safe location.*

---

**Set new Windows password**

If a Windows account with the following username does not exist, it will be created and a new password assigned. If the account exists, its password will be reset.

- If the account already exists, resetting the password can cause the loss of encrypted data secured with the current password, including files and stored passwords. [Learn more](#)

![Username](image)

**New Windows password**

The following is the new Windows password for `domadm`. Copy it and keep it secure. It will not be shown again.

![Password](image)

---

To connect to the ctx-dc VM we will use a double hop RDP method where the ctx-mgmt machine will initiate a RDP session to the ctx-dc VM. The ctx-mgmt has RDP access to all windows machines in the VPC provided the correct firewall rules are in place.

*Note: Ensure that you are connected to the ctx-mgmt machine by verifying the bbgino wallpaper that shows the logon server ctx-mgmt.*

---

Using RDP from your ctx-mgmt machine, right click on the Start Menu then click Run. Type MSTSC. Click Ok.
Enter the internal private IP assigned to the ctx-dc vm. Click Connect: Enter the username domadmin_svc and password copied from the previous step.

Click Yes to accept the certificate.

The RDP connection from the ctx-mgmt machine to the ctx-dc machine is connected. Follow the Google guide for creating your first domain controller for Active Directory.

Note: During the Windows sysprep image build process in GCP, the default local Windows username Administrator is disabled. Prior to installing Active Directory Services, ensure that the local Administrator account has a password assigned that meets the password policy requirements. The account can be enabled to assign a strong password using an elevated command prompt and disabled after. Use the command `net user administrator /active:yes` to enable the account and assign a password then use the command `net user administrator /active:no` to disable the account.
Step 3: Create Infrastructure Citrix Cloud VMs

Next, create VMs to be installed with the required Citrix Cloud components. The Citrix Cloud Connector serves as a channel for communication between Citrix Cloud and your resource locations, enabling cloud management without requiring any complex networking or infrastructure configuration such as VPNs or IPSec tunnels. The Cloud Connector authenticates and encrypts all communication between Citrix Cloud and your resource locations, such as GCP. There are no incoming connections. All connections are established from the Cloud Connector to the cloud. No communications between the Cloud Connector and Citrix Cloud are inbound. The Citrix Cloud Connector is stateless. All logs and alerts are sent back to Citrix Cloud. The connections all use the standard HTTPS port (443) and the TCP protocol. The Cloud Connector performs several key functions infrastructure roles such as:

- **Active Directory (AD)**: Enables AD management, allowing the use of AD forests and domains within your resource locations. It removes the need for adding any additional AD trusts.
- **XenApp and XenDesktop publishing**: Enables publishing from resources in your resource locations.
- **XenMobile**: Enables a XenMobile enterprise mobility management (EMM) environment for managing apps and devices as well as users or groups of users.
- **Delivery group provisioning**: Enables provisioning of machines directly into your resource locations.

Figure 5: Citrix Cloud Connector

Citrix Cloud requires you install the Citrix Cloud Connector on two machines inside GCP to provide continuous availability of your resource location. To ensure HA between connectors, it is recommended to place each connector in a separate zone in the same region. For additional information about how to create Citrix Cloud Connectors, see “Cloud Connector Installation”.

The table below shows the recommended instance configuration for Cloud Connectors in GCP.

<table>
<thead>
<tr>
<th>VM Name</th>
<th>Description</th>
<th>Project Name</th>
<th>Instance</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTX-CC-1</td>
<td>Citrix Cloud Connector</td>
<td>Citrix on Google</td>
<td>n1-standard-2</td>
<td>us-central-1c</td>
</tr>
<tr>
<td>CTX-CC-2</td>
<td>Citrix Cloud Connector</td>
<td>Citrix on Google</td>
<td>n1-standard-2</td>
<td>us-central-1f</td>
</tr>
</tbody>
</table>

Instructions | Visual
In previous steps we leveraged the Google Cloud Portal and Cloud Shell. For the remaining Cloud Connector VMs, we will be using the Google Cloud Shell and modify the previous script.

