

Google Cloud Professional Network Engineer Crash Course

Prepare for one of Google's most Challenging Certification Exams





Introductions

Intro and Understanding the Course Content and Flow

About Your Instructor

Joseph Holbrook, CLO of Techcommanders in Jacksonville, FL

- Certified GCP – Architect/Engineer/Developer/Security and more
- Certified AWS – Practitioner/Architect/SysOps
- Certified Blockchain Solutions Architect (CBSA)
- Brocade Distinguished Architect (BDA)
- EMC Proven Professional – Expert – Cloud (EMCCE)
- Published Course Author on Pearson Safari, Udemy, LinkedIn Learning
- Published Book Author – Architecting Enterprise Blockchain Solutions
- CompTIA Subject Matter Expert, SME
- Prior US Navy Veteran



Let's Learn About You!



GCP Professional Cloud Network Engineer Crash Course

Survey Question #1 (Single Answer)

Which of the following answers would most closely resemble your job role today?

- Enterprise Architect
- Cloud Architect
- Cloud Developer
- Cloud Engineer/Admin
- Security Professional (SecOps, PenTester, Compliance,etc)
- DevOps Engineer/Architect
- Networking Engineer/Architect/Admin
- App Developer
- I do everything basically
- Other Role not listed

GCP Professional Cloud Network Engineer Crash Course

Survey Question #2

What is the industry/vertical you're currently working in?

- Consulting/VAR/Vendor or Integrators
- Financials (Banking/Insurance/Investments)
- Manufacturing
- Government (Federal/State/Local)
- Telcom/Internet/Social Media
- Healthcare and Pharma
- Retail/Online Commerce
- Logistics
- Education
- Other industry not listed

GCP Professional Cloud Network Engineer Crash Course

Survey Question # 4 (Multiple Choice)

What cloud providers are you using in your enterprise deployments?

- AWS
- GCP
- MS Azure
- Alibaba
- Rackspace
- Other Providers
- None currently or not sure.

GCP Professional Cloud Network Engineer Crash Course

Survey Question # 5 (Multiple Choice)

What other GCP Certifications are you considering taking?

- Cloud Digital Leader
- Associate Cloud Engineer
- Professional Cloud Architect
- Professional DevOps Engineer
- Professional Security Engineer
- Professional Cloud Developer
- Professional Data Engineer
- Professional ML Engineer
- Collaboration Engineer

GCP Professional Cloud Network Engineer Crash Course

Survey Question # 6 (Multiple Choice)

Which of the following GCP Focused courses would be of interest to you if offered on O'Reilly?

- Professional DevOps Engineer
- Professional Network Engineer
- Professional Cloud Developer
- Professional ML Engineer
- Kubernetes Engine
- Google Workspace
- Collaboration Engineer



Course Overview

Understanding the Course Content and Flow

GCP Professional Cloud Network Engineer Crash Course

Why you're here?

- Learn about the Certification Objectives
- You want or must get a Google Cloud certification.
- You need a condensed version of content for preparation.



GCP Professional Cloud Network Engineer Crash Course

What you will learn.

- Google Cloud Networking Fundamentals
- Google Cloud Network Services
- Google Cloud Networking Enterprise Best Practices
- Google Cloud Security Features for Production and Development
- Cloud Network Engineer Certification Objectives
- Everything you need to know to pass the exam.

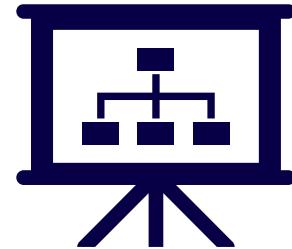
Course Agenda – Day One



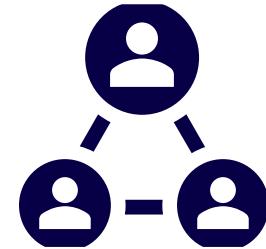
OVERVIEW OF
CERTIFICATION



NETWORKING
BEST PRACTICES



GCP NETWORKING
SERVICES



VPC



CONFIGURE
NETWORK ACCESS

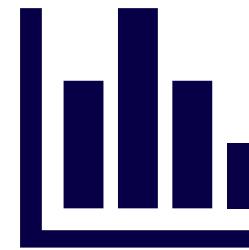
Course Agenda – Day Two



NETWORK SECURITY



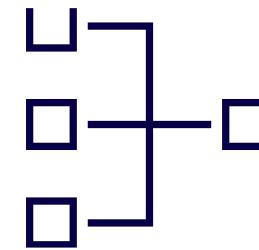
CLOUD OPERATIONS



OPTIMIZE NETWORK
RESOURCES



CLOUD DNS



HYBRID
CONNECTIVITY

Learning Reinforcements

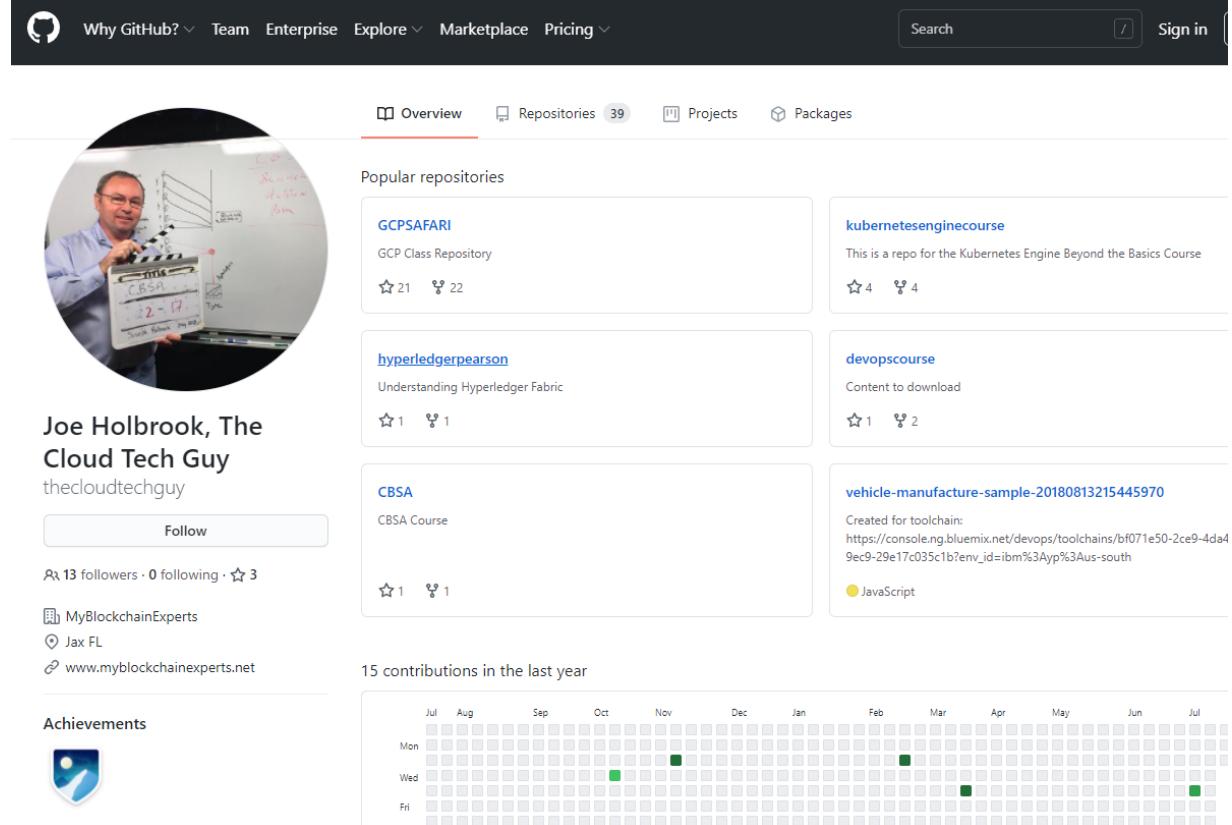
- GCP Service Demos/Exercises
- Whiteboard Discussions
- Documentation Links
- Test Preparation Tips
- Review Questions
- Free eBook Practice Questions
- Community Sites



GCP Professional Cloud Network Engineer Crash Course

Download additional content from GitHub

- [Thecloudtechguy](#)



The screenshot shows Joe Holbrook's GitHub profile. At the top, there is a circular profile picture of him holding a clapperboard in front of a whiteboard. Below the picture, his name is displayed as "Joe Holbrook, The Cloud Tech Guy" and his GitHub handle as "thecloudtechguy". A "Follow" button is present. To the right, a navigation bar includes "Overview", "Repositories 39", "Projects", and "Packages". Under "Popular repositories", several repos are listed: "GCPSAFARI" (GCP Class Repository), "kubernetesenginecourse" (a repo for the Kubernetes Engine Beyond the Basics Course), "hyperledgerpearson" (Understanding Hyperledger Fabric), "devopscourse" (Content to download), "CBSA" (CBSA Course), and "vehicle-manufacture-sample-20180813215445970" (Created for toolchain: https://console.ng.bluemix.net/devops/toolchains/bf071e50-2ce9-4da4-9ec9-29e17c035c1b?env_id=ibm%3Ayp%3Aus-south). Below the repos, a section titled "15 contributions in the last year" shows a grid of activity markers for each day of the year, with green dots appearing in October, November, March, April, and July.

<https://github.com/thecloudtechguy/googlecloudnetworkingcertification>



Course Pre-Requirements

Understanding what you need to be successful with the course.

Pre-Requirements

PRE-REQS

INTERNET

GCP
EXPERIENCE IS
A MUST

GCP
ACCOUNT FOR
PRACTICE

PRACTICE

REVIEW

Pre-Requirements

This course is a significantly condensed customized course

This learning path normally would include 6 days of class training

1 Day - GCP Fundamentals: Core Infrastructure

2 Days - Networking in Google Cloud

3 Days - Security in Google Cloud

Pre-Requirements

Advisable to go thru

Qwiklabs – Networking in GCP Quest (7 hours)

Enterprise Best Practices

Network Engineer Learning Path

Pre-Requirements

**RECOMMENDED
EXPERIENCE: 3+ YEARS OF
INDUSTRY EXPERIENCE
INCLUDING 1+ YEARS
DESIGNING AND MANAGING
SOLUTIONS USING GCP.**

**NOTE: THIS COURSE IS NOT
A SUBSTITUTE FOR HAVING
HANDS-ON EXPERIENCE OR
OTHER GCP TRAINING.**

GCP Professional Cloud Network Engineer Crash Course

Welcome to Day One Content!

We have a lot to cover so let's get started!





GCP Certifications

Overview

GCP Professional Cloud Network Engineer Crash Course

Foundational

Recommended experience:
No hands-on experience with
Google Cloud is required.

Cloud Digital Leader BETA

Associate

Recommended experience: 6+
months building on Google Cloud.

Cloud Engineer

Professional

Recommended experience: 3+ years
industry experience, including 1+ years
on Google Cloud.

Cloud Architect

Cloud Developer

Data Engineer

Cloud DevOps
Engineer

Cloud Security
Engineer

Cloud Network
Engineer

Collaboration
Engineer

Machine Learning
Engineer



Certification Roadmap

<https://cloud.google.com/certification>



Professional Cloud Network Engineer Exam Overview

Objectives Overview

GCP Professional Cloud Network Engineer Crash Course

Examinee Abilities

It validates an examinee's knowledge around how to:

Domain	* Estimated % of The Exam
Designing, planning and prototyping GCP Network	25%
Implementing a Google Cloud Virtual Private Cloud (VPC)	20%
Configuring Network Access	20%
Implementing Hybrid Access	5%
Implementing Network Security	10%
Managing and Monitoring Network Ops	10%
Optimizing Network Resources	10%

** Note: Google does provide exam domain percentages like AWS does. These are only estimates from my BETA exam experience.*

About the Certification

According to Google Cloud, a Professional Cloud Network Engineer is?

- “A Professional Cloud Network Engineer implements and manages network architectures in Google Cloud. This individual may work on networking or cloud teams with architects who design cloud infrastructure.”
- “The Cloud Network Engineer uses the Google Cloud Console and/or command line interface, and leverages experience with network services, application and container networking, hybrid and multi-cloud connectivity, implementing VPCs, and security for established network architectures to ensure successful cloud implementations.”

About the Certification

Exam Costs and Logistics

- Length: 2 hours
- Registration fee: \$200 (plus tax where applicable)
- Language: English
- Exam format: Multiple choice and multiple select
- Delivery Method – Online and In Person

GCP Professional Cloud Network Engineer Crash Course

Professional Cloud Network Engineer Objectives

Information and the Objectives to the exam are located here.

<https://cloud.google.com/certification/cloud-network-engineer>



Section 1 – Designing, Planning and prototyping GCP Networks

Understanding the domain testable objectives

Domain Overview

- Designing the overall network architecture
- Designing a Virtual Private Cloud (VPC)
- Designing a Hybrid Network

1.1 Designing the overall network architecture

Understanding Google approach to design

GCP Professional Cloud Network Engineer Crash Course

- Google Cloud Architecture Framework
- Failover and disaster recovery strategy
- Options for high availability
- DNS strategy
- Choosing the appropriate load balancing options
- Whiteboard - Load Balancing
- Optimizing for latency
- Understanding how quotas are applied per project and per VPC

GCP Professional Cloud Network Engineer Crash Course

- Hybrid connectivity -Private Access
- Container networking
- IAM and security
- SaaS, PaaS, and IaaS services
- Resource Hierarchy
- Micro segmentation for security purposes

GCP Professional Cloud Network Engineer Crash Course

Framework

The Google Cloud Architecture Framework which provides recommendations and describes best practices to help architects, developers, administrators, and other cloud practitioners design and operate a cloud topology that's secure, efficient, resilient, high-performing, and cost-effective.

Framework is broken into six categories

<https://cloud.google.com/architecture/framework>

GCP Professional Cloud Network Engineer Crash Course

Framework Categories

- System design - Define the architecture, components, modules, interfaces, and data needed to satisfy cloud system requirements, and learn about Google Cloud products and features that support system design.
- Operational excellence - Efficiently deploy, operate, monitor, and manage your cloud workloads.
- Security, privacy, and compliance - Maximize the security of your data and workloads in the cloud, design for privacy, and align with regulatory requirements and standards.
- Reliability - Design and operate resilient and highly available workloads in the cloud.
- Cost optimization - Maximize the business value of your investment in Google Cloud.
- Performance optimization - Design and tune your cloud resources for optimal performance.



Failover and disaster recovery strategy

Planning and implementation

GCP Professional Cloud Network Engineer Crash Course

GCP Components to focus on.

- VPCs
- Projects
- Networks
- Regions
- Zones
- Subnets
- Switching
- Routing
- Firewalls

GCP Professional Cloud Network Engineer Crash Course

Understanding DR and BC Terms

- Business Impact Analysis (BIA)
- Recovery Point Objective (RPO) is the maximum amount of time during which the data might be lost.
- Recovery Time Objective (RTO) is the maximum time your application can be offline.
- Service Level Objective (SLO)
- High Availability (HA)

GCP Professional Cloud Network Engineer Crash Course

The series consists of these parts:

- Disaster recovery planning guide
- Disaster recovery building blocks
- Disaster recovery scenarios for data
- Disaster recovery scenarios for applications
- Architecting disaster recovery for locality-restricted workloads
- Architecting disaster recovery for cloud infrastructure outages (this document)

<https://cloud.google.com/architecture/dr-scenarios-planning-guide>

GCP Professional Cloud Network Engineer Crash Course

Google Cloud products are divided into zonal resources, regional resources, or multi-regional resources.

- Zonal resources are hosted within a single zone. A service interruption in that zone can affect all of the resources in that zone.
- Regional resources are redundantly deployed across multiple zones within a region. This gives them higher reliability relative to zonal resources.
- Multi-regional resources are distributed within and across regions. In general, multi-regional resources have higher reliability than regional resources. (Optimize availability, performance, and resource efficiency)



HA, Resiliency and Dependability

What is it and why its important in the cloud.

GCP Professional Cloud Network Engineer Crash Course

Dependency and Resiliency (Resilience)

- System dependability is defined as “the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers”.
- Redundancy is the intentional duplication of system components in order to increase a system’s dependability.
- Resilience refers to a system’s ability to recover from a fault and maintain persistency of service dependability in the face of faults.

GCP Professional Cloud Network Engineer Crash Course

Characteristics of Resiliency

- IT resources can be pre-configured so that if one becomes deficient, processing is automatically handed over to another redundant IT resource.
- Within cloud computing, resiliency can refer to redundant IT resources within the same cloud (but in different physical locations) or across multiple clouds.
- Cloud consumers can increase the reliability and availability of their applications by leveraging the resiliency of cloud-based IT resources.

GCP Professional Cloud Network Engineer Crash Course

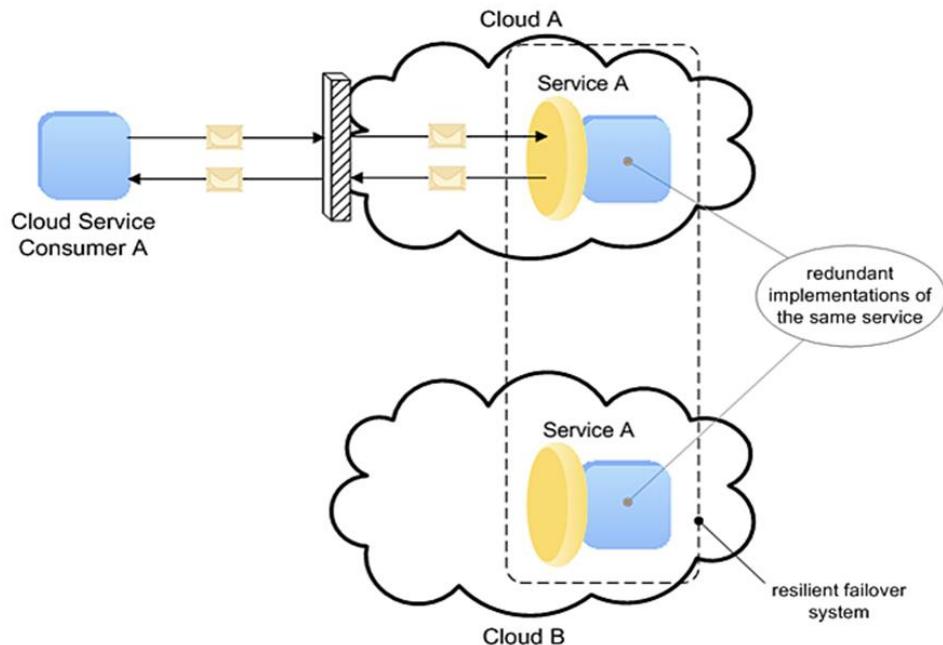


Diagram - VMWare

Resilient computing is a form of failover that distributes redundant implementations of IT resources across physical locations

GCP Professional Cloud Network Engineer Crash Course

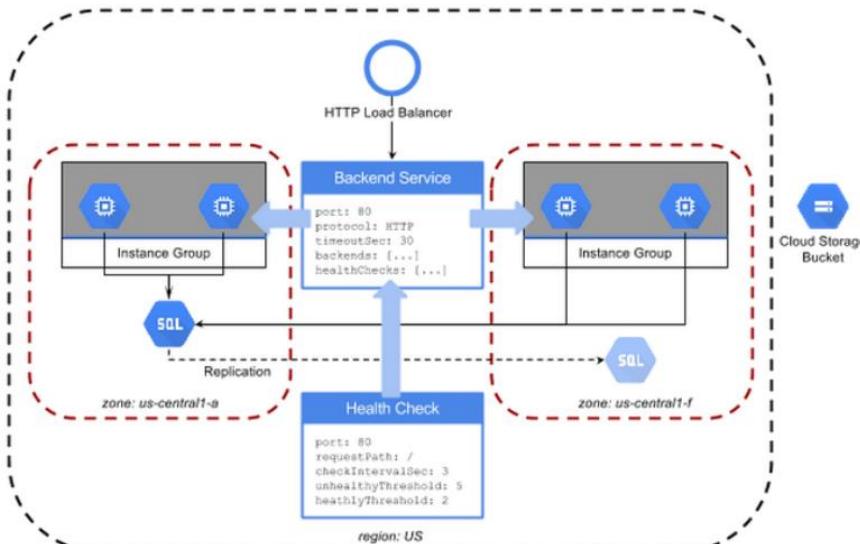


Diagram - GCP

GCP provides resiliency thru:

- Regions/Zones
- Redundant Hardware
- Load Balancing
- HA Services (Cloud DNS, GLB, etc)
- Instance Groups
- Autoscaling
- Health Checks

GCP Professional Cloud Network Engineer Crash Course

Replication

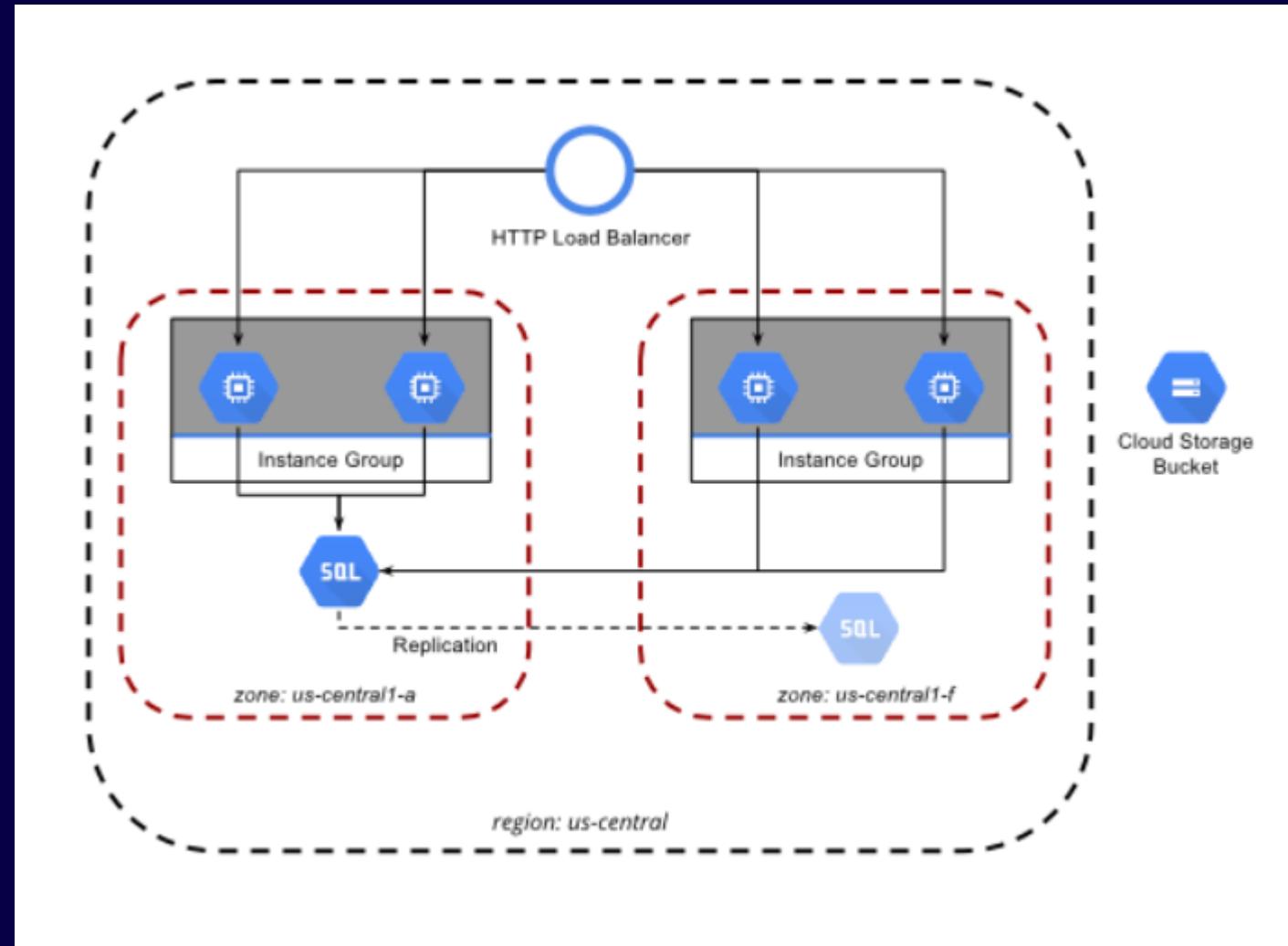
- Replication is sharing information to ensure consistency between redundant resources, such as software or hardware components, to improve reliability, fault-tolerance, or accessibility and avoid a single point of failure.
- Replication ensures that data modifications are written to multiple sources thereby increasing data durability.
- Cloud provides regional and zonal replication based on the service/provider.

GCP Professional Cloud Network Engineer Crash Course

Replication in the cloud can be between

1. Regions
2. Zones
3. Cloud to Cloud
4. Cloud to DC

Example : Replication between zones in GCP



Test Tip



- Resiliency is a result of highly available services that have redundant components which provides for the capacity to be available (recover) during an outage.
- GCP provides resiliency how?

Test Tip



- Replication provides for consistency of data during an outage.
- Replication in GCP could be regional or zonal.



DNS Strategy

DNS Options

GCP Professional Cloud Network Engineer Crash Course

Cloud DNS

- Cloud DNS is a managed DNS service from Google.
- Global Service and maintains a 100% uptime SLA.
- Domain Name Service translates Domains to IP addresses.
- Publish your records without the management overhead
- Private and Public zones.
- Each Domain has its own zone

GCP Professional Cloud Network Engineer Crash Course

In a hybrid environment, DNS resolution can be performed in different locations.

- Use a hybrid approach with two authoritative DNS systems.
- Keep DNS resolution on-premises.
- Move all DNS resolution to Cloud DNS

GCP Professional Cloud Network Engineer Crash Course

Additional Notes = DNS for EXAM

Instances with external IP addresses can allow connections from hosts outside of the project

- Users connect directly using external IP address

- Admins can also publish public-DNS records pointing to instance

- Public DNS records are not published automatically

DNS records for external addresses can be published via DNS servers

DNS zones can be hosted using Google Cloud DNS

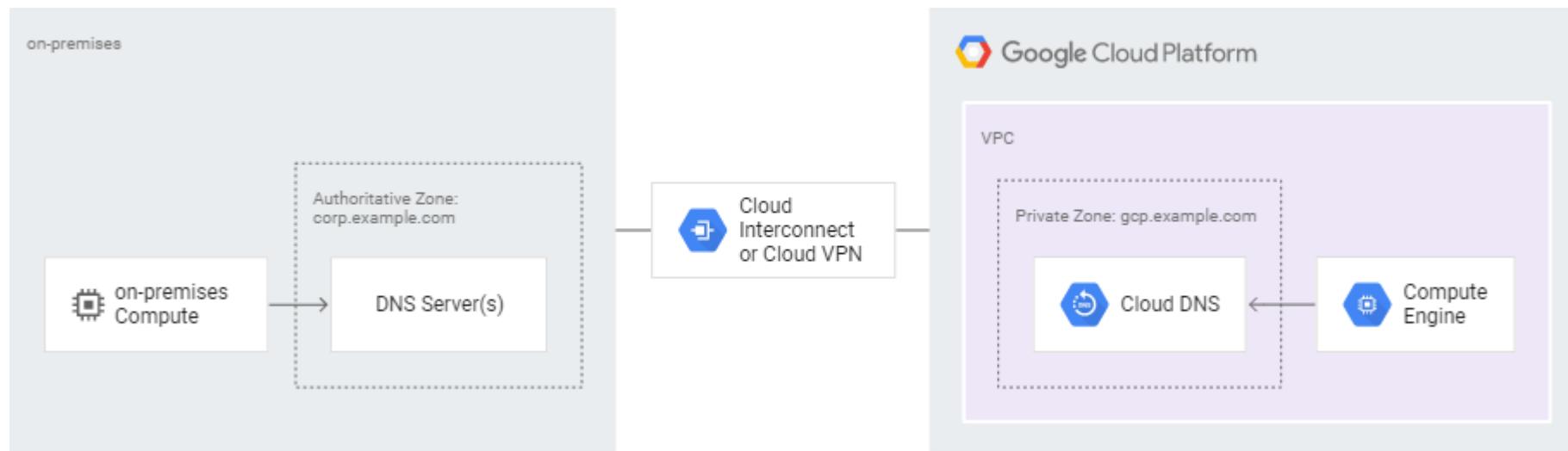
- Create zone and configure domain DNS to use

- Create, update, remove records manually or via API

GCP Professional Cloud Network Engineer Crash Course

Cloud DNS

- Hybrid



GCP Professional Cloud Network Engineer Crash Course

Internal IP Addresses DNS Resolution

- Each instance has a hostname that can be resolved to an internal IP address
 - Hostname is the same as the instance name
 - FQDN is *[hostname].c.[project-id].internal*
 - Example: guestbook-test.c.guestbook-151617.internal
- Name resolution is handled by internal DNS resolver

GCP Professional Cloud Network Engineer Crash Course

DNSSEC

- The Domain Name System Security Extensions (DNSSEC) is a feature of the Domain Name System (DNS) that authenticates responses to domain name lookups.
- DNSSEC does not provide privacy protections for those lookups but prevents attackers from manipulating or poisoning the responses to DNS requests.
- Both Registry and Registrar must support DNSSEC for the TLD being used.

GCP Professional Cloud Network Engineer Crash Course

DNSSEC

Three places where you must enable and configure DNSSEC

1. The DNS zone for your domain must serve special DNSSEC records for public keys (DNSKEY), signatures (RRSIG), and non-existence (NSEC, or NSEC3 and NSEC3PARAM) to authenticate your zone's contents.
2. The top-level domain (TLD) registry must have a DS record that authenticates a DNSKEY record in your zone. Do this by activating DNSSEC at your domain registrar.

GCP Professional Cloud Network Engineer Crash Course

DNSSEC

Three places where you must enable and configure DNSSEC (Cont)

3. Use a DNS resolver that validates signatures for DNSSEC-signed domains

Test Tip



- Cloud DNS is a managed DNS service from Google and is a Global Service and maintains a 100% uptime SLA.
- Three places to configure resolver for DNSSEC



Choosing the correct Load Balancing Options

Options

GCP Professional Cloud Network Engineer Crash Course

Load Balancing allows us to load balance our traffic in a single region or in multiple regions.

- Managed Service
- Front End Service (IP)

Types of Load Balancing

- Network Load Balancing

- HTTPS Load Balancing

- Cross-Region Load Balancing

- Content-based Load Balancing

- Cloud SSL Proxy

GCP Professional Cloud Network Engineer Crash Course

Types of Load Balancers

- HTTPS
- TCP Proxy
- SSL Proxy
- Internal
- Network

Types of Load Balancing

- Global
- Regional
- Internal
- External
- HTTP/TCP/UDP

GCP Professional Cloud Network Engineer Crash Course

Network Load Balancing

- Network load balancing distributes incoming traffic across multiple instances
 - Supports non-HTTP(S) protocols (TCP/UDP)
 - Can be used for HTTPS traffic when you want to terminate connection on your instances (not at HTTPS load balancer)
- Supports autoscaling with managed instance groups

<https://cloud.google.com/compute/docs/load-balancing/network/>

GCP Professional Cloud Network Engineer Crash Course

Network Load
Balancing

Forwarding
rules consist of...

Name

Region

IP Address
(regional, not
global)

IP Protocol (TCP,
UDP; AH, ESP,
ICMP, SCTP)

Ports

Target-pool or
target-instance

GCP Professional Cloud Network Engineer Crash Course

HTTP(S) Load Balancing

HTTP(S) Load Balancing distributes HTTP(S) traffic among instance groups based on proximity to user or URL or both

<https://cloud.google.com/compute/docs/load-balancing/network/>

Autoscalers can be attached to HTTP(S)load balancers

GCP Professional Cloud Network Engineer Crash Course

HTTP(S) Load Balancing

- HTTP(S) The following resources comprise a load balancer
- Global Forwarding Rule
- Target Proxy (w SSL certificate resource for HTTPS proxy)
- URL map
- Backend Service and Backends
- Health Check
- The load balancer leverages additional resources
- Global IP Address (ephemeral or static)
- One or more Instance Groups

GCP Professional Cloud Network Engineer Crash Course

Global Forwarding

- A global forwarding rule provides a single global IP address for an application
- The rule routes traffic by IP address, port, and protocol to an HTTP or HTTPS target proxy
- A global forwarding rule can only forward to a single port
- Global forwarding rules can only be used by an HTTP(S) load balancer

<https://cloud.google.com/compute/docs/load-balancing/http/global-forwarding-rules>

GCP Professional Cloud Network Engineer Crash Course

Target proxies' route incoming HTTP(requests) based on URL maps and backend service configurations

- HTTPS target proxy terminates client SSL session
- HTTPS target proxies require configured SSL certificate resources

<https://cloud.google.com/compute/docs/load-balancing/http/target-proxies>

GCP Professional Cloud Network Engineer Crash Course

Cloud SSL proxy alt type of load balancing

- non-HTTP(S) traffic

- Performs global load balancing, routing clients to the closest instance with capacity

Cloud SSL proxy advantages

- Intelligent routing

- Reduced CPI load on instances

- Certificate management

- Security patching

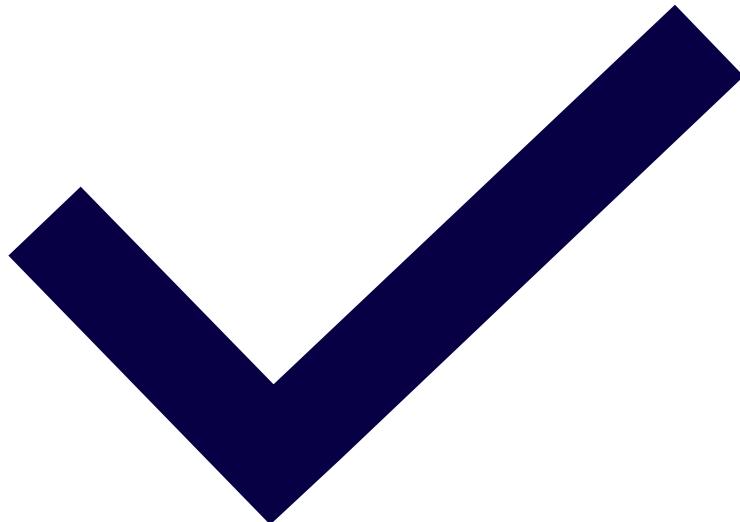
GCP Professional Cloud Network Engineer Crash Course



Cross Region Load Balancing

- HTTP/HTTPS only
- Cross-region using a single global IP address
- Requests routed to the closest region
- Automatically reroutes to next closest once capacity is reached
- Eliminates need for DNS-based load balancing

GCP Professional Cloud Network Engineer Crash Course



Content Based Load Balancing

- HTTP/HTTPS only
- Create multiple backend services to handle content types
- Add path rules to backend services
 - - /video for video services
 - - /static for static content
- Configure different instance types for different content types

GCP Professional Cloud Network Engineer Crash Course

What type of load balancing use cases for exam?

- HTTP, HTTPS, TCP, and SSL load balancing
- Network Load Balancing

<https://cloud.google.com/compute/docs/load-balancing/optimize-app-latency>

GCP Professional Cloud Network Engineer Crash Course

Instance Groups are Managed Groups of VMs

Three Types

1. Unmanaged
2. Managed Instance Group (Zonal)
3. Managed Instance Group (Regional)

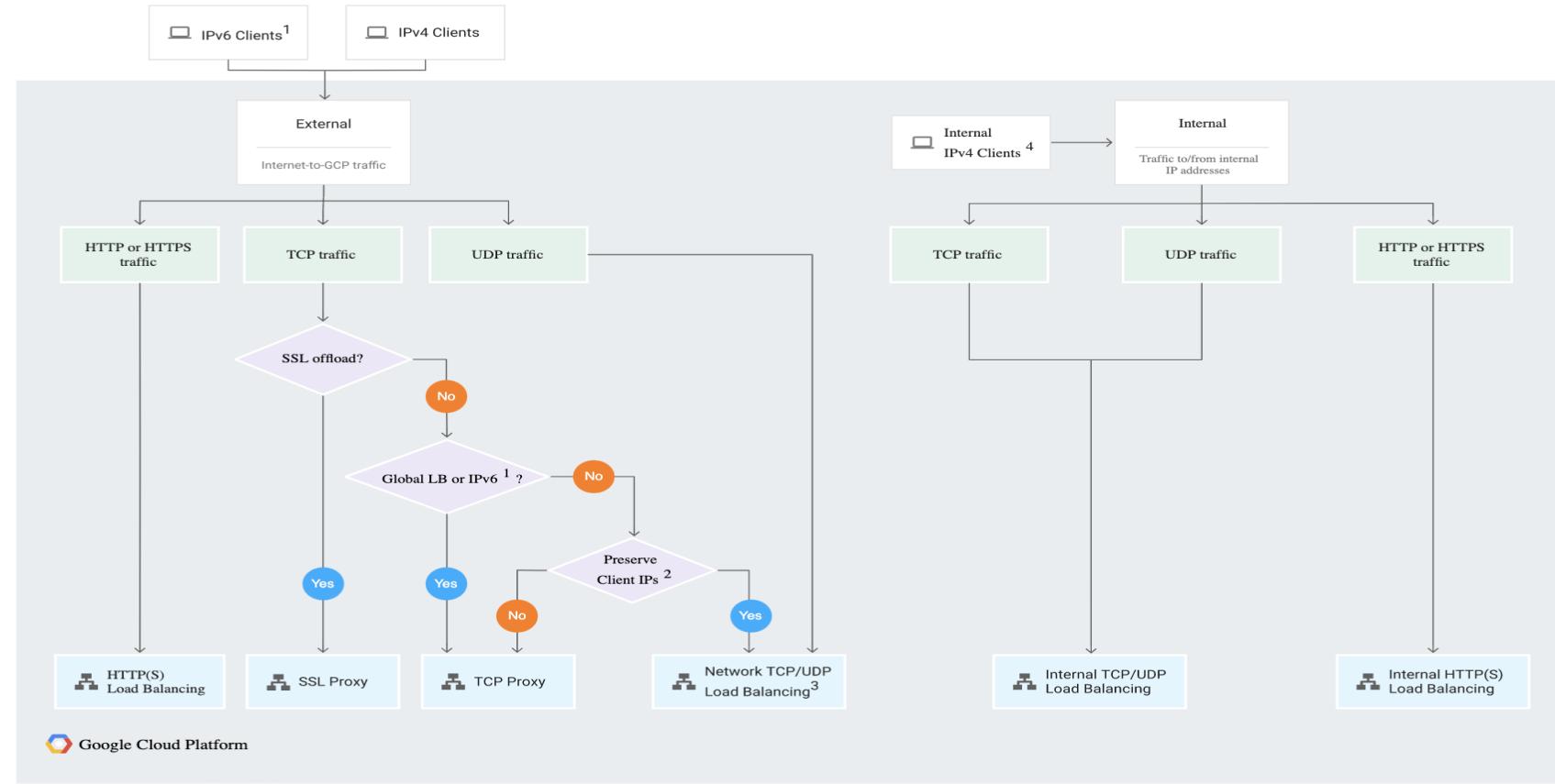
Unmanaged instance groups contain dissimilar instances and wont.

