GCP Marketplace

itopia

Cloud Automation Stack

Architectural Summary

Version 1.1
Last Updated: 9/25/2020

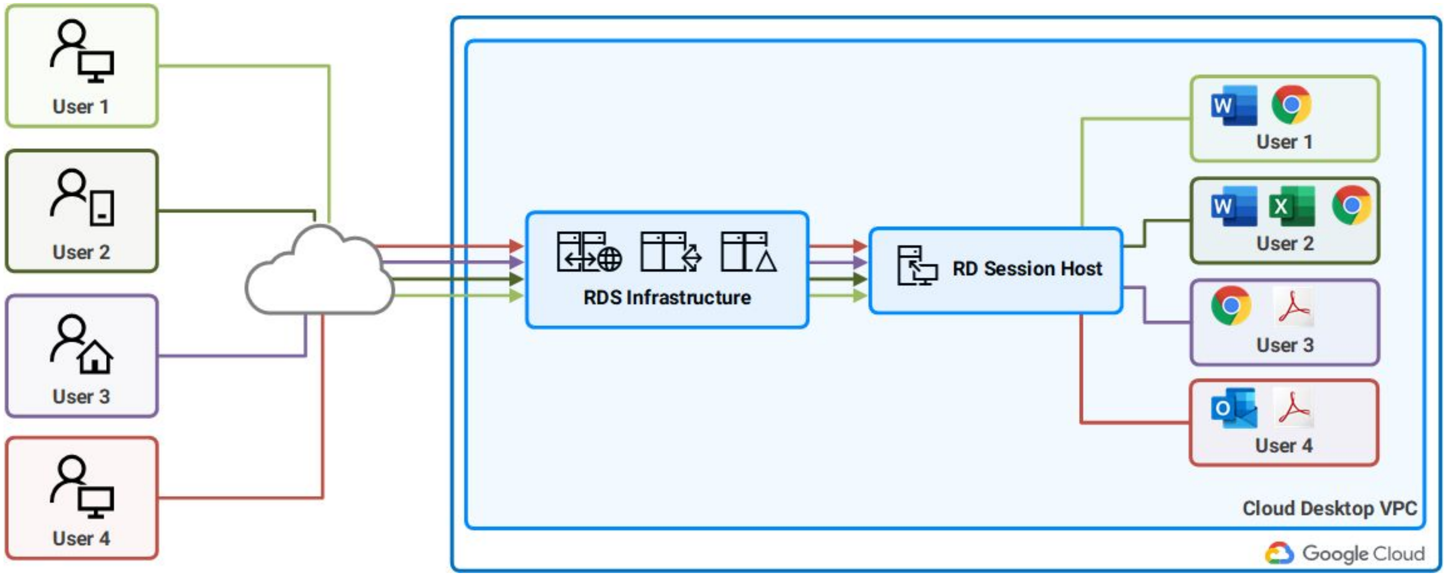
Document Overview

The itopia Cloud Automation Stack (CAS) is an orchestration platform for creating and managing Microsoft Remote Desktop Services (RDS) environments in Google Cloud. With CAS, administrators can launch a customized RDS deployment within minutes, rather than hours or days with manual configuration. CAS also greatly simplifies ongoing management of the RDS 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 the RDS deployments supported by CAS, as well as the CAS platform and its relationship to your environment.

Remote Desktop Services Overview

Microsoft's *Remote Desktop Services* is a technology that enables remote computing for users by enabling the delivery of a standard Windows desktop across a network connection. With RDS, end-users can use a personal device such as a laptop or tablet to securely access their corporate-managed desktop and applications without the need for VPN software. RDS also enables multi-session computing, wherein several users run discreet desktops on a single host server, thereby reducing the number of client devices required.



An RDS deployment consists of several components:

- **Remote Desktop Session Host** - A Session Host is a server that runs user sessions. When a user runs a Remote Desktop or RemoteApp, a Session Host is the server where the desktop or application is actually running; the desktop or application is "streamed" to the end-user's client device via the Remote Desktop Protocol (RDP), allowing them to interact with the session as it if was running on their local device.
- **Remote Desktop Session Broker** - The Session Broker is the "brains" of an RDS environment. The Session Broker maintains the mapping of users to Session Hosts, monitors the status of Session Host servers, and routes users to the correct Session Host. The Session Broker also maintains the primary settings database for the RDS environment.

- **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.
- **Remote Desktop Web** - The RD Web role provides a browser-accessible web portal where users can log in to launch their RDS desktops and applications. The RD Web role also hosts the Remote Desktop Web Client, an HTML5 RDP client that allows users to access their Cloud Desktops directly from a web browser
- **Remote Desktop Licensing** - The RD Licensing role tracks the usage of Remote Desktop Subscriber Access Licenses (RDS SALs) in the environment.

Additionally, RDS deployments require a **Microsoft Active Directory (AD) domain** to provide authentication and permissions. All servers in an RDS deployments must be joined to an AD domain.

CAS Deployments

The itopia Cloud Automation Stack (CAS) simplifies the creation and management of RDS environments built in Google Cloud. CAS offers tremendous flexibility in creating the right RDS solution for your organization and gets you up and running in minutes:

- Automated configuration of Active Directory with multiple options: create a new standalone domain, use an existing domain, create an AD trust to an existing domain
- Single-region or multi-region deployments: build RDS infrastructure in any GCP region and use the MyRDP portal to intelligently route your users to their closest region
- Multiple options for high-availability: deploy infrastructure roles with application-level redundancy, in addition to Google Cloud's many built-in fault-tolerance protections
- Size, scale, and auto-scale your resources as needed: RDS infrastructure and session host resources can be scaled up or down at any time, and user density settings allow CAS to auto-scale the number of session hosts to maximize performance and minimize compute costs

CAS also provides additional features to simplify the management of a Cloud Desktop environment, including:

- OS image management: Create, deploy, and refresh images for Session Host servers from the CAS admin console
- User and group management: Create Active Directory users directly in the CAS admin console and assign them to group
- Manage file shares and mapped drives: Creating network file shares and assign mapped drives to users and groups
- Automated configuration of roaming profiles: Collections can be configured to use FSLogix Profile Containers or to enforce nonpersistent user sessions

CAS offers a simple, wizard-style interface to configure your deployment within minutes; when you're finished, our automated system will provision everything within a few hours, depending on the number of GCP regions included in your deployment.

