Cloud Automation Stack

Windows 10 Reference Architecture

Version 0.3

Last Updated: 11/6/2020

Document Overview

The itopia Cloud Automation Stack (CAS) is an orchestration platform for creating and managing remote computing environments in Google Cloud leveraging Microsoft Remote Desktop Services (RDS) or Windows 10 Enterprise. With CAS, administrators can launch a customized environment within minutes, rather than hours or days with manual configuration. CAS also greatly simplifies ongoing management of the environment by supporting user and group management, disk image refreshes, and simplified connectivity for end-users, all while using native Remote Desktop functionality compatible with any RDP client for any platform.

This document provides a high-level summary of the architecture of Windows 10 deployments supported by CAS, as well as the CAS platform and its relationship to your environment. For information on RDS-based environments, refer to Cloud Automation Stack - RDS Reference Architecture.

NOTE: itopia's Windows 10 Cloud VDI offering is currently in development. While every effort has been made to ensure accuracy, some information presented in this document may be subject to change before the product reaches general availability.

About itopia Cloud VDI

itopia CAS orchestrates and manages Cloud VDI deployments within customers' Google Cloud projects. This allows customers to maintain full ownership of their infrastructure and data, and also allows customers much greater control over their environment. Customers can deeply integrate their Cloud VDI environment with their existing IT infrastructure and leverage existing monitoring and management solutions, maintain the Cloud VDI environment as an isolated environment with no connectivity to their other infrastructure, or anything in between.

For general information on planning your Cloud VDI environment, refer to the Getting Started section of the itopia Documentation Portal.

Glossary of Terms

The following table provides a quick reference of terms that may be used in this document.

Term	Definition / Description
Client Project	The GCP project owned by the customer into which Cloud VDI resources are deployed
Dedicated Collection	A Windows 10 Collection Pool in which each user is assigned a specific Windows 10 VM. The user connects only to this VM.
Deployment Region(s)	The GCP regions in which the Cloud VDI deployment is created. Cloud VDI deployments can be single-region or multi-region across all geographical regions supported by Google Cloud.
Deployment Network	The VPC network on which the Cloud VDI deployment resides.

Pooled Collection	A Windows 10 Collection Pool in which users may connect to any available Windows 10 VM.

Architecture Summary

Cloud Automation Stack (CAS) is itopia's orchestration and management system for Cloud VDI environments. Within CAS, each Cloud Desktop environment is referred to as a *deployment*. When you sign up for itopia CAS, you create a new *organization* that is tied to your email address; this organization can then contain one or more Cloud Desktop deployments. Detailed information on CAS deployments is available from the itopia Documentation Portal.

itopia CAS supports two distinct deployment types:

- **Cloud VDI using Windows 10 Only** - Deployments that are created to support Windows 10 only will provision custom services for itopia's Windows 10 desktop delivery.
- **Cloud VDI using Remote Desktop Services and Windows 10** - Deployments that are created to support both *Remote Desktop Services* (RDS) and Windows 10 will provision the necessary infrastructure for RDS as well as custom services for itopia's Windows 10 desktop delivery.