- Autoscaling
- Rolling updates
- Instance creation using instance templates

<https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances>

GCP Professional Cloud Network Engineer Crash Course

GCP Cloud Load Balancing Decision Tree



¹ IPv6 clients are supported for TCP traffic if you configure the load balancer in Premium Tier. IPv6 clients aren't supported for UDP traffic.

² Another reason to choose Network TCP/UDP Load Balancing is if you need to ensure that the load balancer is located in a particular region.

³ Network TCP/UDP load balancers use regional external IP addresses that are accessible by clients anywhere.

⁴ Clients in a VPC network or in a network connected to a VPC network.

Test Tip



Load Balancing

- Google Cloud SSL proxy terminates user SSL (TLS) connections at the global load balancing layer/ then balances the connections across your instances via SSL or TCP.
- Cloud SSL proxy is intended for non-HTTP(S) traffic.
- For HTTP(S) traffic -HTTP(S) load balancing is used



Whiteboard – Putting it all Together

Discussion and Review

GCP Network Engineer

- *Load Balancing*



Whiteboard





Optimize for Latency

MTU, Cache, CDN

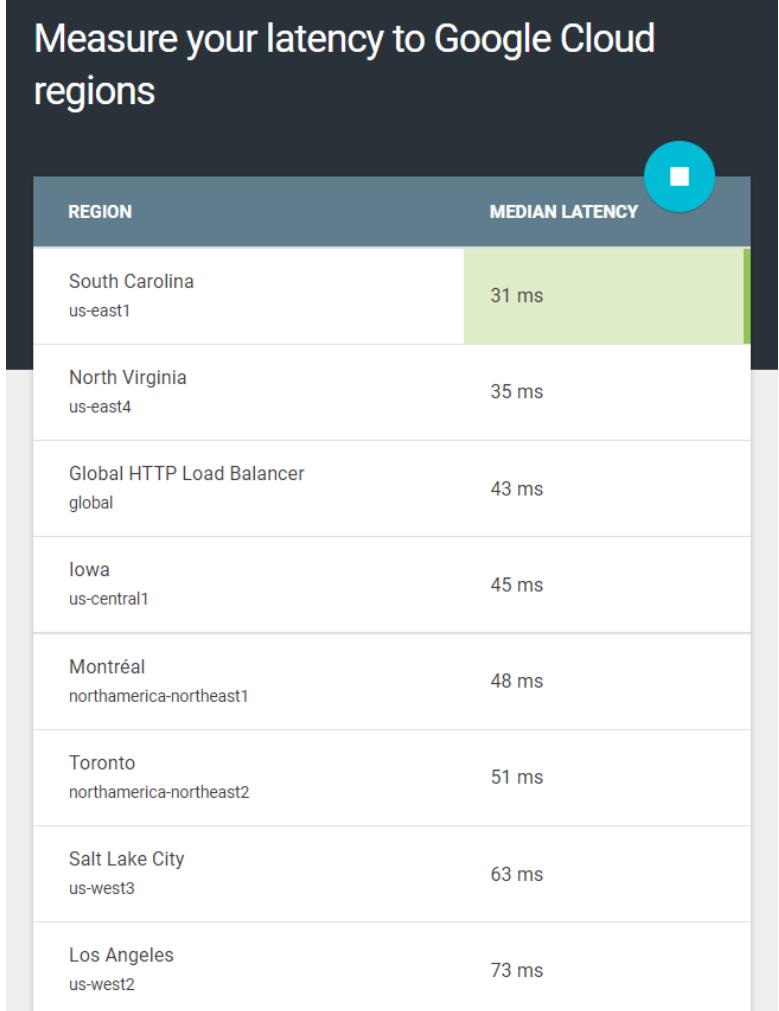
GCP Professional Cloud Network Engineer Crash Course

Optimize Latency by

- Load Balancing Options (Network and HTTP)
- Content Delivery Network (CDN)
- MTU Size
- Caching
- Tiering (Free or Premium)

GCP Professional Cloud Network Engineer Crash Course

- Latency is generally measured in milliseconds, or during speed tests, it's referred to as a ping rate.
- Use GCPING for an estimate.
<https://www.gcping.com/>
- Latency can be minimized in some cases by choosing the right region for the right service/user base.



GCP Professional Cloud Network Engineer Crash Course

Measure Latency

- Ping – ICMP – Does NOT measure end user latency but measures reachability (ping -c 5 compute-engine-vm)
- Curl - measures Time To First Byte (TTFB)
- Review this page ---- <https://cloud.google.com/load-balancing/docs/tutorials/optimize-app-latency>

GCP Professional Cloud Network Engineer Crash Course

Options for Load Balancing

- HTTP Load Balancing (Global) - Supports HTTP(S) traffic and advanced features, such as URL mapping and SSL offloading. TCP Proxy Load Balancing or SSL Proxy Load Balancing for non-HTTP traffic on specific ports.
- Network Load Balancing (Regional) - Allows TCP/UDP traffic using any port to pass through the load balancer.

GCP Professional Cloud Network Engineer Crash Course

Caching

- CDNs cache and compress mirror versions of your web pages, which are then stored in strategically placed data centers.
- Content is then delivered to users based on their geolocation, thereby reducing round trip times and latency.
- DNS Time, Fetch Time, Wait Time can impose some latency.
- Use cURL to grab this information.

GCP Professional Cloud Network Engineer Crash Course

Caching – Cloud CDN

- Cloud CDN is a content delivery network that accelerates your web and video content delivery by using Google's global edge network to bring content as close to your users as possible.
- Global anycast IP provides a single IP for global reach
- Route users to the nearest edge cache automatically and avoid DNS propagation delays that can impact availability.
- It supports HTTP/2 end-to-end and the QUIC protocol from client to cache.

GCP Professional Cloud Network Engineer Crash Course

MTU Size

- The maximum transmission unit (MTU) is the size, in bytes, of the largest packet supported by a network layer protocol, including both headers and data. MTU Size can cause latency issues so set appropriately in your VPN
- Configure your peer VPN gateway to use an MTU of no greater than **1460 bytes**.
- GCP recommends a value of **1460 bytes** because that matches the default MTU setting for Google Cloud virtual machine (VM) instances.

GCP Professional Cloud Network Engineer Crash Course

MTU Size in VPC

[Create a VPC network](#)

Allow/Deny	Action	IP ranges	Ports	Protocol	Allow/Deny	MTU
allow-rdp	Ingress	Apply to all	0.0.0.0/0			
networkengineerdemo-allow-ssh	Ingress	Apply to all	0.0.0.0/0	tcp:22	Allow	65,534
networkengineerdemo-deny-all-ingress	Ingress	Apply to all	0.0.0.0/0	all	Deny	65,535
networkengineerdemo-allow-all-egress	Egress	Apply to all	0.0.0.0/0	all	Allow	65,535

Dynamic routing mode [?](#)

Regional
Cloud Routers will learn routes only in the region in which they were created

Global
Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

Enable DNS API to pick a DNS policy [ENABLE](#)

Maximum transmission unit (MTU)

1460

1500

[VPC network](#)

[VPC networks](#)

default

Description
Default network for the project

Subnet creation mode
Auto subnets

Dynamic routing mode
Regional

DNS server policy

Enable DNS API
Applying DNS server policies to the network requires DNS API. This is a one-time enablement per project and may take a few minutes to complete.

[ENABLE API](#)

None

Maximum transmission unit
1460

Test Tip



- Exam will have questions around how to determine latency for a service and how to resolve these issues.
- Use cURL to grab latency information
- Configure your peer VPN gateway to use an MTU of no greater than 1460 bytes.



Quotas

Limiting Resource Usage

GCP Professional Cloud Network Engineer Crash Course

Quotas

- Google Cloud uses quotas to restrict how much of a particular shared Google Cloud resource that you can use
- Project quotas protect Google Cloud users from unforeseen spikes in usage but can be raised with contact to support
- The default limit for number of networks per project is 15.
- Review this page -- <https://cloud.google.com/vpc/docs/quota>

GCP Professional Cloud Network Engineer Crash Course

Compute Engine enforces quotas on resource usage for various reasons

- serviceusage.quotas.get permissions. (View)
- serviceusage.quotas.update permissions (Update)

Check Project Wide Quotas

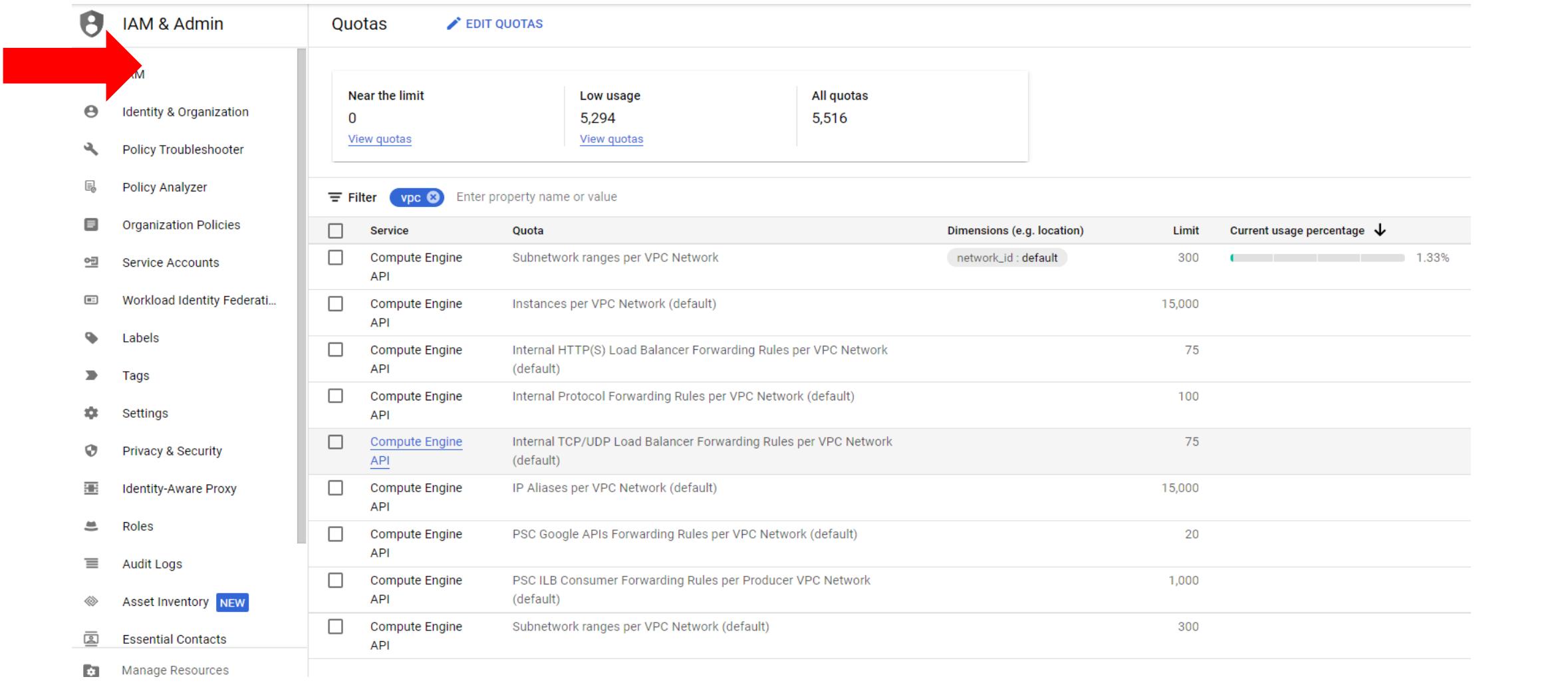
- gcloud compute project-info describe --project PROJECT_ID
- Request more quota limits or view quotas for your other services on the Quotas page, found in IAM & admin. Contact Support

GCP Professional Cloud Network Engineer Crash Course

```
holbrookjp@cloudshell:~ (encoded-hangout-331014)$ gcloud compute project-info describe --project encoded-hangout-331014
commonInstanceMetadata:
  fingerprint: tWv1m4EEB1U=
  kind: compute#metadata
creationTimestamp: '2021-12-01T12:40:40.848-08:00'
defaultNetworkTier: PREMIUM
defaultServiceAccount: 439862965988-compute@developer.gserviceaccount.com
id: '1304923698952299303'
kind: compute#project
name: encoded-hangout-331014
quotas:
- limit: 1000.0
  metric: SNAPSHOTS
  usage: 0.0
- limit: 5.0
  metric: NETWORKS
  usage: 1.0
- limit: 100.0
  metric: FIREWALLS
  usage: 4.0
- limit: 100.0
  metric: IMAGES
  usage: 0.0
- limit: 8.0
  metric: STATIC_ADDRESSES
  usage: 0.0
- limit: 200.0
  metric: ROUTES
  usage: 1.0
- limit: 15.0
  metric: FORWARDING_RULES
```

gcloud compute project-info describe --project PROJECT_ID

GCP Professional Cloud Network Engineer Crash Course



A screenshot of the Google Cloud Platform (GCP) IAM & Admin Quotas page. A red arrow points from the left margin towards the sidebar. The sidebar contains links for IAM, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Workload Identity Federation, Labels, Tags, Settings, Privacy & Security, Identity-Aware Proxy, Roles, Audit Logs, Asset Inventory (marked as NEW), Essential Contacts, and Manage Resources. The main content area shows quota usage statistics: Near the limit (0), Low usage (5,294), and All quotas (5,516). Below this is a table of quotas for various Compute Engine API resources, filtered by 'vpc'. The table includes columns for Service, Quota, Dimensions (e.g. location), Limit, and Current usage percentage.

Service	Quota	Dimensions (e.g. location)	Limit	Current usage percentage
Compute Engine API	Subnetwork ranges per VPC Network	network_id : default	300	1.33%
Compute Engine API	Instances per VPC Network (default)		15,000	
Compute Engine API	Internal HTTP(S) Load Balancer Forwarding Rules per VPC Network (default)		75	
Compute Engine API	Internal Protocol Forwarding Rules per VPC Network (default)		100	
Compute Engine API	Internal TCP/UDP Load Balancer Forwarding Rules per VPC Network (default)		75	
Compute Engine API	IP Aliases per VPC Network (default)		15,000	
Compute Engine API	PSC Google APIs Forwarding Rules per VPC Network (default)		20	
Compute Engine API	PSC ILB Consumer Forwarding Rules per Producer VPC Network (default)		1,000	
Compute Engine API	Subnetwork ranges per VPC Network (default)		300	

Test Tip



- Exam will have questions around how to determine latency for a service and how to resolve these issues.
- Use cURL to grab latency information
- Configure your peer VPN gateway to use an MTU of no greater than 1460 bytes.



Private Access RFC1918

Enabling

GCP Professional Cloud Network Engineer Crash Course

Private Access /Google Access

- Google Cloud provides several private access options that let virtual machine (VM) instances reach supported APIs and services without requiring an external IP address.
- Private Google Access is enabled on a **per-subnet basis and you must use a VPC network**.
- Private Google Access does not automatically enable any API.

GCP Professional Cloud Network Engineer Crash Course

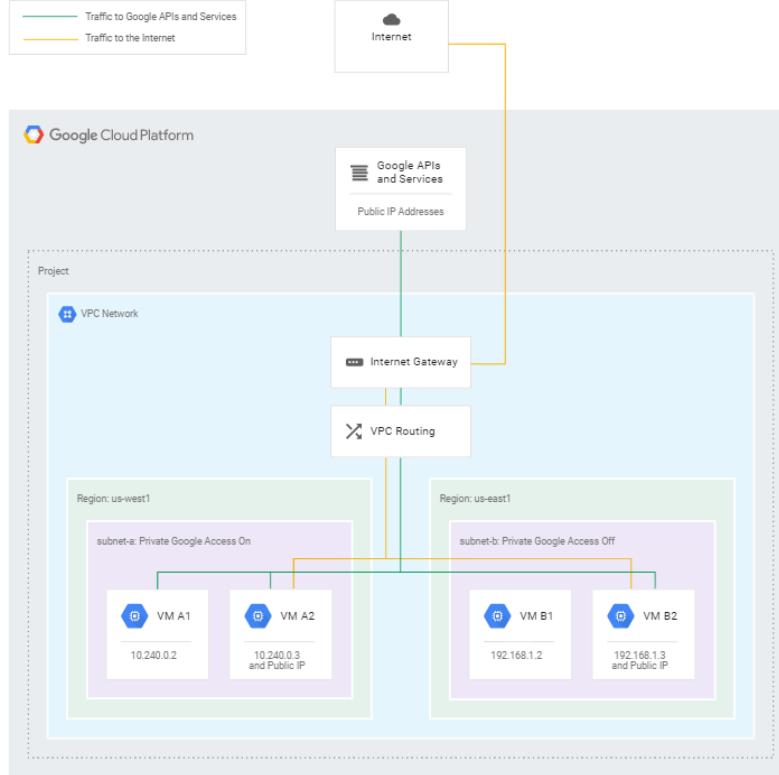
Private Google Access

Private Google Access for On Premises Hosts

Private Service Access

Private Serverless Access

GCP Professional Cloud Network Engineer Crash Course



Why and How for Google Private Access

- Private Google access clients consist of Google cloud VM instances that do not have external IP addresses.
- Use private Google access when you want to connect to Google APIs and services without the need to assign external IP addresses to your resources in Google cloud.
- Diagram – Google Cloud

GCP Professional Cloud Network Engineer Crash Course

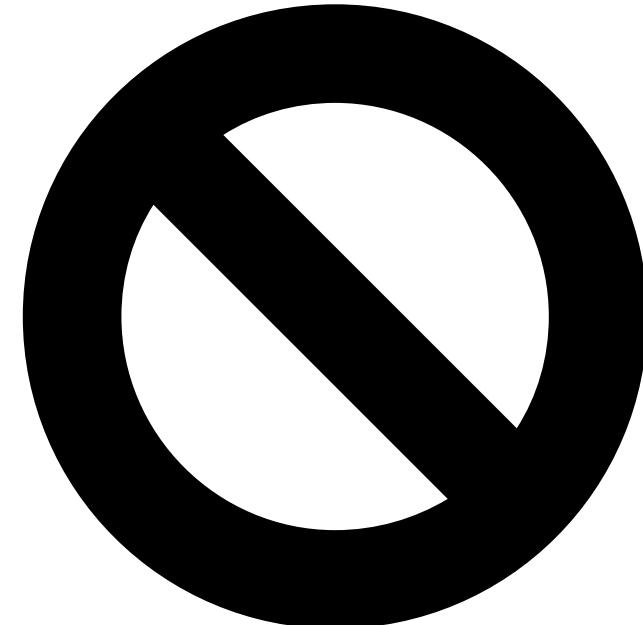
Access Type	About
Private Google Access	Private Google access clients consist of Google cloud VM instances that do not have external IP addresses
Private Google Access for On	For on-prem hosts is used with on-prem hosts.
Private Service Access	May be used with VM instances in Google cloud with or without external IP addresses assigned to them.
Private Serverless Access	Works with Google cloud VM instances that may or may not have external IP addresses assigned to them. Y

GCP Professional Cloud Network Engineer Crash Course

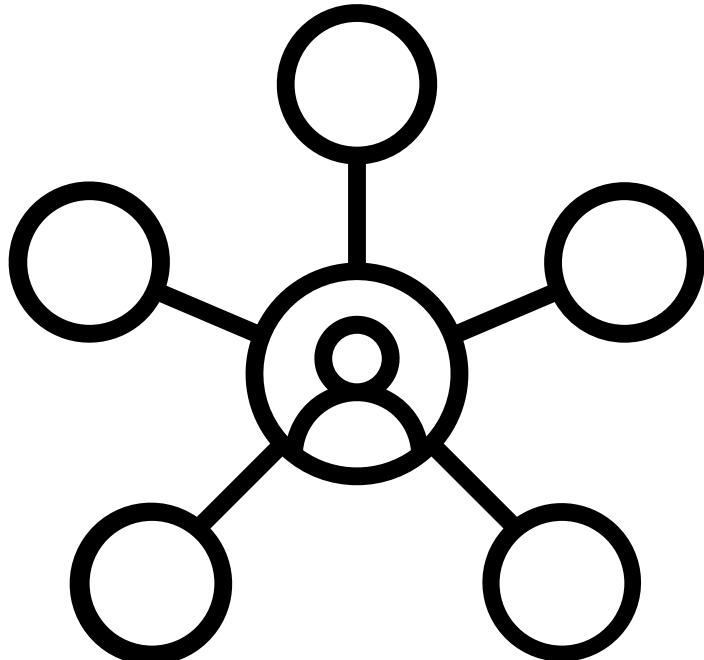
Private Google Access permits access to Cloud and Developer APIs and most Google Cloud services, except for the following services:

- App Engine MemCache
- Filestore
- Memory store

####Instead, private services access might support one or more of them.



GCP Professional Cloud Network Engineer Crash Course



Some Requirements

- Does not support legacy networks
- Must enable APIS you need in VPC
- private.googleapis.com or restricted.googleapis.com domain names to access APIs. (you're going to have to create DNS records)
- Defined Routes need to have the Internet Gateway as the next hop
- Egress FW Rules

GCP Professional Cloud Network Engineer Crash Course

● Resources

Configure VPC for Private Access

<https://cloud.google.com/vpc/docs/configure-private-google-access>

Private Access Options

<https://cloud.google.com/vpc/docs/private-access-options>

Private Google Access

<https://cloud.google.com/vpc/docs/private-google-access>

Test Tip



Private Access

- The four types of private access include private Google access, private Google access for on-prem hosts, private services Access, and serverless VPC Access.
- Private Google Access is enabled on a per-subnet basis and you must use a VPC network.



Whiteboard – Private Google Access

Discussion and Review

GCP Network Engineer

- *Understanding GPA*



Whiteboard



GCP Professional Cloud Network Engineer Crash Course





Container Networking

Enabling

GCP Professional Cloud Network Engineer Crash Course

Container IP Options

- ClusterIP: The IP address assigned to a Service. In other documents, it might be called the "Cluster IP". This address is stable for the lifetime of the Service, as discussed in the Services section in this topic.
- Pod IP: The IP address assigned to a given Pod. This is ephemeral, as discussed in the Pods section in this topic.
- Node IP: The IP address assigned to a given node

GCP Professional Cloud Network Engineer Crash Course

Kubernetes Control Plane

- The control plane manages the control plane processes, including the Kubernetes API server.
- Access depends on the version of your GKE cluster and the type of your cluster.
- For all private clusters, the control plane has both a private IP address and a public IP address.

GCP Professional Cloud Network Engineer Crash Course

Each of the five network types has a different capacity for communication with other network entities.

- Host networking: The container shares the same IP address and the network namespace as that of the host. Services running inside of this container have the same network capabilities as services running directly on the host.
- Bridge networking: The container runs in a private network internal to the host. Communication with other containers in the network is open. Communication with services outside of the host goes through network address translation (NAT) before exiting the host. ***This is the default mode of networking when the --net option isn't specified.***
- Custom bridge networking: This is the same as bridge networking but uses a bridge created specifically for this (and other) containers.
- Container-defined Networking: A container can share the address and network configuration of another container. This enables process isolation between containers, where each container runs one service but where services can still communicate with one another on 127.0.0.1.
- No networking. Disables networking for the container

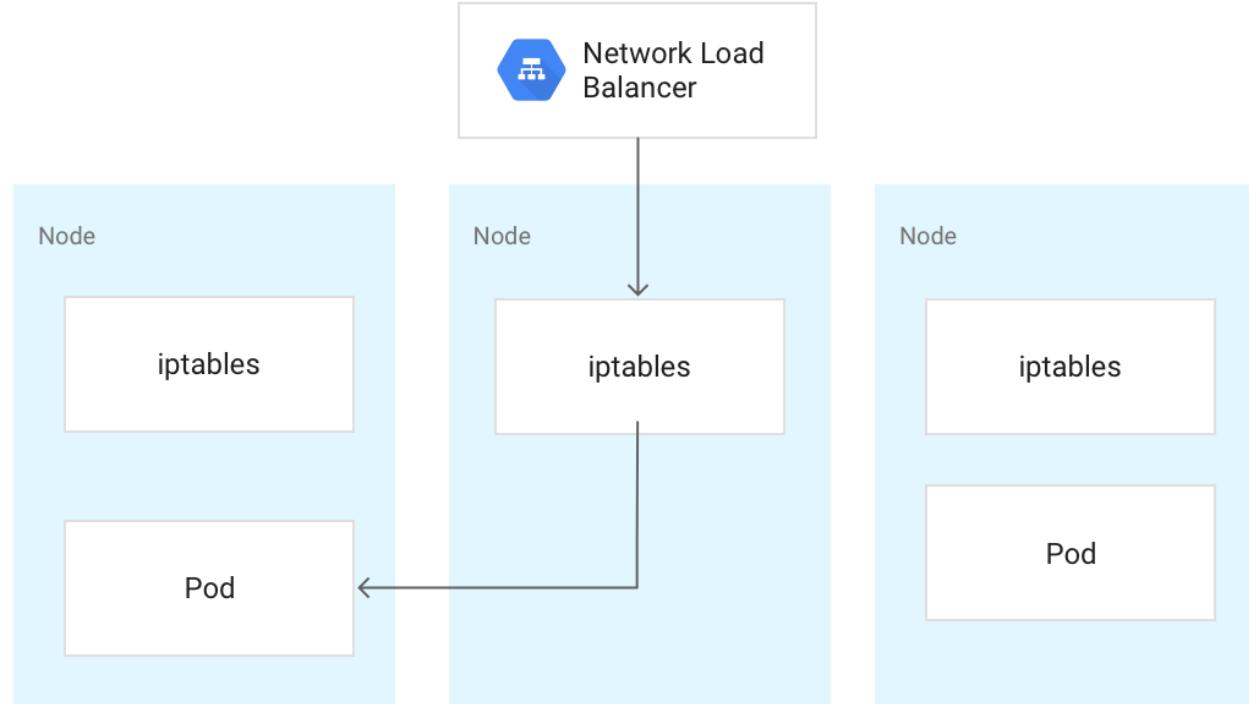
GCP Professional Cloud Network Engineer Crash Course

GKE provides three different types of load balancers :

- External load balancers manage traffic coming from outside the cluster and outside your Google Cloud VPC network. They use forwarding rules associated with the Google Cloud network to route traffic to a Kubernetes node.
- Internal load balancers manage traffic coming from within the same VPC network. Like external load balancers, they use forwarding rules associated with the Google Cloud network to route traffic to a Kubernetes node.
- HTTP(S) load balancers are specialized external load balancers used for HTTP(S) traffic. They use an Ingress resource rather than a forwarding rule to route traffic to a Kubernetes node

GCP Professional Cloud Network Engineer Crash Course

```
apiVersion: v1
kind: Service
metadata:
  name: my-lb-service
spec:
  type: LoadBalancer
  externalTrafficPolicy: Local
  selector:
    app: demo
    component: users
  ports:
    - protocol: TCP
      port: 80
      targetPort: 8080
```





Test Tips

- For all private clusters, the control plane has both a private IP address and a public IP address.
- There are three types of load balancers for GKE which are External, Internal and HTTPS
- Which LB does not need a forwarding rule?



IAM And Security

Planning and implementation

GCP Professional Cloud Network Engineer Crash Course

What are GCP Network and Security Best Practices?

- Google Cloud Platform (GCP) has a wealth of best practices for network security.
- Let's discuss the main points for this exam.
- (Note: You will want to review the Google Enterprise Guide before the exam)
- https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#networking_and_security

GCP Professional Cloud Network Engineer Crash Course

Best Practices

- Use VPC to define your network
- Manage traffic with firewall rules
- Limit external access
- Centralize network control
- Connect your enterprise network
- Secure your apps and data

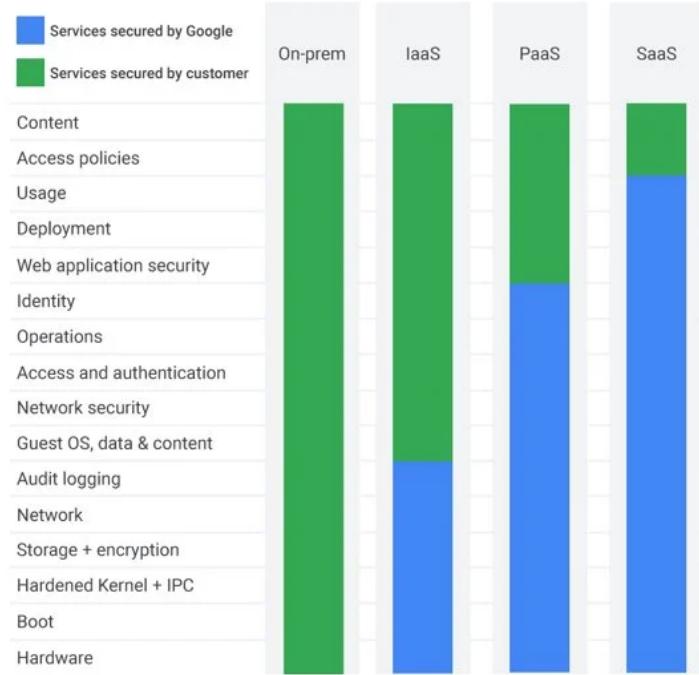


Figure 1: Responsibility chart

<https://cloud.google.com/security/incident-response>

IAM And Security

- IAM
- IAM Federation
- IAM Roles, Members and Service Accounts
- Organization Nodes
- Private Google Access
- VPC
- GCDS
- Cloud Identity

GCP Professional Cloud Network Engineer Crash Course

IAM

- Google Cloud Identity and Access Management (IAM) lets administrators authorize who can take what action on which resources
- IAM provides a unified view into security policy across the entire organization, with built-in auditing to ease compliance processes.
- IAM manages access control by defining who (identity) has what access (role) for which resource

GCP Professional Cloud Network Engineer Crash Course

IAM

- A member can be a Google Account (for end users), a service account (for apps and virtual machines), a Google group, or a Google Workspace or Cloud Identity domain that can access a resource.
- Identity of a member is an email address associated with a user, service account, or Google group; or a domain name associated with Google Workspace or Cloud Identity domains.

GCP Professional Cloud Network Engineer Crash Course

- Use your own authentication mechanism and manage your own credentials
- Federate your identities to Google Cloud Platform
- Users do not have to login a second time to access Cloud Platform resources
- Revoke access to Cloud Platform using your existing credential management
- Google Apps Directory Sync integrates with LDAP

GCP Professional Cloud Network Engineer Crash Course

Identity and Access Management (IAM)

Cloud IAM, you grant access to members. Members can be of following types:

Google account

Service account

Google group

G Suite domain

Cloud Identity domain

GCP Professional Cloud Network Engineer Crash Course

There are three types of roles in GCP Cloud IAM:

Primitive roles: The original roles available in the Google Cloud Platform Console. These are the Owner, Editor, and Viewer roles. Still assigned by default to projects. Primitive roles are quite broad.

Curated roles: Curated roles are new IAM roles that give finer-grained access control than the primitive roles

Custom Roles - provide granular access according to a user-specified list of permissions

GCP Professional Cloud Network Engineer Crash Course

Service Accounts

- A service account is an *identity for your programs to use to authenticate and gain access to GCP APIs.* (Server to Server)
- Service accounts authenticate applications running on your virtual machine instances to other GCP services.
- Each service account is associated with a key pair, which is managed by GCP. It is used for service-to-service authentication within GCP.
- Google rotates the keys daily.

Identity Federation

- Using identity federation, on-premises or multi-cloud workloads can be granted access to GCP resources, without using a service account key.
- Identity federation can be used with AWS, or with any identity provider that supports OpenID Connect (OIDC)
- With identity federation, IAM can be used to grant external identities IAM roles, including the ability to impersonate service accounts using short-lived access tokens, and eliminates the maintenance and security burden associated with service account keys

Organization Nodes

- A large number of projects can become unwieldy to manage at scale.
This is why IAM includes the concept of an Organization Node.
- The Organization Node sits above Projects and is your company's root node for Google Cloud resources.
- (Cloud Identity/Workspace), when you enable the Organization Node, any project created by users in your domain will automatically belong to your Organization Node
- The account with Organization Owner role is empowered to modify all projects within the organization.

Private Access

- Google Cloud provides several private access options that let virtual machine (VM) instances reach supported APIs and services without requiring an external IP address.
- Options support the APIs and services that you need to access.
- Private Google Access, Private Google Connect, etc

GCP Professional Cloud Network Engineer Crash Course

VPC

- “A Virtual Private Cloud (VPC) is a global private isolated virtual network partition that provides managed networking functionality for your Google Cloud Platform (GCP) resources.”
- Provides flexibility to scale and control how workloads connect regionally and globally.
- Access VPCs without needing to replicate connectivity or administrative policies in each region
- Bring your own IP addresses to Google’s network infrastructure across all regions
- A Sandbox of cloud resources in GCP

GCP Professional Cloud Network Engineer Crash Course



Google Cloud Directory Sync



GSuite Admin can automatically add, modify, and delete users, groups, and non employee contacts to synchronize the data in a GSuite domain with an LDAP directory server or MS Active Directory.



The data in the LDAP directory server is never modified or compromised. (one way update)



GCDS is a secure tool that help keep track of users and groups.

Cloud Identity

- Cloud Identity is an Identity as a Service (IDaaS) solution that centrally manages users and groups.
- Configure Cloud Identity to federate identities between Google and other identity providers, such as Active Directory and Azure Active Directory.
- Use Identity and Access Management (IAM) to manage access to Google Cloud resources for each Cloud Identity account.
- Use to create a GCP Organization (Super User is the Org Admin)
- Two Editions – Free and Premium

GCP Professional Cloud Network Engineer Crash Course

Common IT Security Best Practices

- Use the Principle of least privilege
- Always apply the minimal access level required
- Use groups and add users to the groups
- Control who can change policies and group memberships
- Audit policy changes

GCP Professional Cloud Network Engineer Crash Course

Google Cloud Security Best Practices

- Apply only minimal access level required for roles
- Use predefined roles over primitive roles
- Grant roles at smallest scope needed
- Service accounts should be treated as a separate trust boundary
- Child resources can't restrict parent access
- Create a separate service account for each service
- Restrict access to service accounts

GCP Professional Cloud Network Engineer Crash Course

Google Cloud Security Best Practices

- Audit logs record project-level permission changes
- Use Cloud Audit logs to audit IAM policy changes
- Export Audit logs to Cloud Storage
- Restrict Audit logs to appropriate users

GCP Professional Cloud Network Engineer Crash Course

Google Cloud Security Best Practices

- Rotate Service account keys
- Don't delete service accounts in use
- Don't leave keys in source code or in unsecure directories.
- Organizational level policies should be used to grant access to projects
- Grant roles to groups instead of individual users
- User groups whenever possible to simplify management



Test Tips

- On the exam questions will infer that you understand GCP best practices around IAM and security and can apply this while answering questions
- A parent can't be restricted to accessing child resources.