When the initial provisioning is finished, you'll be up and running with a single *Collection Pool*; each pool de. You can create additional *Collection Pools* to host different OS images or configure different user densities and VM sizes

itopia and Google Cloud

Cloud Desktop isn't just RDS on Google Cloud, it's RDS *for* Google Cloud. itopia purpose-built Cloud Desktop 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.

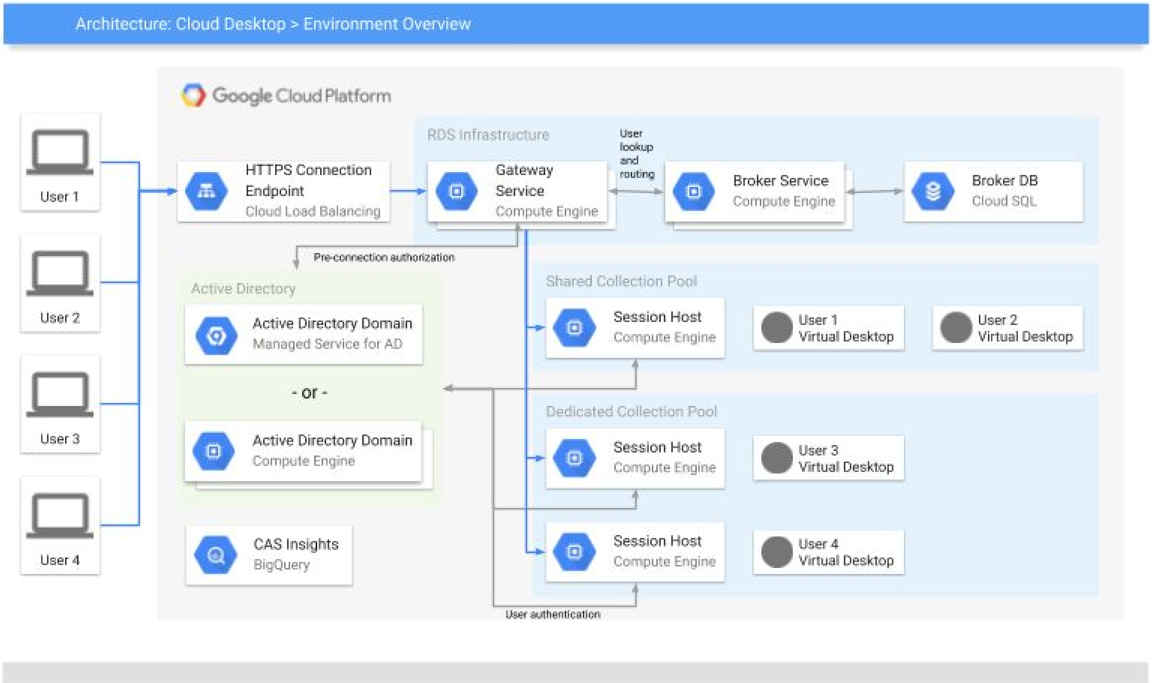
With itopia and Google Cloud, you own your environment; all resources created by CAS reside in your own Google Cloud project, and CAS functions solely as an orchestration and automation platform. Cloud Desktop deployments use native technologies and APIs from Microsoft and Google Cloud, offering you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

CAS uses two methods to manage a Cloud Desktop deployment: Google Cloud APIs for managing resources and configuration at the infrastructure level, and private network connectivity to the Windows server instances for managing the OS, RDS, and application configuration.

The diagram below provides a conceptual overview of a typical CAS deployment:

- Highly-available and load-balanced RDS infrastructure
- Multiple Collection Pools to provide subsets of users with different OS images, applications, and session host resources
- CAS Insights to provide real-time and historical analytics of user activity

Cloud Desktop > Environment Overview



GCP Administration

In order to perform administrative tasks at the resource level in the customer's Google Cloud project, CAS relies on the use of a *service account*. The service account is provisioned using GCP's *Identity and Access Management* (IAM) API and is used to perform resource-level tasks (such as creating Compute instances and firewall rules, and starting/stopping instances).

