Community Cloud

In this reading, you will learn about community cloud and how it is implemented with reference to Google Cloud as an example.

What is a community cloud?

A community cloud is defined by NIST SP 800-145 as:

“Cloud infrastructure [that] is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.”

Why community cloud?

Community cloud approach is used by organizations for the following reasons:

- The community cloud members work under the same set of security controls.
- The approach provides the members the same attributes like citizenship and authorization controls while giving limited physical and/or logical access to resources.
- It also supports data localization and some data sovereignty requirements based on the location of the community cloud’s data centers.
- The approach defines a perimeter security model encompassing the community cloud.

Implementation of software-defined community cloud

To establish a security perimeter, most legacy community clouds depend on physical separation from other clouds. However, this implementation could not meet the advanced security, manageability, or compliance requirements of the industry.

In the modern architecture, a software-defined community cloud is designed to deliver the required benefits. Google Cloud is a software-defined approach that provides security and compliance assurances without the strict physical infrastructure constraints of legacy approaches. The Google community clouds use a combination of technologies referred to as “assured clouds” that can:

- Define communities around common projects, security and compliance requirements, and policy.
- Separate shared community projects from other projects.
- Modify capabilities of a community’s boundary based on policy-controlled and audited configuration changes.

Comparison between traditional and software-defined community cloud

The software-defined community cloud provides many benefits to the users in comparison to the traditional community cloud implementation. The following table depicts the comparison between the two implementations based on the characteristics as stated in the definition given by NIST.

Characteristic	NIST Definition SP 800-145	Traditional Cloud Community Implementation	Software-Defined Community Cloud
Infrastructure Exclusivity	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns	Separate data centers with separate infrastructure	Each project is effectively a private cloud with isolated infrastructure primitives
All users subject to common security controls	(implied)	Same security controls apply across exclusive infrastructure shared by the community	Assured Workloads controls are scoped to the community and enforced through terms of service
Personhood and citizenship of support staff	It may be owned, managed, and operated by one or more of the	Personnel must be physically located at dedicated facilities	Access management service restricts support to personnel with required

Characteristic	NIST Definition SP 800-145	Traditional Cloud Community Implementation	Software-Defined Community Cloud
	organizations in the community, a third party, or some combination of them,		attributes (personhood, citizenship, work location, and more)
Data localization	and it may exist on or off premises	Community dedicated storage devices	Enforced by software
Defined security parameter	(implied)	The community is the enclave	Each project is its own enclave

Software defined community cloud as a new type of “Government Cloud”

In Google Cloud Platform (GCP), a project is a unique, logical grouping of “infrastructure primitives.” In this context, an infrastructure primitive is any atomic unit of capacity in GCP – a virtual machine (VM), a persistent disk (PD), a storage bucket, and others. Projects are “global resources” that can be assigned infrastructure primitives from any region or zone.

Every project is an individual project separate from other customers’ projects. Low-level resources like hypervisors, blocks in our distributed blockstore that underlies Google Cloud Storage (GCS), and other components are isolated with resource abstractions that enforce the isolation both logically and cryptographically.

A Private Cloud deployment model is defined in NIST SP 800-145 as:

Cloud infrastructure [that] is provisioned for exclusive use by a single organization comprising multiple consumers (such as business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

When a project is created within GCP, the infrastructure primitives that are assigned to that project are scoped to only that project. This scoping of infrastructure primitives effectively creates an “enclave” per Project.

When overlaid with Assured Workloads constraints for data residency, support personnel attributes, and security controls common to that community, these per-project private cloud enclaves become software-defined community clouds.

Benefits of a software-defined community cloud

The approach Google Cloud has taken brings multiple benefits such as meeting security and compliance requirements. New hardware, new services, and improvements to existing services are accessed faster than in traditional community clouds. The process by which new cloud technology can be onboarded and made available is also faster. Overall efficiency is improved in this model due to the scale of infrastructure available to the community; this can translate to improved availability and performance. Security enhancements can be scaled and implemented more quickly.