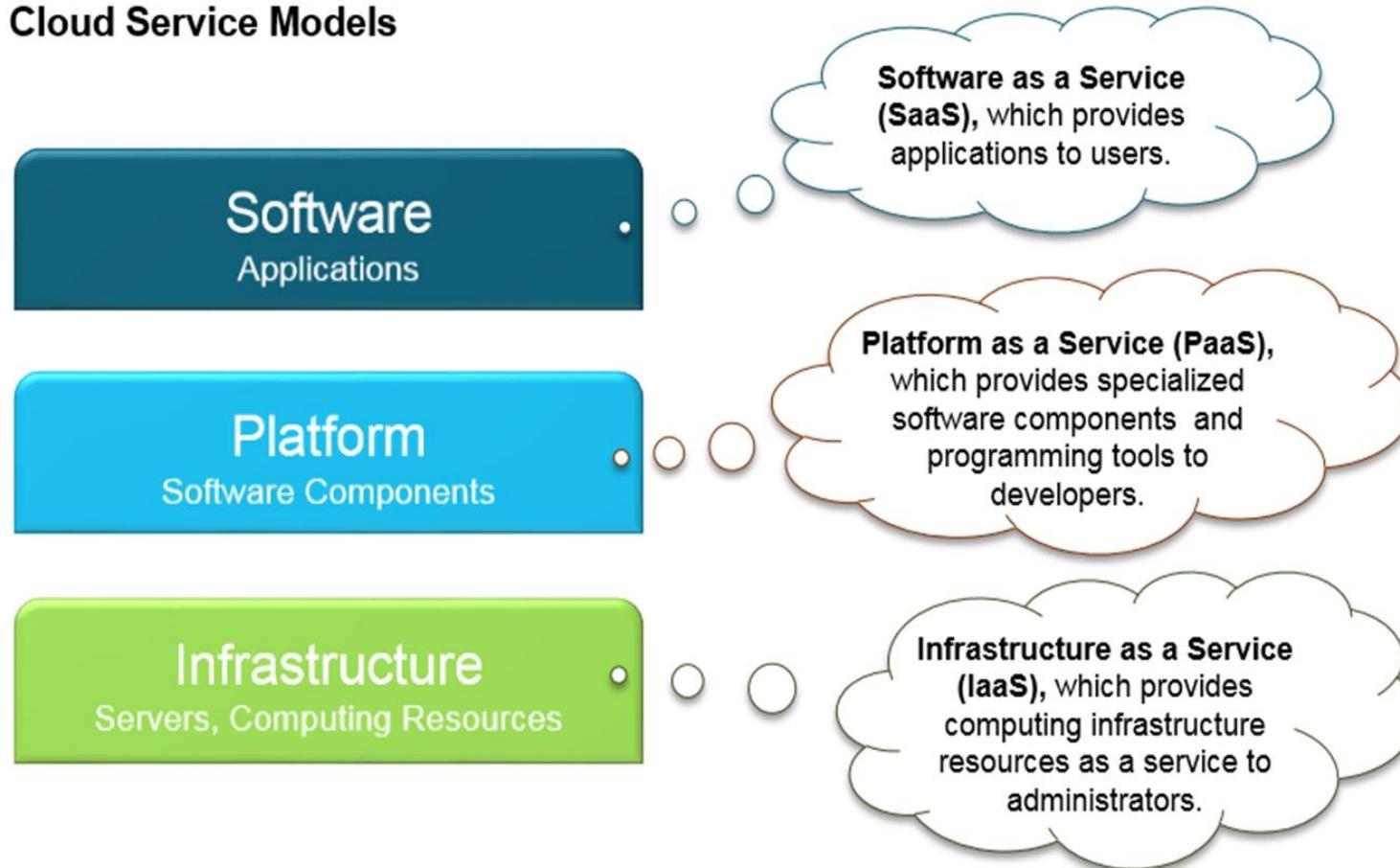


Service Models

Understanding Service Models IaaS, PaaS, SaaS

GCP Professional Cloud Network Engineer Crash Course

Cloud Service Models



GCP Professional Cloud Network Engineer Crash Course



Infrastructure as a Service (IaaS) contains the basic building blocks for cloud IT and typically provides access to networking features, computers and data storage space.



IaaS provides the highest level of flexibility and management control over the infrastructure (Example – GCP Compute Engine and AWS EC2)

GCP Professional Cloud Network Engineer Crash Course



Platform as a Service (PaaS) removes the need for your organization to manage the underlying infrastructure and allows you to focus on the deployment and mgmt. of your applications.

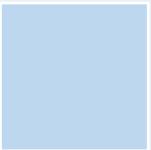


PaaS provides the second highest level of flexibility and management control over the infrastructure. (Example – GCP App Engine and AWS Elastic Beanstalk)

GCP Professional Cloud Network Engineer Crash Course



Software as a Service (SaaS) provides you a complete product that is run and managed by the service provider.



You worry only about using the software and not about infrastructure.



SaaS provides the lowest level of flexibility and management control over the infrastructure. (Example – Google Gsuite and MS O365)

GCP Professional Cloud Network Engineer Crash Course

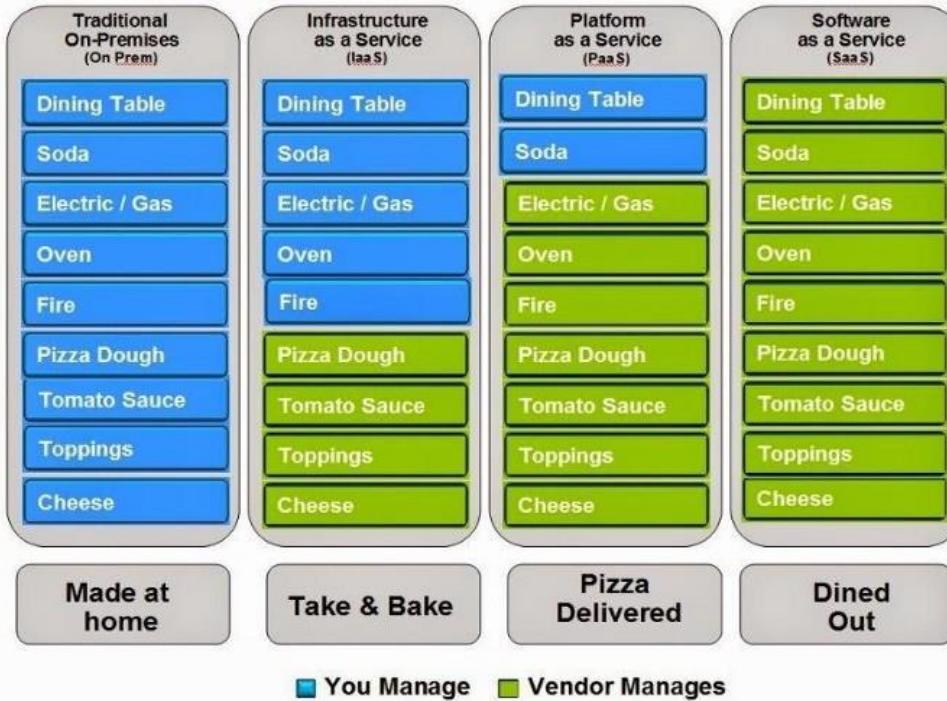


Difference between Service Models?

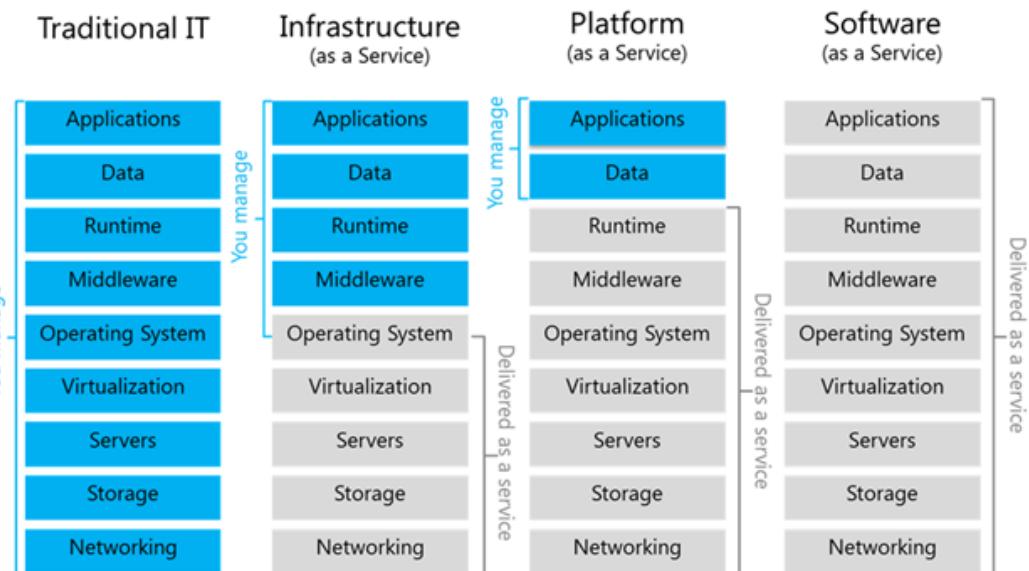
- Mainly the functionality and services offered
- Shared Responsibility model (How much customer and provider perform)
- Like the Pizza Model

GCP Professional Cloud Network Engineer Crash Course

Pizza as a Service



Graphic – Paul Kerrison



Graphic - VMware

GCP Professional Cloud Network Engineer Crash Course

Service	Description
IaaS	Data center resources: computer, network, and storage resources
PaaS	Platform resources: databases, web services, and other middleware applications
IaaS	Software resources: customer applications

GCP Cloud Developer Overview

Selecting the Correct Service Model

When choosing a service in GCP you want to be aware of the options that are provided compared to the NIST Cloud Service Model

There are trade offs between flexibility, scalability, performance, security and management



Test Tips

- Three Service Models
- SaaS provides the lowest level of flexibility while IaaS provides the highest level of flexibility.



Resource Hierarchy

Organizations, Projects and Folders

GCP Professional Cloud Network Engineer Crash Course

The hierarchy of GCP is broken into the following structure:

- Organizations
- Folders
- Projects
- Resources

GCP Professional Cloud Network Engineer Crash Course

Organization – MyCompany.com

Folders

Projects (Project 1, Project 2)

Resources (Compute, Storage, Data Services, etc)

GCP Professional Cloud Network Engineer Crash Course

Organizations

- The Organization resource is the root node of the Google Cloud resource hierarchy and all resources that belong to an organization are grouped under the organization node.
- The Organization resource is associated with a Google Workspace or Cloud Identity account.
- The Google Workspace super admin is the individual responsible for domain ownership verification and the contact in cases of recovery.

GCP Professional Cloud Network Engineer Crash Course

Google Cloud resources are organized hierarchically.

- Organization is the top of the hierarchy and does not have a parent.
- Projects are the first level, and they contain other resources.

GCP Professional Cloud Network Engineer Crash Course



AN ORGANIZATION RESOURCE
IS AVAILABLE FOR WORKSPACE
AND CLOUD IDENTITY
CUSTOMERS.



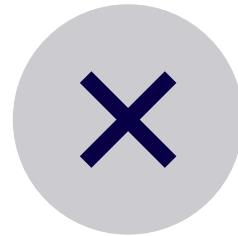
LINK YOUR ORG DOMAIN TO
GCP.



THINK OF AN ORGANIZATION
AS A HIERARCHY.



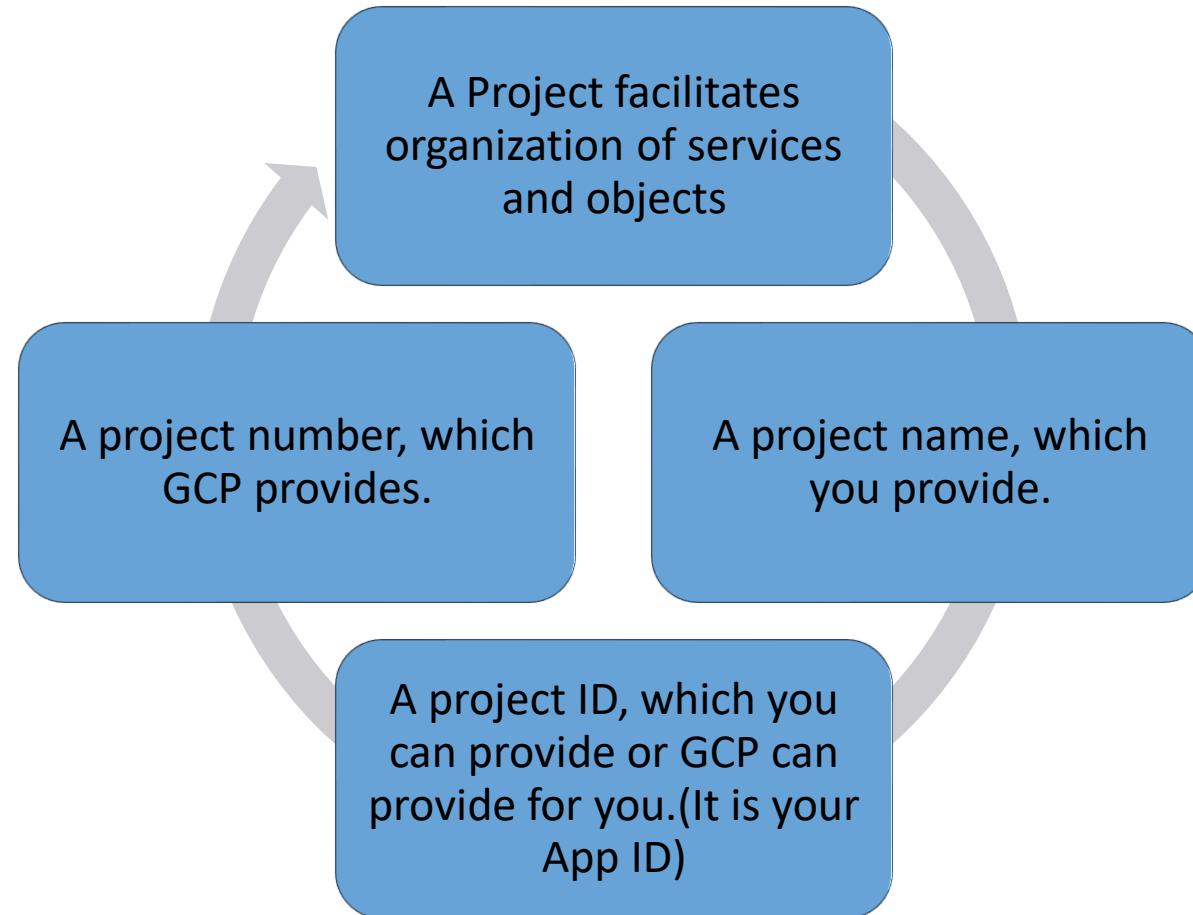
SET ACCESS CONTROL AND
CONFIGURATION SETTINGS AT
THE ORGANIZATION OR
PROJECT LEVEL



BILLING ACCOUNTS, PROJECTS,
AND RESOURCES ARE NOT
DELETED WHEN AN EMPLOYEE
LEAVES THE COMPANY.
FOLLOWS CORPORATE
LIFECYCLE.

GCP Professional Cloud Network Engineer Crash Course

Projects



GCP Professional Cloud Network Engineer Crash Course

Projects

A Project facilitates organization of services and objects and uses this method of segmentation for billing and accounting.



Project info

Project name

My Python Hello World

Project ID

my-python-hello-world-191118

Project number

452326268329

→ Go to project settings

GCP Professional Cloud Network Engineer Crash Course

Projects in GCP

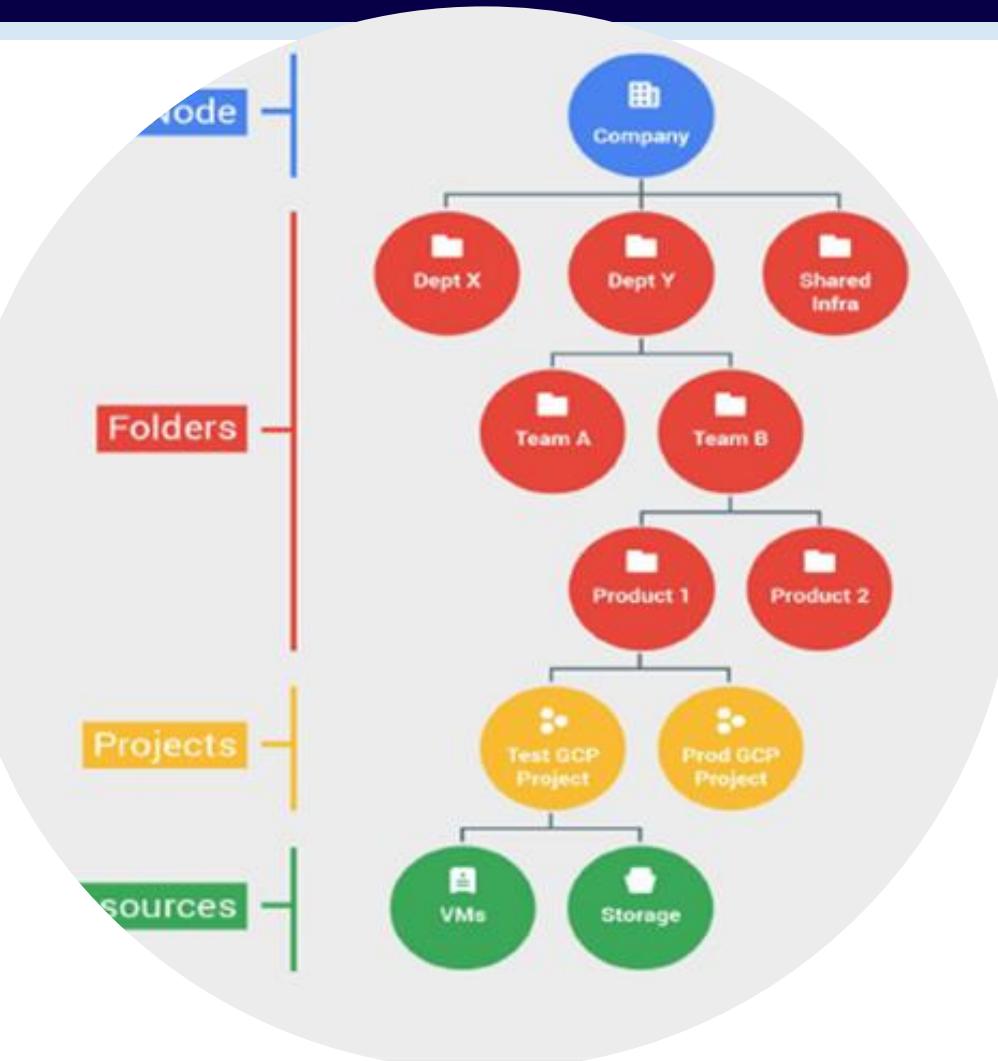
Projects

All Google Cloud Platform services are associated with a project that is used to:

- Track resource and quota usage
- Enable billing
- Manage permissions and credentials
- Enable services and APIs

```
jholbrookln@projectidgpcourse1:~$ gcloud projects list
PROJECT_ID          NAME                PROJECT_NUMBER
gpcourse1234        gpcourse1234        824698542660
my-awesome-project-198000  My Awesome Project  577767719453
my-test-project-2-192418  My Test Project 2  174359988401
projectidgpcourse1      Project AWS and GCP Course  409356428059
projectnetworking101    projectnetworking101  251983216344
test123-203018         test123            918409078391
jholbrookln@projectidgpcourse1:~$
```

GCP Professional Cloud Network Engineer Crash Course



Projects and Hierarchy

- Folders are also introduced when you use Cloud IAM.
- The Cloud IAM Folders feature lets you assign policies to resources at a level of granularity you choose.
- The resources in a folder can share IAM policies



Test Tips

- Organizations represent a company.
- Organizations are tied to Cloud Identity or Workspace accounts/deployments root node. (Domain)
- Organizations are managed by Google Workspace Super Admin



Test Tips

- A Folder resources provide an additional grouping mechanism and isolation boundaries between projects.
- Folders are similar to a sub-organizations within the Organization.



Test Tips

- A Project segments our cloud deployment. (Similar to a Sandbox)
- A project consists of a set of users; a set of APIs; and billing, authentication, and monitoring settings for those APIs
- A project ID is the customized name you chose when you created the project



Microsegmentation for security purposes

Using metadata, tags, Services, etc

GCP Professional Cloud Network Engineer Crash Course

What is Microsegmentation?

- Micro-segmentation is a network security technique that enables security architects to logically divide the data center into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment.
- Defense in Depth

GCP Professional Cloud Network Engineer Crash Course

Google Defense in Depth – Must know for the exam

- Secure your internet-facing services
- Secure your VPC for private deployments
- Micro-segment access to your applications and services

Refer to this page. <https://cloud.google.com/blog/products/networking/google-cloud-networking-in-depth-three-defense-in-depth-principles-for-securing-your-environment>

GCP Professional Cloud Network Engineer Crash Course

Graphic –
Google
Cloud

Defense in depth - network security *in the cloud*

Micro-segment access to
your applications and
services

Secure your VPC for
private deployments.

Secure your
internet-facing apps

IAM	API based access
Istio security based	Micro-segmentation based on HTTP/S ID
Firewalls per Service Account	Micro-segmentation for VM based apps
GKE Network Policies	Micro-segmentation within GKE cluster

Global LB	Anycast IP, DDoS protection.
TLS everywhere	Application encryption
Cloud Armor	Application based controls
IAP	Identity based controls

VPC Service Controls	Secure your sensitive data - lock data within a trusted perimeter
VPC level firewalls	Secure your VPC boundaries
Outbound NAT proxy	Egress internet access without public IP
VPN and Interconnect	Private access to on-prem
Private Google Access	Private Access to GCS, BigQuery, SQL, Redis
Private GKE, VMs	Private deployments: No public IP

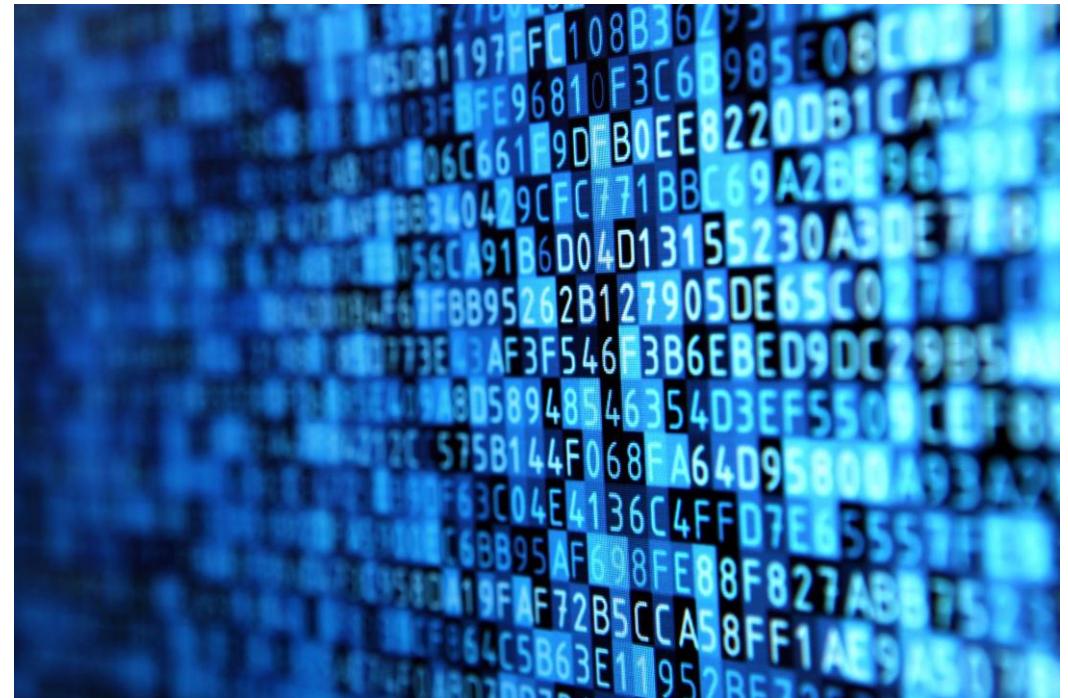
Near Real-time telemetry

Partner solutions

GCP Professional Cloud Network Engineer Crash Course

What is Micro segmentation?

- Micro-segmentation is a network security technique that enables security architects to logically divide the data center into distinct security segments down to the individual workload level.
- Define security controls and deliver services for each unique segment.



GCP Professional Cloud Network Engineer Crash Course

Segmentation on GCP

- Projects and Orgs
- VPC
- IAM and Folders
- Subnets
- Regions

GCP Professional Cloud Network Engineer Crash Course

Services to facilitate micro segmentation on GCP

- Cloud IAP
- Cloud Armor
- IAM Folders
- Cloud WAD
- Binary Authorization and Network Policies (GKE)

GCP Professional Cloud Network Engineer Crash Course

Metadata and Tags

- Metadata is stored as key:value pairs. There is a default set of metadata keys that are available for VMs running on Compute Engine.
- Tags are simply a character string added to a tags field in a resource. Tags enable you to make firewall rules and routes applicable to specific VM instances. The network tags that you assign to an instance apply to all of the instance's network interfaces. ***A network tag only applies to the VPC networks that are directly attached to the instance's network interfaces***

GCP Professional Cloud Network Engineer Crash Course

Metadata and Tags

CLI

```
gcloud compute instances create INSTANCE_NAME --zone ZONE --tags TAGS
```

```
gcloud compute instances list --filter='tags:TAG_EXPRESSION'
```

API

GET

```
https://compute.googleapis.com/compute/v1/projects/myproject/zones/us-central1-f/instances/example-instance
```



Test Tips

- Google Defense in Depth – Must know for the exam
- A network tag only applies to the VPC networks that are directly attached to the instance's network interfaces



1.2 Designing a VPC.

Understanding hybrid networks

GCP Professional Cloud Network Engineer Crash Course

VPC

- “A Virtual Private Cloud (VPC) is a global private isolated virtual network partition that provides managed networking functionality for your Google Cloud Platform (GCP) resources.”
- Provides flexibility to scale and control how workloads connect regionally and globally.
- Access VPCs without needing to replicate connectivity or administrative policies in each region
- Bring your own IP addresses to Google’s network infrastructure across all regions
- A Sandbox of cloud resources in GCP

GCP Professional Cloud Network Engineer Crash Course

API must be
enabled



Google Cloud Platform Google Analytics ▾

Compute Engine API

Google Enterprise API

Compute Engine API

TRY THIS API

OVERVIEW DOCUMENTATION SUPPORT

Overview

Creates and runs virtual machines on Google Cloud Platform.

Additional details

Type: [SaaS & APIs](#)
Last updated: [7/22/21](#)
Category: [Compute](#), [Networking](#), [Google Enterprise APIs](#)
Service name: [compute.googleapis.com](#)

GCP Professional Cloud Network Engineer Crash Course

Google Cloud Platform Google Analytics Search products and resources 1

VPC network VPC networks + CREATE VPC NETWORK ⏪ REFRESH

VPC networks	Name	Region	Subnets	MTU	Mode	IP address ranges	Gateways	Firewall Rules	Global dynamic routing	Flow logs
	default	29	1460	Auto		10.128.0.0/20 10.132.0.0/20 10.138.0.0/20 10.140.0.0/20 10.142.0.0/20 10.146.0.0/20 10.148.0.0/20 10.150.0.0/20 10.152.0.0/20	10.128.0.1 10.132.0.1 10.138.0.1 10.140.0.1 10.142.0.1 10.146.0.1 10.148.0.1 10.150.0.1 10.152.0.1	4	Off	Off
External IP addresses	us-central1	default								
Bring your own IP	europe-west1	default								
Firewall	us-west1	default								
Routes	asia-east1	default								
VPC network peering	us-east1	default								
Shared VPC	asia-northeast1	default								
Serverless VPC access	asia-southeast1	default								
Packet mirroring	us-east4	default								
	australia-	default								

GCP Cloud Developer Overview

Subnet Notes for exam

- E.G - if you want to keep instances in your testing and production systems from talking to one another except through external IPs, you can put the instances in different networks.
- Instances in different networks are completely isolated and can have overlapping address ranges. (Comms across networks is only possible through external public IP space)
- Comms over external IP space requires security investments but also can incur additional costing (Egress)

GCP Cloud Developer Overview

Subnet Notes Continued

- Each instance created within a subnetwork gets assigned an IPv4 address from that subnetwork's range.
- Google App Engine Flexible Environment: Supported only on auto subnetwork networks. Cannot be deployed in a custom subnet networks.



Test Tips

- What is a VPC and how to configure.
- Subnetting notes
- Instances in different networks are completely isolated and can have overlapping address ranges.



CIDR range for subnets

CIDR

GCP Cloud Developer Overview

CIDR Range is the address range for this subnet, in CIDR notation.

Use a standard private VPC network address range: for example, 10.0.0.0/9.

← Create a VPC network

New subnet

Name * ?

Lowercase letters, numbers, hyphens allowed

Description

Region * ?

IP address range * ?

Secondary IP ranges ?

Subnet range name	Secondary IP range *
Example: range-1	Example: 10.0.1.0/24

+ ADD IP RANGE



IP Addressing

IP Fundamentals and limits – static, ephemeral or

GCP Cloud Developer Overview

IP Addresses

- Internal
- External
- Static
- Ephemeral
- Private
- Bring your own

GCP Cloud Developer Overview

IP Addresses

- Internal and external IP addresses can be ephemeral or static.
- An ephemeral IP address is an IP address that doesn't persist beyond the life of the resource
- Reserving a static IP address assigns the address to your project until you explicitly release it.

GCP Cloud Developer Overview

IP Addresses

- Regional internal addresses (VPC Subnet ranges)
- Global internal addresses (Private ranges)
- Regional external addresses (Internet accessible external IPv4 addresses that are usable by regional resources)
- Global external addresses (Internet accessible anycast external IPv4 or IPv6 addresses for global load balancing)

Refer to this page/table before exam.

- https://cloud.google.com/vpc/docs/ip-addresses?hl=en&_ga=2.3848240.-1459696889.1607613118

GCP Cloud Developer Overview

IP Addresses

- An external IP address makes an attached project resource available on another Google Cloud Platform network or the Internet.
- You can attach an ephemeral address to a resource, or you can use a static IP address that never changes.

← Reserve a static address

Name * ?

Lowercase letters, numbers, hyphens allowed

Description

Network Service Tier ?

Premium (Current project-level tier, [change](#)) ?

Standard ?

IP version

IPv4

IPv6

Type

Regional

Global (to be used with Global forwarding rules [Learn more](#))

Region ▼ ?

Attached to ▼ ?

GCP Cloud Developer Overview

Bring your own IP

- You can use your own public IP addresses with Google Cloud Platform
- Use your Public Advertised Prefix and validate it.

[←](#) Create PAP

1 Enter PAP — 2 Confirm ownership — 3 Reverse lookup — 4 Validation

Route Origin Authorization Verification

Before you can add a PAP, you must submit a Route Origin Authorization (ROA) request for your prefix. [Learn more](#)

Enter the public advertised prefix

Enter details for the prefix that you want to bring to Google Cloud. [Learn more](#)

Name *	<input type="text"/>	?
--------	----------------------	-------------------

Lowercase letters, numbers, hyphens allowed

Description

Prefix *

Example: 203.0.113.0/24



Test Tips

- Understand the IP Address types and the use case for them.



VPC Peering

What are the security properties with a VPC?

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Peering

- VPC Peering allows private RFC1918 connectivity across two VPC networks regardless of whether they belong to the same project or the same organization

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Peering Use Cases

- Organizations with several network administrative domains.
- Organizations that want to peer with other organizations.

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Benefits

- Use to make services available across VPCs and Organizations
- Organizations that want to peer with other organizations.
- Stays in the Google Network and does not traverse internet.
- Better security, lower latency and lower costs.

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Properties

- Administratively separate and are setup independently
- Subnets and Static routes are global
- Dynamic routes can be regional or global
- A VPC can peer with multiple VPC networks.
- Peering will be active only when the configuration from both sides matches. Either side can choose to delete the peering association at any time.

GCP Professional Cloud Network Engineer Crash Course

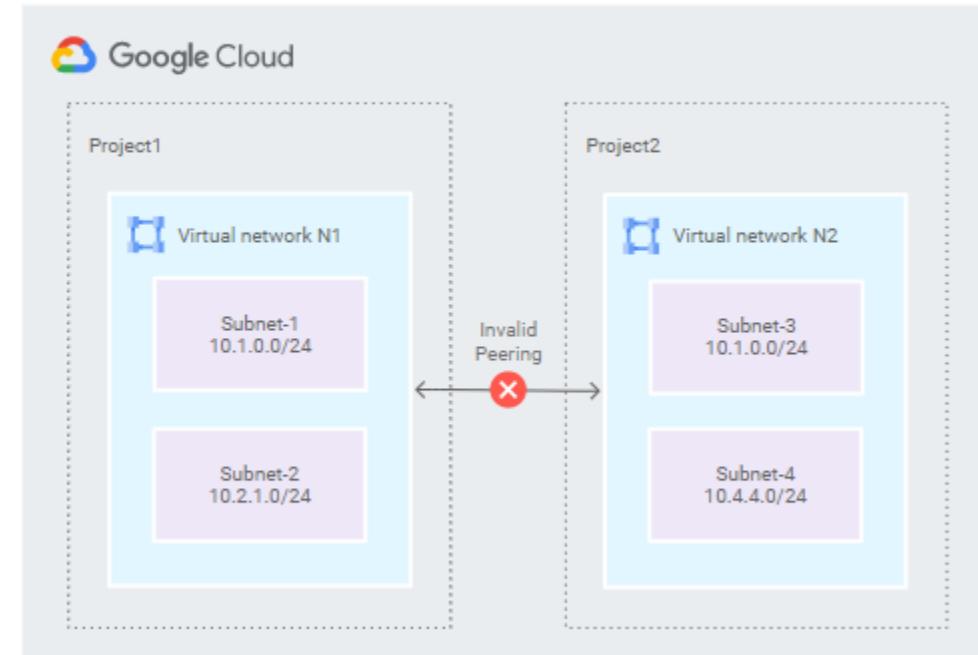
Virtual Private Cloud - Restrictions

- Google does perform a validation before peering, creating a static route or a new subnet in a Peered network.
- Tags are independent of each peered network
- Service accounts are independent of each peered network.

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Failures

- Peering will fail when the CIDR range has overlapping networking (CIDR, Subnets)
- This rule covers both subnet routes and static routes



Test Tip



VPCS

- VPC will be heavily tested around networking configuration .
- VPC Peering will be tested. Understand use case for peering vs use case of Shared VPC
- Shared VPC allows an organization to connect resources from multiple projects to a common VPC network via **internal IPs** from that network.



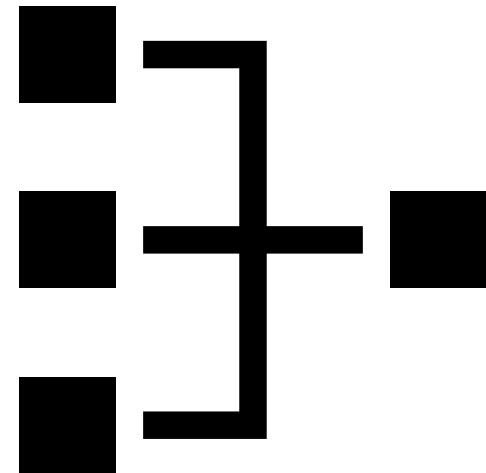
Routing

Fundamentals

Routing

Routing is of course obvious important to route traffic.

- Control flow of data and direct traffic where you want it
- Default Routes work in most case but if you need a custom route that you can do as well



GCP Cloud Developer Overview

Routing

- Cloud Router enables you to dynamically exchange routes between your Virtual Private Cloud (VPC) and on-premises networks by using Border Gateway Protocol (BGP).
- Cloud Router automatically learns new subnets in your VPC network and announces them to your on-premises network.

GCP Cloud Developer Overview

Dynamic Routing in VPC

Regional - Cloud Routers will learn routes only in the region in which they were created

Global dynamic routing - allows all subnetworks regardless of region to be advertised to your on-premise router and region when using cloud router.