Service Account Provisioning

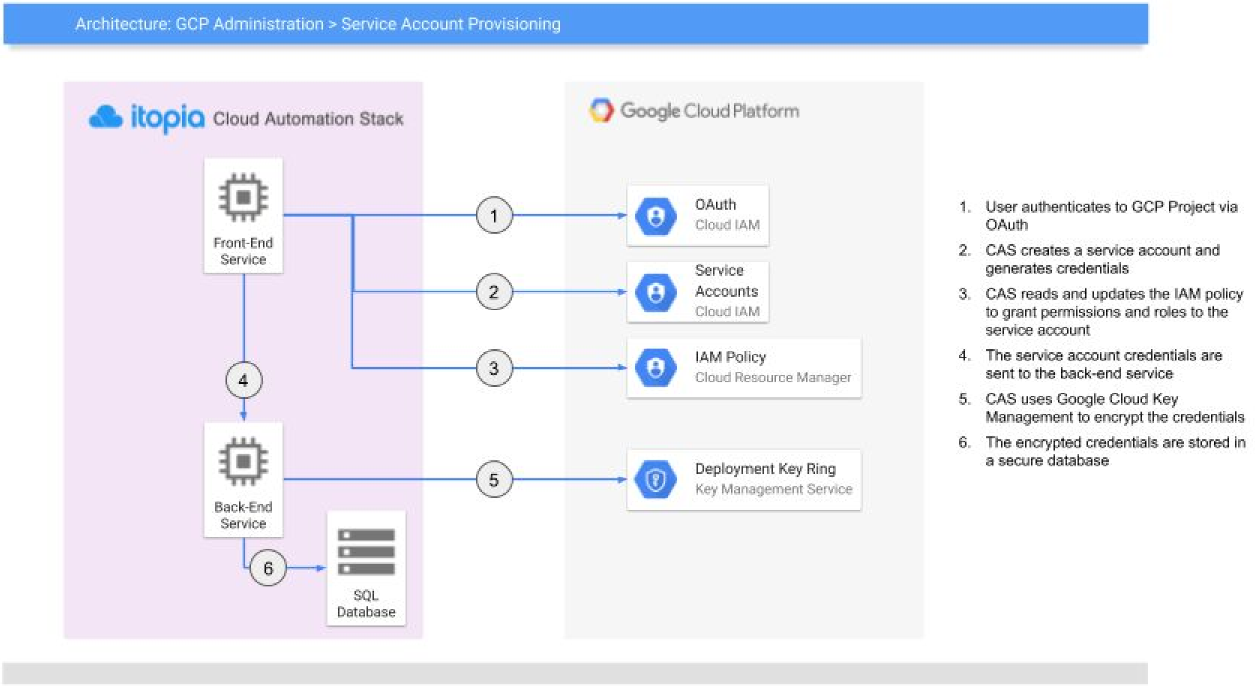
When creating a new deployment, the CAS wizard prompts the administrator to provide credentials for their GCP environment using Google's OAuth interface. These credentials are not read or stored by itopia, and an OAuth token is granted to the CAS to allow access to GCP. The CAS portal client-side code (running within the administrator's browser) uses the OAuth token to create a service account for the selected project. This service account is created using GCP's *Identity and Access Management* (IAM) API.

The CAS portal sends a request to generate the Service Account Key using GCP's *Identity and Access Management* (IAM) API. The CAS portal reads all IAM policies using GCP's *Cloud Resource Manager* API and sets the policy of the IAM service account through *Cloud Resource Manager* API.

The CAS portal sends the service account integration data to the backend CAS service to encrypt and save. The CAS service encrypts the service account credentials using the deployment's dedicated KMS key and saves the encrypted service account credentials in its database.

The diagram below provides an overview of how itopia CAS securely creates and manages the GCP service account. Alternatively, administrators can directly provide CAS with credentials for a pre-created service account that has the necessary permissions.

GCP Administration > Service Account Provisioning



1. User authenticates to GCP Project via OAuth
2. CAS creates a service account and generates credentials
3. CAS reads and updates the IAM policy to grant permissions and roles to the service account
4. The service account credentials are sent to the back-end service
5. CAS uses Google Cloud Key Management to encrypt the credentials
6. The encrypted credentials are stored in a secure database

Service Account Permissions

By default, the service account created during the Deployment creation is assigned the *Project Editor* role to ensure itopia has access to all Google services within the project in the event they become necessary as we add new features to our software. However, if the customer chooses, it can reduce the Service Account access to the following roles:

- Compute Admin
- Deployment Manager Editor
- BigQuery Admin
- Google Cloud Managed Identities Admin
- Storage Admin
- Cloud Filestore Editor *(required for future functionality)*
- Cloud SQL Admin *(required for future functionality)*
- Kubernetes Engine Admin *(required for future functionality)*

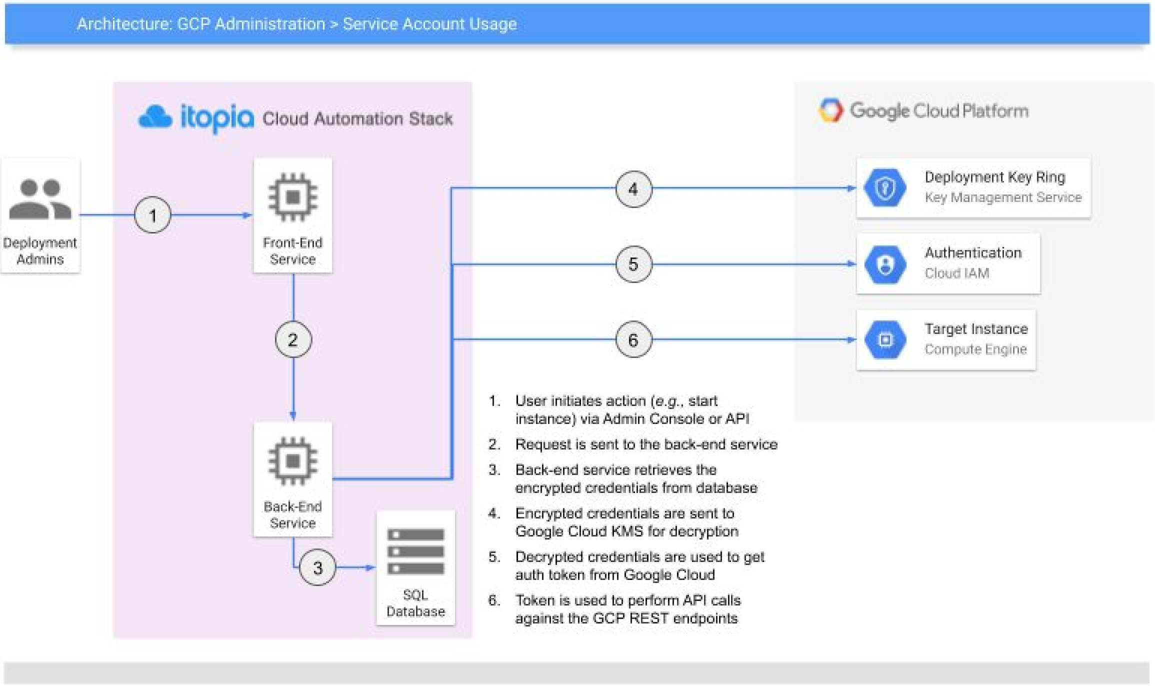
A detailed list of the permissions required for the service account can be found ***here*** (Google Sheets spreadsheet).