In the GCP console, open the Google Cloud Shell console.

Verify what Windows images you have in your region, by entering the following command:

gcloud compute images list --project windows-cloud --no-standard-images

To create the first Cloud Connector using Google Cloud Shell, copy the script from the right side into a text editor like notepad. In the command, replace the "project_name" and service-account "number" with the project name and number with your account. Note: In the images list ensure that the name in script reflects the most current version displayed.

Note: At the time of writing this guide v20171010 was the most up to date Windows Server 2016 instance.

Copy and paste the script into Cloud Shell and hit Enter.
The instance process creation begins.

<table>
<thead>
<tr>
<th>Name</th>
<th>Zone</th>
<th>Machine type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctx-cc-1</td>
<td>us-central1-c</td>
<td>2 vCPUs, 7.5 GB</td>
</tr>
</tbody>
</table>

Wait approximately 10 minutes before continuing with the next steps to assign a Windows password. To check the status of the deployment, Google Cloud Shell type `gcloud compute instances get-serial-port-output ctx-cc-1`. This will display the VM deployment status.

Click the cloud connector ctx-cc-1. Click Set Windows Password.

Enter the username ctxadmin, then click Set.

Set new Windows password

If a Windows account with the following username does not exist, it will be created and a new password assigned. If the account exists, its password will be reset. If the account already exists, resetting the password can cause the loss of unsaved data associated with the current password, including files and stored passwords.

- **Username**: ctxadmin

New Windows password

The following is the new Windows password for ctxadmin. Copy it and keep it secure. It will not be shown again.

To create the second Cloud Connector ctx-cc-2 in the us-central1-f second zone using Google Cloud Shell, copy the script from the right side into a text editor like notepad. In the command, replace the "project_name" and service-account "number" with the project name and number of your account.

```bash
```
Copy and paste the script into Cloud Shell and hit Enter.

Switch windows from the Google Cloud Shell back to the previous RDP connection to the bastion instance ctx-mgmt. From the ctx-mgmt instance we will perform a double hop and RDP into the first Cloud Connector ctx-cc-1. The IP of the first Cloud Connector can be found in the GCP console for the VM. Right click on the Start Menu and type mstsc. Enter in the IP address of the ctx-cc-1. Click Connect.

Enter the credentials saved earlier for the first Cloud Connector. Click OK. Click Yes to accept the RDP security certificate message.

The next steps will prepare the Cloud Connector ctx-cc-1 to be domain joined so that the agent can be installed. These steps need be repeated later on for second Cloud Connector ctx-cc-2.

Change the preferred DNS server to be the Active Directory DNS Server using PowerShell. Open PowerShell with elevated Administrator privilege and
paste the command in below.

**Note:** The DNS IP address for your domain VM instance may not be the same as shown below.
Set-
DnsClientServerAddress -
InterfaceAlias
("Ethernet") -
ServerAddresses
("10.128.0.3")
Hit Enter.

Change the DNS suffix to be the AD domain DNS address.
Open PowerShell with elevated administrative privilege and paste the command in below.

```powershell
$NetConf = Get-WmiObject
Win32_NetworkAdapterConfiguration -filter
"ipEnabled = "true""
$NetConf.SetDnsDomain("ctx.gcp")
$NetConf.SetDynamicDNSRegistration(True,True)
ipconfig /registerdns
Press Enter.
```

Join the machines to the AD domain.
Type `add-computer -computername ctx-cc-1 -domainname ctx.gcp -credential ctx\domain_svc -restart` -force and press Enter.
Type a password for the domain administrator account when prompted.
Click Ok.

Remote into the second Cloud Connector ctx-cc-2.
Repeat the processes above for setting the DNS.
information and joining the domain. This will prepare the VM for installing the Cloud Connector agent.

Cloud Connectors require outbound 443 internet access to communicate with Citrix Cloud. Since the connectors do not have a public IP address assigned, a NAT instance and tag will need to be applied to them for internet access.