GCP Cloud Developer Overview

Routing

- ASN - You can use any private ASN (64512 - 65534, 4200000000 - 4294967294) that you are not using elsewhere in your network
- BGP Keep Alive - This is the interval in seconds between BGP keepalive messages that are sent to the peer. If set, this value must be between 20 and 60. The default is 20
- Gcloud - `gcloud compute routers create routerdemo --project=encoded-hangout-331014 --region=us-east1 --network=default`

GCP Cloud Developer Overview

Routing

Cloud Routers

 CREATE ROUTER

 REFRESH

 DELETE

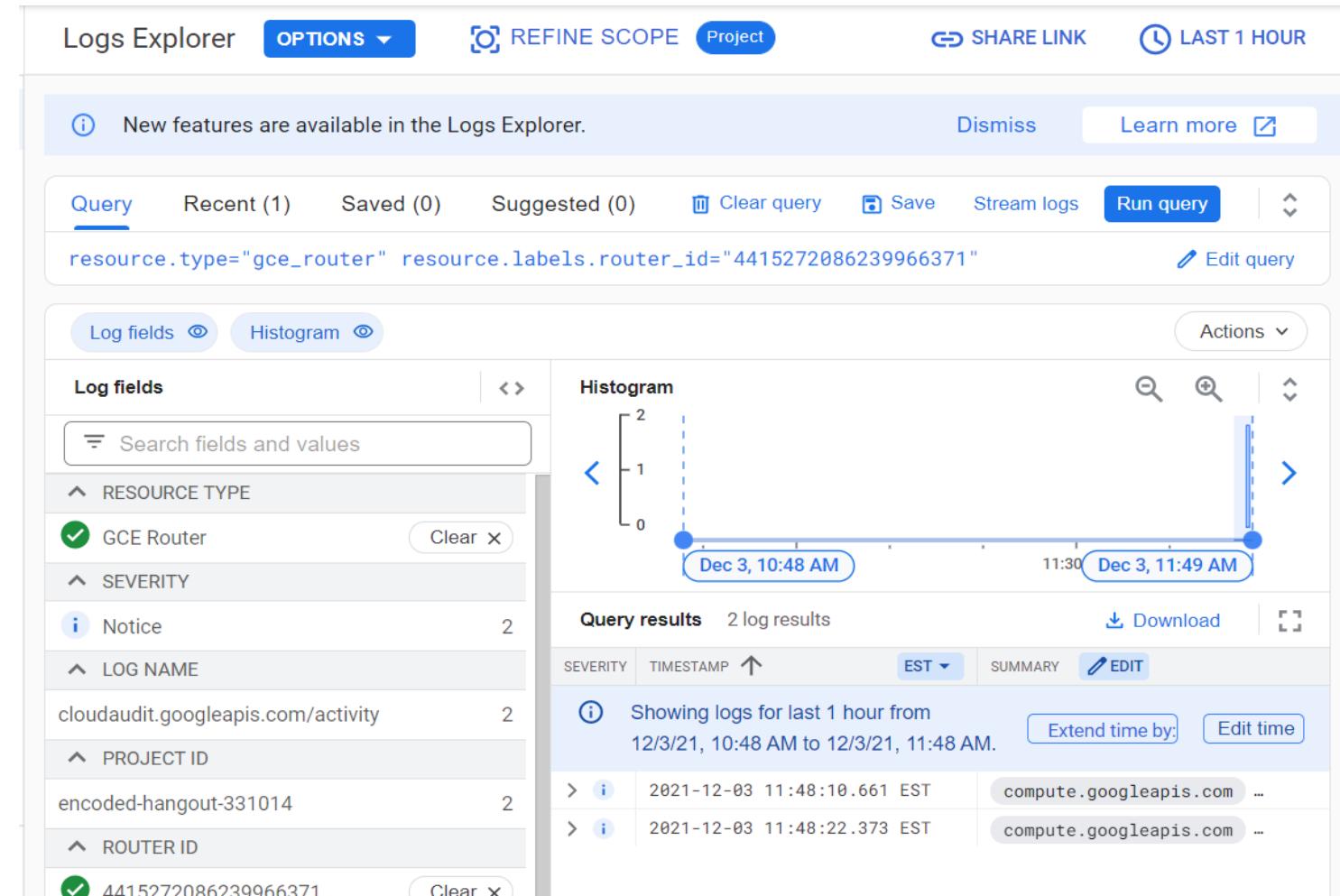
 Filter Enter property name or value

<input type="checkbox"/>	Name 	Network	Region	Google ASN	Interconnect	Connection	BGP sessions	Logs
<input type="checkbox"/>	routerdemo	default	us-east1		None			View

GCP Cloud Developer Overview

Routing

- Logs Explorer



GCP Cloud Developer Overview

Firewalls (TAGS)

- Used to identify routes and firewall rules for VMS.
- Tags are user defined
- Not limited to topology like an IP address.
- 64 tags to an instance
- Console, gcloud and API
- gcloud compute instances add-tags Instance1 --tag1 tag2
- <https://cloud.google.com/vpc/docs/add-remove-network-tags>

GCP Cloud Developer Overview

Default Routes

Routes							
		CREATE ROUTE	REFRESH	DELETE			
	ALL	DYNAMIC	PEERING				
<input type="text"/> Filter Enter property name or value							
<input type="checkbox"/>	Name ↑	Description	Destination IP range	Priority	Instance tags	Next hop	Network
<input type="checkbox"/>	default-route-0128f5a8d55cfbce	Default local route to the subnetwork 10.180.0.0/20.	10.180.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-1b4c688724bcc3fa	Default local route to the subnetwork 10.138.0.0/20.	10.138.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-2142390b5c02ab5b	Default local route to the subnetwork 10.146.0.0/20.	10.146.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-24566e483a7df689	Default local route to the subnetwork 10.192.0.0/20.	10.192.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-2fd24919de1cd615	Default route to the Internet.	0.0.0.0/0	1000	None	Default internet gateway	default
<input type="checkbox"/>	default-route-30916aa3c20f04b7	Default local route to the subnetwork 10.186.0.0/20.	10.186.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-30dbe1bc183ee8a2	Default local route to the subnetwork 10.148.0.0/20.	10.148.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-3461h9aa7h3aaa69	Default local route to the subnetwork 10.140.0.0/20	10.140.0.0/20	0	None	Virtual network default	default

GCP Cloud Developer Overview

Create Route and add tags

← Create a route

Name * ?

Lowercase letters, numbers, hyphens allowed

Description

Network * ▼ ?

Destination IP range * ?

E.g. 10.0.0.0/16

Priority * ?

Priority should be a positive integer (lower values take precedence)

Instance tags ?

Next hop ▼ ?

CREATE

CANCEL



Test Tips

- Know the syntax for adding and removing a tag.
- `gcloud compute instances add-tags Instance1 --tag1 tag2`



VPC Firewall

Fundamentals

GCP Cloud Developer Overview

Firewalls as a Resource

- Global Resource
- Control traffic incoming (Priority as well)
- Default allows ingress (Allow Only)

Matches dest. IP CIDR ranges, protocols, ports & target Tags

- ICMP
- SSH
- RDP

Supports Allows for ingress not Denies (Remember this)

GCP Cloud Developer Overview

Firewalls as a VPC Resource

VPC networks have two implied firewall rules. Note that these “implied” rules CAN NOT be removed..

- implied allow egress rule (65535 Priority)
- implied deny ingress rule (65535 Priority)

<https://cloud.google.com/vpc/docs/firewalls>

GCP Cloud Developer Overview

Firewalls as a VPC Resource

Always-blocked traffic - GCP always blocks the following traffic.

<https://cloud.google.com/vpc/docs/firewalls>

Firewall rules **cannot** be used to un-block traffic that is always blocked.

Rules are evaluated for priority. 0-65535 Default is 1000

Differences between Google Cloud Networking and other cloud platforms

Networking differences

GCP Cloud Developer Overview

Some differences between AWS and GCP Networking

Google Cloud Platform VPCs are relatively flat with controls targeting the instance. Amazon Web Services VPCs are hierarchical with multiple layers of control at the region, zone, subnet, and instance.

GCP Subnets are associated with regions; traffic transparently moves across zones while AWS Subnets are associated with (availability) zones; moving traffic across zones requires routing between multiple subnets

GCP Routes are associated with the VPC while in AWS there in a routing table.

GCP Cloud Developer Overview

- GCP Firewall rules can be automatically applied to all instances while in AWS its more manually applied
- GCP firewall rules can have both allow and deny rules while AWS has allow rules. (Network ACLs)



Test Tips

- Understand the high level differences between GCP and other providers.



1.3 Designing a hybrid network.

Understanding hybrid networks

GCP Cloud Developer Overview

Hybrid Network to connect your networks to GCP and ensure we provide for redundancy.

Hybrid connectivity products

- Interconnects
- VPN
- Peering



Connectivity Options

Connectivity options and best practices

GCP Professional Cloud Network Engineer Crash Course

Options for connectivity to Google Cloud

- Cloud VPN
- Public Ips
- Direct Peering
- Carrier Peering
- Cloud Interconnect (10/100 Gbps)
- Partner Interconnect (50Mbps to 10Gps)

GCP Professional Cloud Network Engineer Crash Course

Options for connectivity to Google Cloud

- Make the best decision
- <https://cloud.google.com/hybrid-connectivity>



GCP Professional Cloud Network Engineer Crash Course

Cloud VPN

- Cloud VPN provides private-to-private connectivity and your internet connection meets your business requirements.
- Ensure VMs that you provisioned in GCP can communicate directly with on-premises resources via a private IP range.
- Private RFC1918 addresses
- IPSEC Tunnels
- Ipsec VPN tunnels encrypt data by using industry-standard Ipsec protocols as traffic traverses the public Internet.

GCP Professional Cloud Network Engineer Crash Course

Public IP

- Using a public IP provides connectivity if your internet connection meets your business requirements.
- Uses Public internet connection
- Connection not encrypted

GCP Professional Cloud Network Engineer Crash Course

Direct Peering

- Direct Peering connects your on-premises network to Google services, including Google Cloud products that can be exposed via one or more public IP addresses.
- Traffic from Google's network to your on-premises network also takes that same connection, including traffic from VPC networks in your projects.

GCP Professional Cloud Network Engineer Crash Course

Direct Peering

- Direct Peering exists outside of Google Cloud Platform. So, unless you need to access Google Workspace applications, the recommended methods of access to Google Cloud Platform are via Dedicated Interconnect or Partner Interconnect.

GCP Professional Cloud Network Engineer Crash Course

Carrier Peering

- Carrier Peering is an option when support by a carrier with a connection to Google. Unlike Direct Peering where your enterprise provides equipment, the carrier provides the equipment.
- Run BGP over a link to exchange network routes.
- With carrier peering, traffic flows through an intermediary.
- Cost

GCP Professional Cloud Network Engineer Crash Course

Interconnections (Partner and Direct)

- Interconnects are similar to peering in that the connections get your network as close as possible to the Google network.
- Interconnects are different from peering in that they give you connectivity using private address space into your Google VPC.
- If you need RFC1918-to-RFC1918 private address connectivity then you'll need to provision either a dedicated or partner interconnect.
- Low Latency, Secure and Costly

GCP Professional Cloud Network Engineer Crash Course

Interconnections (Partner and Direct)

Cloud Interconnect offers two options to extend your on-premises network to the Google Cloud Platform:

- Dedicated Interconnect
- Direct physical Connection to Google's network.
- Partner Interconnect
- Provides connectivity through a supported service provider.

GCP Professional Cloud Network Engineer Crash Course

Interconnections (Partner and Direct)

- Partner Interconnect – Equipment and links are owned and managed by service provider.
- Direct Interconnect – Enterprise provides equipment are installed directly to Google
- 10 Gbps or 100 Gbps pipes.
- Virtual attachment circuit over the physical link

GCP Professional Cloud Network Engineer Crash Course

What Connection is best?

Connection Type	Best For	Benefits
Cloud VPN	Extends Private Peer network with IPSEC	Secure and Low Overhead
Public IPs	Connection ease	Low Overhead
Direct Peering	Equipment Available	SLA, Higher Security
Carrier Peering	Carrier Provisioned	SLA, Lower Overhead
Direct Interconnect	Direct Connection to Google	SLA, Low Latency and HA
Partner Interconnect	Connectivity by Provider	SLA, Low Latency and HA

<https://cloud.google.com/blog/products/networking/google-cloud-network-connectivity-options-explained>



Test Tips

- Know the connection strategies and options.
- Use Cloud VPN if you have to ensure that the VMs that you provisioned in GCP can communicate directly with on-premises resources via a private IP range.



Failover and disaster recovery strategy

Handling and Options

GCP Professional Cloud Network Engineer Crash Course

DR is a subset of business continuity planning.

DR planning begins with a business impact analysis that defines two key metrics:

- A recovery time objective (RTO), which is the maximum acceptable length of time that your application can be offline. This value is usually defined as part of a larger service level agreement (SLA).
- A recovery point objective (RPO), which is the maximum acceptable length of time during which data might be lost from your application due to a major incident. This metric varies based on the ways that the data is used.

GCP Professional Cloud Network Engineer Crash Course

DR is a subset of business continuity planning.

- HA helps to ensure an agreed level of operational performance, usually uptime, for a higher than normal period.
- When you run production workloads on Google Cloud, you might use a globally distributed system so that if something goes wrong in one region, the application continues to provide service even if it's less widely available. In essence, that application invokes its DR plan.

GCP Professional Cloud Network Engineer Crash Course

Traditional DR planning requires you to account for a number of requirements, including the following:

- Capacity: securing enough resources to scale as needed.
- Security: providing physical security to protect assets.
- Network infrastructure: including software components such as firewalls and load balancers.
- Support: making available skilled technicians to perform maintenance and to address issues.
- Bandwidth: planning suitable bandwidth for peak load.
- Facilities: ensuring physical infrastructure, including equipment and power.

GCP Professional Cloud Network Engineer Crash Course

DR patterns are considered to be *cold, warm, or hot.*

- These patterns indicate how readily the system can recover when something goes wrong.



GCP Professional Cloud Network Engineer Crash Course

Google Cloud offers several features that are relevant to DR planning

- A global network
- Redundancy
- Scalability
- Security
- Compliance

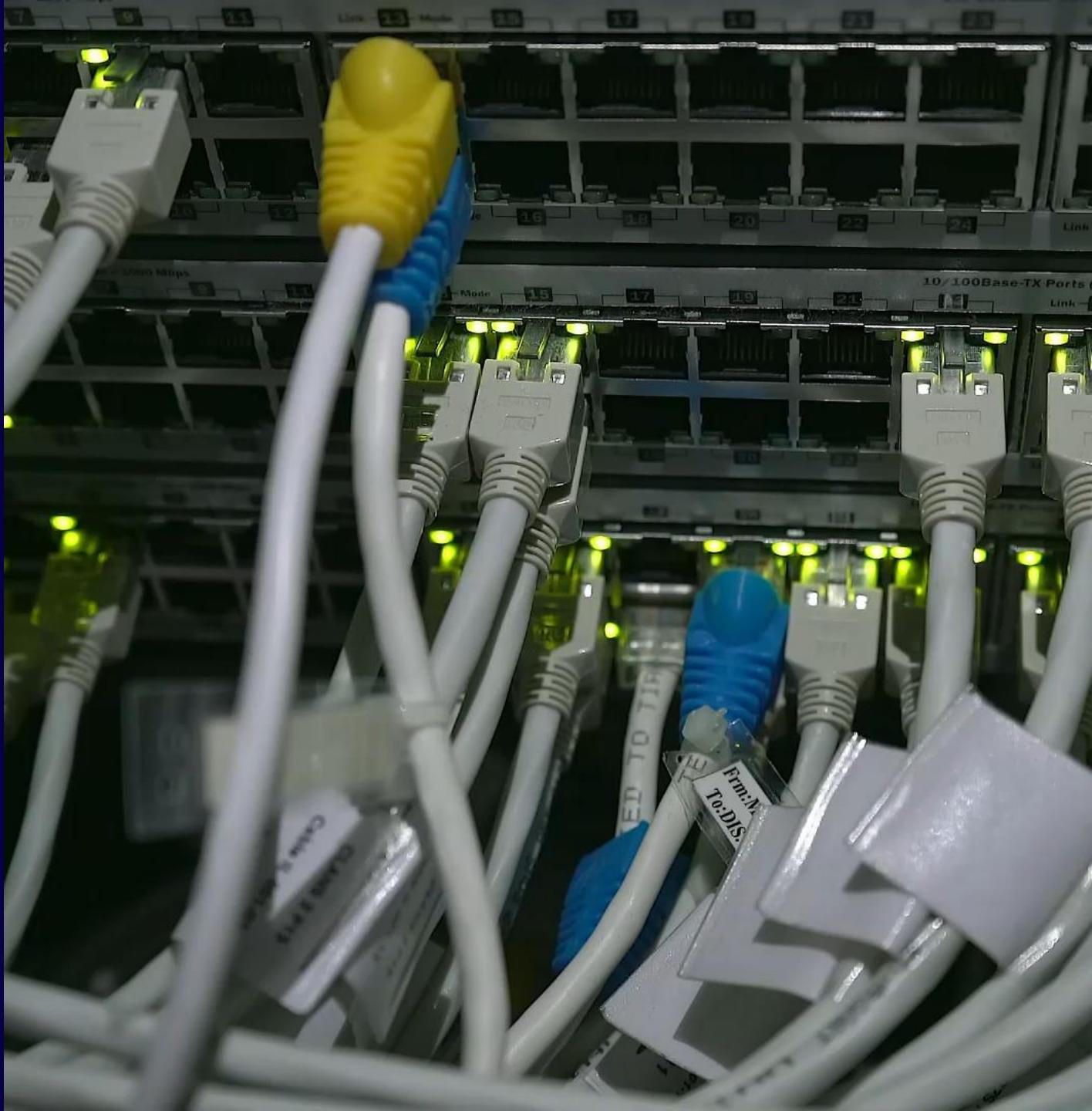


Shared vs. standalone VPC interconnect access

Differences

Shared vs. standalone VPC interconnect access

- Shared VPC allows an organization to connect resources from multiple projects to a common VPC network to communicate with each other securely and efficiently using internal IPs from that network.
- Requires designating a project as a host project and attach one or more other service projects to it.



GCP Professional Cloud Network Engineer Crash Course

Shared VPC

- Shared VPC allows an organization to connect resources from multiple projects to a common VPC network to communicate with each other securely and efficiently using internal IPs from that network.
- Requires designating a project as a host project and attach one or more other service projects to it.

GCP Professional Cloud Network Engineer Crash Course

Why Use a Shared VPC?

- Implement a security best practice of least privilege for network administration, auditing, and access control.
- Apply and enforce consistent access control policies at the network level for multiple service projects in the organization while delegating administrative responsibilities
- Use service projects to separate budgeting or internal cost centers

GCP Professional Cloud Network Engineer Crash Course

Shared VPC

- A host project contains one or more Shared VPC networks
- A service project is any project that has been attached to a host project by a **Shared VPC Admin**
- Roles are Org Admin, Shared VPC Admin and Service Project Admin

GCP Professional Cloud Network Engineer Crash Course

Shared VPC and Cloud Interconnect

- Host project contains a common Shared VPC network that VMs in service projects can use.
- VLAN attachments and Cloud Routers for an Interconnect connection must be created only in the Shared VPC host project.
- The combination of a VLAN attachment and its associated Cloud Router is unique to a given Shared VPC network.
- VMs that use the Shared VPC network can use the custom dynamic routes for VLAN attachments available to that network

GCP Professional Cloud Network Engineer Crash Course

To Share or Not to Share.

- VPC Network Peering allows peering with a Shared VPC.
- A Shared VPC host project is a project that allows other projects to use one of its networks
- A single-project VPC provides full access to the VPC and its resources, which makes configuration easier

GCP Professional Cloud Network Engineer Crash Course

To Share or Peer.

Peering	Shared
2 peered VPCs can not share the same subnet ranges	Shared VPCs can share the same subnet ranges
Peering requires a certain level of access to projects. The 2 projects are on-par (both ends must allow the peering).	Shared VPC creates a hierarchical relation where one end is the manager of the network and FW rules.
VPC peering can do passthru (daisy chain) up to 1 level	Shared VPC can exhaust its resources (IPv4 ranges) faster
Peering needs rules setup on both ends	Shared VPC allows for a simplified FW setup as you have only one central point to setup your FW rule



Whiteboard – Putting it all Together

Discussion and Review

GCP Network Engineer

- *Let's review what we covered in this section*



Whiteboard



Section Summary

Section 1 : Designing, Planning and prototyping a GCP Network



1

Section

Section Summary

- The Google Cloud Architecture Framework which provides recommendations and describes best practices to help architects, developers, administrators, and other cloud practitioners design and operate a cloud topology that's secure, efficient, resilient, high-performing, and cost-effective.
- Private Google Access is enabled on a per-subnet basis and you must use a VPC network.
- Google Defense in Depth is focused on 1. Secure your internet-facing services, 2. Secure your VPC for private deployments and 3. Micro-segment access to your applications and services

- A recovery time objective (RTO), which is the maximum acceptable length of time that your application can be offline.
- An ephemeral IP address is an IP address that doesn't persist beyond the life of the resource
- A Shared VPC connects projects within the same organization
- A Shared VPC lets you apply and enforce consistent access control policies at the network level for multiple service projects in the organization while delegating administrative responsibilities

Section Review Questions

**Section 1 : Designing, Planning
and prototyping a GCP
Network**



Review Questions

Which service provides a cost-effective solution to cache the static content and reduce the load on the origin servers in Google Cloud? (Select One)

- Cloud DNS
- Load Balancing
- Cloud CDN
- Cloudflare

Review Questions

Which service provides a cost-effective solution to cache the static content and reduce the load on the origin servers in Google Cloud? (Select One)

- Cloud DNS
- Load Balancing
- **Cloud CDN**
- Cloudflare

Review Questions

Which of the following two statements are true about Edge locations in GCP?
(Select Two)

- Edge Locations are GCP endpoints that cache content locally
- Services Supported are Amazon CloudFront, S3, Amazon Route 53, GCP Firewall Manager, GCP Shield, and GCP WAF
- Edge Locations are Regions that cache content locally.
- Services Supported are only compute and storage services.

Review Questions

Which of the following two statements are true about Edge locations in GCP?
(Select Two)

- Edge Locations are GCP endpoints that cache content locally
- Services Supported are Amazon CloudFront, S3, Amazon Route 53, GCP Firewall Manager, GCP Shield, and GCP WAF
- Edge Locations are Regions that cache content locally.
- Services Supported are only compute and storage services.

Review Questions

Where should you create the Cloud Router instance in a Shared VPC to allow connection from service projects across a new Dedicated Interconnect to your data center? (Select One)

- VPC network in all projects
- VPC network in the IT Project
- VPC network in the Host Project
- VPC network in the Sales, Marketing, and IT Projects

Review Questions

Where should you create the Cloud Router instance in a Shared VPC to allow connection from service projects across a new Dedicated Interconnect to your data center? (Select One)

- VPC network in all projects
- VPC network in the IT Project
- **VPC network in the Host Project**
- VPC network in the Sales, Marketing, and IT Projects

GCP Professional Cloud Network Engineer Crash Course

Review Questions

VPC Network Peering allows you to peer two VPC networks so that the VMs in the two networks can communicate via internal, private IP addresses. This provides advantages since the organization is exposing its service to the public internet.

Which of the following is NOT true about VPC Network Peering? (Select One)

- A. VPC Network Peering works with Compute Engine, Kubernetes Engine and App Engine Standard
- B. Peered VPC networks remain administratively separate.
- C. Each side of a peering association is set up independently.
- D. A given VPC network can peer with multiple VPC networks
- E. VPC Network Peering works with Compute Engine and App Engine Flexible

GCP Professional Cloud Network Engineer Crash Course

Review Questions

VPC Network Peering allows you to peer two VPC networks so that the VMs in the two networks can communicate via internal, private IP addresses. This provides advantages since the organization is exposing its service to the public internet.

Which of the following is NOT true about VPC Network Peering? (Select One)

- A. VPC Network Peering works with Compute Engine, Kubernetes Engine and App Engine Standard
- B. Peered VPC networks remain administratively separate.
- C. Each side of a peering association is set up independently.
- D. A given VPC network can peer with multiple VPC networks
- E. VPC Network Peering works with Compute Engine and App Engine Flexible

GCP Professional Cloud Network Engineer Crash Course

Review Questions

How do you isolate VM systems within one project to guarantee that they can't communicate over the internal IP address? (Select One)

- A. Place them in different zones
- B. Place them in different networks
- C. Place them in separate organizations
- D. Place them in a separate project

GCP Professional Cloud Network Engineer Crash Course

Review Questions

How do you isolate VM systems within one project to guarantee that they can't communicate over the internal IP address? (Select One)

- A. Place them in different zones
- B. Place them in different networks
- C. Place them in separate organizations
- D. Place them in a separate project

GCP Professional Cloud Network Engineer Crash Course





Section 2 – Implementing a GCP VPC

Understanding the domain testable objectives

Domain Overview

- Configuring VPCs
- Configuring Routing
- Configuring and maintaining GKE clusters
- Configuring and managing firewall rules



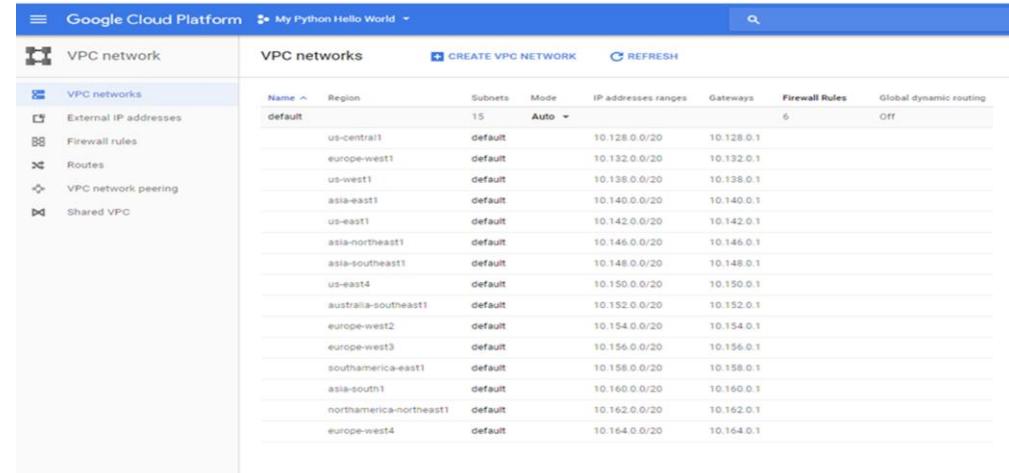
Configuring Virtual Private Cloud (VPC)

What is a VPC?

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud

- A Virtual Private Cloud (VPC) is a **GLOBAL** private isolated virtual network partition that provides managed networking functionality for your Google Cloud Platform (GCP) resources
- Software Defined Sandbox



Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules	Global dynamic routing
default	us-central1	15	Auto	10.128.0.0/20	10.128.0.1	6	Off
	europe-west1	default		10.132.0.0/20	10.132.0.1		
	us-west1	default		10.138.0.0/20	10.138.0.1		
	asia-east1	default		10.140.0.0/20	10.140.0.1		
	us-east1	default		10.142.0.0/20	10.142.0.1		
	asia-northeast1	default		10.146.0.0/20	10.146.0.1		
	asia-southeast1	default		10.148.0.0/20	10.148.0.1		
	us-east4	default		10.150.0.0/20	10.150.0.1		
	australia-southeast1	default		10.152.0.0/20	10.152.0.1		
	europe-west2	default		10.154.0.0/20	10.154.0.1		
	europe-west3	default		10.156.0.0/20	10.156.0.1		
	southamerica-east1	default		10.158.0.0/20	10.158.0.1		
	asia-south1	default		10.160.0.0/20	10.160.0.1		
	northamerica-northeast1	default		10.162.0.0/20	10.162.0.1		
	europe-west4	default		10.164.0.0/20	10.164.0.1		

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud

- Each GCP project contains one or more VPC networks.
- Each VPC network is a global entity spanning all GCP regions.
- This global VPC network allows VM instances and other resources to communicate with each other via internal, private IP addresses

GCP Professional Cloud Network Engineer Crash Course

VPC Features

Global Communications Space

Thru the Google backbone directly..

(This is a big differentiator between other clouds)

GCP Professional Cloud Network Engineer Crash Course

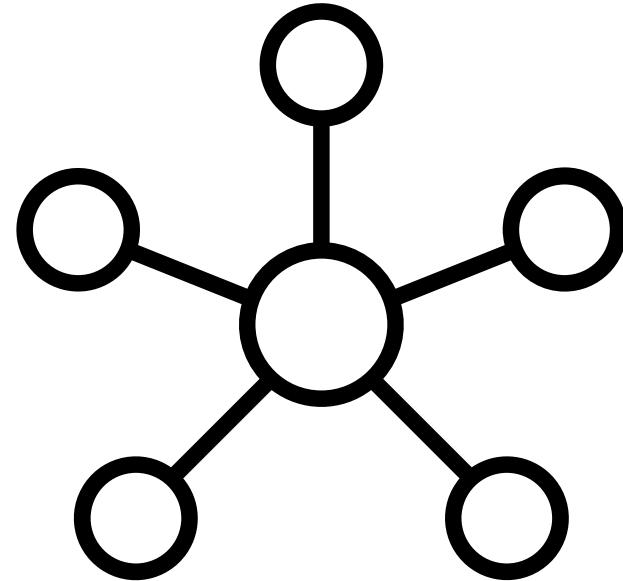
Virtual Private Cloud

- Global Communications Space
- Compute or GCP Services
- Shared VPC
- Hybrid Support
- Private Peering
- Two Types (Auto & Custom)

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Subnets

- A Subnet is a regional resource and can span multiple zones.
- This is somewhat different than other providers.
- When deploying a custom VPC you can specify the subnets



GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Routing and Firewalls

- Routing defines paths for data packets entering or exiting your network. (VPC)
- Firewall rules are what control traffic into the VPC
- Firewalls rules can be ingress or egress.

- Gcloud --- gcloud compute firewall-rules list

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Connecting with On Premises

- Cloud Interconnect
- Cloud VPN
- Peering

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Modes

Auto Mode

- VPC Network is created with one subnet from each region is automatically created within it
- Uses predefine IP Range
- Adds new regions automatically with subnets
- Can add manually

Custom Mode

- Custom Config
- VPC Network is created (no subnets are created automatically)
- Uses your custom IP Range
- You have control and add subnets as required.

GCP Professional Cloud Network Engineer Crash Course

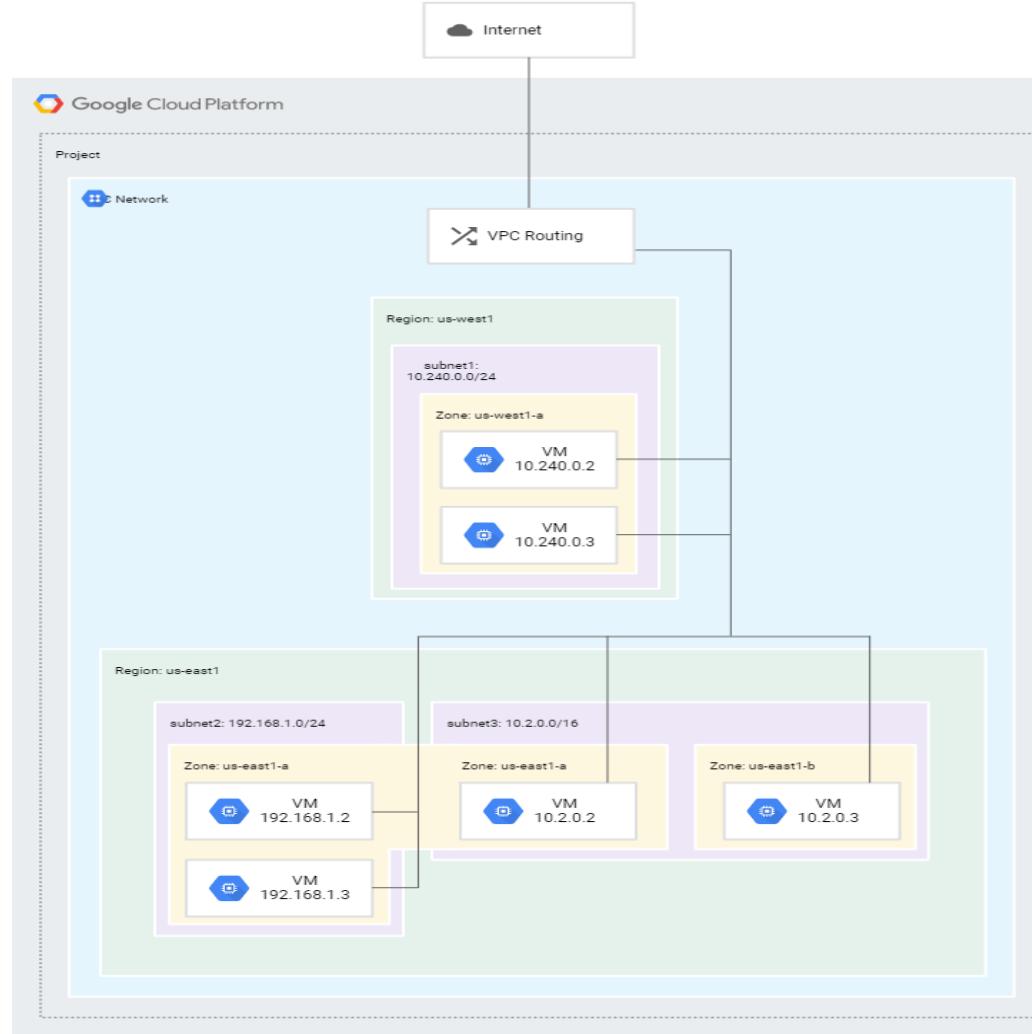
Virtual Private Cloud - Network

- A network must have at one subnet before it can be used
- VPC Networks support IPv4 unicast traffic

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Network

- Lets Discuss



Test Tip



VPCS

- VPC will be heavily tested around networking configuration .
- VPC Peering will be tested. Understand use case for peering vs use case of Shared VPC
- Shared VPC allows an organization to connect resources from multiple projects to a common VPC network via **internal IPs** from that network.

GCP Professional Cloud Network Engineer Crash Course





Whiteboard – Putting it all Together

Discussion and Review

GCP Network Engineer

- *VPC Networking*

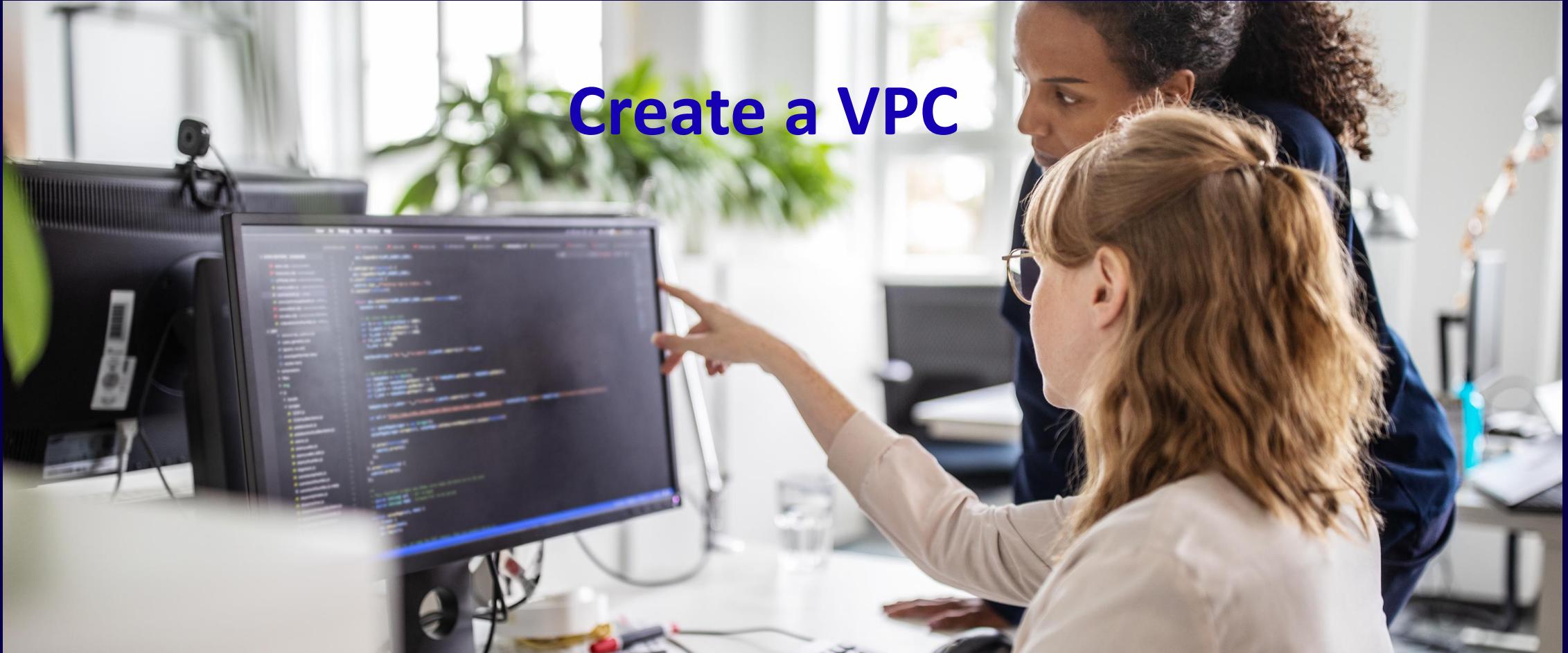


Whiteboard



Hands-on exercise

Create a VPC





Configuring VPC peering

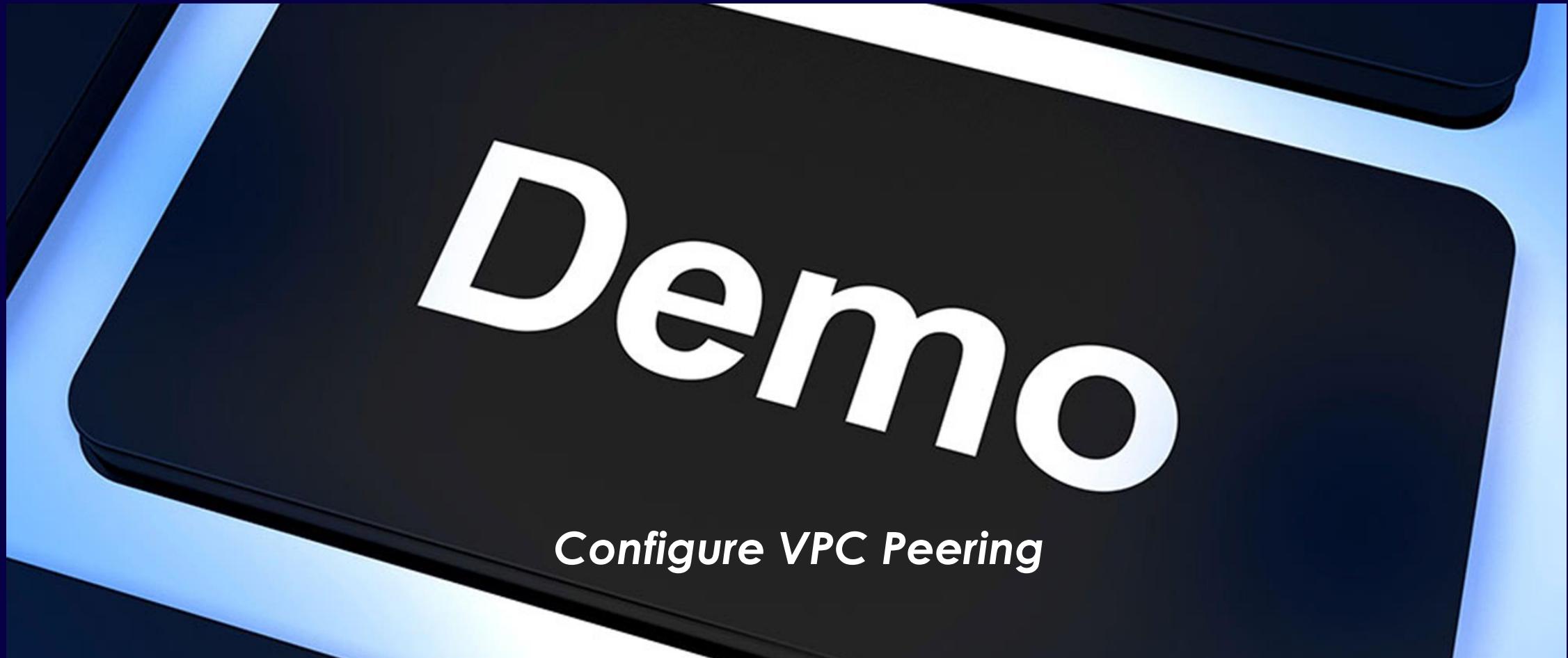
VPC Peering

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Peering

- VPC Peering allows private RFC1918 connectivity across two VPC networks regardless of whether they belong to the same project or the same organization

GCP Professional Cloud Network Engineer Crash Course





Creating a shared VPC

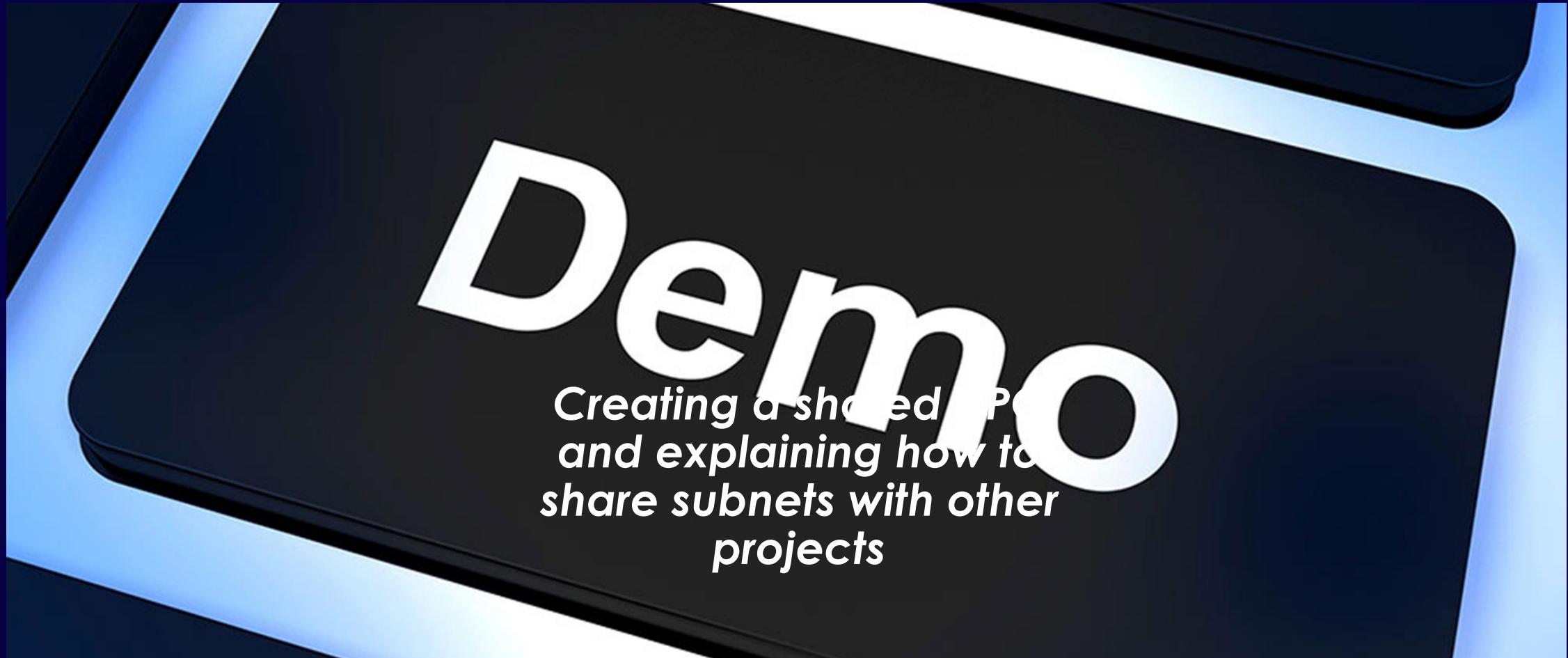
Shared VPC

GCP Professional Cloud Network Engineer Crash Course

Shared VPC

- Shared VPC allows an organization to connect resources from multiple projects to a common VPC network to communicate with each other securely and efficiently using internal IPs from that network.
- Requires designating a project as a host project and attach one or more other service projects to it.