Service Account Usage

1. When an action is initiated in the CAS portal (such as starting or stopping an instance), the request is sent to the backend CAS service.
2. The CAS service retrieves the encrypted service account credentials from the database.
3. The CAS service decrypts the service account credentials using the crypto extension.
4. The CAS service uses the service account to perform OAuth authentication against the GCP project and receives an auth token.
5. The CAS service uses Google Cloud's REST API to perform the requested action, providing the auth token for validation.
6. All CAS interactions with a GCP project are logged and audited to monitor for unauthorized access.

The diagram below provides an overview of how itopia CAS securely uses the service account to perform administrative actions against Google Cloud resources.

GCP Administration > Service Account Usage



1. User initiates action (*e.g.*, start instance) via Admin Console or API
2. Request is sent to the back-end service
3. Back-end service retrieves the encrypted credentials from database
4. Encrypted credentials are sent to Google Cloud KMS for decryption
5. Decrypted credentials are used to get auth token from Google Cloud
6. Token is used to perform API calls against the GCP REST endpoints

CAS Insights and BigQuery

CAS Insights is a free, optional feature included with every Cloud Desktop deployment that provides usage analytics for your CAS deployment. CAS Insights offers a number of metrics to help track user activity and server utilization through a real-time dashboard and historical reporting. CAS Insights monitors granular information including:

- Application usage by individual users, or user activity by application
- File and folder access statistics for network file shares
- Historical user concurrency and Session Server uptime
- Detailed GCP cost breakdowns for compute, networking, and other resource usage

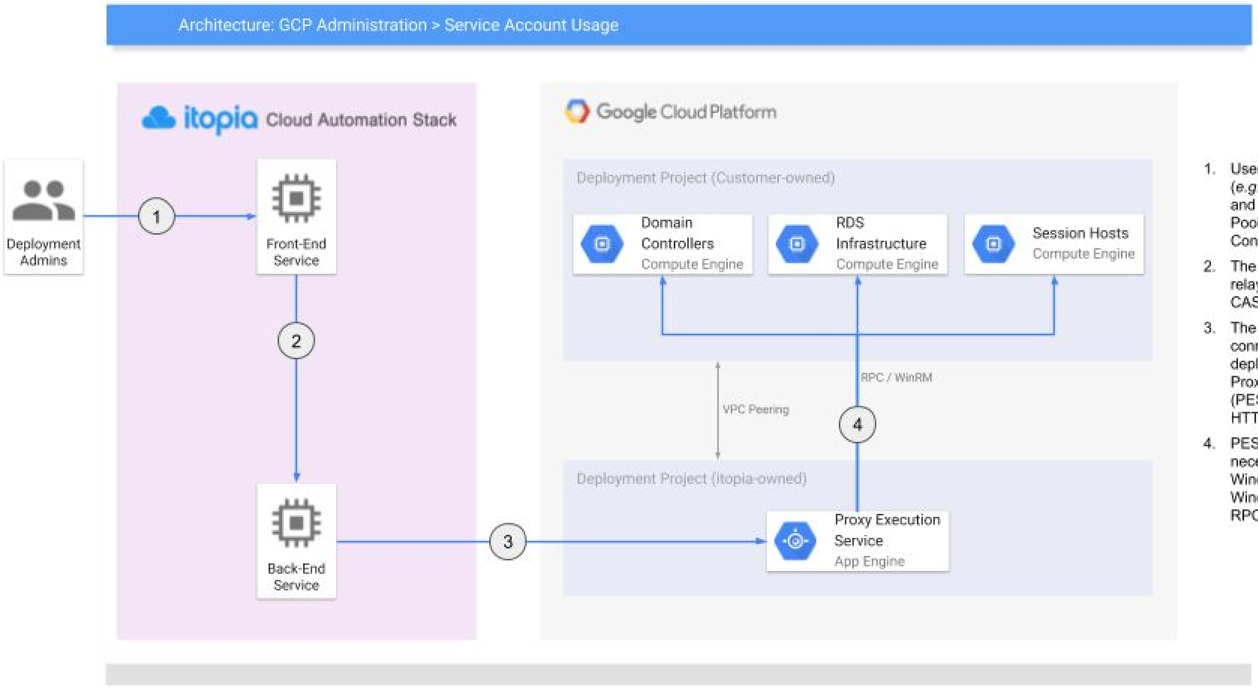
CAS Insights leverages GCP BigQuery for its backend data warehouse. When you enable Insights, CAS provisions a BigQuery dataset in your GCP project and installs several Windows services on the servers in your Cloud Desktop deployment; these services regularly collect usage data and securely upload them to BigQuery. You can then use the built-in reporting in CAS or craft your own custom queries in BigQuery directly. Customers use CAS Insights to understand users' usage patterns, perform software licensing audits, and to help optimize their GCP costs.