Copy and paste the commands below into Google Cloud Shell.

gcloud compute instances add-tags natted-servers --tags internet-nat

Note: in the command above natted-servers refers to the instance names of the VM in Google Cloud that the tags need to be applied to.

Press Enter.

After joining the domain for both VM instances, RDP back into the Cloud Connector machine ctx-cc-1 and install the Cloud Connector agent.

The Citrix Cloud Connector agent uses an IE frame window for authentication. In order for the installation to authenticate properly, the IE Sec feature needs to be disabled for Admins. From Server Manager click on Local Server then in the IE Enhanced Security Config, Click the On setting. Disable this for administrators by selecting Off then click Ok.
Create a Citrix Cloud account at [https://onboarding.cloud.com](https://onboarding.cloud.com).

Note: An automated email will be sent to your inbox upon approval. Follow the email from Citrix on activating your Citrix Cloud service and choosing your region before continuing.

Once you have been approved for Citrix Cloud and the XenApp and XenDesktop Service, open IE and browse to [https://cloud.citrix.com](https://cloud.citrix.com). Login with your Citrix Cloud credentials.

Click on the top left corner menu next to Citrix Cloud and select Resource Locations.

In the Resource Locations click on the + Resource Location. Enter the name GCP then click Save.
Click on the + Cloud Connectors

<table>
<thead>
<tr>
<th>GCP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>+ Cloud Connectors</td>
</tr>
</tbody>
</table>

Click **Download** to save the Cloud Connector installer.

**Add a Cloud Connector**
The Connector serves as a channel that authenticates and encrypts all communication between Citrix Cloud and your resources.

**Requires:** [Details]

**Install:** [Details]

**Install** the Cloud Connector to continue.

Install the Connector. Click **Sign In**.
Login with the Citrix Cloud Subscription credentials click **Sign In** and complete the installation.

**Sign into Citrix Cloud to continue**

<table>
<thead>
<tr>
<th>Sign In</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

The installation can take up to 5 minutes. After the installation has finished, the service connectivity tests are performed, and the result should display **Connectivity Test Successful**.
Click **Close** to continue.

Repeat the previous processes to install the
**Cloud Connector on ctx-cc-2.**

After completion, two cloud connectors should appear inside the Citrix Cloud Resource Locations.

### Cloud Connectors

- ctx-cc-1.ctx-gcp
- ctx-cc-2.ctx-gcp

---

**Step 4. Prepare the XenApp Golden Image VM**

The Citrix VDA enables the machine to register with the Citrix Cloud Connector, which in turn allows the machine and the resources it is hosting to be made available to users. In this release of Citrix Cloud with GCP, there is no integrated MCS provisioning. Manual or out-of-band provisioning is required. This means that each VM is created independently, and there is no cloning of machines available for XenApp VMs in GCP. For details, see "[Configure VDAs](#)".

<table>
<thead>
<tr>
<th>Instructions</th>
<th>Visual</th>
</tr>
</thead>
<tbody>
<tr>
<td>To create the first XenApp VM using cloud shell, copy the commands from the right side into a text editor like notepad. In the command, replace the &quot;project_name&quot; and &quot;service-account &quot;number&quot; with the project name and number of your account.</td>
<td></td>
</tr>
<tr>
<td>Copy and paste the script into Cloud Shell and hit Enter.</td>
<td>InstanceSetup: Instance setup finished. ctx-xa-1 is ready to use.</td>
</tr>
<tr>
<td>Wait approximately 10 minutes before continuing with the next steps to assign a Windows password. To check the status of the deployment, Google Cloud Shell type gcloud compute instances get-serial-port-output ctx-xa-1. This will display the VM deployment status and when it is ready for use.</td>
<td></td>
</tr>
<tr>
<td>Click the VM instance ctx-xa-1. Click Set Windows Password.</td>
<td>Connect</td>
</tr>
<tr>
<td></td>
<td>RDP: ctx-xa-1</td>
</tr>
<tr>
<td></td>
<td>RDP: Set Windows password</td>
</tr>
</tbody>
</table>
Enter the username ctxadmin, then click Set.