GCP Professional Cloud Network Engineer Crash Course





VPC Security Permissions and Roles

What are the security properties with a VPC?

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Security Permissions and Roles

- VPC Networking is part of Compute Engine IAM Roles
- Administration is thru Cloud IAM

Roles

- Compute Admin - Full access to instance and network admin role
- Compute Network Admin – Full Network Admin role

GCP Professional Cloud Network Engineer Crash Course

Virtual Private Cloud - Security Permissions and Roles

- A network must have at **one subnet before it can be used**
- VPC Networks support IPv4 unicast traffic



Demo - VPC Security Properties

Demo

GCP Professional Cloud Network Engineer Crash Course





Configure VPC Flow Logs

Obtaining insight into your VPC

GCP Professional Cloud Network Engineer Crash Course

VPC flow logs record a sample of network flows sent from and received by VM instances.

- VPC logs can be used for network monitoring, forensics,
- Real-time security analysis, and expense optimization.
- Flow logs can be viewed within Operations logging (aggregated by connection from VMs and exported in real time.)
- Real time -- subscribe to cloud Pub/Sub which will allow you to stream those logs into your analysis tool of choice.
- Flow logs can be **enabled or disabled per VPC subnet, and each flow record covers all TCP and UDP flows.**
- Filters can also be applied to select which flow logs should be excluded from Operations logging and exported to external APIs.

Proactive Security with Flow Logs

- Flow logs will allow you to find out which IPs talk to **whom and when**.
- You can also **analyze incoming and outgoing network flows** for any compromised IPs.
- VPC flow logs allow you to do real-time security analysis.

Proactive Security with Flow Logs

- Networking Monitoring
- Network Usage Insights
- Network Forensics
- Real Time Security Analysis

GCP Professional Cloud Network Engineer Crash Course

Enable Flow Logs

- Configure Flow Logs in VPC > Enable on subnet

Flow logs

On

[View flow logs](#)

Aggregation Interval

5 sec

Additional fields



Include metadata

Sample rate

50%

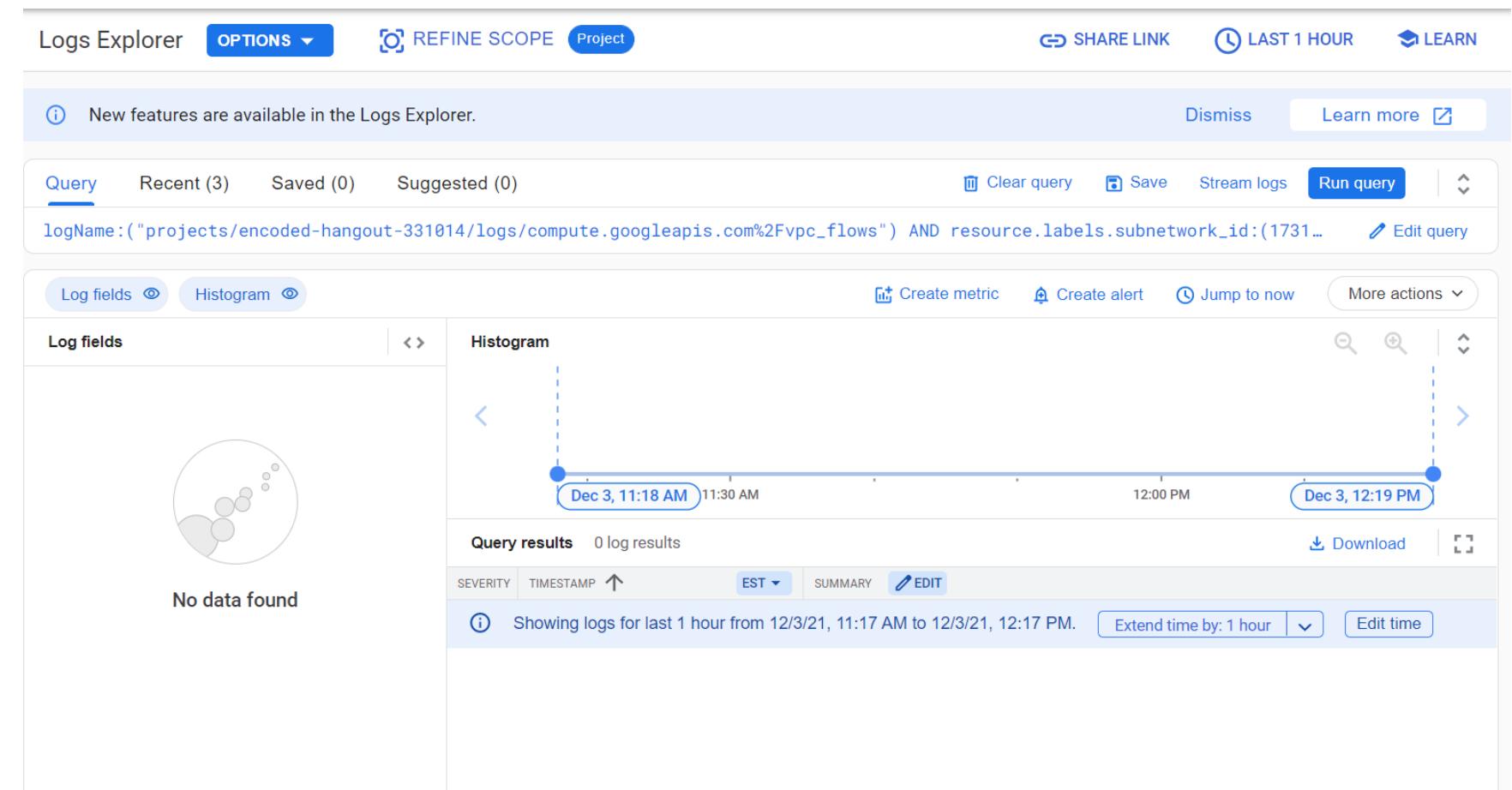
[▲ LESS](#)

[EQUIVALENT REST](#)

GCP Professional Cloud Network Engineer Crash Course

View Flow Logs

- View in Logs Explorer

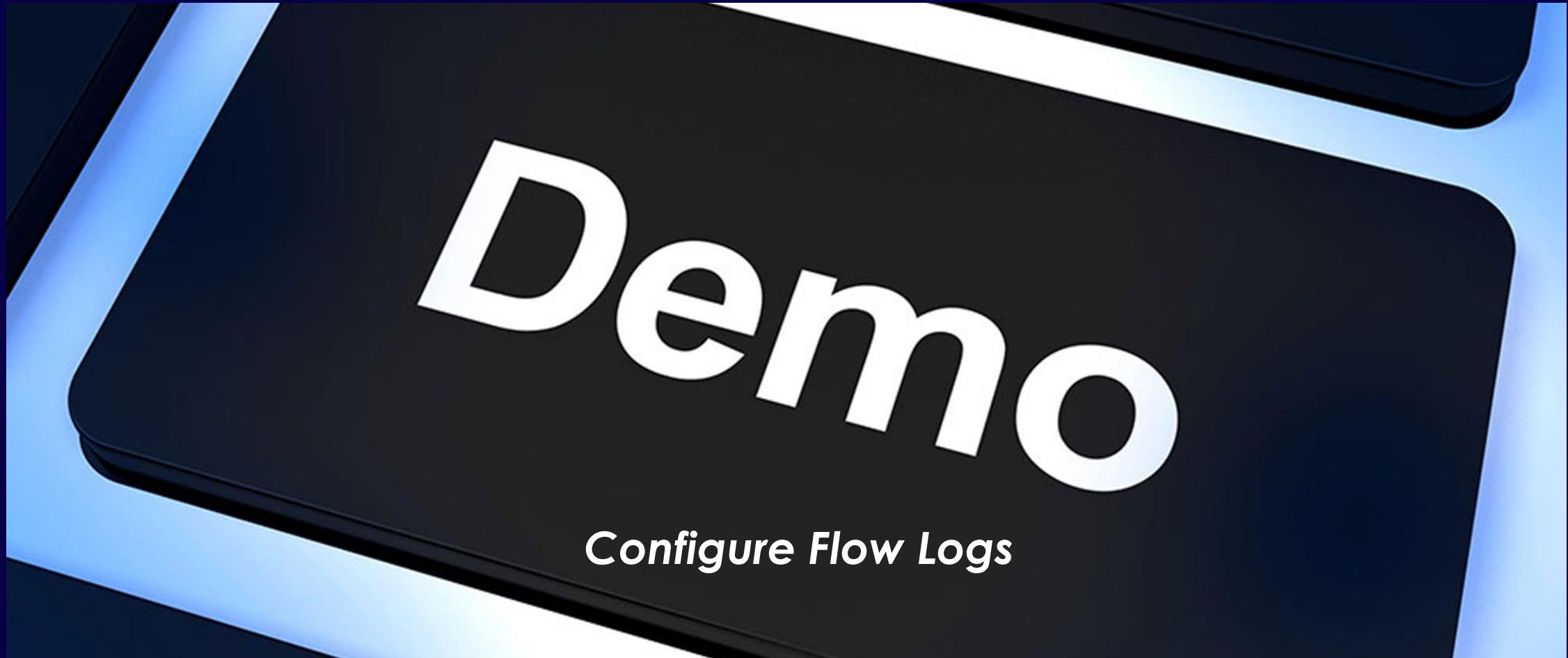




Test Tips

- Know the use case for VPC Flow logs.
- They allow you to provide for real time security analysis

GCP Professional Cloud Network Engineer Crash Course





Configure Firewall Rules

Setting them correctly

GCP Professional Cloud Network Engineer Crash Course

VM Networking Protocols

Supported Protocols

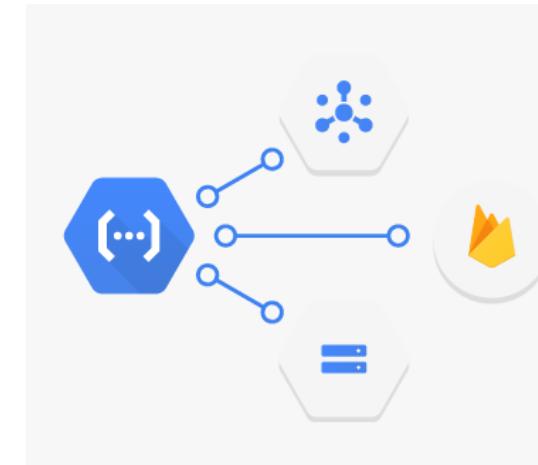
- TCP
- UDP
- ICMP

Note – Supports Ipv4 only

Every VM Instances belongs to a network.

Default network is used if none selected...

Legacy and Subnets....



GCP Professional Cloud Network Engineer Crash Course

Firewalls as a Resource

- Global Resource
- Control traffic incoming (Priority as well)
- Default allows ingress (Allow Only)

Matches dest. IP CIDR ranges, protocols, ports & target
Tags

- ICMP
- SSH
- RDP

Supports Allows for ingress not Denies (Remember this)

GCP Professional Cloud Network Engineer Crash Course

VPC- Firewall Rules

- Virtual Private Cloud (VPC) firewall rules apply to a given project and network.
- VPC firewall rules let you allow or deny connections to or from your virtual machine (VM) instances based on a configuration that you specify
- Allow or Deny Rules to the Virtual Machines
- Firewall rules are **stateful** and always enforced.
- **VPC Firefall rules are defined at the VPC level and enforced at the instance level.**
- Rules are enforced between networks and VMs.

GCP Professional Cloud Network Engineer Crash Course

Firewalls as a VPC Resource

Always-blocked traffic - GCP always blocks the following traffic.

<https://cloud.google.com/vpc/docs/firewalls>

Firewall rules **cannot** be used to un-block traffic that is always blocked.

Rules are evaluated for **priority**. 0-65535 Default is 1000

GCP Professional Cloud Network Engineer Crash Course

VPC- Firewall Rules

*Every Network has **two Implied FW Rules**.*

- Allow Egress Rules
- Deny Ingress Rules
- (Low Priority)

GCP Professional Cloud Network Engineer Crash Course

Firewalls as a VPC Resource

VPC networks has two implied firewall rules.

Note that these “implied” rules CAN NOT be removed..

- **implied allow egress rule (65535 Priority)**
- **implied deny ingress rule (65535 Priority)**

<https://cloud.google.com/vpc/docs/firewalls>

GCP Professional Cloud Network Engineer Crash Course

VPC- Firewall Rules

Always Blocked Traffic.

- GRE Traffic (Tunnelling)
- Unsupported protocols
- Egress traffic on TCP Port 25 (SMTP)

GCP Professional Cloud Network Engineer Crash Course

VPC- Firewall Rules

Always Allowed Traffic.

- DNS
- DHCP
- Instance Metadata
- NTP

GCP Professional Cloud Network Engineer Crash Course

VPC- Firewall Rule Components

- Priority
- Traffic Direction
- Action
- Target (Instance, tag, service account)
- Source or Destination
- Protocols and Ports
- Enforcement Status

GCP Professional Cloud Network Engineer Crash Course

VPC- Network Tags

- Apply firewall to an instance of a group of instances with tags.

GCP Professional Cloud Network Engineer Crash Course

Subnetworks Benefits

Subnets are ways to group similar or related resources

- If you have a VPN this allows you to target the VPN tunnels To a specific region for better control and performance.
- Benefit where you don't need to know much networking nor layout a network right away.
- Define IP ranges in two ways.
 - ---Auto
 - ---Custom

GCP Professional Cloud Network Engineer Crash Course

Routing

Routing is of course obvious important to route traffic.

- Control flow of data and direct traffic where you want it
- Default Routes work in most case but if you need a custom route that you can do as well

GCP Professional Cloud Network Engineer Crash Course

Firewalls (TAGS)

- Tags are needed to know for exam
- Used to identify routes and firewall rules for VMs.
- Tags are user defined
- Not limited to topology like an IP address.
- 64 tags to an instance
- Console, gcloud and API
- `gcloud compute instances add-tags Instance1 --tag1 tag2`
- <https://cloud.google.com/vpc/docs/add-remove-network-tags>

GCP Professional Cloud Network Engineer Crash Course

Subnet Notes for exam

- E.G - if you want to keep instances in your testing and production systems from talking to one another except through external IPs, you can put the instances in different networks.
- Instances in different networks are completely isolated and can have overlapping address ranges. (Comms across networks is only possible through external public IP space)
- Comms over external IP space requires security investments but also can incur additional costing (Egress)

GCP Professional Cloud Network Engineer Crash Course

Subnet Notes Continued

- Each instance created within a subnetwork gets assigned an IPv4 address from that subnetwork's range.
- Google App Engine Flexible Environment: Supported only on auto subnetwork networks. Cannot be deployed in a custom subnet networks.

Test Tip



Firewall rules cannot be used to un-block traffic that is always blocked.

Firewall rules can use tags to filter traffic for logs, etc.

Rules are evaluated for priority. 0-65535 Default is 1000

Test Tip



You can add a subnet to a region of an existing VPC network.

The primary IP range of this new subnet cannot overlap the IP range of existing subnets in the current network, in peered VPC networks, or in on-premises networks connected via VPN or Interconnect.

Test Tip



You can optionally assign a secondary IP range to the subnet for use with Alias IP.

The secondary IP range also cannot overlap the IP ranges of existing connected subnets.

Test Tip



CIDR Blocks

Expanding a subnet? Yes.
You can expand the IP range of a
subnet. **You cannot shrink it.**

Test Tip

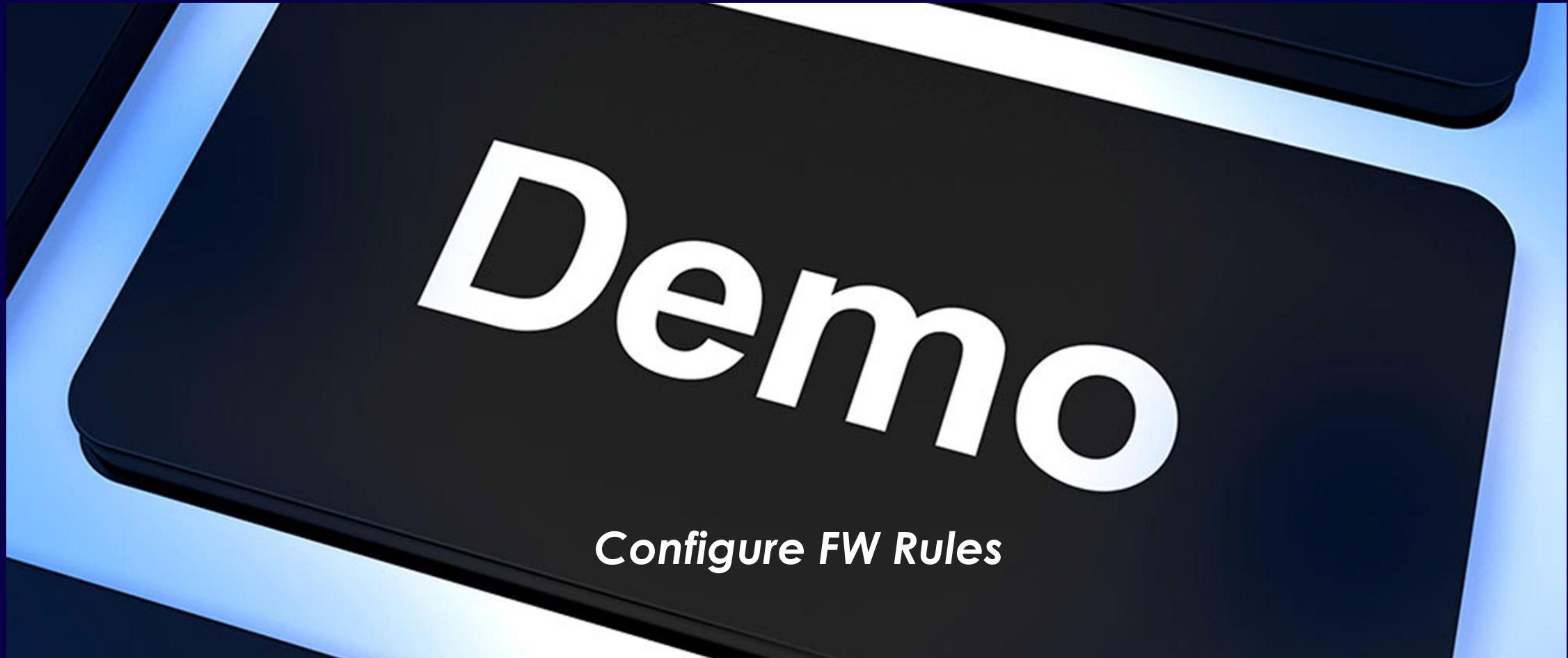


External IPs

Know the two types of external IP addresses

- Regional
- Global

GCP Professional Cloud Network Engineer Crash Course





Configuring Routing

Tasks

GCP Professional Cloud Network Engineer Crash Course

Routing

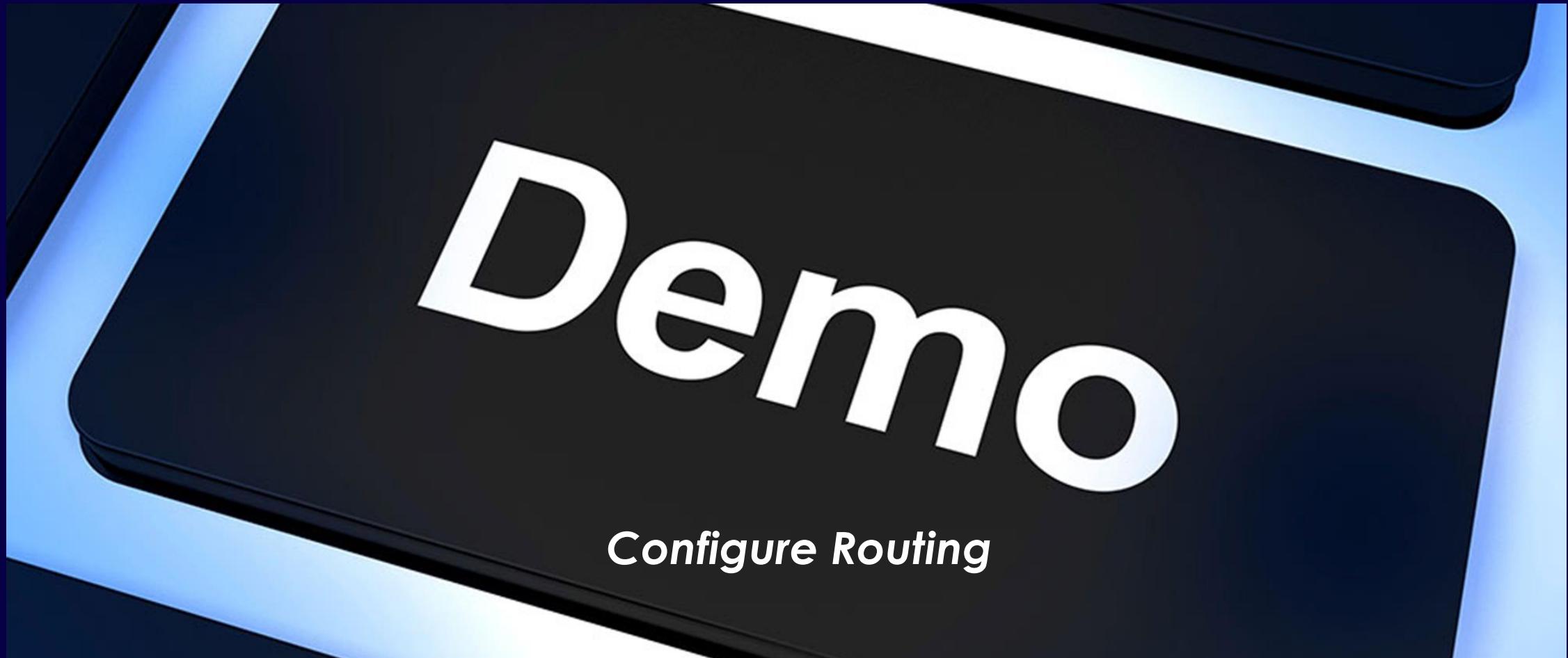
- Cloud Router
- Internal
- External
- Static
- Dynamic
- NAT



Configuring internal static/dynamic routing

Demo

GCP Professional Cloud Network Engineer Crash Course

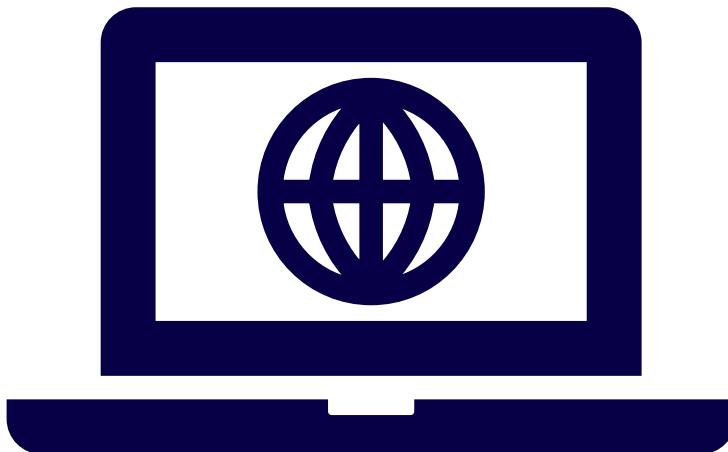




Configure NAT

Demo

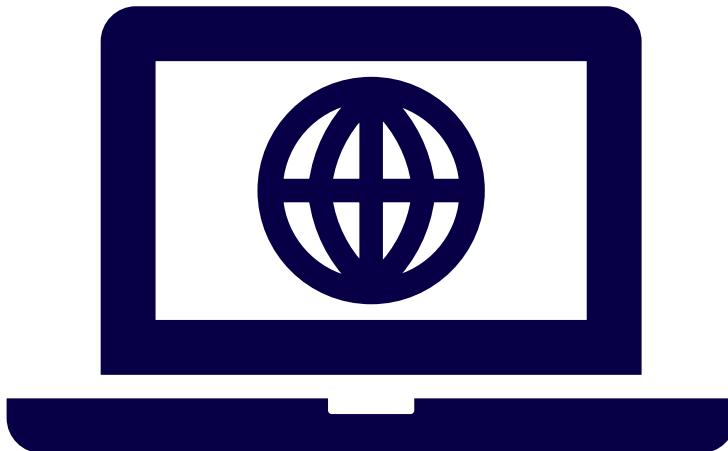
Cloud NAT



Cloud NAT is a distributed, software-defined managed service. **It's not based on proxy VMs or appliances.**

- Cloud NAT allows **outbound** and established inbound responses to those connections
- Cloud NAT works for the VM's network interface's **primary IP address and alias IP address** provided that the network interface doesn't have an external IP address assigned to it, in which case its routed through internet gateway.

Cloud NAT



- *Important: Cloud NAT does not implement inbound connections from the internet.*
- DNAT is only performed for packets that arrive as responses to outbound packets.
- Cloud NAT gateway is associated with a single VPC network, region, and Cloud Router

Bastion Hosts



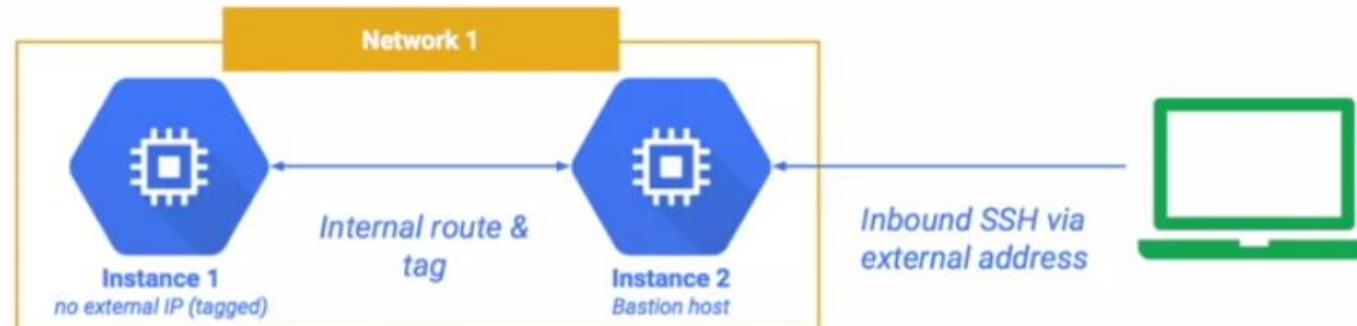
Bastion Hosts are used for connecting to your VMS in Compute Engine or to scale your access to your **SSH based instances (Linux)**

Connecting with an External IP --- Bastion Hosts

Why.. Perhaps you need to scale with SSH(Limit by SSH and CIDR)

You could also connect with a Site to Site VPN

You could also use a NAT Gateway (DNAT)...



Bastion Hosts or Cloud NAT?

Why Bastion for Hosts over Cloud NAT for SSH?

- The bastion host is used for incoming access to GCP (Or any Site)
- NAT instance is for providing outgoing access to the instance you select (Example: Compute Engine instances can initiate internet connection through NAT instance)
- A NAT (Network Address Translation) instance can be similar to a bastion host in the sense the instance lives in your public subnet.
- A NAT instance, however, allows your private instances outgoing connectivity to the Internet, while at the same time blocking inbound traffic from the Internet



Configuring and maintaining Google Kubernetes Engine clusters.

GKE

Basics

- Kubernetes Engine is a managed environment for deploying containerized applications
- Serves fast efficient docker format container deployments with portability
- Before you deploy a workload on a KE cluster, package the workload into a container.



Kubernetes Engine Beyond the Basics

Clusters

- A cluster is a set of computers working as an instance managed by Kubernetes.
- Clusters are managed by Kubernetes which is an orchestrator which manages jobs (processes or pods)
- Regional clusters have masters and these nodes spread across 3 zones.
- Default Three Nodes in a cluster.

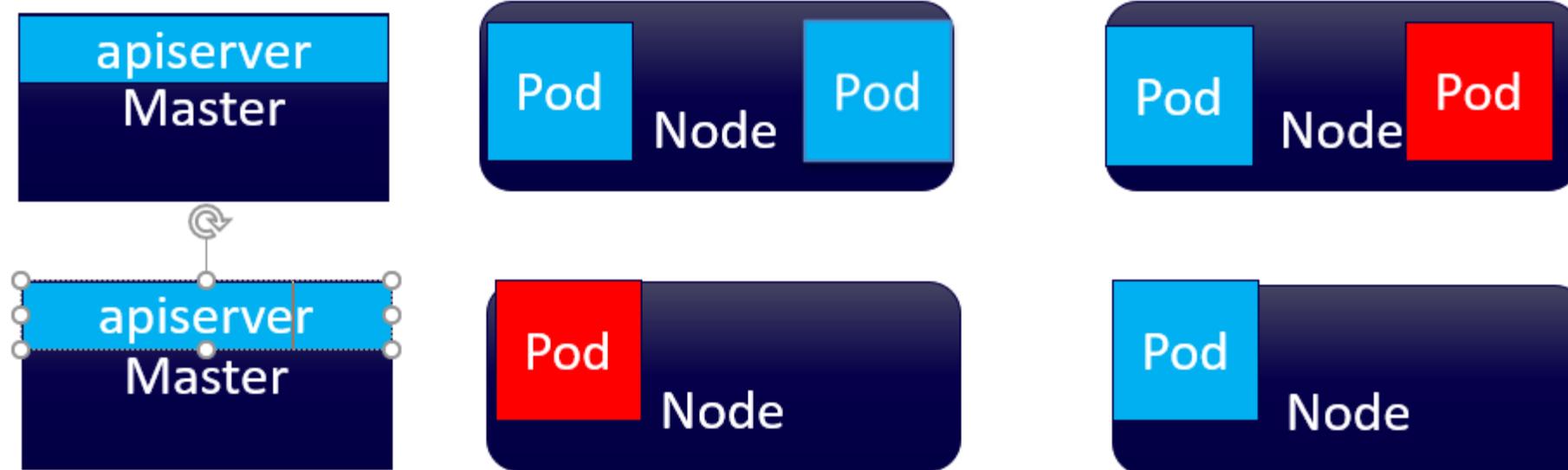
Kubernetes Engine Beyond the Basics

Pods

- Job
- Multiple Containers
- Shares networking and storage from node
- Similar to a VM
- Defined by YAML files

Kubernetes Engine Beyond the Basics

Cluster running a deployment of pods.



Kubernetes Engine Beyond the Basics

Pods

- Defined by a YAML Metadata
- Unique Namespace
- IP
- Ports
- Stores on persistent storage

```
apiVersion: v2.1
kind: Pod
metadata:
  name: demoapp
spec:
  replicas: 2
  containers:
    - name: demoapp
      image: demoapp1
    - name: nginx-ssl
      image: nginx
      ports:
        - containerPort: 80
        - containerPort: 443
```

Kubernetes Engine Beyond the Basics

Deployments

- Defined in YAML
- Unique Namespace
- IP
- Ports
- Stores on persistent storage

```
apiVersion: v2.1
kind: Deployment
metadata:
  name: demoapp
spec:
  containers:
    - name: demoapp
      image: demoapp1
    - name: nginx-ssl
      image: nginx
  ports:
    - containerPort: 80
    - containerPort: 443
```

Kubernetes Engine Beyond the Basics

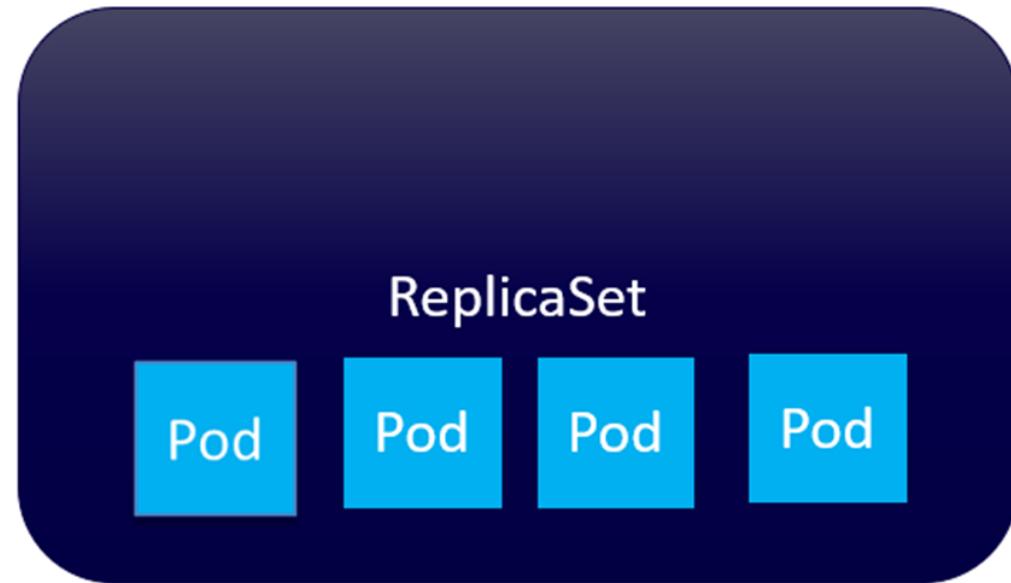
```
apiVersion: v2.1
kind: Deployment
metadata:
  name: demoapp
spec:
  containers:
    - name: demoapp
  ReplicaSet
    - replicas: 4
    - selector:
      - app: demoapp
```

Deployments

- Monitors and clears/fixes issues.
- ReplicaSet

Kubernetes Engine Beyond the Basics

Deployment of pods.