The data collected by Insights is not shared with itopia or any third-party service; only administrators in your CAS deployment and your GCP project have access to the data collected by Insights. Insights is not enabled by default, and can be disabled at any time.

Windows Server Administration

itopia CAS leverages a *proxy execution service* (PES) to transmit administrative commands on the internal GCP network. The PES is an itopia-managed App Engine instance running in an isolated *virtual private cloud* (VPC); the PES receives execution bundles (i.e. target server IP, credentials, and commands to execute), performs the requested operation on the RDS server, and communicates the result back to the CAS. A unique PES instance and dedicated VPC is deployed for each itopia customer; this VPC is *peered* with the VPC in the customer's project to allow secure, internal network connectivity.

Windows Administration > Proxy Execution Service



1. User initiates action (*e.g.*, Create new user and assign to Collection Pool) via the Admin Console or API.
2. The front-end service relays the request to the CAS back-end.
3. The back-end service connect's to the deployment's dedicated Proxy Execution Service (PES) instance via HTTPS REST
4. PES performs the necessary actions on the Windows VMs via Windows APIs (WinRM / RPC / PowerShell)

Sample Reference Architectures

The following sections provide several reference architectures for Cloud Desktop deployments using itopia CAS. Note that regardless of the Deployment type selected (Basic, Standard, Enterprise, or Advanced), all Cloud Desktop deployments support the following options:

- Deploying into multiple Google Cloud regions
- Deploying Shared Collection Pools and Dedicated Collection Pools
- Deploying multiple Collection Pools
- Scaling Collection Pools with multiple Session Host servers
- Using an existing Active Directory domain
- Connecting to existing servers and systems via VPC peering or a VPN

The difference between Deployment types is the placement of RDS infrastructure roles on dedicated and/or redundant servers; Advanced Deployment types also provide additional configuration options such as using an existing VPC.

Basic Deployment

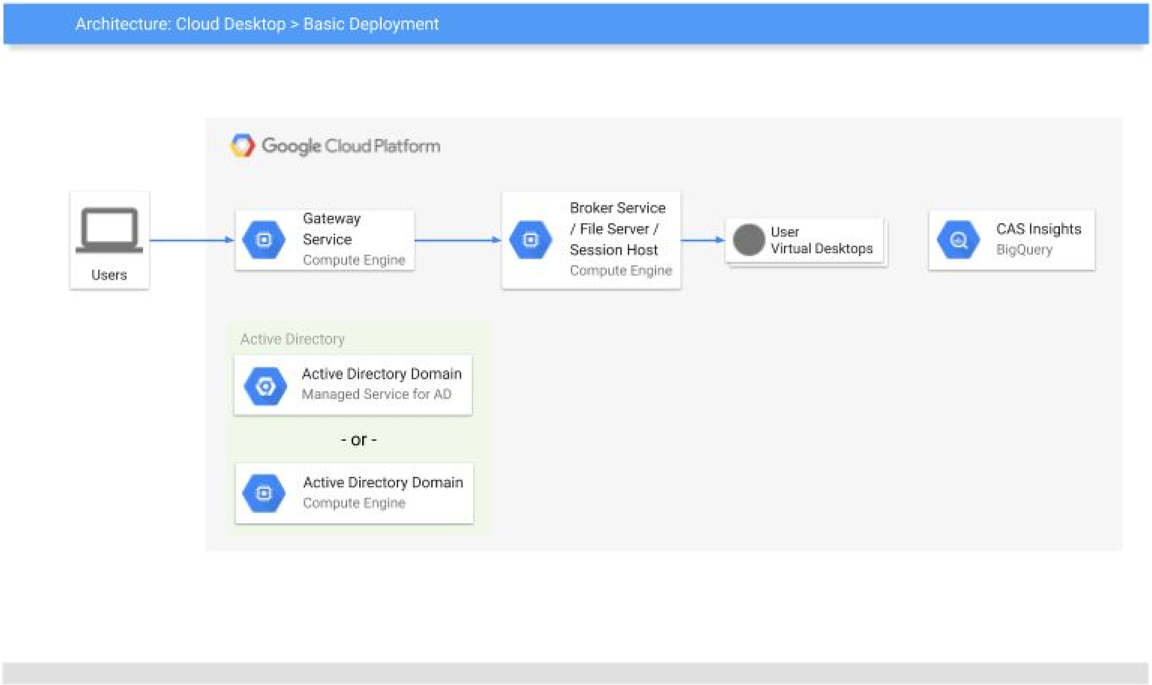
In itopia CAS, a *Basic Deployment* provides the minimal infrastructure required to host Cloud Desktops. RDS roles are co-hosted, and high-availability is not configured for any of the roles or services.

Basic Deployments are intended for non-critical workloads, such as proof-of-concept solutions or secondary environments that do not require maximum performance or availability. Additional user capacity can be added by provisioning multiple Session Host servers.

A Basic Deployment consists of the following initial components (per region):

- An Active Directory domain, provided either via Google Managed Service for Microsoft Active Directory (Google Managed AD), a traditional Active Directory domain created by CAS, or an existing AD domain
- A GCE VM instance running the RD Broker, RD Licensing, and RD Session Host roles. This VM instance also serves as the network file share
- A GCE VM instance running the RD Web and RD Gateway roles