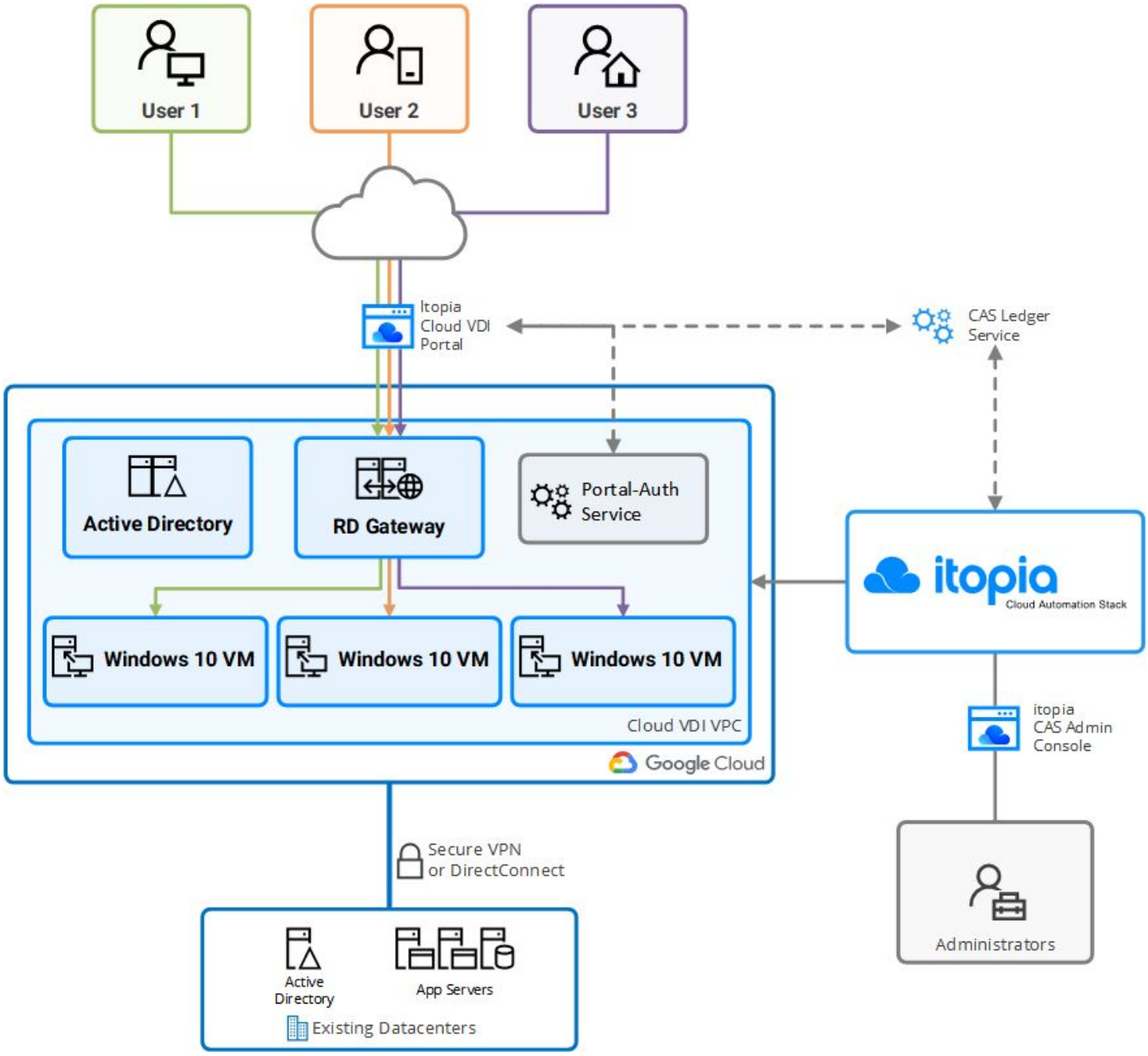
An itopia Windows 10 Cloud VDI deployment has several key infrastructure components that reside within the *client project*:

- **Windows 10 Session Hosts** - Windows 10 Session Hosts are the individual VMs to which your users connect.
- **Active Directory Domain** - CAS deployments require an *Active Directory* (AD) to handle user authentication. When creating your deployment, CAS offers several options to fulfill this requirement: create a new standalone AD domain, deploy into an existing AD domain, or create a new AD domain and configure an AD trust to an existing domain. Additional information on Active Directory is available in the itopia Documentation Portal.
- **Remote Desktop Gateway** - The RD Gateway role acts as a "proxy" device that provides a secure way of accessing Session Hosts, particularly across the public Internet. When a user accesses their Cloud Desktop, they actually connect to a Gateway server using encrypted HTTPS; the gateway server then creates a separate, encrypted connection to a Session Host and "relays" the input and output between the end-user and their Cloud Desktop session. In this way, access to the internal network is extremely limited, and user sessions are protected via TLS when traversing the Internet.
    - **Portal-Auth Service** - The Portal-Auth Service is a custom itopia webservice that is installed on RD Gateway servers to provide Active Directory pre-authentication for users accessing the Cloud VDI Portal.
- **File Server for Profiles and Shares** - CAS deployments support FSLogix Profile Containers for providing persistent, roaming user profiles across different Session Hosts. Additionally, CAS allows for the creation and management of simple network shares and mapped drives for users. The data for these profiles and shares are stored on an SMB file share in each deployment region, using either a Windows-based file server VM or the NetApp Cloud Volume Service.