GCP Professional Cloud Network Engineer Crash Course

Kubernetes Engine Container Services

Service	Why Use
Google Container Registry	Easy to store and access your private Docker images in GCP. Push and Pull images.
Google Cloud Build	Deploy your containers on Kubernetes Engine without needing to setup authentication.
Google Source Repositories	A single place for your team to store, manage, and track code. Private Github

GCP Professional Cloud Network Engineer Crash Course

Why use GKE?

Workload portability

- Run in many environments, across cloud providers
- Implementation is open and modular

Rolling updates

- Upgrade application with zero downtime

Autoscaling

- Automatically adapt to changes in workload

GCP Professional Cloud Network Engineer Crash Course

	Kubernetes Engine	App Engine Std	App Engine Flex
Language	Any	Version Centric Java, Python, Go, PHP, Node.js, etc.	Any
Service Model	Hybrid	PaaS	PaaS
Use Case	Containers	Web & Mobile	Web and Mobile container based.

App Engine or Kubernetes Engine?



Test Tips

- Container registry provides an easy to store features and secure access to your private Docker images in GCP.
- Kubernetes Engine is a container orchestration service hosted in GCP

GCP Professional Cloud Network Engineer Crash Course





Configure GKE Cluster Network Policy

Network Policy

GCP Professional Cloud Network Engineer Crash Course





Configure GKE Cluster Network Policy

GKE Networking

GCP Professional Cloud Network Engineer Crash Course





2.4 Configuring and managing firewall rules.

Demo

GCP Professional Cloud Network Engineer Crash Course

Firewall Rules

- Service accounts
- Tags
- Priority
- Network protocols
- Ingress and egress rules
- Firewall logs



Service Accounts

What is a Service account

GCP Professional Cloud Network Engineer Crash Course

- By default, all projects come with the Compute Engine default service account.
- When you start a new instance using gcloud, the default service account is enabled on that instance.
- Apart from the default service account, all projects come with a Google APIs service account, identifiable using the email:
- {project-number}@cloudservices.gserviceaccount.com
- ***Service Accounts management is under IAM & admin section***

GCP Professional Cloud Network Engineer Crash Course



For server-to-server interactions, first create a service account for your project in the API Console



Then your application prepares to make authorized API calls by using the service account's credentials to request an access token from **the OAuth 2.0 auth server**.



Application can now use the access token (Google APIs)



Key Formats --- Json or p12 formats

GCP Professional Cloud Network Engineer Crash Course

Some notes to consider

- When you use the Marketplace to install an application for your domain, the required permissions are automatically granted to the application.
- You do not need to manually authorize the service accounts
- Enable domain-wide delegation for an existing service accounts

GCP Professional Cloud Network Engineer Crash Course

```
{  
  "type": "service_account",  
  
  "project_id": "myproject",  
  
  "private_key_id": "e5703451d59c7f115ddd17122a9e8824",  
  
  "private_key": "-----BEGIN PRIVATE KEY-----  
  
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCGGPVstF25mezS  
  
SRIQ+jW0neRqEaCi3800d5Sm5F36cq2vTl9kFkahz4zmQiyNqgyBayQbipHJxVV0  
  
feI65nh+BXj4nX2ZC1vLGRllcRwzauW/58wcMAtaTPRstXwk/LkJURG1kISF+kD  
  
p3bD6VzpE5njt396jy0g7q/Mlh/gGNzTS05BsWHl4+iurtlqCzB5XKiKpDf9CC8  
  
sa/tAvex1mCuUgjZKcMMpqSOuVVFQeyk9xx6TO3GbQfYvHPwpZBrEY14Aplw2Ikg  
  
4qiQHBVSBACA9LHRTRHYGmwvrAYx7sWQk8WI9Q/oN5xzZOp5rrWJGI1XzlryLKL  
  
-----END PRIVATE KEY-----
```

Compute Engine default service account

DETAILS PERMISSIONS KEYS METRICS LOGS

Keys

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the [Workload Identity Federation](#).

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using [organization policies](#).
[Learn more about setting organization policies for service accounts](#)

ADD KEY ▾

Type	Status	Key	Key creation date	Key expiration date	⋮
PKCS8	Active	90075149a70e42e76f02f4bb392c425e0a3bb63b	Jul 20, 2021	Dec 31, 9999	

GCP Professional Cloud Network Engineer Crash Course

Some notes to consider

- Users are authenticated with? “**Email and Password**”
- Service accounts are authenticated with? “**Key file**”
- Consider proper storage of the keys.
- Service Accounts management is under IAM & admin section
- Service Accounts are granted access based on both their scope and IAM.
- Scopes are used to determine if the authenticated identity is authorized for the task.

GCP Professional Cloud Network Engineer Crash Course



Edit - gives you just possibility
to change Service Account
Description



Delete - deletes the Service
Account



Create Key(s) - this furnishes
new key / file.



Modify Roles - assigned to
Service Account.

Some common operations around service accounts

GCP Professional Cloud Network Engineer Crash Course

Some common operations around service accounts

- Other users or service accounts cannot impersonate a service account.
- Service Accounts are not members of the Google Workspace domain (user accounts)
- Users need to be granted **serviceAccountUser** role to be able to use service accounts are both a member (who) and a resource (what)
- Services accounts are granted permissions to a resource (what)
- Users are granted the **serviceAccountUser** role (who)

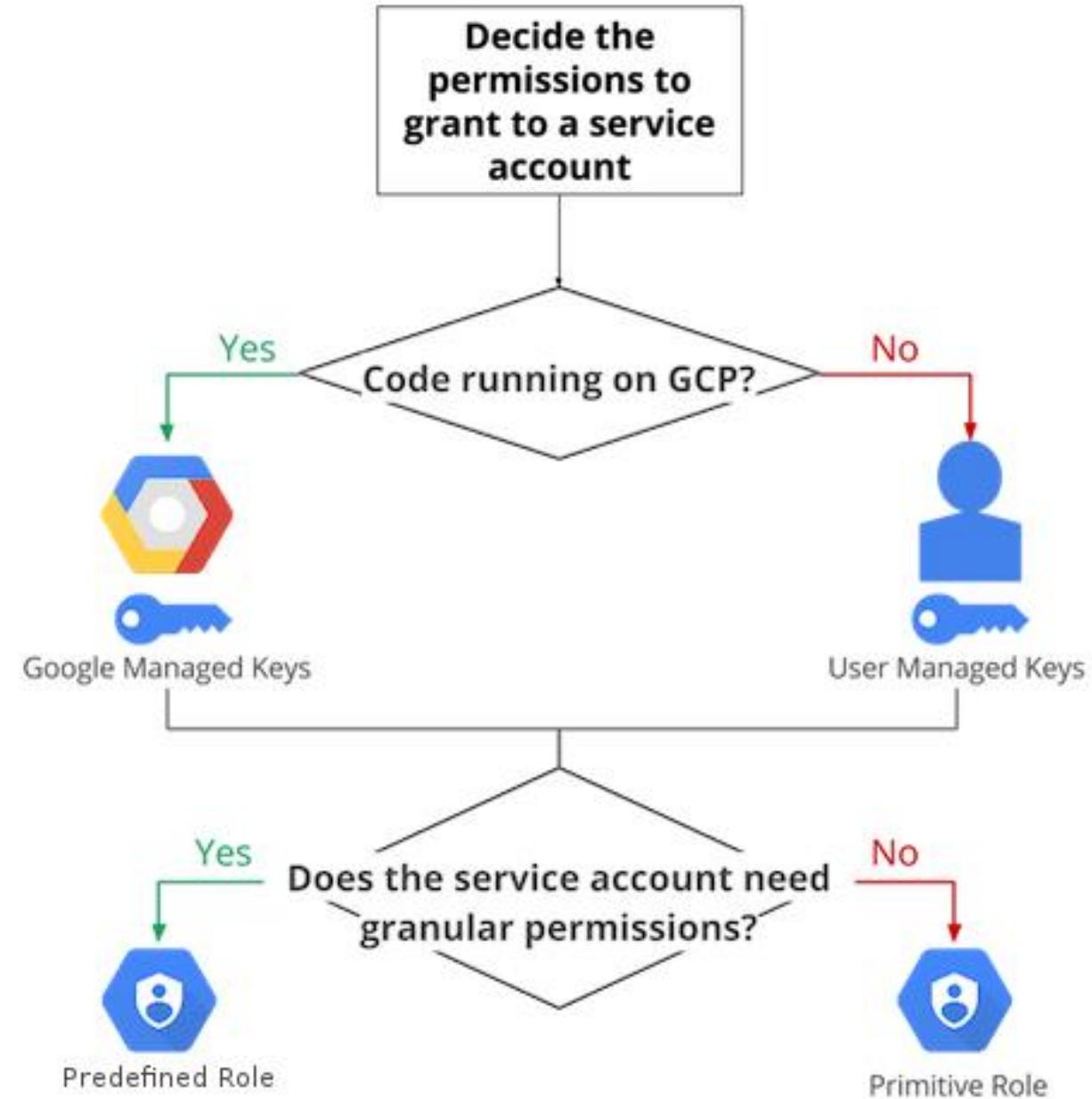
GCP Professional Cloud Network Engineer Crash Course

Service Account Scopes

- Legacy Method of granting service account permissions for individual instances.
- Determines permissions for that instance
- Default Service Accounts will use **scopes**
- Custom Service Accounts will use **IAM Roles**

GCP Professional Cloud Network Engineer Crash Course

Google Provided Decision Tree





Test Tips

- Services account questions come up frequently on the exam so please get to know scopes, keys and types.
- Service accounts are both a member and a resource.
- Service accounts are granted permissions to resources.
- Users are granted the serviceAccountUser role.



Priority

FW Rule Priority need to know

GCP Professional Cloud Network Engineer Crash Course

Firewall Rules - Priority

- You can specify the order that a rule will be applied within a network. Rules with lower numbers get prioritized first.
- Default is 1000.

GCP Professional Cloud Network Engineer Crash Course

Firewall rules for network default

Filter Enter property name or value									?	☰
Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Logs	Hit count	?	
default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	Off	-	▼	
default-allow-internal	Ingress	Apply to all	IP ranges: 10.0.0.0/16	tcp:0-65535 udp:0-65535 icmp	Allow	65534	Off	-	▼	
default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	Off	-	▼	
default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	Off	-	▼	

DONE



Tags and Priority

Demo

GCP Professional Cloud Network Engineer Crash Course





Firewall Logs

Demo

GCP Professional Cloud Network Engineer Crash Course





2.4 Configuring and managing firewall rules.

Demo



Whiteboard – Putting it all Together

Discussion and Review

Google Cloud Digital Leader

- *Let's review what we covered in this section*



Whiteboard



Section Summary

Section 2 : Implementing a Google Cloud Virtual Private Cloud (VPC)



2

Section

Section Summary

- Cloud VPN and Cloud Interconnect are normally used to connect GCP resources to on-premise resources.
- A shared VPC is normally used when you need to centrally manage access to a host project from several service projects, which is not the case here.
- VPC Network Peering enables you to connect VPC networks so that workloads in different VPC networks can communicate internally and traffic stays within Google's network and doesn't traverse the public internet.
- Private Google Access is enabled on a per-subnet basis and you must use a VPC network.
- Google Cloud Platform (GCP) has a wealth of best practices for network security. Get to Know these.
- The Domain Name System Security Extensions (DNSSEC) is a feature of the Domain Name System (DNS) that authenticates responses to domain name lookups
- Google Cloud maintains the following traffic as always blocked traffic - GRE Traffic (Tunnelling), Unsupported, protocols and Egress traffic on TCP Port 25 (SMTP)
- Bastion Hosts are used for connecting to your VMs in Compute Engine or to scale your access to your SSH based instances (Linux)

Section Review Questions

Section 2 : Implementing a Google Cloud Virtual Private Cloud (VPC)



Review Questions

Your new customer is collaborating with another company to build an application on Compute Engine. The customer is building the application tier in their GCP Organization, and this partner company is building the storage tier in a different GCP Organization. This is a 3-tier web application. Communication between portions of the application must not traverse the public internet by any means. Which connectivity option should be implemented? (Select One)

- VPC Peering
- Shared VPC
- Cloud VPN
- Cloud Interconnect

Review Questions

Your new customer is collaborating with another company to build an application on Compute Engine. The customer is building the application tier in their GCP Organization, and this partner company is building the storage tier in a different GCP Organization. This is a 3-tier web application. Communication between portions of the application must not traverse the public internet by any means. Which connectivity option should be implemented? (Select One)

- VPC Peering
- Shared VPC
- Cloud VPN
- Cloud Interconnect

Review Questions

Which of the following traffic types are always blocked by Google?
(Select Two)

- GRE Traffic (Tunnelling)
- Supported protocols
- Egress traffic on TCP Port 25 (SMTP)
- Ingress traffic on TCP Port 25 (SMTP)

Review Questions

Which of the following traffic types are always blocked by Google?
(Select Two)

- GRE Traffic (Tunnelling)
- Supported protocols
- Egress traffic on TCP Port 25 (SMTP)
- Ingress traffic on TCP Port 25 (SMTP)



Section 3 : Configuring Network Access

Understanding the domain testable objectives

Domain Overview

- Configuring Load Balancing
- Configure Cloud CDN

3.1 Configuring load balancing.

Options and demo

Section Overview

- Creating backend services
- Firewall and security rules
- HTTP(S) load balancer
- TCP and SSL proxy load balancers
- Network load balancer
- Internal load balancer
- Session affinity
- Capacity scaling

GCP Professional Cloud Network Engineer Crash Course

Load Balancing

The screenshot shows the GCP Network Services Load Balancing configuration interface. The left sidebar lists various network services: Network services, Load balancing (selected), Cloud DNS, Cloud CDN, Cloud NAT, Traffic Director, Service Directory, Cloud Domains, and Private Service Connect. The main area is titled "Create a load balancer" and contains three configuration cards:

- HTTP(S) Load Balancing**: Layer 7 load balancing for HTTP and HTTPS applications. It includes "Configure" (HTTP LB, HTTPS LB (includes HTTP/2 LB)), "Options" (Internet-facing or internal, Single or multi-region), and a "START CONFIGURATION" button.
- TCP Load Balancing**: Layer 4 load balancing or proxy for applications that rely on TCP/SSL protocol. It includes "Configure" (TCP LB, SSL Proxy, TCP Proxy), "Options" (Internet-facing or internal, Single or multi-region), and a "START CONFIGURATION" button.
- UDP Load Balancing**: Layer 4 load balancing for applications that rely on UDP protocol. It includes "Configure" (UDP LB), "Options" (Internet-facing or internal, Single-region), and a "START CONFIGURATION" button.



Creating backend services

Options and demo

GCP Professional Cloud Network Engineer Crash Course

← New HTTP(S) load balancer

Name * ?

Lowercase, no spaces.

- Backend configuration
- Host and path rules
- Frontend configuration
- Review and finalize (optional)

CREATE CANCEL

Backend configuration

Create or select a backend service for incoming traffic. You can add multiple backend services and backend buckets to serve different types of content.

ⓘ Only backend services created for HTTP(S) Load Balancer with Advanced Traffic Management will be visible. Backend services created for the Classic HTTP(S) Load Balancer cannot be used.

DISMISS

Backend services & backend buckets

Filter Type to filter

No matches for ""

CREATE A BACKEND SERVICE **CREATE A BACKEND BUCKET**

CANCEL OK

GCP Professional Cloud Network Engineer Crash Course

Load Balancing

Create backend service

Name * ?
Lowercase, no spaces.

Description

Backend type Instance group

Protocol HTTP ? Named port * http ?

Timeout * 30 seconds ?

Backends

New backend

Instance group *

Port numbers *

Balancing mode ?
 Utilization
 Rate

Maximum backend utilization * 80 % ?

CREATE CANCEL

GCP Professional Cloud Network Engineer Crash Course

← New HTTP(S) load balancer

Load balancers

Name *

Lowercase, no spaces.

Backend configuration

Host and path rules

Frontend configuration

Review and finalize (optional)

CREATE CANCEL

Frontend

Protocol	IP:Port	Certificate	SSL Policy	Network Tier
HTTP	:80	-	-	Premium
HTTP	:80	-	-	Premium

Host and path rules

Hosts	Paths	Backend
All unmatched (default)	All unmatched (default)	oreilly

Backend

Backend buckets

1. oreilly

Storage bucket name Cloud CDN
oreillybucket1 Disabled

GCP Professional Cloud Network Engineer Crash Course





Firewall and security rules

Options and demo

GCP Professional Cloud Network Engineer Crash Course





Load Balancer

Options and demo

GCP Professional Cloud Network Engineer Crash Course

Load Balancing allows us to load balance our traffic in a single region or in multiple regions.

- Managed Service
- Front End Service (IP)

Types of Load Balancing

- Network Load Balancing

- HTTPS Load Balancing

- Cross-Region Load Balancing

- Content-based Load Balancing

- Cloud SSL Proxy

GCP Professional Cloud Network Engineer Crash Course

Types of Load Balancers

- HTTPS
- TCP Proxy
- SSL Proxy
- Internal
- Network

Types of Load Balancing

- Global
- Regional
- Internal
- External
- HTTP/TCP/UDP

GCP Professional Cloud Network Engineer Crash Course

Network Load Balancing

- Network load balancing distributes incoming traffic across multiple instances
 - Supports non-HTTP(S) protocols (TCP/UDP)
 - Can be used for HTTPS traffic when you want to terminate connection on your instances (not at HTTPS load balancer)
- Supports autoscaling with managed instance groups

<https://cloud.google.com/compute/docs/load-balancing/network/>

GCP Professional Cloud Network Engineer Crash Course

Network Load
Balancing

Forwarding
rules consist of...

Name

Region

IP Address
(regional, not
global)

IP Protocol (TCP,
UDP; AH, ESP,
ICMP, SCTP)

Ports

Target-pool or
target-instance

GCP Professional Cloud Network Engineer Crash Course

HTTP(S) Load Balancing

HTTP(S) Load Balancing distributes HTTP(S) traffic among instance groups based on proximity to user or URL or both

<https://cloud.google.com/compute/docs/load-balancing/network/>

Autoscalers can be attached to HTTP(S)load balancers

GCP Professional Cloud Network Engineer Crash Course

HTTP(S) Load Balancing

- HTTP(S) The following resources comprise a load balancer
- Global Forwarding Rule
- Target Proxy (w SSL certificate resource for HTTPS proxy)
- URL map
- Backend Service and Backends
- Health Check
- The load balancer leverages additional resources
- Global IP Address (ephemeral or static)
- One or more Instance Groups

GCP Professional Cloud Network Engineer Crash Course

Global Forwarding

- A global forwarding rule provides a single global IP address for an application
- The rule routes traffic by IP address, port, and protocol to an HTTP or HTTPS target proxy
- A global forwarding rule can only forward to a single port
- Global forwarding rules can only be used by an HTTP(S) load balancer

<https://cloud.google.com/compute/docs/load-balancing/http/global-forwarding-rules>

GCP Professional Cloud Network Engineer Crash Course

Target proxies' route incoming HTTP(requests) based on URL maps and backend service configurations

- HTTPS target proxy terminates client SSL session
- HTTPS target proxies require configured SSL certificate resources

<https://cloud.google.com/compute/docs/load-balancing/http/target-proxies>

GCP Professional Cloud Network Engineer Crash Course

Cloud SSL proxy alt type of load balancing

- non-HTTP(S) traffic

- Performs global load balancing, routing clients to the closest instance with capacity

Cloud SSL proxy advantages

- Intelligent routing

- Reduced CPI load on instances

- Certificate management

- Security patching

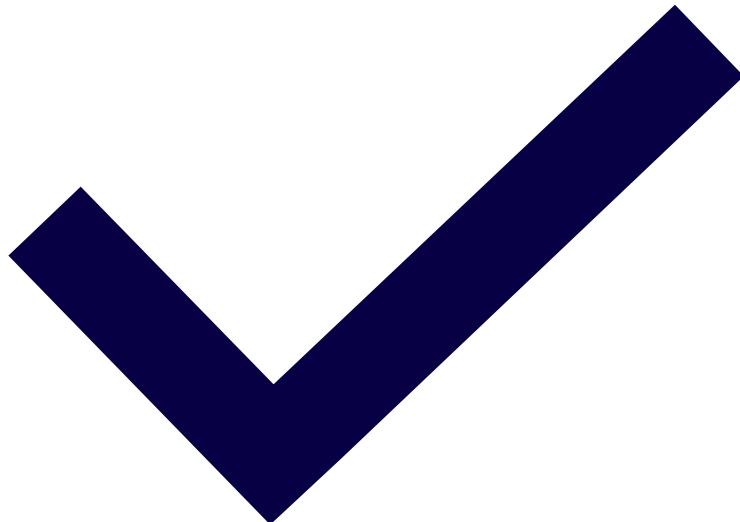
GCP Professional Cloud Network Engineer Crash Course



Cross Region Load Balancing

- HTTP/HTTPS only
- Cross-region using a single global IP address
- Requests routed to the closest region
- Automatically reroutes to next closest once capacity is reached
- Eliminates need for DNS-based load balancing

GCP Professional Cloud Network Engineer Crash Course



Content Based Load Balancing

- HTTP/HTTPS only
- Create multiple backend services to handle content types
- Add path rules to backend services
 - - /video for video services
 - - /static for static content
- Configure different instance types for different content types

GCP Professional Cloud Network Engineer Crash Course

What type of load balancing use cases for exam?

- HTTP, HTTPS, TCP, and SSL load balancing
- Network Load Balancing

<https://cloud.google.com/compute/docs/load-balancing/optimize-app-latency>

GCP Professional Cloud Network Engineer Crash Course

Instance Groups are Managed Groups of VMs

Three Types

1. Unmanaged
2. Managed Instance Group (Zonal)
3. Managed Instance Group (Regional)

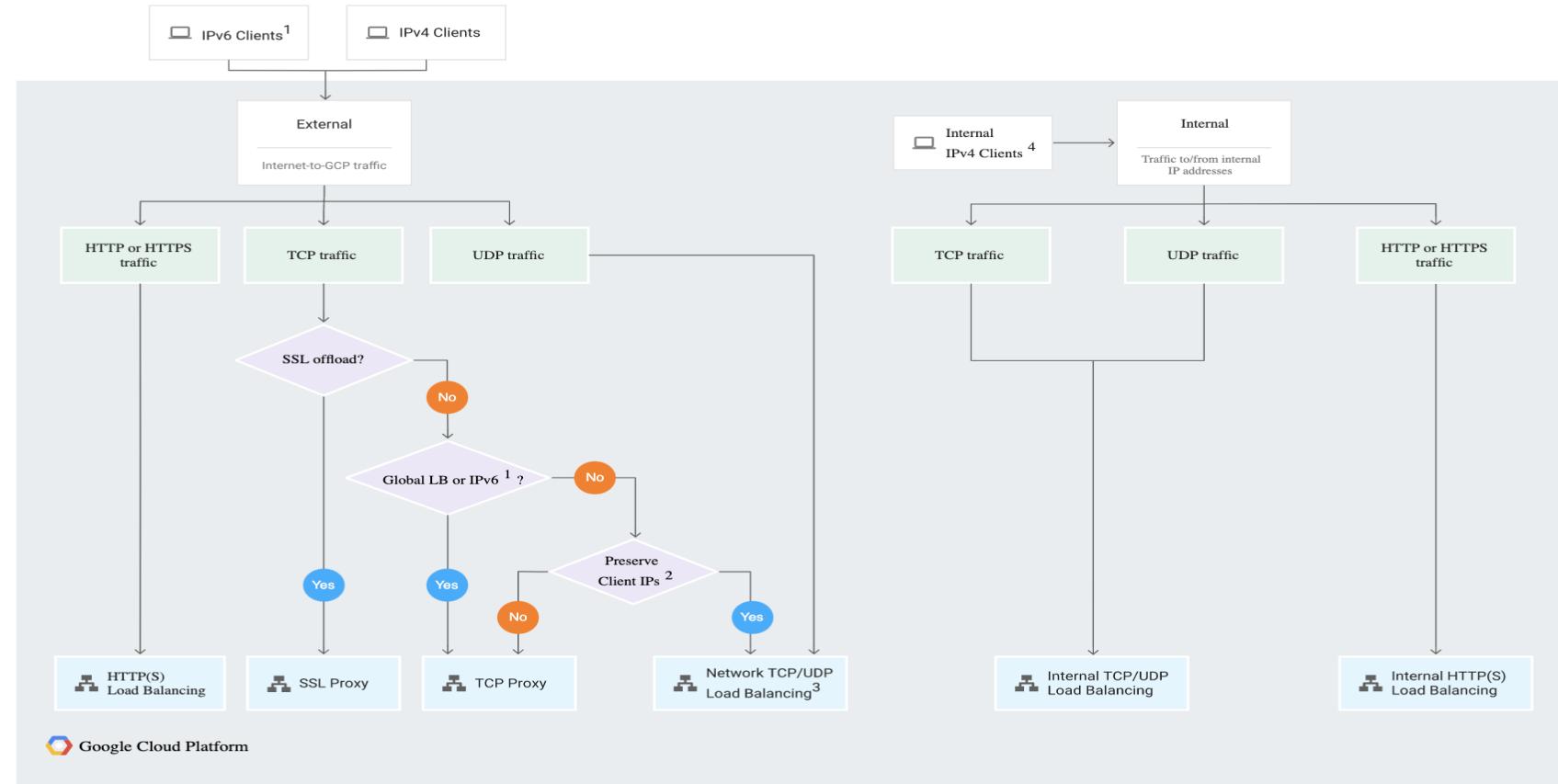
Unmanaged instance groups contain dissimilar instances and wont.

- Autoscaling
- Rolling updates
- Instance creation using instance templates

<https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances>

GCP Professional Cloud Network Engineer Crash Course

GCP Cloud Load Balancing Decision Tree



¹ IPv6 clients are supported for TCP traffic if you configure the load balancer in Premium Tier. IPv6 clients aren't supported for UDP traffic.

² Another reason to choose Network TCP/UDP Load Balancing is if you need to ensure that the load balancer is located in a particular region.

³ Network TCP/UDP load balancers use regional external IP addresses that are accessible by clients anywhere.

⁴ Clients in a VPC network or in a network connected to a VPC network.

Test Tip



Load Balancing

- Google Cloud SSL proxy terminates user SSL (TLS) connections at the global load balancing layer/ then balances the connections across your instances via SSL or TCP.
- Cloud SSL proxy is intended for non-HTTP(S) traffic.
- For HTTP(S) traffic -HTTP(S) load balancing is used

GCP Professional Cloud Network Engineer Crash Course





Session Affinity

What is?

GCP Professional Cloud Network Engineer Crash Course

Session Affinity

- Session affinity is a feature available on load balancers that allows all subsequent traffic and requests from an initial client session to be passed to the same server in the pool.
- Session affinity is also referred to as session persistence, server affinity, server persistence, or server sticky.
- Google Cloud HTTP(S) Load balancer. (IP or Cookie)



3.2 Configuring Cloud CDN.

Content Delivery

GCP Professional Cloud Network Engineer Crash Course

Session Affinity

- Enable and Disable CDN
- Cache Keys
- Cache Validation
- Signed URLs

GCP Professional Cloud Network Engineer Crash Course

Cloud CDN (Content Delivery Network) uses Google's globally distributed edge points of presence to cache external HTTP(S) load balanced content close to your users.

Caching content at the edges of Google's network provides faster delivery of content to your users while reducing serving costs

GCP Professional Cloud Network Engineer Crash Course

Cloud CDN content can be sourced from various types of backends:

- Instance groups
- Zonal network endpoint groups (NEGs)
- Serverless NEGs: One or more App Engine, Cloud Run, or Cloud Functions services
- Internet NEGs for external backends
- Buckets in Cloud Storage

GCP Professional Cloud Network Engineer Crash Course

CDN

Prepare these resources before configuring origin details

- 1. Make sure you have an existing HTTPS load balancer, or create a new HTTPS Load Balancer.
- 2. Create a backend containing a Google Cloud Storage bucket, Instance Group or Ne

Network Services

CDN

Google Cloud CDN uses Google's globally distributed edge points to cache your HTTP(S) content closer to users, resulting in faster delivery and reduced serving costs. To get started, click "Add origin". [Learn more](#)

[ADD ORIGIN](#)

GCP Professional Cloud Network Engineer Crash Course

Configure CDN Origins (Origins = backends)

← Add origin to Cloud CDN

Prepare

2 Configure origin details

Origin type

Use an existing Google Cloud Platform resource

Compute Engine, Kubernetes Engine and/or Google Cloud Storage

Use an external backend

Backends external to GCP

Load balancer

Choose a load balancer as origin. Responses from the origin will be cached by Cloud CDN.

oreillydemolb1

Backend buckets

Cloud CDN will cache responses from the checked backend buckets

Name Cache mode Signed URL

oreilly Unspecified None Configure

Add

Cancel

GCP Professional Cloud Network Engineer Crash Course

A cacheable response is an HTTP response that Cloud CDN can store and quickly retrieve, thus allowing for faster load times.

Not all HTTP responses are cacheable.

Cloud CDN offers three cache modes, which define how responses are cached, whether Cloud CDN respects cache directives sent by the origin, and how cache TTLs are applied.

GCP Professional Cloud Network Engineer Crash Course

Cache Modes

- CACHE_ALL_STATIC
- USE_ORIGIN_HEADERS
- FORCE_CACHE_ALL

<https://cloud.google.com/cdn/docs/caching>

GCP Professional Cloud Network Engineer Crash Course

Cache Keys

- Each cache entry in a Cloud CDN cache is identified by a cache key. When a request comes into the cache, the cache converts the URI of the request into a cache key, and then compares it with keys of cached entries.
- If it finds a match, the cache returns the object associated with that key.
- For backend services, Cloud CDN defaults to using the complete request URI as the cache key

<https://cloud.google.com/cdn/docs/caching#cache-keys>

GCP Professional Cloud Network Engineer Crash Course

Cache Invalidation

- After an object is cached, it normally remains in the cache until it expires or is evicted to make room for new content.
- Manage the expiration time through standard HTTP headers.
- Each invalidation request specifies a path pattern that identifies the object or set of objects that should be invalidated. The path pattern can be either a specific path, such as /cat.jpg, or an entire directory structure, such as /pictures/*.

GCP Professional Cloud Network Engineer Crash Course

Signed URLs

- Cloud CDN signed URLs and signed cookies let you serve responses from Google Cloud's globally distributed caches, even when you need requests to be authorized.
- Cloud CDN signed URLs and signed cookies achieve similar goals: they both control access to your cached content.
- A signed URL is a URL that provides limited permission and time to make a request.

GCP Professional Cloud Network Engineer Crash Course





3.3 Configuring and maintaining Cloud DNS

Domain Name Service

GCP Professional Cloud Network Engineer Crash Course

Cloud DNS

- Managing zones and records
- Migrating to Cloud DNS
- DNS Security (DNSSEC)
- Global serving with Anycast
- Cloud DNS
- Internal DNS
- Integrating on-premises DNS with Google Cloud

GCP Professional Cloud Network Engineer Crash Course

Cloud DNS

- Cloud DNS is a managed DNS service from Google.
- Global Service and maintains a 100% uptime SLA.
- Domain Name Service translates Domains to IP addresses.
- Publish your records without the management overhead
- Private and Public zones.
- Each Domain has its own zone

GCP Professional Cloud Network Engineer Crash Course

Internal IP Addresses DNS Resolution

- Each instance has a hostname that can be resolved to an internal IP address
 - Hostname is the same as the instance name
 - FQDN is *[hostname].c.[project-id].internal*
 - Example: guestbook-test.c.guestbook-151617.internal
- Name resolution is handled by internal DNS resolver

GCP Professional Cloud Network Engineer Crash Course

Additional Notes = DNS for EXAM

Instances with external IP addresses can allow connections from hosts outside of the project

- Users connect directly using external IP address

- Admins can also publish public-DNS records pointing to instance

- Public DNS records are not published automatically

DNS records for external addresses can be published via DNS servers

DNS zones can be hosted using Google Cloud DNS

- Create zone and configure domain DNS to use

- Create, update, remove records manually or via API

GCP Professional Cloud Network Engineer Crash Course

DNSSEC

- The Domain Name System Security Extensions (DNSSEC) is a feature of the Domain Name System (DNS) that authenticates responses to domain name lookups.
- DNSSEC does not provide privacy protections for those lookups but prevents attackers from manipulating or poisoning the responses to DNS requests.
- Both Registry and Registrar must support DNSSEC for the TLD being used.



DNSSEC

Domain Name Service Security

GCP Professional Cloud Network Engineer Crash Course

DNSSEC

Three places where you must enable and configure DNSSEC

- The DNS zone for your domain must serve special DNSSEC records for public keys (DNSKEY), signatures (RRSIG), and non-existence (NSEC, or NSEC3 and NSEC3PARAM) to authenticate your zone's contents.
- The top-level domain (TLD) registry must have a DS record that authenticates a DNSKEY record in your zone. Do this by activating DNSSEC at your domain registrar.

GCP Professional Cloud Network Engineer Crash Course

DNSSEC

Three places where you must enable and configure DNSSEC (Cont)

- Use a DNS resolver that validates signatures for DNSSEC-signed domains

3.4 Enabling other network services.

API, DevOps, Health Checks

GCP Professional Cloud Network Engineer Crash Course



GCP Professional Cloud Network Engineer Crash Course

Other Services

- Health checks for your instance groups
- Canary (A/B) releases
- Distributing backend instances using regional managed instance groups
- Enabling private API access



Putting it all together

Whiteboard

Google Professional Cloud Network Engineer

- *Let's review what we covered in the section*



Whiteboard



Section Summary

Section 3 : Configure Network Access



3

Section

Section Summary

- A global forwarding rule provides a single global IP address for an application
- Network load balancing distributes incoming traffic across multiple instances Supports non-HTTP(S) protocols (TCP/UDP)
- Cloud CDN (Content Delivery Network) uses Google's globally distributed edge points of presence to cache external HTTP(S) load balanced content close to your users.
-

Section Review Questions

Section 3 :Configure Network Access



Review Questions

Connectivity to GCP can be determined by many requirements such as cost, latency, security, infrastructure and numerous other requirements. What solution would select if your organization needed to migrate petabytes of data in a small window over a low latency network. Funding would not be an issue. (Choose One)

- Cloud VPN
- Carrier Peering
- Cloud Interconnect
- Public IP

Review Questions

Connectivity to GCP can be determined by many requirements such as cost, latency, security, infrastructure and numerous other requirements. What solution would select if your organization needed to migrate petabytes of data in a small window over a low latency network. Funding would not be an issue. (Choose One)

- Cloud VPN
- Carrier Peering
- **Cloud Interconnect**
- Public IP

GCP Professional Cloud Network Engineer Crash Course



Welcome to Day Two Content!

We have a lot to cover so let's get started!



Section 4 : Implementing Hybrid interconnectivity

Understanding the domain testable objectives

Domain Overview

- Configuring Cloud Interconnect
- Configure a site-to-site VPN
- Configure Cloud Router for reliability



4.1 Configuring interconnect.

Understanding the connection requirements

GCP Professional Cloud Security Engineer Bootcamp

Interconnections (Partner and Direct)

- Interconnects are similar to peering in that the connections get your network as close as possible to the Google network.
- Interconnects are different from peering in that they give you connectivity using private address space into your Google VPC.
- If you need RFC1918-to-RFC1918 private address connectivity then you'll need to provision either a dedicated or partner interconnect.
- Low Latency, Secure and Costly

GCP Professional Cloud Security Engineer Bootcamp

Interconnections (Partner and Direct)

Cloud Interconnect offers two options to extend your on-premises network to the Google Cloud Platform:

- Dedicated Interconnect
- Direct physical Connection to Google's network.
- Partner Interconnect
- Provides connectivity through a supported service provider.

GCP Professional Cloud Security Engineer Bootcamp

Interconnections (Partner and Direct)

- Partner Interconnect – Equipment and links are owned and managed by service provider.
- Direct Interconnect – Enterprise provides equipment are installed directly to Google
- 10 Gbps or 100 Gbps pipes.
- Virtual attachment circuit over the physical link

GCP Professional Cloud Network Engineer Crash Course





Virtualizing using VLAN attachments

Demo

GCP Professional Cloud Network Engineer Crash Course





Bulk storage uploads

Demo

GCP Professional Cloud Network Engineer Crash Course

Resumable Uploads

- A *resumable upload* allows you to resume data transfer operations to Cloud Storage after a communication failure has interrupted the flow of data
- The gsutil command-line tool uses resumable uploads in the gsutil cp and gsutil rsync commands when uploading data to Cloud Storage.