Cloud Desktop > Basic Deployment



Standard Deployment

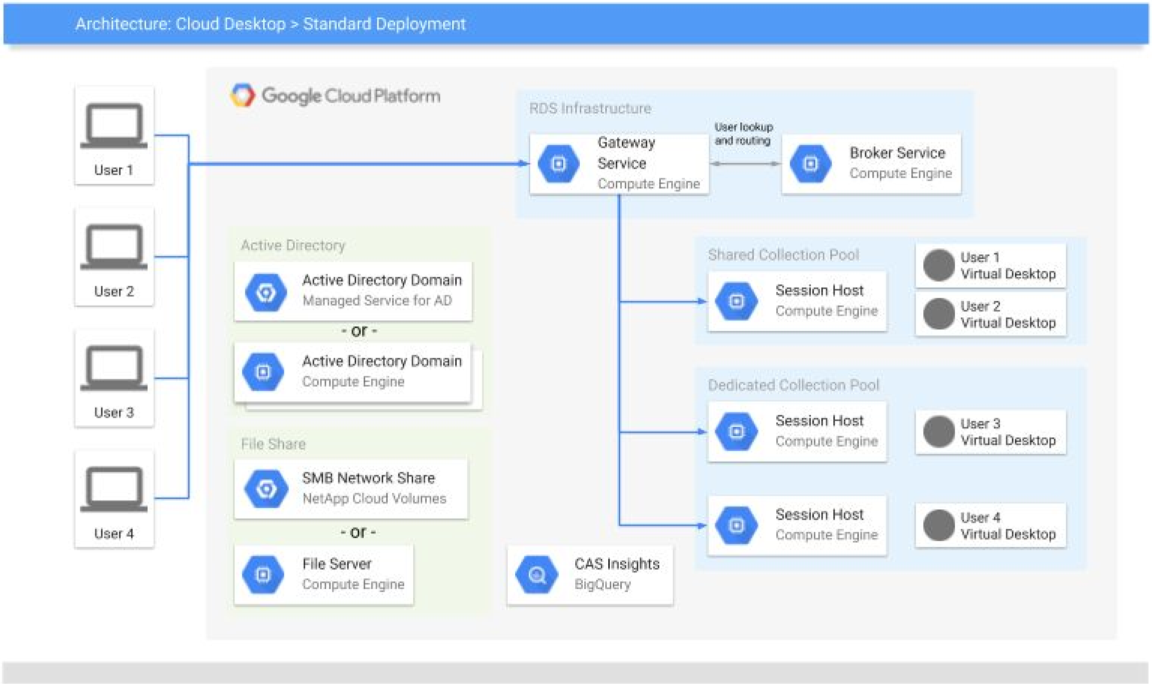
In itopia CAS, a *Standard Deployment* provides greater scalability by deploying the RD Broker role on a dedicated server, but RDS infrastructure roles do not have fault tolerance capabilities.

A Standard Deployment consists of the following initial components (per region):

- An Active Directory domain, provided either via Google Managed Service for Microsoft Active Directory (Google Managed AD), a traditional Active Directory domain created by CAS, or an existing AD domain

- A GCE VM instance running the RD Broker and RD Licensing roles
- A GCE VM instance running the RD Web Access and RD Gateway roles
- A network file share, provided either via NetApp Cloud Volume Service or a GCE VM instance configured as a Windows file server
- At least one GCE VM instance running the RD Session Host role

Cloud Desktop > Standard Deployment



Enterprise / Advanced Deployment

In itopia CAS, an *Enterprise Deployment* provides a robust infrastructure with a focus on scalability and availability. RDS infrastructure roles are installed on dedicated instances (except where co-hosting has a minimal impact), and all aspects of the infrastructure are configured with high availability and fault tolerance.

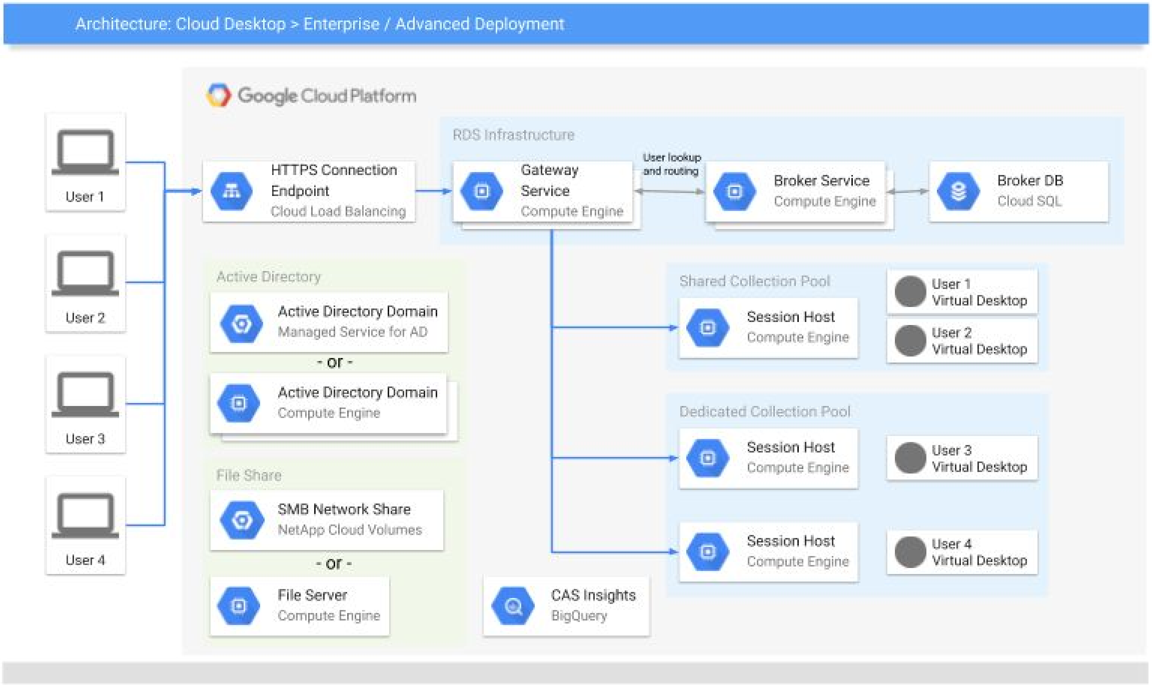
itopia CAS also supports *Advanced Deployments*, wherein the administrator can fully customize the configuration of sizing and redundancy for each RDS infrastructure role. Advanced deployments let you configure individual deployment parameters as you need: high availability can be configured per role, servers can use custom VM sizes, and you can choose to deploy to an existing VPC network rather than creating a new one.