The password for the username is created and should appear. Copy the password temporarily into your buffer and then into notepad so that it can be used to RDP into the machine. Click Close.

The next steps will prepare the ctx-xa-1 VM instance to be domain joined so that the Virtual Delivery Agent can be installed.

Change the preferred DNS server to be the Active Directory DNS Server using PowerShell. Open PowerShell with elevated Administrator privilege and paste the command in below.

Note: The DNS IP address for your domain VM instance may not be the same as shown below.

```
Set-DnsClientServerAddress -InterfaceAlias "(Ethernet)" -ServerAddresses ("10.128.0.3")
```

Hit Enter.

Change the DNS suffix to be the AD domain DNS address.

Open PowerShell with elevated administrative privilege and paste the command in below.

```
$sNetworkConfig = Get-WmiObject Win32_NetworkAdapterConfiguration -filter "ipEnabled = "true""
$sNetworkConfig.SetDnsDomain("ctx.gcp")
$sNetworkConfig.SetDynamicDNSRegistration($true,$true)
ipconfig /registerdns
```

Press Enter.

Join the machines to the AD domain.

```
type add-computer -computername ctx-xa-1 -domainname ctx.gcp -credential ctxxdomadm_svc -restart -force and press Enter.
```
Type a password for the domain administrator account when prompted. Click Ok.

In order to install the Citrix VDA, it has to be copied to the cbx-xa-1 VM from the cbx-mgmt VM instance which has internet access. From the cbx-mgmt VM instance open IE and browse to https://cloud.citrix.com. Login with the Citrix Cloud credentials. Click Sign In.

After logging into Citrix Cloud click Manage on the XenApp and XenDesktop Service. Click Downloads the top right corner.

Select the Download VDA. A browser window will open redirecting you to Citrix.com.

Click Download File to download the latest VDA.

Once the VDA has downloaded click Open Folder. Copy the VDAInstaller.exe into clipboard buffer.
RDP into the cbx-xa-1 VM instance. Paste the VDAServerSetup_7.16.exe onto the desktop.

Right click the VDAServerSetup_7.16.exe and chose Run as Administrator. The XenDesktop 7.16 installer window will appear. Select Enable connections to a server machine and click Next.

Uncheck the Citrix Receiver agent, then click Next.
Uncheck the components for App-V VDA and App Disk, then click Next.

Select Do it manually. Enter in the FQDN of two Cloud Connectors. Once they have been verified, click Next.

Select Optimize performance and click Next.
Select **Automatically** and click **Next** to configure firewall rules automatically.

Click **Install** to start installation and it will take approximately 5 minutes.

The XenApp prerequisites such as the RDS role will be enabled and will prompt for an immediate reboot. Click **Yes** to perform the reboot.

Once the reboot has completed, RDP back into the VM instance to continue the XenApp VDA installation. Once the installation is complete the Smart Tools Call Home option appears. Click **Connect**.
Enter in the Citrix account credentials for Citrix Cloud then click Ok.

If successful the connect button will have a green checkmark box next to it. Click Next.

Click Finish to restart the VM instance.

Step 5: Create a Machine Catalog
The next step constructs a machine catalog to contain machines generated from a master image. The virtual hard disk for the GCP VM containing the XenApp golden image is used as the master software image.

Note: In this early release of Citrix Cloud with Google Cloud Platform, the Citrix Machine Creation Services (MCS), power management, and Google Cloud as a hosting connection are not available; however manual connections can still be made.
For connections to a GCE instance in GCP, an out-of-band connection uses Citrix Cloud and NetScaler Gateway Service for secure access to the XenApp sessions. The following process shows how to create and out-of-band machine catalog to an instance in GCE.

**Instructions**

Log in to the [Citrix Cloud console](#)
Select the appropriate customer you have subscribed to.

Choose the Citrix XenApp and XenDesktop Service from the list of services and click on Manage.