GCP Professional Cloud Network Engineer Crash Course





4.2 Configuring a site-to-site IPsec VPN

Demo

GCP Professional Cloud Network Engineer Crash Course



Section Summary

Section 4 : Implementing Hybrid Connectivity



Section Review Questions

Section 4 : Implementing Hybrid Connectivity



Review Questions

Connectivity to GCP can be determined by many requirements such as cost, latency, security, infrastructure and numerous other requirements. What solution would select if your organization needed to migrate petabytes of data in a small window over a low latency network. Funding would not be an issue. (Choose One)

- Cloud VPN
- Carrier Peering
- Cloud Interconnect
- Public IP

Review Questions

Connectivity to GCP can be determined by many requirements such as cost, latency, security, infrastructure and numerous other requirements. What solution would select if your organization needed to migrate petabytes of data in a small window over a low latency network. Funding would not be an issue. (Choose One)

- Cloud VPN
- Carrier Peering
- **Cloud Interconnect**
- Public IP



Section 5 : Implementing Network Security

Understanding the domain testable objectives



Domain Objectives

What are the exam objectives covered?

Domain Overview

- Configure IAM
- Configure Cloud Armor Policies
- Configuring third-party device insertion into VPC using multi-nic
- Managing SSH Keys

5.1 Configuring identity and access management (IAM).

IAM Basics, roles,

GCP Professional Cloud Network Engineer Crash Course

- An identity and access management (IAM) service provides administrators with a single place to manage all users and cloud applications.
- An IAM service provides your users with a unified sign-on across all their enterprise cloud applications.
- In Google Cloud the IAM Service is called Cloud IAM



GCP Professional Cloud Network Engineer Crash Course

Identity and Access Management (IAM)

Cloud IAM allows you to manage access control by defining who can do what on which resource.

Who

What

Which
Resource?

GCP Professional Cloud Network Engineer Crash Course

Who

What

Which
Resource?

GCP Professional Cloud Network Engineer Crash Course

Who --- Known Members can be:

- Google Account/Cloud Identity User
- Service Account
- Google Group
- Cloud Identity/G Suite Domain

GCP Professional Cloud Network Engineer Crash Course

Google Account/Cloud Identity User

- Person
- Email

GCP Professional Cloud Network Engineer Crash Course

Service Account

- Account used for machine-to-machine use
- Has a service account email

GCP Professional Cloud Network Engineer Crash Course

Google Group

- ❑ Named collection of Google Accounts
- ❑ Can be service accounts

GCP Professional Cloud Network Engineer Crash Course

Cloud Identity/G Suite Domain

❑ Represents a virtual group of all Google Accounts

GCP Professional Cloud Network Engineer Crash Course

Identifiers

- AllAuthenticatedUsers (Exception Anonymous Users)
- AllUsers

GCP Professional Cloud Network Engineer Crash Course

Who

What

Which
Resource?

GCP Professional Cloud Network Engineer Crash Course

What --- Known Members can do:

- Determined by IAM Role
- Permissions are grouped together in role
- Collection of permissions

GCP Professional Cloud Network Engineer Crash Course

Roles

- ❑ Don't directly grant permissions, grant roles.
- ❑ Roles are bundled permissions
- ❑ Collection of permissions

GCP Professional Cloud Network Engineer Crash Course

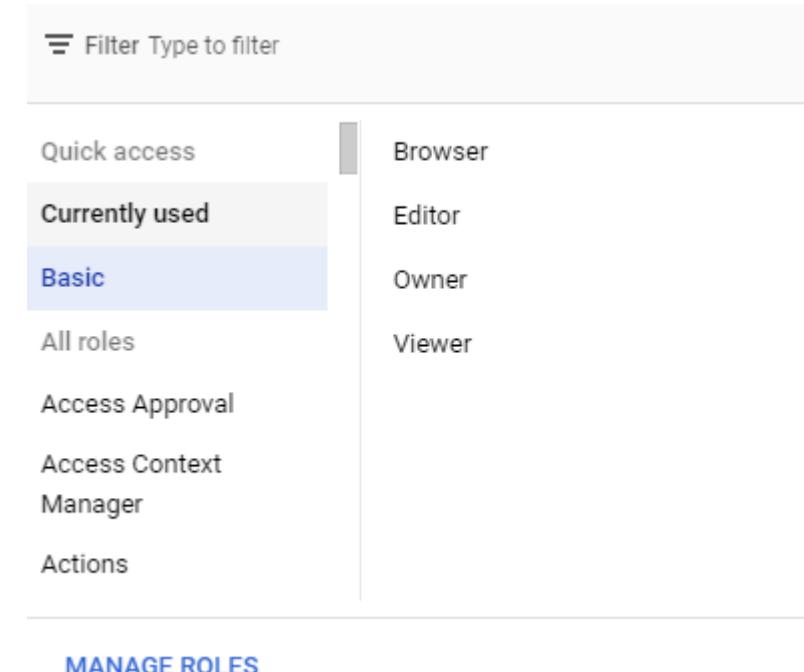
There are three kinds of roles in Cloud IAM:

- Primitive roles*
- Predefined (Curated) roles*
- Custom Roles*

GCP Professional Cloud Network Engineer Crash Course

Primitive Roles:

- The original roles available in the Google Cloud Platform Console.
- These are the **Owner, Editor, and Viewer** roles.
- Assigned by default to projects.
- Primitive roles are quite broad.



A screenshot of the Google Cloud Platform Roles interface. At the top, there is a search bar labeled "Filter Type to filter". Below it, a sidebar on the left lists categories: "Quick access", "Currently used", "Basic" (which is highlighted with a blue background), "All roles", "Access Approval", "Access Context", "Manager", and "Actions". To the right of the sidebar, there is a vertical list of roles: "Browser", "Editor", "Owner" (which is also highlighted with a blue background), and "Viewer". At the bottom of the interface, there is a blue button labeled "MANAGE ROLES".

GCP Professional Cloud Network Engineer Crash Course

Predefined Roles:

- Predefined roles are new IAM roles that give finer-grained access control than the primitive roles
- Updated by Google
- Applied to single services

Role / Member ↑	Name
▶ App Engine Admin (1)	
▶ App Engine Deployer (1)	
▶ App Engine Service Admin (1)	
▶ App Engine Viewer (1)	
▶ BigQuery Data Viewer (1)	
▶ Cloud Build Editor (1)	
▶ Cloud Build Service Account (1)	
▶ Cloud Datastore User (1)	
▶ Cloud Run Admin (1)	
▶ Cloud SQL Admin (1)	
▶ Cloud SQL Viewer (1)	
▶ Compute Admin (2)	
▶ Editor (2)	
▶ Eventarc Admin (1)	
▶ Firebase Admin SDK Administrator Service Agent (1)	

GCP Professional Cloud Network Engineer Crash Course

Custom Roles:

- Provide granular access according to a user-specified list of permissions
- Not Updated by Google
- Finer grained access control

Add members to "GKEClass"

Add members, roles to "GKEClass" project

Enter one or more members below. Then select a role for these members to grant them access to your resources. Multiple roles allowed. [Learn more](#)

New members

devopscourse@gkeclass1.iam.gserviceaccount.com [X](#) [?](#)

Role [Kubernetes Engine Cluster ...](#) Condition [Add condition](#) [?](#)

Get and list access to GKE Clusters.

Role [Editor](#) Condition [Add condition](#) [?](#)

Edit access to all resources.

Role [App Engine Admin](#) Condition [Add condition](#) [?](#)

Full management of App Engine apps (but not storage).

[+ ADD ANOTHER ROLE](#)

Send notification email

This email will inform members that you've granted them access to these roles for "GKEClass"

Your message

Welcome to the Club!

Optional message sent to added members

20 / 500

[SAVE](#)

[CANCEL](#)

GCP Professional Cloud Network Engineer Crash Course

Role Name	Role Title	Description	Resource Type
roles/appengine.appAdmin	App Engine Admin	Read/Write/Modify access to all application configuration and settings.	Project
roles/appengine.serviceAdmin	App Engine Service Admin	Read-only access to all application configuration and settings. Write access to module-level and version-level settings. Cannot deploy a new version.	Project
roles/appengine.deployer	App Engine Deployer	Read-only access to all application configuration and settings. Write access only to create a new version; cannot modify existing versions other than deleting versions that are not receiving traffic.	Project
roles/appengine.appViewer	App Engine Viewer	Read-only access to all application configuration and settings.	Project
roles/appengine.codeViewer	App Engine Code Viewer	Read-only access to all application configuration, settings, and deployed source code.	Project

<https://cloud.google.com/iam/docs/understanding-roles>

GCP Professional Cloud Network Engineer Crash Course

Who

What

Which
Resource?

GCP Professional Cloud Network Engineer Crash Course

Resources:

- Are the components of GCP
- Resources includes Organizations, Folders, Projects and the resources included in them.

Manage resources		+ CREATE PROJECT	+ CREATE FOLDER	MOVE	DELETE
Filter Filter					
<input type="checkbox"/> Name	ID				
<input type="checkbox"/> No organization					
<input type="checkbox"/> GKEClass	gkeclass1				
<input type="checkbox"/> digitalleader	digitalleader-314717				
<input type="checkbox"/> stormwinds123	stormwinds123				
RESOURCES PENDING DELETION					

GCP Professional Cloud Network Engineer Crash Course

Policies and Bindings

- States who has access to what resources
- Enforces access control
- These policies are attached.
- Policies are represented by a policy object.
- Bindings are members attached to a role

Organization policies

Organization policies for project "GKEClass"

Cloud Organization Policies let you constrain access to resources at and below this organization, folder or project. You can edit restrictions on the policy detail page.

Name ↑	ID
Allow extending lifetime of OAuth 2.0 access tokens to up to 12 hours	constraints/iam.allowServiceAccountCredentialLifetimeExtension
Allowed AWS accounts that can be configured for workload identity federation in Cloud IAM	constraints/iam.workloadIdentityPoolAwsAccounts
Allowed Binary Authorization Policies (Cloud Run)	constraints/run.allowedBinaryAuthorizationPolicies
Allowed Destinations for Exporting Resources	constraints/resourcemanager.allowedExportDestinations
Allowed external identity Providers for workloads in Cloud IAM	constraints/iam.workloadIdentityPoolProviders
Allowed ingress settings (Cloud Functions)	constraints/cloudfunctions.allowedIngressSettings
Allowed ingress settings (Cloud Run)	constraints/run.allowedIngress
Allowed Sources for Importing Resources	constraints/resourcemanager.allowedImportSources
Allowed VPC Connector egress settings (Cloud Functions)	constraints/cloudfunctions.allowedVpcConnectorEgressSettings

GCP Professional Cloud Network Engineer Crash Course

Roles are enforced (inheritance) from the top down

Organizations

Folders

Project

Resource



Viewing account IAM assignments

Demo

GCP Professional Cloud Network Engineer Crash Course

Listing grantable roles

- 1.In the Cloud Console, go to the IAM page. Go to the IAM page.
- 2.Click the "Select a project" drop-down menu at the top of the page.
- 3.Select the project or organization for which you want to view roles.
- 4.Click Add.
- 5.Enter the principal's email address, domain, or other identifier in Principals.

GCP Professional Cloud Network Engineer Crash Course

The screenshot shows the Google Cloud IAM Permissions page. At the top, there's a search bar labeled "Search products and resources". Below it, tabs for "PERMISSIONS", "RECOMMENDATIONS", and "HISTORY" are visible. The "PERMISSIONS" tab is selected. On the left, a sidebar titled "Permissions for project" lists "PRINCIPALS" and "ROLES". A modal window titled "Select a project" is open in the center. It contains a search bar "Search projects and folders" and a list of recent projects. The "RECENT" tab is selected, showing two entries: "Google Analytics" (selected) and "GKEClass". Both entries have a star icon and a question mark icon. To the right of the modal, a table for managing permissions is partially visible. The table has columns for "Name", "ID", "Insights", and "Inheritance". Each row has a "Edit" icon. At the bottom of the modal, there are "CANCEL" and "OPEN" buttons.

GCP Professional Cloud Network Engineer Crash Course

Permissions for project "Google Analytics"

These permissions affect this project and all of its resources. [Learn more](#)

View By: [PRINCIPALS](#) [ROLES](#)

[Include Google-provided role grants](#) [?](#)

Filter Enter property name or value ? ☰						
<input type="checkbox"/> Type	Principal ↑	Name	Role	Security insights ?	Inheritance	
<input type="checkbox"/>	Compute Engine default service account	439862965988-compute@developer.gserviceaccount.com	Editor		Edit	
<input type="checkbox"/>	Google APIs Service Agent	439862965988@cloudservices.gserviceaccount.com	Editor		Edit	
<input type="checkbox"/>	firebase-measurement@system.gserviceaccount.com		Editor	4418/4427 excess permissions ▼	Edit	
<input type="checkbox"/>	Joe Techcommanders	holbrookjp@thegcpgurus.com	Owner	4766/4797 excess permissions ▼	Edit	

GCP Professional Cloud Network Engineer Crash Course





Assigning IAM roles to accounts or Google Groups

Demo

GCP Professional Cloud Network Engineer Crash Course

Add a principal to assign

Add principals to "Google Analytics"

Add principals and roles for "Google Analytics" resource

Enter one or more principals below. Then select a role for these principals to grant them access to your resources. Multiple roles allowed. [Learn more](#)

New principals ?

! Enter at least one principal

Select a role ▼

+ ADD ANOTHER ROLE

Conditions Add condition

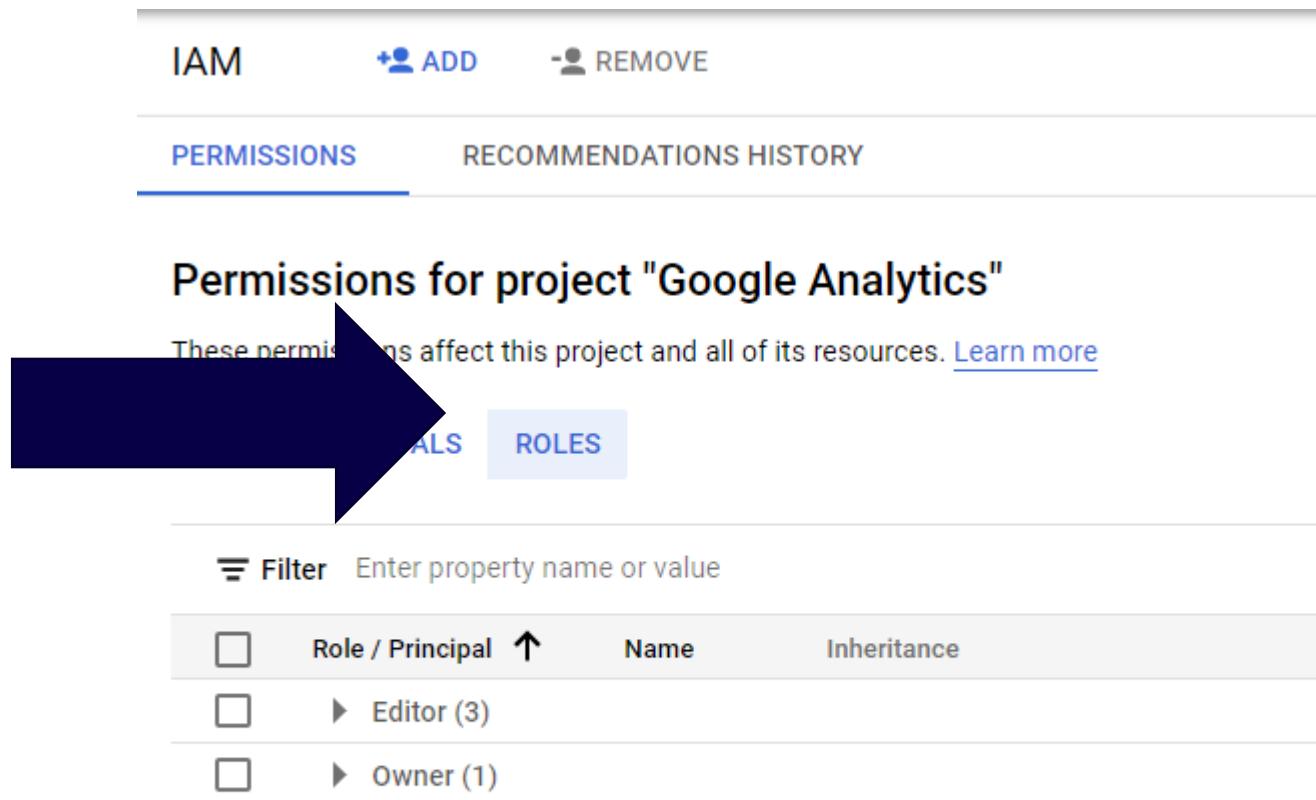
SAVE CANCEL

Add one or more of the following: X

- Google Account email: user@gmail.com
- Google Group: admins@googlegroups.com
- Service account: server@example.gserviceaccount.com
- Google Workspace domain: example.com

GCP Professional Cloud Network Engineer Crash Course

Or Add a role to assign



IAM +
ADD -
REMOVE

PERMISSIONS RECOMMENDATIONS HISTORY

Permissions for project "Google Analytics"

These permissions affect this project and all of its resources. [Learn more](#)

▼ Filter Enter property name or value

ROLE / PRINCIPAL ↑ NAME INHERITANCE

Role / Principal	Name	Inheritance
<input type="checkbox"/> Editor (3)		
<input type="checkbox"/> Owner (1)		



Defining custom IAM roles

Demo

GCP Professional Cloud Network Engineer Crash Course

Select Roles



Google Cloud Platform Google Analytics Search products and resources

IAM & Admin

- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer
- Organization Policies
- Service Accounts
- Workload Identity Federati...
- Labels
- Tags
- Settings
- Privacy & Security
- Identity-Aware Proxy
- Roles**
- Audit Logs

Roles + CREATE ROLE CREATE ROLE FROM SELECTION — DISABLE DELETE

Roles for "Google Analytics" project

A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. [Learn more](#)

Filter Enter property name or value

Type	Title	Used in	Status	⋮
<input type="checkbox"/>	AAM Admin	Dialogflow	Enabled	⋮
<input type="checkbox"/>	AAM Conversational Architect	Dialogflow	Enabled	⋮
<input type="checkbox"/>	AAM Dialog Designer	Dialogflow	Enabled	⋮
<input type="checkbox"/>	AAM Lead Dialog Designer	Dialogflow	Enabled	⋮
<input type="checkbox"/>	AAM Viewer	Dialogflow	Enabled	⋮
<input type="checkbox"/>	Access Approval Approver	Access Approval	Enabled	⋮
<input type="checkbox"/>	Access Approval Config Editor	Access Approval	Enabled	⋮
<input type="checkbox"/>	Access Approval Viewer	Access Approval	Enabled	⋮
<input type="checkbox"/>	Access Context Manager Admin	Access Context Manager	Enabled	⋮
<input type="checkbox"/>	Access Context Manager Editor	Access Context Manager	Enabled	⋮
<input type="checkbox"/>	Access Context Manager Reader	Access Context Manager	Enabled	⋮
<input type="checkbox"/>	Access Transparency Admin	Organization Policy	Enabled	⋮
<input type="checkbox"/>	Actions Admin	Actions	Enabled	⋮

GCP Professional Cloud Network Engineer Crash Course

Select Create Role



Create Role

Custom roles let you group permissions and assign them to principals in your project or organization. You can manually select permissions or import permissions from another role. [Learn more](#)

Title * my new custom role 18 / 100

Description Created on: 2021-12-02 22 / 256

ID * LNUsers

Role launch stage Alpha

+ ADD PERMISSIONS

3 assigned permissions

Filter	Enter property name or value	?	☰
<input checked="" type="checkbox"/>	Permission ↑	Status	
<input checked="" type="checkbox"/>	appengine.applications.get	Supported	
<input checked="" type="checkbox"/>	appengine.applications.update	Supported	
<input checked="" type="checkbox"/>	appengine.instances.delete	Supported	

Some permissions might be associated with and checked by third parties.
These permissions contain the third party's service and domain name in the permission prefix.

GCP Professional Cloud Network Engineer Crash Course

Shows a Custom

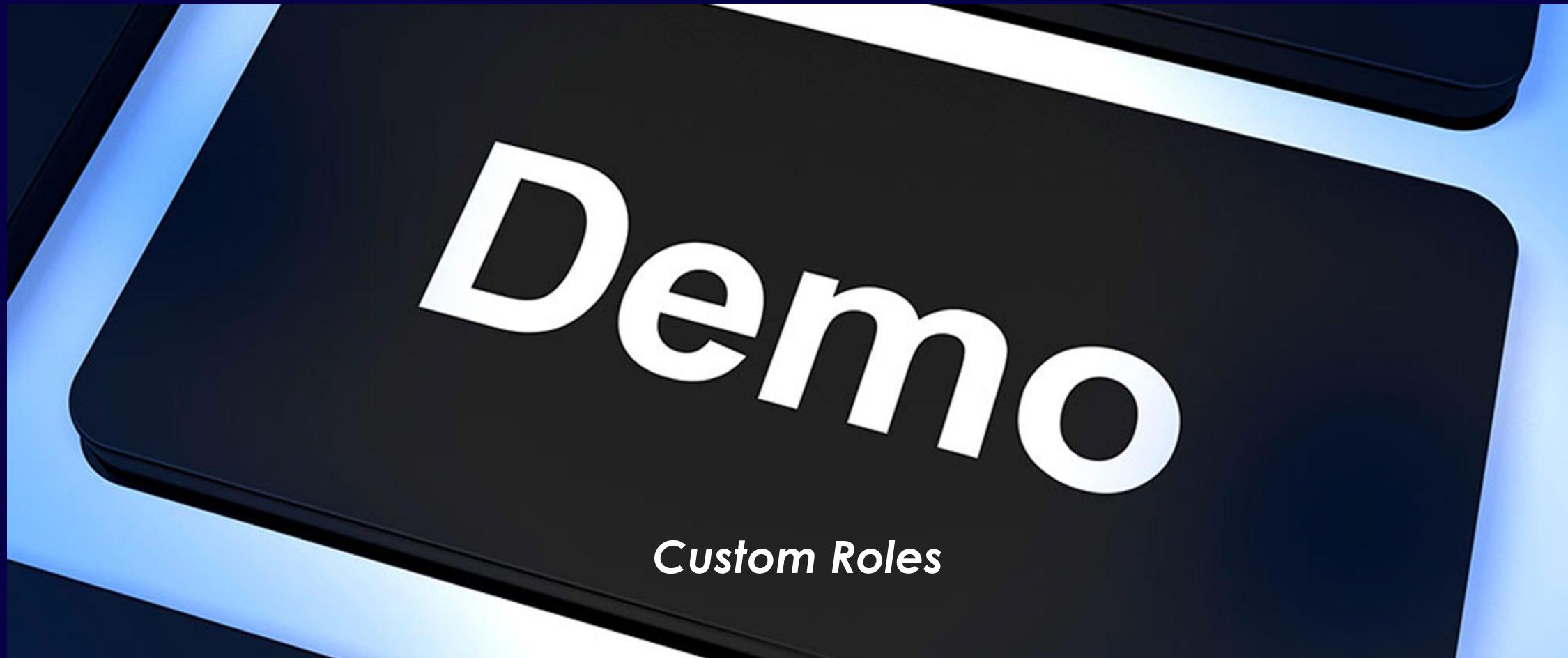
Roles for "Google Analytics" project

A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. [Learn more](#)

Filter Enter property name or value

Type	Title	Used in	Status	⋮
<input type="checkbox"/>	My New Custom Role Oreilly	Custom	Enabled	⋮
<input type="checkbox"/>	AAM Admin	Dialogflow	Enabled	⋮
<input type="checkbox"/>	AAM Conversational Architect	Dialogflow	Enabled	⋮
<input type="checkbox"/>	AAM Dialog Designer	Dialogflow	Enabled	⋮
<input type="checkbox"/>	AAM Lead Dialog Designer	Dialogflow	Enabled	⋮

GCP Professional Cloud Network Engineer Crash Course





Using pre-defined IAM roles

Demo

GCP Professional Cloud Network Engineer Crash Course

Predefined Roles:

- Predefined roles are new IAM roles that give finer-grained access control than the primitive roles
- Updated by Google
- Applied to single services

<input type="checkbox"/> Role / Member ↑	Name
<input type="checkbox"/>	▶ App Engine Admin (1)
<input type="checkbox"/>	▶ App Engine Deployer (1)
<input type="checkbox"/>	▶ App Engine Service Admin (1)
<input type="checkbox"/>	▶ App Engine Viewer (1)
<input type="checkbox"/>	▶ BigQuery Data Viewer (1)
<input type="checkbox"/>	▶ Cloud Build Editor (1)
<input type="checkbox"/>	▶ Cloud Build Service Account (1)
<input type="checkbox"/>	▶ Cloud Datastore User (1)
<input type="checkbox"/>	▶ Cloud Run Admin (1)
<input type="checkbox"/>	▶ Cloud SQL Admin (1)
<input type="checkbox"/>	▶ Cloud SQL Viewer (1)
<input type="checkbox"/>	▶ Compute Admin (2)
<input type="checkbox"/>	▶ Editor (2)
<input type="checkbox"/>	▶ Eventarc Admin (1)
<input type="checkbox"/>	▶ Firebase Admin SDK Administrator Service Agent (1)

GCP Professional Cloud Network Engineer Crash Course



Demo

Predefined Roles



5.2 Configuring Cloud Armor Policies

Cloud Armor basics and policies

GCP Professional Cloud Network Engineer Crash Course

Cloud Armor

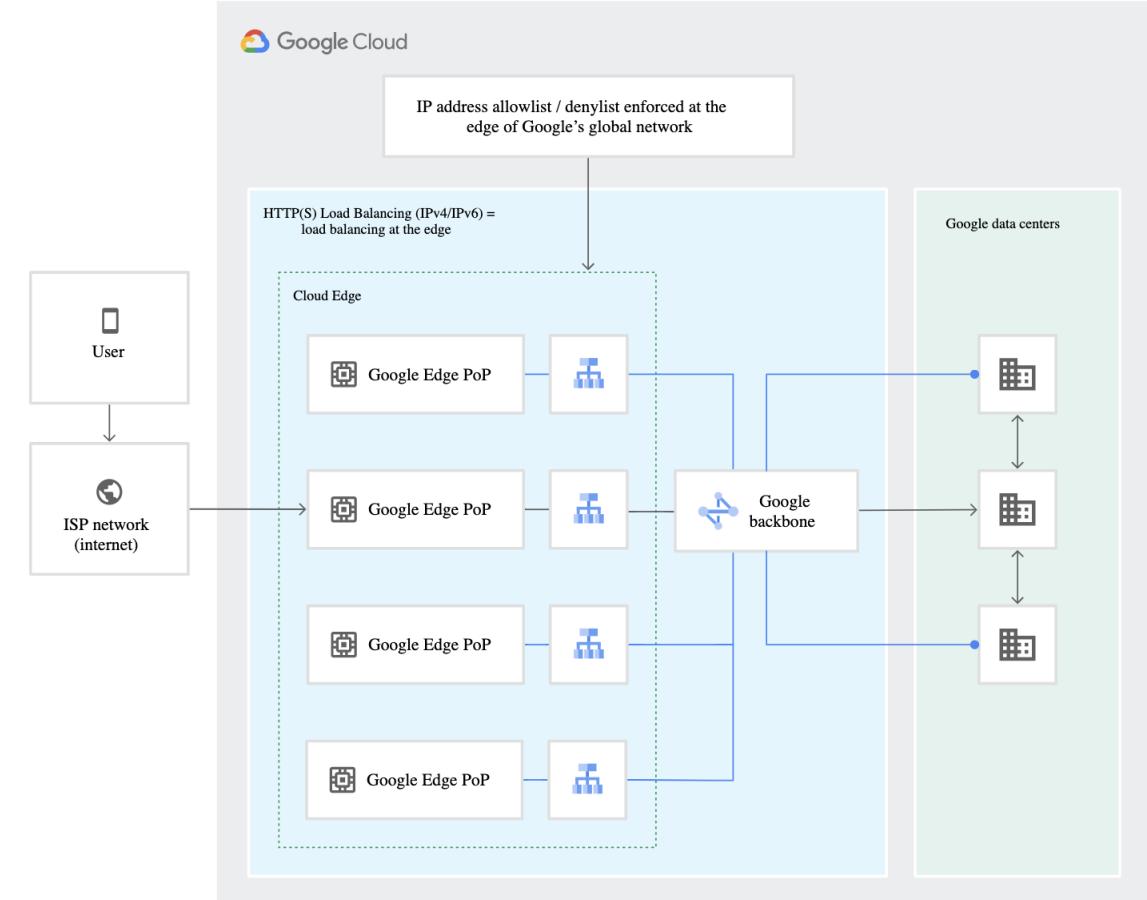
Google Cloud Armor helps protect the **applications from multiple types of threats**, including distributed denial-of-service (DDoS) attacks and application attacks like cross-site scripting (XSS) and SQL injection (SQLi).

- Google Cloud Armor provides protection only to applications running **behind an external load balancer**, and several features are only available for external HTTP(S) and TCP/SSL Proxy load balancers.
- Use Rules to mitigate attacks and has a “**Preview Mode**” to understand how the rules will affect your deployment.

GCP Professional Cloud Network Engineer Crash Course

Cloud Armor

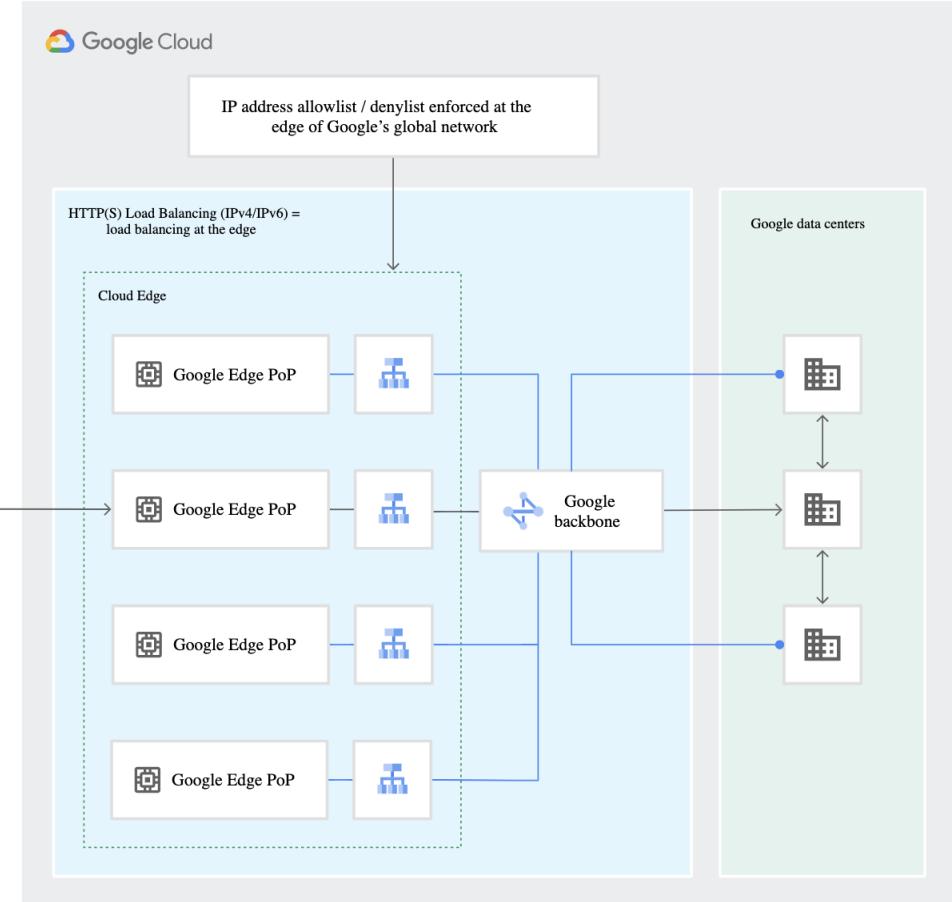
- Layer 7 filtering
- Cloud Armor supports applications deployed on Google Cloud, in a hybrid deployment, or in a multi-cloud architecture.
- Cloud Armor is implemented at the edge of Google's network in **Google's points of presence (PoP)**.



GCP Professional Cloud Network Engineer Crash Course

Cloud Armor

- Traffic is filtered similar to a firewalls allow and deny rules/lists.



GCP Professional Cloud Network Engineer Crash Course

Cloud Armor

The screenshot shows the Google Cloud Platform Network Security interface. On the left, there's a sidebar with icons for Network Security, Cloud Armor (which is selected and highlighted in blue), SSL policies, and Cloud IDS. The main content area is titled "Cloud Armor". A prominent yellow warning banner at the top states: "Cloud Armor Adaptive Protection is now generally available. To receive access to full Adaptive Protection alerts, attack signatures, and mitigating rules, you must enroll this project in Managed Protection Plus. Unless you subscribe to Managed Protection Plus and enroll this project, Adaptive Protection alerts of potential attacks will continue to be generated, but the alerts will no longer contain the attack signature and you will not receive mitigating rules. This change will go in effect on Jan 11, 2022." Below the banner, there are three tabs: POLICIES (which is underlined in blue), ADAPTIVE PROTECTION, and MANAGED PROTECTION. A large callout box on the right is titled "Network security" and "Security policies". It explains that security policies let you control access to Google Cloud Platform resources at your network's edge and can protect non-CDN HTTP(S) load balancers. A "Create policy" button is at the bottom of this box.

GCP Professional Cloud Network Engineer Crash Course





IP-based access control

Cloud Armor

GCP Professional Cloud Network Engineer Crash Course

Cloud Armor

- Google Cloud Armor security policies are available only for backend services behind an external HTTP(S) load balancer.
- The load balancer can be in Premium Tier or Standard Tier.
- Create a whitelist where traffic is filtered similar to a firewalls allow and deny rules/lists.

GCP Professional Cloud Network Engineer Crash Course

Cloud Armor

- Google Cloud Armor security policies are available only for backend services behind an external HTTP(S) load balancer.
- The load balancer can be in Premium Tier or Standard Tier.



GCP Professional Cloud Network Engineer Crash Course

Cloud Armor

What are security policies

- Cloud Armor security policies are sets of rules that match on attributes from Layer 3 to Layer 7 to protect externally facing applications or services. Each rule is evaluated with respect to incoming traffic.
- Two Types - **Backend and Edge**

GCP Professional Cloud Network Engineer Crash Course

Cloud Armor

Requirements for using Google Cloud Armor security policies:

- The load balancer must be an external HTTP(S) load balancer.
- The backend service's load balancing scheme must be EXTERNAL.
- The backend service's protocol must be one of HTTP, HTTPS, or HTTP/2.

<https://cloud.google.com/armor/docs/security-policy-overview>

5.3 Configuring third-party device insertion into VPC using multi-nic

VPC

GCP Professional Cloud Network Engineer Crash Course

VPC

- By default, every instance in a VPC network has a single network interface.
- You can create additional network interfaces attached to your VMs, but each interface must attach to a different VPC network.
- Multiple network interfaces enable you to create configurations in which an instance connects directly to several VPC networks.
- Each of the interfaces must have an internal IP address, and each interface can also have an external IP address.
- Each instance can have up to **8 interfaces**, depending on the instance's type.
-

GCP Professional Cloud Network Engineer Crash Course

VPC

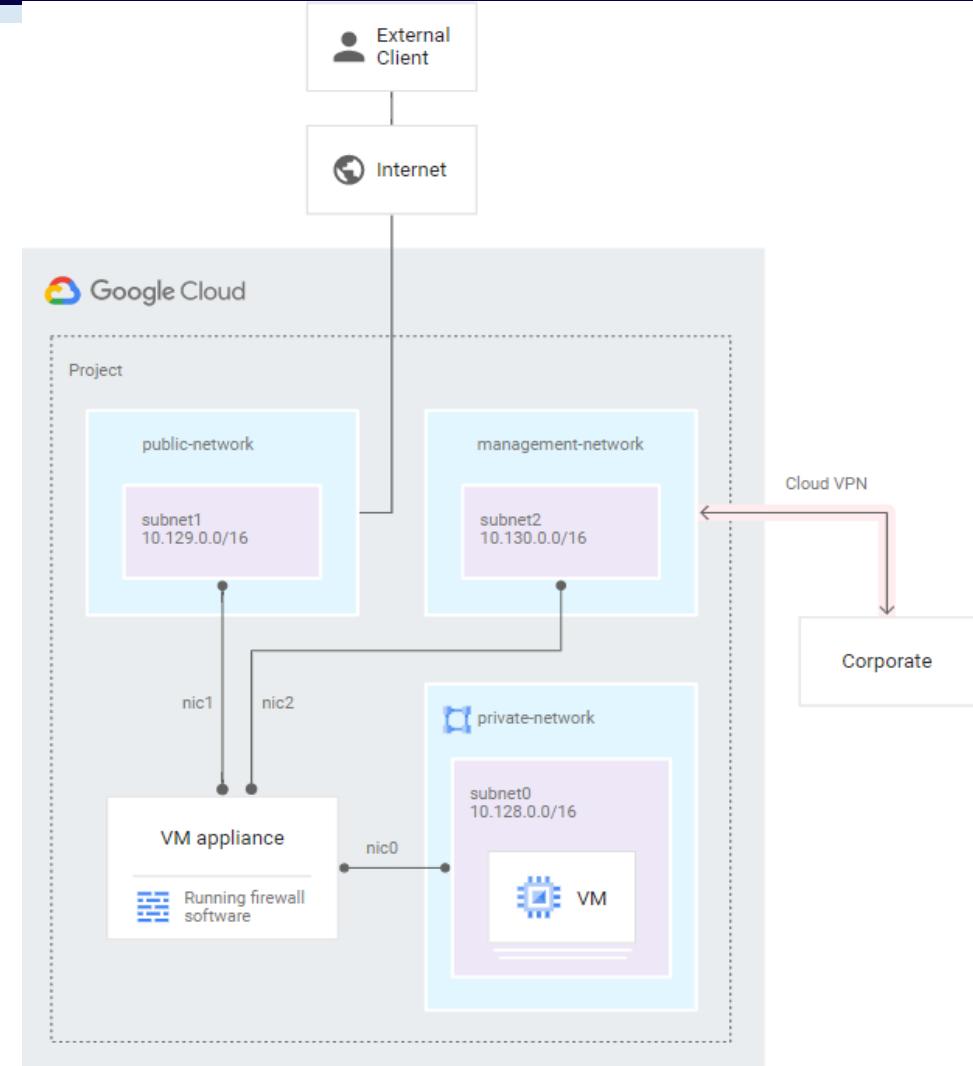
- Third Party Devices such as Intrusion Detection and Prevention (IDS/IPS), Web Application Firewall (WAF), or WAN optimization can be connected (attached) to the VPC.
- Networking and security virtual appliances, such as web application firewalls (WAF), security application- level firewalls, and WAN accelerators, are usually configured with multiple virtual interfaces.
- Each of the multiple interfaces is configured with its own internal IP address and, optionally, with its own external IP address.