Additionally, Cloud VDI environments include the following components that are hosted and managed by itopia:

- **Proxy Execution Service (PES)** - The *proxy execution service* (PES) is responsible for performing management tasks against the Windows VMs running Cloud VDI infrastructure. Each deployment is assigned a unique PES instance, which is deployed into an itopia-owned GCP project. Each PES instance resides on a dedicated VPC network, which is *peered* with the deployment network; CAS configures a minimal number of firewall rules to permit management traffic only *from* the PES instance and only *to* the Cloud VDI infrastructure VMs.
- **CAS Ledger Service** - The CAS Ledger Service monitors user session status on Windows 10 Session Hosts and routes users to the appropriate Session Host when they connect from the Cloud VDI Portal
- **Cloud VDI Portal** - The Cloud VDI portal is a web-based method for users to access their Cloud VDI sessions. Users log into Cloud VDI with their Active Directory credentials; the credentials are securely proxied to the RD Gateway server(s) in the Cloud VDI environment, which then performs Active Directory authentication of the user's credentials and assigns a short-lived token for the user to view and access their Cloud VDI resources (published Remote Desktops and RemoteApps). When a user connects to their resource, the portal downloads a customized RDP file that is launched using the Remote Desktop client on the user's local device.

The diagram below represents these components for a Windows 10 Cloud VDI deployment.



About Windows 10 in Google Cloud

Google Cloud supports GCE VM instances running Windows 10 only when used with sole-tenant nodes (STNs). A sole-tenant node is a hypervisor host server that is reserved only for your GCP project, effectively providing your project with dedicated usage of the server. STNs can be beneficial for regulatory and compliance needs where shared workloads are not permitted, as well as for fixed budgeting purposes, as STNs are billed at a constant price regardless of the number of VMs running on the nodes. Additional information about sole-tenant nodes is available from Google.

STNs also facilitate the use of bring-your-own-license (BYOL) for Microsoft operating systems and certain applications. BYOL allows GCP customers to leverage their existing Microsoft licenses (with appropriate usage

rights) for VMs running in Google Cloud. This licensing typically requires licensing of "all CPU processors and/or cores" on the physical server; STNs facilitate this requirement by providing a fixed number of CPUs on which the VMs can run, thus allowing the license to be applied to all of them.

Using the BYOL framework, Microsoft allows running properly licensed versions of Window 10 Enterprise in Google Cloud. Therefore, itopia CAS deployments that deliver Windows 10 desktops *must* meet the following requirements:

- The GCP project must have sole-tenant nodes in each region to which CAS will deploy desktops
- CAS must be configured to leverage the sole-tenant nodes
- Proper OS images that are configured for BYOL must be used for all Windows 10 desktops. Additional information on BYOL in Google Cloud is available from Google.
- Customers must provide valid licensing for their Windows 10 Enterprise desktops

It is important to note that Windows 10 desktops in Google Cloud are single-session only; that is, each VM only supports a single concurrent user session. Customers interested in multi-session desktops should explore itopia's RDS-based Cloud VDI deployments.

Google Cloud Infrastructure

To support the Windows 10 Cloud VDI deployment, customers must provide a Google Cloud *project* for the deployment resources. This project will contain all resources provisioned by CAS for the Cloud VDI environment.

Cloud VDI deployments can be provisioned in one or more Google Cloud regions. itopia CAS supports all GCP regions, however certain features or instance types may not be available in all regions.

Cloud VDI infrastructure and Session Host VMs must be configured on a *Virtual Private Cloud* network. CAS supports deploying onto a new VPC network in the GCP project, an existing network in the project, or a *shared VPC network* in another GCP project.

Regardless of the VPC option chosen, the Cloud VDI environment can be connected to existing network infrastructure using either VPC peering or a VPN or Dedicated Interconnect.

Active Directory

itopia Cloud VDI supports several options for its Active Directory infrastructure:

- **Standalone AD** - Deploying a new Active Directory domain/forest (using either Windows Active Directory or Google's Managed Service for Microsoft Active Directory) and maintaining it as a standalone domain
- **Trusted AD** - Deploying a new Active Directory domain/forest (using either Windows Active Directory or Google's Managed Service for Microsoft Active Directory) and establishing an Active Directory trust with an existing domain
- **Extended AD** - Deploying into an existing Active Directory domain that will be extended into the Cloud VDI environment with additional domain controllers

Each option has its own advantages and disadvantages, and the decision ultimately depends on the level of integration (or isolation) that the customer requires. Many enterprise organizations elect to use the Trusted Active Directory model, wherein the Cloud VDI infrastructure is isolated to its own AD domain, but end-users can still access their desktops and existing resources (such as file shares and intranet sites) using their existing Active Directory credentials. Additional information is available in the itopia Documentation Portal: Active Directory in CAS Deployments.