Click the top left menu, click XenApp and XenDesktop Service.
From the XenApp and XenDesktop Service site, click Manage, then select the Full Configuration menu. This opens a Citrix Receiver remote session to the Citrix Studio management console.

In the Studio console, click Create Machine Catalog.

The Studio window appears. Click Next.
In the Operating System section, select Server OS to deploy a XenApp Catalog. Click Next.

In the Machine Management screen, select Machines that are not power managed. Select Another service or technology. Click Next.

Locate the machine on which VDA is installed on in Active Directory by searching in Add computers. Click OK. Click Next.
Enter a description for the Catalog, then click Finish.
Step 6: Create a Delivery Group
The next step uses Citrix Studio to create a Delivery Group for the XenApp deployment. A Delivery Group's characteristics are based on the desktops or machines within the group's machine catalog. A desktop is a virtual or physical machine that is created manually through the Create Machine Catalog wizard. The desktop characteristics come from the machine catalog to which they are assigned.

<table>
<thead>
<tr>
<th>Instructions</th>
<th>Visual</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the Studio console, right click <strong>Delivery Groups</strong>. Click <strong>Create Delivery Group</strong>. Click <strong>Next</strong>.</td>
<td><img src="image_url" alt="Instructions and Visual" /></td>
</tr>
</tbody>
</table>
Select the new catalog created called XenApp on GCP.

Click Next.

In the Users section, select Leave user management to Citrix Cloud.

Click Next.
On the applications screen, click Next.

In the Delivery Group Name and Display name field, enter XenApp.
Click Finish.

The Delivery Group is created.
**Step 7: Assigning access to users**

After the Citrix Cloud connectors, Machine Catalogs, and Delivery groups are created, the base XenApp instance can be accessed remotely. In order to assign the correct subscribers to the instance, you need to apply appropriate permissions with the Citrix Cloud Library.

<table>
<thead>
<tr>
<th>Instructions</th>
<th>Visual</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the top left menu, click Library.</td>
<td><img src="Image" alt="Citrix Cloud Library" /></td>
</tr>
<tr>
<td>Locate the XenApp (Desktops) published resource created earlier. Click on the ellipsis (...) icon. Click Manage Subscribers.</td>
<td><img src="Image" alt="Manage Subscribers" /></td>
</tr>
<tr>
<td>Enter the name of the Active Directory account or group you wish to assign access to.</td>
<td>Manage Subscribers for</td>
</tr>
<tr>
<td>Add Subscribers</td>
<td><img src="Image" alt="Add Subscribers" /></td>
</tr>
<tr>
<td>Selected 1 of 1 Subscriber(s)</td>
<td>Remove Selected</td>
</tr>
<tr>
<td>The resource should now be published.</td>
<td><img src="Image" alt="XenApp (Desktops) Published" /></td>
</tr>
</tbody>
</table>

**Step 8: Access GCE securely using NetScaler Gateway Service**

NetScaler Gateway provides users with secure VPN access to XenApp, XenDesktop, and XenMobile applications across a range of devices including laptops, desktops, thin clients, tablets, and smartphones. NetScaler Gateway Service enables secure, remote access to XenApp and XenDesktop applications, without having to deploy NetScaler Gateway in the DMZ or reconfigure your firewall. The entire infrastructure overhead of using NetScaler Gateway moves to the cloud and hosted by Citrix. You enable NetScaler Gateway Service in the Citrix Cloud. After enabling the service, users can access their VDAs in GCP from outside their network, as shown in the following diagram.
**Instructions**

- On the Citrix Cloud > Apps and Desktops menu, choose Manage > Service Delivery. The Service Delivery screen appears.

- Click Enable to activate NetScaler Gateway.

- Click Use cloud hosted NetScaler Gateway Service. Click Save.

- Login to the XenApp and XenDesktop NetScaler Gateway Service URL [https://customername.xendesktop.net](https://customername.xendesktop.net) where customer name is the unique URL assigned to you in the Service Delivery site.

  If needed, install the Citrix Receiver client or use the light version.