An Enterprise Deployment consists of the following initial components (per region):

- An Active Directory domain, provided either via Google Managed Service for Microsoft Active Directory (Google Managed AD), a traditional Active Directory domain created by CAS, or an existing AD domain
- Two GCE VM instances running the RD Broker and RD Licensing roles
- Two GCE VM instances running the RD Web Access and RD Gateway roles
- A Google Cloud SQL instance hosting the RD Connection Broker database in a high-availability configuration
- A Google Cloud Load Balancer to route client connections to the RD Web / RD Gateway servers

- A network file share, provided either via NetApp Cloud Volume Service or a GCE VM instance configured as a Windows file server
- At least one GCE VM instance running the RD Session Host role

Cloud Desktop > Enterprise / Advanced Deployment

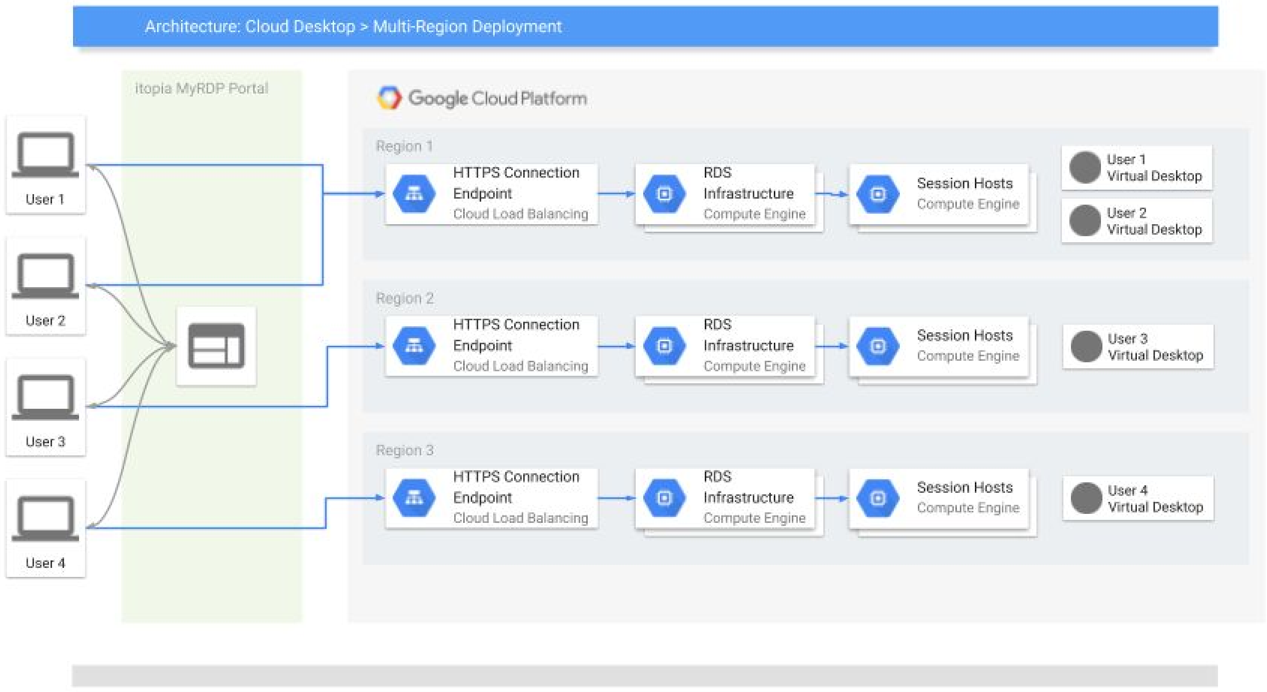


Multi-Region Deployment

In a multi-region deployment, CAS deploys Cloud Desktop infrastructure to two or more Google Cloud regions and directs user connections to their nearest region. Any Deployment Type (Basic, Standard, Enterprise, or Advanced) can be configured as a multi-region deployment.

A multi-region deployment replicates the configuration of a single-region deployment to each region in the deployment. Users can then access the MyRDP Portal via a web browser to generate a custom RDP file that will connect them to the appropriate region and Collection Pool.