Collection Pools

In itopia's Cloud Automation Stack (CAS), Collection Pools allow you to create unique sets of RD Session Host servers and configuration settings for different workloads and users. Each Collection Pool lets you define the following:

- The method for assigning users to Session Hosts: either as a *shared* Collection where users can connect to any available Session Host, or as a *dedicated* Collection where each users is assigned a specific Session Host to which they always connect
- Whether to use persistent or non-persistent user profiles
- The regions in which to deploy the Session Host VMs
- The disk image to use for the Session Host VMs
- The CPU, RAM, and disk sizing of Session Host VMs
- Session Host autoscaling and Dynamic Uptime settings
- Session timeouts and other client connection options

Many organizations leverage multiple Collection Pools to provide different OS images to different groups of users, or to enforce different policies (such as GPOs or network firewall rules) for different pools. Collection Pools can be created, managed, and deleted at any time.

End-User Experience

When users wish to connect to their Windows 10 VMs, they will use the Cloud VDI Portal to view available Cloud VDI resources (such as different Windows 10 VMs if they are assigned to multiple Collection Pools). When they select a resource, the portal will provide a customized RDP file that will open with the native RDP client on the user's local device; itopia recommends Microsoft's first-party Remote Desktop client, available for Windows, MacOS, Android, and iOS and iPadOS. When the RDP file is launched, the Remote Desktop client will connect via HTTPS to the RD Gateway server and on to their Windows 10 VM.

If a *multi-factor authentication* solution is configured, the user will be presented with the Windows 10 login screen and the Custom Windows Credential Provider; when the user completes their MFA challenge, the Windows 10 desktop will appear.

When their session is complete, the user may log off or simply close the Remote Desktop window; CAS will automatically terminate the user's session after approximately a minute and, in a *Pooled Collection*, make the VM available for other users.

itopia Cloud VDI Security Controls

itopia Cloud VDI isn't just Remote Desktop on Google Cloud, it's Remote Desktop *for* Google Cloud. itopia purpose-built Cloud VDI and the Cloud Automation Stack to offer a deep level of integration with Google Cloud and to leverage its exceptional performance, security, and cost efficiency to provide a stable, scalable remote computing platform for our customers.

With itopia and Google Cloud, you own your environment; all resources created by CAS reside in your own Google Cloud project, and CAS functions solely as an orchestration and automation platform. Cloud Desktop deployments use native technologies and APIs from Microsoft and Google Cloud, offering you unrivaled control and flexibility in customizing your environment.

In designing Cloud VDI and the Cloud Automation Stack, itopia strictly adheres to several key security guidelines:

- All system privileges are assigned using the *principle of least privilege*; service accounts in your GCP project and your Cloud VDI Active Directory have tightly-scoped permissions and can only perform the specific duties that they require. Similarly, firewall rules and access points are secured to only permit the necessary traffic for normal Cloud VDI functions
- itopia engineers and staff have no access to your environment unless it is explicitly granted. Your Google Cloud project, CAS deployment, and Cloud VDI infrastructure cannot be accessed by anyone to whom you do not grant access.
- All Cloud VDI infrastructure enforces encryption across all data and communication: Cloud VDI VM disks are encrypted at-rest by Google Cloud, CAS orchestration uses HTTPS for all administrative tasks, and end-user access is secured by SSL (via HTTPS encapsulation of the RDP protocol).
- Cloud VDI user credentials are not stored by itopia. Your Cloud VDI Active Directory domain is responsible for user authentication; CAS does not store passwords or password hashes for any user accounts. *NOTE: Administrator accounts in the CAS admin console may be encrypted and stored by CAS if local authentication is configured; the CAS admin console can be configured to require single sign-on with Google or Microsoft identity providers.*

With their deep integration with Google Cloud, itopia Cloud VDI and the Cloud Automation Stack inherit many of the security controls provided natively by Google. Additionally, itopia and the Cloud Automation Stack are regularly subject to external security and compliance audits; summaries of these reports and detailed documentation on security architecture are available upon request.

itopia also helps many organizations implement their own security and compliance requirements in Cloud VDI. Whether customers need to segregate network traffic between specific Collection Pools or enforce stricter encryption algorithms, the flexibility of the Cloud VDI solution allows customers to harden their environment to suit their needs.

Conclusion

itopia's Cloud Automation Stack is exclusive to Google Cloud and offers deep integration with GCP's tools and services to provide a secure, cost-effective remote computing solution. itopia Cloud VDI offers unparalleled customization and extensibility while providing a simple way to manage your VDI environment.