**Visual**

![NetScaler Gateway Service diagram](image-url)

![Citrix Cloud Service Delivery](image-url)

![NetScaler Gateway Settings](image-url)
Enter in the Active Directory credentials for a user assigned earlier in the Library. Click Log On.

The XenApp on GCP instance is now available for user login.
Learn more
For more information about deploying Citrix XenApp on Google Cloud Platform, see also these resources.

<table>
<thead>
<tr>
<th>Resource</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Cloud</td>
<td><a href="https://www.citrix.com/products/citrix-cloud/">https://www.citrix.com/products/citrix-cloud/</a></td>
</tr>
<tr>
<td>Google Cloud Trial FAQ</td>
<td><a href="https://support.google.com/cloud/answer/6330231?hl=en">https://support.google.com/cloud/answer/6330231?hl=en</a></td>
</tr>
<tr>
<td>Google Cloud Billing</td>
<td><a href="https://cloud.google.com/billing/docs/how-to/billing-access">https://cloud.google.com/billing/docs/how-to/billing-access</a></td>
</tr>
<tr>
<td>Google Cloud Sustained User Discounts</td>
<td><a href="https://cloud.google.com/compute/docs/sustained-use-discounts">https://cloud.google.com/compute/docs/sustained-use-discounts</a></td>
</tr>
<tr>
<td>Google Cloud Startup Scripts</td>
<td><a href="https://cloud.google.com/compute/docs/startupscript">https://cloud.google.com/compute/docs/startupscript</a></td>
</tr>
<tr>
<td>Google Compute Engine Pricing</td>
<td><a href="https://cloud.google.com/compute/pricing">https://cloud.google.com/compute/pricing</a></td>
</tr>
<tr>
<td>Google Cloud Storage</td>
<td><a href="https://cloud.google.com/compute/docs/disks/">https://cloud.google.com/compute/docs/disks/</a></td>
</tr>
<tr>
<td>Google Cloud Firewall rules</td>
<td><a href="https://cloud.google.com/compute/docs/vpc/firewalls">https://cloud.google.com/compute/docs/vpc/firewalls</a></td>
</tr>
<tr>
<td>Google Cloud NAT gateway</td>
<td><a href="https://cloud.google.com/compute/docs/vpc/special-configurations#natgateway">https://cloud.google.com/compute/docs/vpc/special-configurations#natgateway</a></td>
</tr>
<tr>
<td>Google Cloud Special Configurations</td>
<td><a href="https://cloud.google.com/compute/docs/vpc/special-configurations">https://cloud.google.com/compute/docs/vpc/special-configurations</a></td>
</tr>
<tr>
<td>Google Cloud External IP Addresses</td>
<td><a href="https://cloud.google.com/compute/docs/ip-addresses/#externaladdresses">https://cloud.google.com/compute/docs/ip-addresses/#externaladdresses</a></td>
</tr>
<tr>
<td>Google Cloud Platform Troubleshooting</td>
<td><a href="https://cloud.google.com/compute/docs/troubleshooting">https://cloud.google.com/compute/docs/troubleshooting</a></td>
</tr>
<tr>
<td>Google Cloud Migration</td>
<td><a href="https://cloud.google.com/compute/docs/tutorials/migrating-vms-compute-engine">https://cloud.google.com/compute/docs/tutorials/migrating-vms-compute-engine</a></td>
</tr>
<tr>
<td>Google Cloud Secure VM Instances</td>
<td><a href="https://cloud.google.com/solutions/connecting-securely">https://cloud.google.com/solutions/connecting-securely</a></td>
</tr>
<tr>
<td>Google Cloud Instance Groups</td>
<td><a href="https://cloud.google.com/compute/docs/instance-groups/">https://cloud.google.com/compute/docs/instance-groups/</a></td>
</tr>
</tbody>
</table>
Revision and Signoff Sheet

Change Record

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Change Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/5/2017</td>
<td>Citrix</td>
<td>1.1</td>
<td>Tony Sanchez</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>