Cloud Desktop > Multi-Region Deployment



Extended Deployments

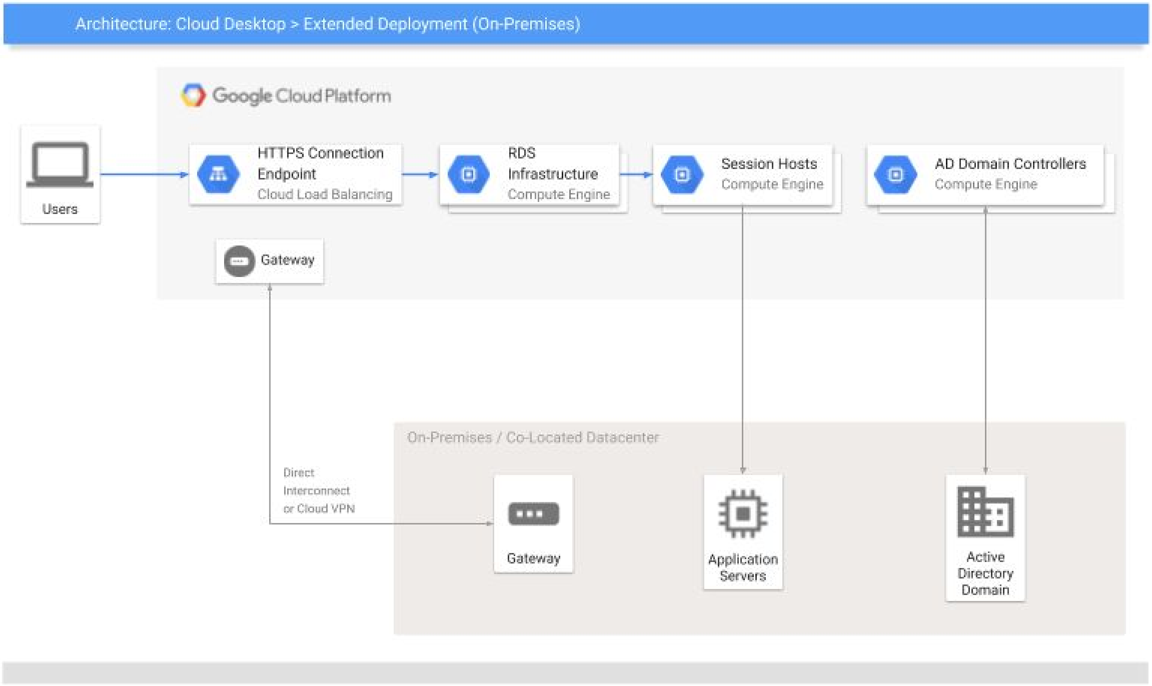
An Extended Deployment allows Cloud Desktop users to access servers and services outside of the deployment network. If you have on-premises infrastructure, CAS can help you configure a VPN connection (or Google Cloud Direct Interconnect) to your existing datacenter. Similarly, if you have existing servers and services in a separate Google Cloud VPC, you can configure VPC peering to allow the Cloud Desktop environment to access the existing infrastructure Any Deployment Type (Basic, Standard, Enterprise, or Advanced) can be configured as an Extended Deployment.

Using an Extended Deployment also allows you to use an existing Active Directory domain for your Cloud Desktop. With network connectivity to your existing infrastructure, you can either deploy directly into your existing AD domain or establish an AD trust between a standalone Cloud Desktop domain and your existing AD domain.

On-Premises Infrastructure

To connect your Cloud Desktop environment to on-premises infrastructure, you can use a *virtual private network* (VPN) or a Google Cloud Dedicated Interconnect. The CAS Admin Console can help you configure a native VPN gateway in Google Cloud, or you can use a third-party VPN solution.

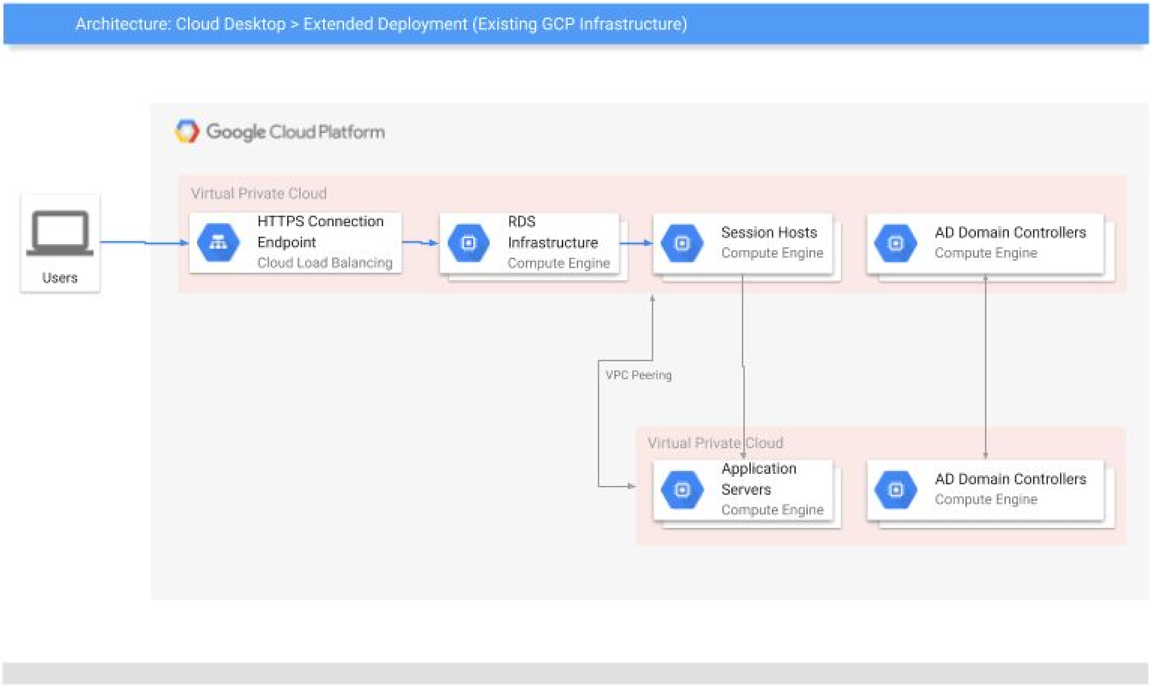
Cloud Desktop > Extended Deployment



Existing GCP Infrastructure

To connect your Cloud Desktop environment to infrastructure hosted in Google Cloud, you can configure a peered VPC between the Cloud Desktop VPC network and your existing VPC networks.

Cloud Desktop > Extended Deployment



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. Cloud Desktop offers unparalleled customization and extensibility while providing a simple way to manage your Remote Desktop environment.

itopia Cloud Automation Stack is available in the Google Cloud Marketplace.