GCP Professional Cloud Network Engineer Crash Course

VPC

- Diagram – Google Cloud
- Note Multiple interfaces

<https://cloud.google.com/vpc/docs/multiple-interfaces-concepts#third-party>





5.4 Managing keys for SSH access

Access Control

GCP Professional Cloud Network Engineer Crash Course

- Secure Shell Protocol (SSH) is a way to verify identity to log in remotely from one host to another
- When SSH is used to connect to a VM in Google Compute Engine for example. The public key is saved in the project-wide metadata.
- This allows a user (with the matching private key) to connect to any of the Linux VMs in the project with root access unless they have project-wide public SSH keys blocked.
- Compute Engine Instances need to have keys created.
- This is where OS Login should come in.

GCP Professional Cloud Network Engineer Crash Course

Gcloud Syntax

```
gcloud compute ssh example-instance
```

By default, gcloud expects keys to be located at the following paths:

- \$HOME/.ssh/google_compute_engine – private key
- \$HOME/.ssh/google_compute_engine.pub – public key
- If you want to reuse keys from a different location with gcloud, consider either making symlinks or pointing gcloud there using the --ssh-key-file flag.

GCP Professional Cloud Network Engineer Crash Course

- OS Login simplifies SSH access management by linking your Linux user account to your Google identity.
- Use OS Login to manage SSH access to your instances using IAM without having to create and manage individual SSH keys.
- OS Login maintains a consistent Linux user identity across VM instances and **is the recommended way to manage many users across multiple instances or projects.**

<https://cloud.google.com/compute/docs/oslogin/>

GCP Professional Cloud Network Engineer Crash Course

Add public SSH key to the list of authorized_keys on GCP instance.

Copy you `~/.ssh/id_rsa.pub` in case you have generated your SSH keys, if not follow this to generate it first.

Create an instance if not already created, to which you want to SSH.

Metadata

Metadata

SSH Keys

Edit

GCP Professional Cloud Network Engineer Crash Course

- Example: If you just want to give a user the ability to connect to a virtual machine instance using SSH, but don't want to grant them the ability to manage Compute Engine resources, add the user's public key to the project, or add a user's public key to a specific instance.
- You can avoid adding a user as a project member, while still granting them access to specific instances.
- `gcloud compute os-login remove-profile`

<https://cloud.google.com/compute/docs/access/>

GCP Professional Cloud Network Engineer Crash Course

OS Login Admin Access

`roles/compute.osLogin`, which doesn't grant administrator permissions

`roles/compute.osAdminLogin`, which grants administrator permissions

Enable OS Login CLI – Project Wide

- `gcloud compute project-info add-metadata --metadata enable-oslogin=TRUE`

Remove profile

- `gcloud compute os-login remove-profile`

<https://cloud.google.com/compute/docs/instances/managing-instance-access#gcloud>



Identity Aware Proxy

Cloud IAP

GCP Professional Cloud Network Engineer Crash Course

Cloud IAP

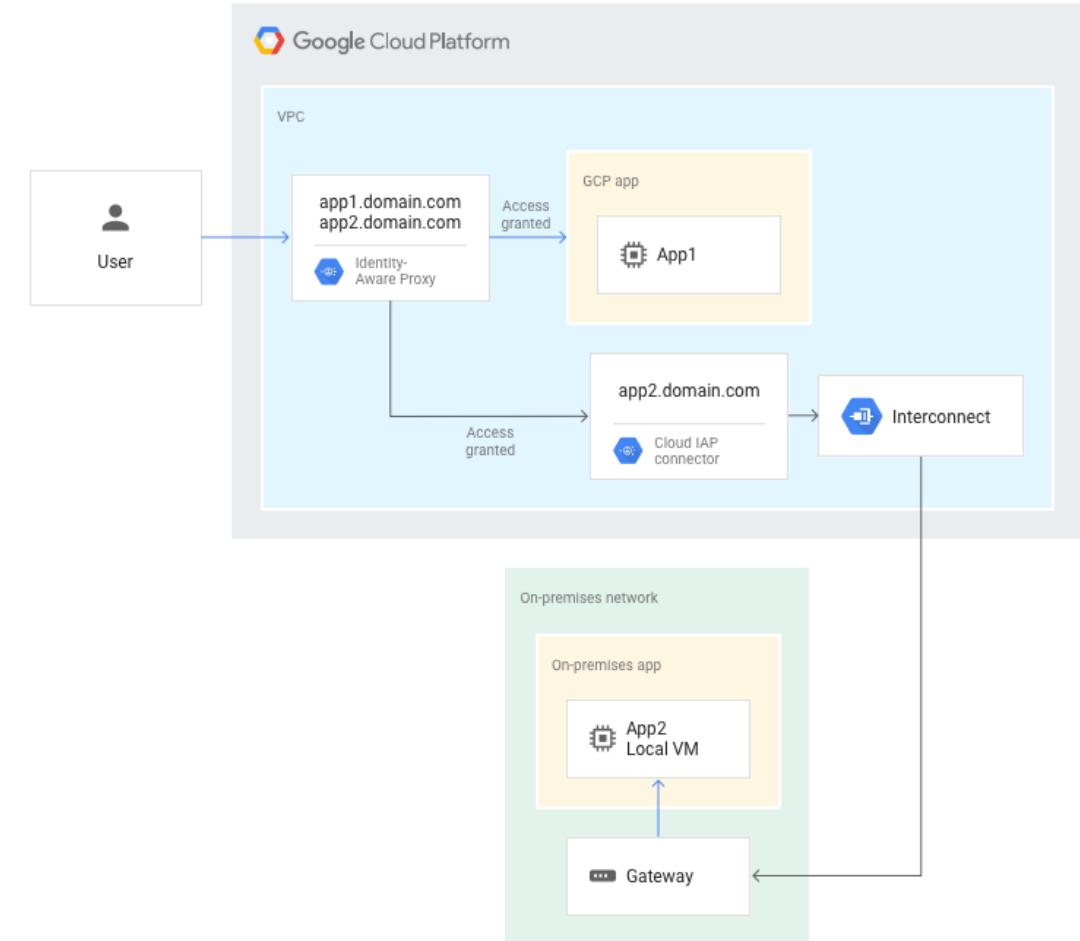
Cloud IAP works by verifying user identity and context of the request to determine if a user should be allowed to access an application or a VM. (**Whitelisting**)

- Think of Cloud IAP as both an efficiency since it provides faster sign in but also a security feature that will block unauthorized VM access.
- The main selling point for IAP is to control access to your enterprise applications from unauthorized external networks while integrating with existing IAM policies. Effectively whitelisting meaning that you're choosing your winners on the list.

GCP Professional Cloud Network Engineer Crash Course

Cloud IAP

- SSH/TCP access can be used with App Engine, Kubernetes Engine and Compute Engine.
- HTTP based access can be used with the HTTPS Load balancer.



GCP Professional Cloud Network Engineer Crash Course

Cloud IAP

The screenshot shows the Google Cloud Platform Identity-Aware Proxy (IAP) interface. The left sidebar lists various security services: Security Command Center, Identity-Aware Proxy (selected), Cryptographic Keys, Access Context Manager, VPC Service Controls, Binary Authorization, Data Loss Prevention, Access Approval, and Web Security Scanner. The main content area is titled "Identity-Aware Proxy" and contains a brief description of what IAP does. Below this, there are two tabs: "HTTPS RESOURCES" (selected) and "SSH AND TCP RESOURCES". Under "HTTPS RESOURCES", a table lists three entries:

Resource	IAP	Published	Configuration
All Web Services	On	OK	⋮
App Engine app	On	OK	⋮
default	On	OK	⋮

A message on the right side of the screen says "No resources selected" and "Please select at least one resource".

GCP Professional Cloud Network Engineer Crash Course

Cloud IAP

IAP provides two distinct levels of security authorization goodness.

- Resource Authorization — Uses what are OAuth2 flows which generate a signed access token. As expected IAP will use this token to validate identity for application-level access.
- App Validation — This works at a user's identity level by using signed headers that are generated by IAP. Consider this as a secondary level of protection since it would catch a bypass IAP attempt.

GCP Professional Cloud Network Engineer Crash Course

Cloud Identity Aware Proxy – Notes for exam

- Cloud IAP sessions are tied to the underlying Google login session.
- Cloud IAP uses this cookie to confirm that the user is still signed into their Google account.
- Standard Cloud IAP login flow has a one-hour expire time in the Cloud IAP session cookie and is ignored after.
- Login sessions are instead secured with account state checks.



GCP Professional Cloud Network Engineer Crash Course

Cloud IAP requires a user to sign back into their Google account before accessing a Cloud IAP-secured app.

The following are a few situations that require the user to sign back in:

- The user signed out of their account
- Their account was suspended
- The account requires a password reset

If a user is signed out, Cloud IAP detects a Google account state change within a couple minutes.

Once detected, Cloud IAP invalidates the session.

Expired session response. AJAX Vs Non-AJAX

AJAX vs Non-AJAX

Non – Ajax - redirect to Google Oath

Ajax – 401 Code is issued (CORS restriction)

Review page here before exam. Several questions I experienced here.

GCP Professional Cloud Network Engineer Crash Course

Handling an HTTP 401 AJAX response???

1. Update your app code to handle the error
2. Provide a refresh link
3. Close the window

```
if (response.status === 401) {  
    statusElm.innerHTML = 'Login stale. <input type="button" value="Refresh" onclick="sessionRefreshClicked();"/>';  
}
```

Test Tip



Cloud IAP

- Cloud IAP sessions are tied to the underlying Google login session.
- Cloud IAP is effectively whitelisting access from a specific domain.

Test Tip



Session Management

- IAP - Non – Ajax - redirect to Google Oath
- Ajax – 401 Code is issued (CORS restriction)
- Cloud IAP sessions are tied to the underlying Google login session.



Test Tips

- OS Login maintains a consistent Linux user identity across VM instances and is the recommended way to manage many users across multiple instances or projects.
- OSLogin can be set with gcloud. -
-metadata enable-oslogin=TRUE

Section Summary

Section 5 : Implementing Network Security



5

Section

Section Summary

- There are three kinds of roles in Cloud IAM which are Primitive roles , Predefined (Curated) roles and Custom Roles
- Each instance can have up to 8 interfaces, depending on the instance's type.
- Secure Shell Protocol (SSH) is a way to verify identity to log in remotely from one host to another
- When SSH is used to connect to a VM in Google Compute Engine for example. The public key is saved in the project-wide metadata.
- Cloud IAP works by verifying user identity and context of the request to determine if a user should be allowed to access an application or a VM.
- Cloud IAP sessions are tied to the underlying Google login session.

Section Review Questions

Section 5 : Implementing Network Security



Review Questions

You have currently migrated to GCP and now would like to monitor and manage log files on compute services. What GCP service would you select that would provide this native capacity? (Choose One)

- Cloud Logging
- Cloud Operations
- Splunk
- Kubernetes Engine

Review Questions

You have currently migrated to GCP and now would like to monitor and manage log files on compute services. What GCP service would you select that would provide this native capacity? (Choose One)

- Cloud Logging
- Cloud Operations
- Splunk
- Kubernetes Engine

Review Questions

How should a customer reliably deliver Cloud Operations logs from GCP to their on-premises SIEM system? (Select One)

- Send Logs directly to the SIEM System
- Configure a project to export logs to Cloud Storage and then use Cloud Pub/Sub
- Configure Organizational Log Sinks to export logs to Cloud Pub/Sub, Dataflow.
- Configure a project to export logs to BigQuery and then use Cloud Pub/Sub

Review Questions

How should a customer reliably deliver Cloud Operations logs from GCP to their on-premises SIEM system Splunk? (Select One)

- Send Logs directly to the SIEM System
- Configure a project to export logs to Cloud Storage and then use Cloud Pub/Sub
- **Configure Organizational Log Sinks to export logs to Cloud Pub/Sub, Dataflow.**
- Configure a project to export logs to BigQuery and then use Cloud Pub/Sub

Review Questions

You have currently migrated to GCP and now would like to monitor and manage log files on compute services. What GCP service would you select that would provide this native capacity? (Choose One)

- Cloud Logging
- Cloud Operations
- Splunk
- Kubernetes Engine

Review Questions

You have currently migrated to GCP and now would like to monitor and manage log files on compute services. What GCP service would you select that would provide this native capacity? (Choose One)

- **Cloud Logging**
- Cloud Operations
- Splunk
- Kubernetes Engine



Section 6 : Managing and Monitoring Network Operations

Understanding the domain testable objectives

Domain Overview

- Logging and Monitoring with Cloud Operation and the console
- Managing and maintaining security
- Managing and troubleshooting network connectivity
- Monitoring, managing and troubleshoot latency issues



6.1 Logging and Monitoring with Cloud Operations or Cloud Console

Obtaining insight into your cloud deployment

Google Cloud Digital Leader Certification Course

Cloud Operations is a hybrid Monitoring, logging, and diagnostics for applications on Cloud Platform and AWS.

GCP Purchased Stackdriver and rebranded it to Google Stackdriver. (Now Cloud Operations)

Cloud Operations monitors the clouds service layers in a single SaaS solutions.

Native integration with Google Cloud data tools BigQuery, Cloud Pub/Sub, Cloud Storage, Cloud Datalab, and out-of-the-box integration with all your other application components.

Access from GCP Console

Google Cloud Digital Leader Certification Course



Monitoring



Debugger



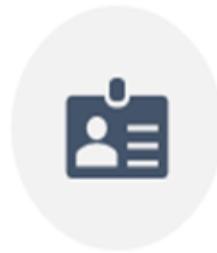
Logging



Trace



Error Reporting



Profiling

Google Cloud Digital Leader Certification Course

Benefits

- Monitors multi cloud
- Identify trends and prevents issues
- Lowers Monitoring headaches
- Fix problems faster
- Reduces monitoring noise!
- Aids with Cloud Security
- Aids with Compliance



Cloud Operations

Cloud Operations Account Options

- Create Operations account for project
- Create Operations account that monitors multiple projects

STACKDRIVER

 Monitoring

 Debug

 Trace >

 Logging >

 Error Reporting

 Profiler

Google Cloud Digital Leader Certification Course



Cloud Operations

- Monitoring
- Defaults are intelligent and dynamic
- Health checks
- Metrics = Platform, system, application
 - >>>Ingest Data Metrics, events and metadata
 - >>>>Then provides insight thru dashboards, charts and alerts

Google Cloud Digital Leader Certification Course

Cloud Operations



Cloud APIs



Cloud Deployment Manager



Cloud Endpoints



Debugger



Error Reporting



Logging



Monitoring



Stackdriver



Trace

- Metrics Examples

Compute Engine

- firewall/dropped_bytes_count
- firewall/dropped_packets_count
- instance/cpu/reserved_cores
- instance/cpu/usage_time
- instance/cpu/utilization
- instance/disk/read_bytes_count
- instance/disk/read_ops_count
- instance/disk/throttled_read_bytes_count
- instance/disk/throttled_read_ops_count

Google Cloud Digital Leader Certification Course

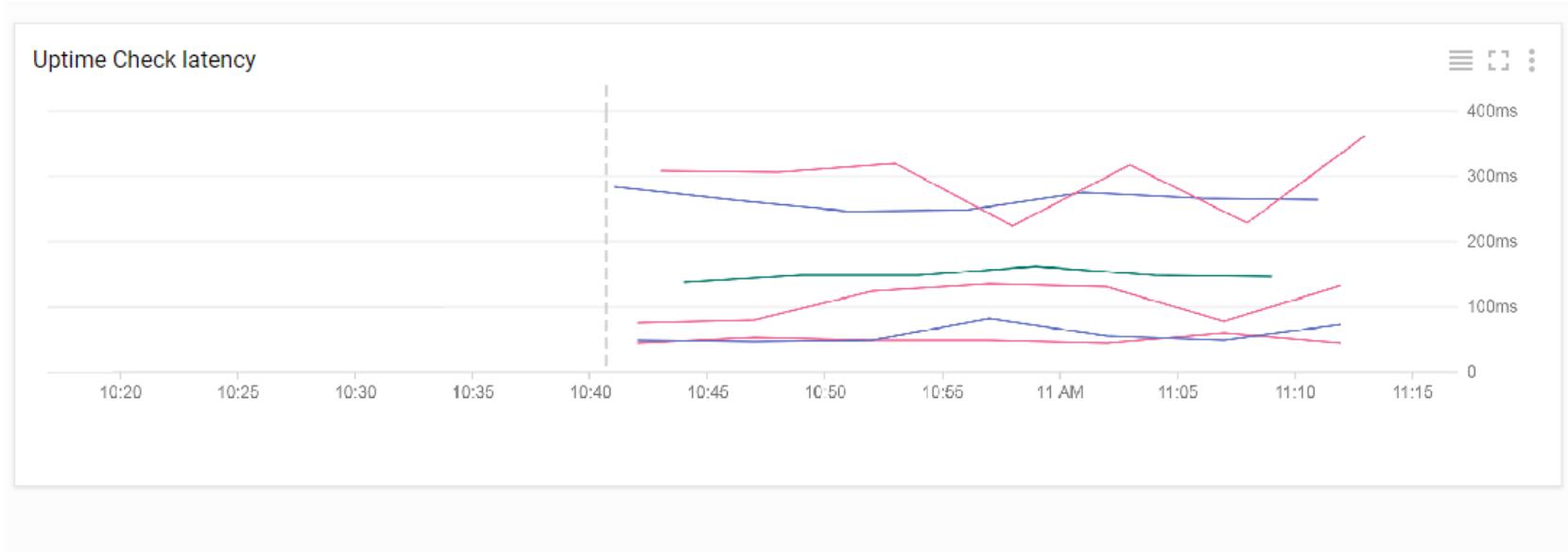
Workspaces

- Workspace is a tool for monitoring resources contained in one or more GCP projects or AWS accounts.
- Each Workspace can have between 1 and 100 **monitored projects**, including one or more GCP projects and any number of AWS accounts.
- You can have as many Workspaces as you wish, but GCP projects and AWS accounts cannot be monitored by more than one Workspace.
- A Workspace contains the custom dashboards, alerting policies, uptime checks, notification channels, and group definitions that you use with your monitored projects.
- A Workspace can access metric data from its monitored projects, but the metric data and log entries remain in the individual projects.

Google Cloud Digital Leader Certification Course

Uptime checks verify 6 Global locations.

When you make a change to an uptime check delay could be 25 minutes



Google Cloud Platform Google Analytics Search products and resources

DASHBOARD ACTIVITY RECOMMENDATIONS FILTER

Today

1:26 PM	⚠ Failed: beta.compute.securityPolicies.insert	holbrookjp@thegcpgurus.com failed to execute beta.compute.securityPolicies.insert on vpcnetworkengineer
1:26 PM	⚡ beta.compute.securityPolicies.insert	holbrookjp@thegcpgurus.com has executed beta.compute.securityPolicies.insert on vpcnetworkengineer
1:14 PM	⚡ google.iam.admin.v1.UpdateRole	holbrookjp@thegcpgurus.com has executed google.iam.admin.v1.UpdateRole on LNusers
1:14 PM	⚡ google.iam.admin.v1.CreateRole	holbrookjp@thegcpgurus.com has executed google.iam.admin.v1.CreateRole on LNusers

Yesterday

3:41 PM	⚡ google.longrunning.Operations.GetOperation	holbrookjp@thegcpgurus.com has executed google.longrunning.Operations.GetOperation on acf.p2-439862965988-f522f350-4806-4611-b6f0-05f66db24...
3:41 PM	⚡ Completed: google.api.serviceusage.v1.ServiceUsage.EnableService	holbrookjp@thegcpgurus.com has executed google.api.serviceusage.v1.ServiceUsage.EnableService on compute.googleapis.com
3:41 PM	⚡ google.longrunning.Operations.GetOperation	holbrookjp@thegcpgurus.com has executed google.longrunning.Operations.GetOperation on acf.p2-439862965988-f522f350-4806-4611-b6f0-05f66db24...
3:41 PM	⚡ google.longrunning.Operations.GetOperation	holbrookjp@thegcpgurus.com has executed google.longrunning.Operations.GetOperation on acf.p2-439862965988-f522f350-4806-4611-b6f0-05f66db24...



Test Tips

- Cloud Operations is a hybrid monitoring and management solution.



Cloud Operations

Demo

GCP Professional Cloud Network Engineer Crash Course





Log Sinks

What are Logs for?

GCP Professional Cloud Network Engineer Crash Course

Log Exports

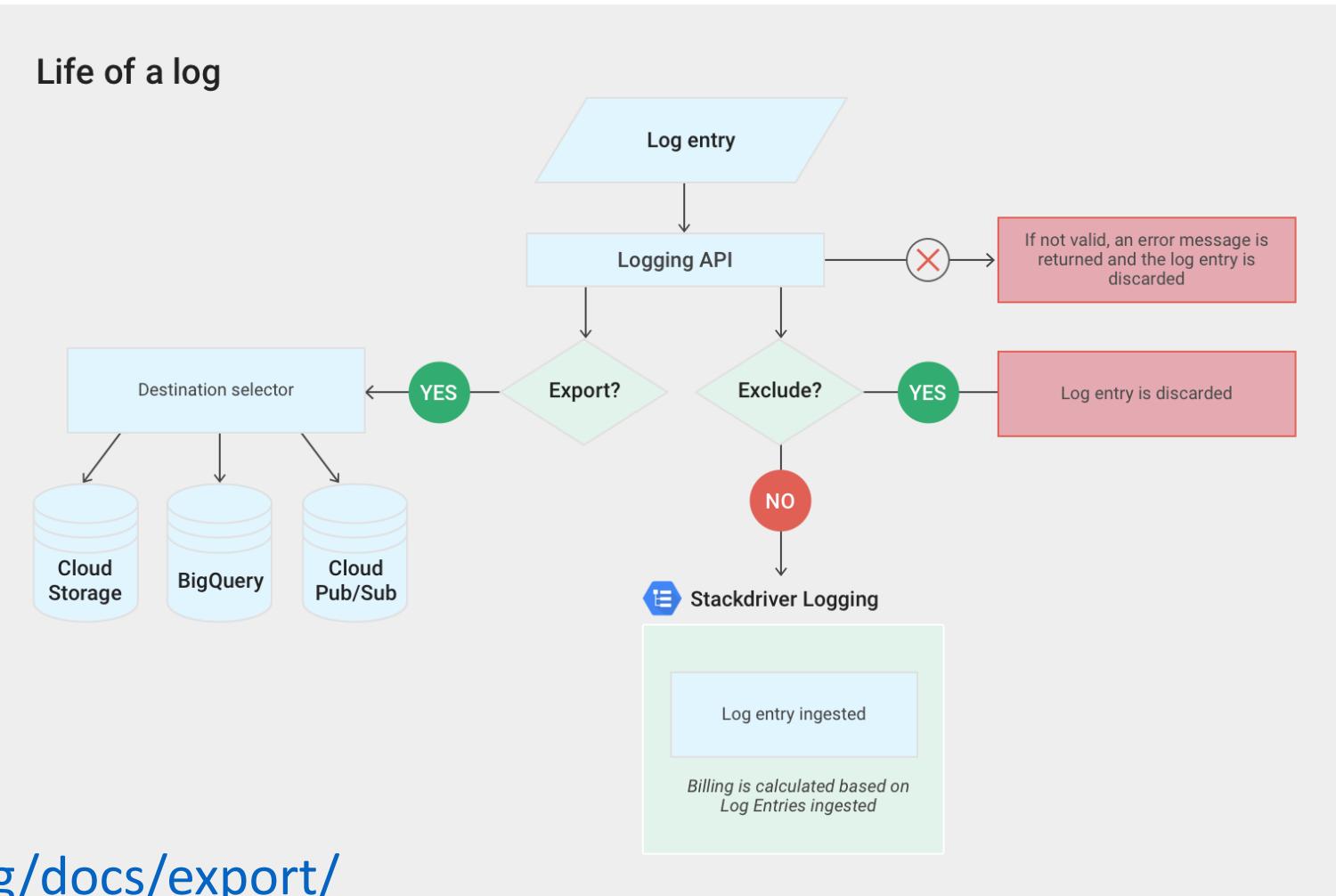
Export Logs via Logging API

- Cloud Storage
- Cloud Pub/Sub
- BigQuery

GCP Professional Cloud Network Engineer Crash Course

Log Life

Exam will test you knowledge about Log Life Cycle



<https://cloud.google.com/logging/docs/export/>

GCP Professional Cloud Network Engineer Crash Course

Log Trivia to Learn

Log Entry Size – 256KB

Log Retention - 30 days to 400 days

<https://cloud.google.com/logging/quotas>

<https://cloud.google.com/logging/docs/audit/>

GCP Professional Cloud Network Engineer Crash Course

Logging Commands

- gcloud logging
- gcloud logging logs list
- gcloud logging sinks create

GCP Professional Cloud Network Engineer Crash Course

SIEM Log Sinks

Google allows you to create an organization log sink and export the logs to Cloud Pub/Sub. From there it's possible to use Cloud Dataflow to send data to a SIEM.

Splunk --- there is already a default Cloud Dataflow template created by GCP.

<https://cloud.google.com/dataflow/docs/guides/templates/provided-streaming#pubsub-to-splunk>

GCP Professional Cloud Network Engineer Crash Course

Log Sinks

Sink Permissions

- To create or modify a sink, you must have the **IAM roles Owner or Logging/Logs Configuration Writer** in the sink's parent resource.
- To view existing sinks, you must have the **IAM roles Viewer or Logging/Logs Viewer** in the sink's parent resource
- `gcloud logging sinks create`



6.2 Managing and Maintaining Security

Firewalls and IAM

GCP Professional Cloud Network Engineer Crash Course

- The GCP approach to security mirrors the way Google secures its own products and users.
- GCP secures resources by building a security structure according to its various layers.
- Access to the physical locations of Google's servers is strictly limited and managed as a critical priority.
- **GCP ensures communication is secure at the transport layer, through secure TLS connection management and front-end controls to prevent DoS attacks**

GCP Professional Cloud Network Engineer Crash Course

- Google owns their network and infrastructure and the communications is done outside the public internet.
- This enables Google to ensure secure delivery of communications, both in transit and at rest. Note it also applies to data that is contributed from third-parties.
- Google's Titan chip establishes trust at the hardware root for all machines and assets in GCP. (This is an additional layer to authenticate access for hardware handling your data.)

GCP Professional Cloud Network Engineer Crash Course

- With personal public key certificates and multi-factor authentication, GCP maintains control and keeps a trail of usage to ensure compliance among those who have legitimate access to applications at the application layer.
- Review Best Practices for Enterprise Organizations
- <https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations>



Test Tips

- Google's Titan chip establishes trust at the hardware root for all machines and assets in GCP
- GCP ensures communication is secure at the transport layer, through secure TLS connection management and front-end controls to prevent DoS attacks



Security Best Practices

IT Security and GCP Security Best Practices

GCP Professional Cloud Network Engineer Crash Course

Common IT Security Best Practices

- Use the Principle of least privilege
- Always apply the minimal access level required
- Use groups and add users to the groups
- Control who can change policies and group memberships
- Audit policy changes

GCP Professional Cloud Network Engineer Crash Course

Google Cloud Security Best Practices

- Apply only minimal access level required for roles
- Use predefined roles over primitive roles
- Grant roles at smallest scope needed
- Service accounts should be treated as a separate trust boundary
- Child resources can't restrict parent access
- Create a separate service account for each service
- Restrict access to service accounts

GCP Professional Cloud Network Engineer Crash Course

Google Cloud Security Best Practices

- Audit logs record project-level permission changes
- Use Cloud Audit logs to audit IAM policy changes
- Export Audit logs to Cloud Storage
- Restrict Audit logs to appropriate users

GCP Professional Cloud Network Engineer Crash Course

Google Cloud Security Best Practices

- Rotate Service account keys
- Don't delete service accounts in use
- Don't leave keys in source code or in unsecure directories.
- Organizational level policies should be used to grant access to projects
- Grant roles to groups instead of individual users
- User groups whenever possible to simplify management



Firewall

Fundamentals

GCP Cloud Developer Overview

- Firewall rules help define allow or deny connections and apply to both outgoing (egress) and incoming (ingress) traffic in the network.
- Firewall rules control traffic even if it is entirely within the VPC network, including communication among VM instances.
- Firewall rules apply to a given project and network, and connections are allowed or denied on a per-instance basis.
- VPC firewall rules are stateful

GCP Cloud Developer Overview

Firewall

+ CREATE FIREWALL RULE

REFRESH

CONFIGURE LOGS

DELETE

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Note: App Engine firewalls are managed in the [App Engine Firewall rules section](#).

Filter Enter property name or value

<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	Logs	Hit count	?	Last modified
<input type="checkbox"/>	default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default	Off	—	—	
<input type="checkbox"/>	default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default	Off	—	—	
<input type="checkbox"/>	default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	default	Off	—	—	
<input type="checkbox"/>	default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default	Off	—	—	

GCP Cloud Developer Overview

Firewall rules always allow the following traffic

- DHCP
- DNS
- Instance metadata (169.254.169.254)
- NTP

Firewall rules always block the following traffic

- GRE traffic – Tunneling protocol
- Protocols other than TCP, UDP, ICMP, and IPIP
- Egress traffic on TCP port 25 (SMTP)

GCP Cloud Developer Overview

Firewall Rule notes

- Firewall Rules Logging enables auditing, verifying, and analyzing the effects of the firewall rules.
- Firewall Rules Logging can be enabled individually for each firewall rule whose connections need to log
- Google Cloud creates an entry called a connection record each time the firewall rule allows or denies traffic.
- Firewall Rules Logging only records TCP and UDP connections.

GCP Cloud Developer Overview

Firewalls as a Resource

- Global Resource
- Control traffic incoming (Priority as well)
- Default allows ingress (Allow Only)

Matches dest. IP CIDR ranges, protocols, ports & target Tags

- ICMP
- SSH
- RDP

Supports Allows for ingress not Denies (Remember this)

GCP Cloud Developer Overview

Firewalls as a VPC Resource

VPC networks have two implied firewall rules. Note that these “implied” rules CAN NOT be removed..

- implied allow egress rule (65535 Priority)
- implied deny ingress rule (65535 Priority)

<https://cloud.google.com/vpc/docs/firewalls>

GCP Cloud Developer Overview

Firewalls as a VPC Resource

Always-blocked traffic - GCP always blocks the following traffic.

<https://cloud.google.com/vpc/docs/firewalls>

Firewall rules **cannot** be used to un-block traffic that is always blocked.

Rules are evaluated for priority. 0-65535 Default is 1000



Test Tips

- On the exam questions will infer that you understand GCP best practices around IAM and security and can apply this while answering questions
- A parent can't be restricted to accessing child resources.

GCP Professional Cloud Network Engineer Crash Course



6.3 Maintaining and troubleshooting connectivity issues.

Traffic

GCP Cloud Developer Overview

Cloud Endpoints

API Gateway

NGINX based proxy

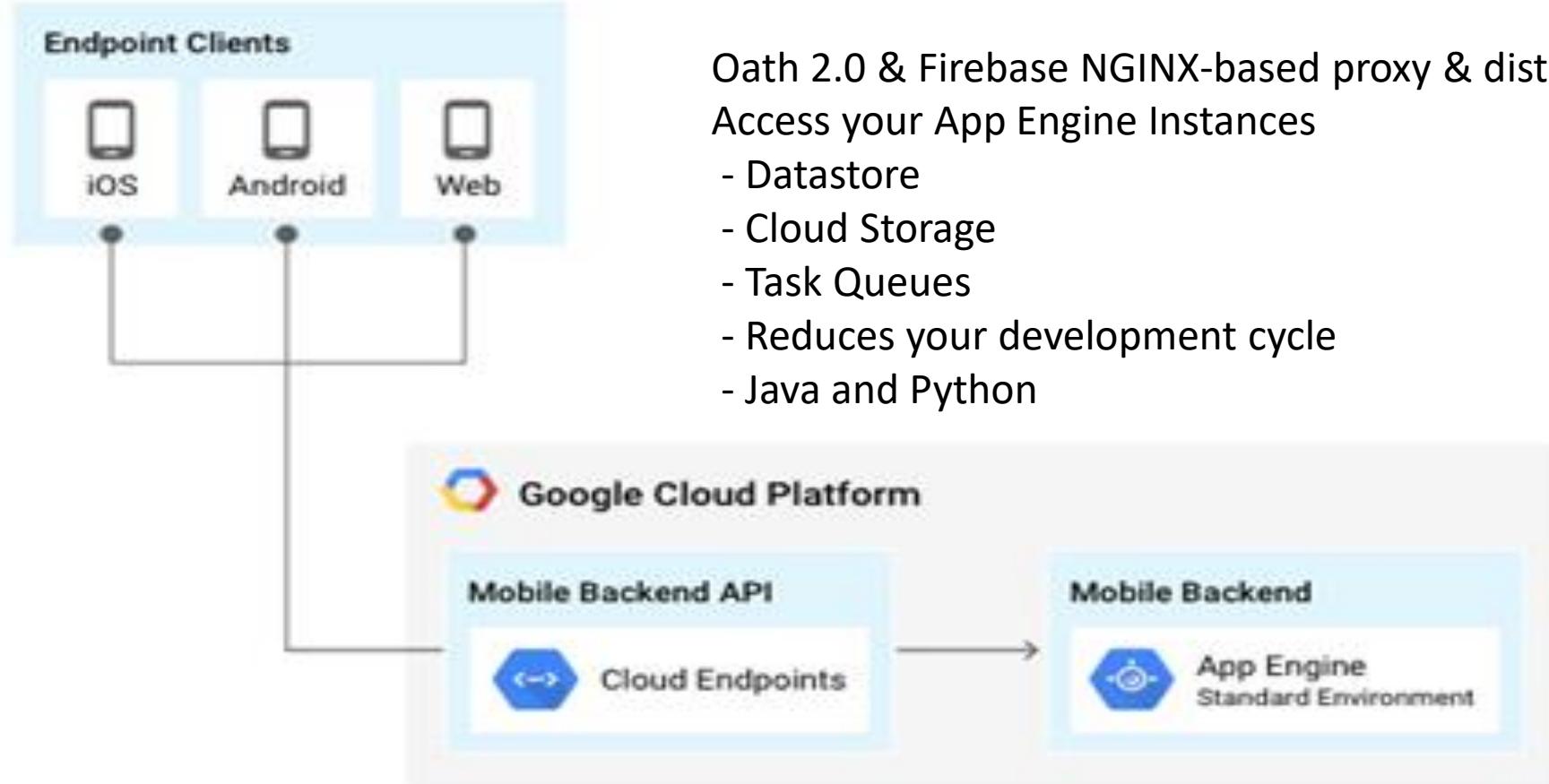
Cloud Endpoints
are used to create
a web backend.

Used for web and
mobile clients

Deploy with App
Engine

Tools and Library

GCP Cloud Developer Overview



**Endpoints use Google Protocol
RPC for HTTP service calls**

Steps include:

- Configure application
- Define message classes
- Write endpoint code
- Run and test API

To use an endpoint from a JavaScript client

Step one: include the
Google-hosted
JavaScript client library

Step two: load your
endpoint

Step three: call the
endpoint API

GCP Cloud Developer Overview

```
<script src='https://apis.google.com/js/client.js?onload=init'>
</script>

function init() {
    var path = '//' + window.location.host + '/_ah/api';
    gapi.client.load('yourAPI', 'v1', loadCallback, path);
}
```

Test Tip



Cloud Endpoints

- Use case could be either for GCP Cloud Endpoints or for Apigee.
- Determine if apps are hosted on GCP or may be tied to on premises.

6.3 Maintaining and troubleshooting connectivity issues.

Traffic



Identifying traffic flow topology

Load Balancing. endpoints

GCP Cloud Developer Overview

Network Topology is a visualization tool that shows the topology of your Virtual Private Cloud (VPC) networks, hybrid connectivity to and from your on-premises networks, connectivity to Google-managed services, and the associated metrics.

- View metrics and details of network traffic to other Shared VPC networks and inter-region traffic.
- Network Topology combines configuration information with real-time operational data in a single view.
- Understand networking relationships between various workloads on Google Cloud and their current state

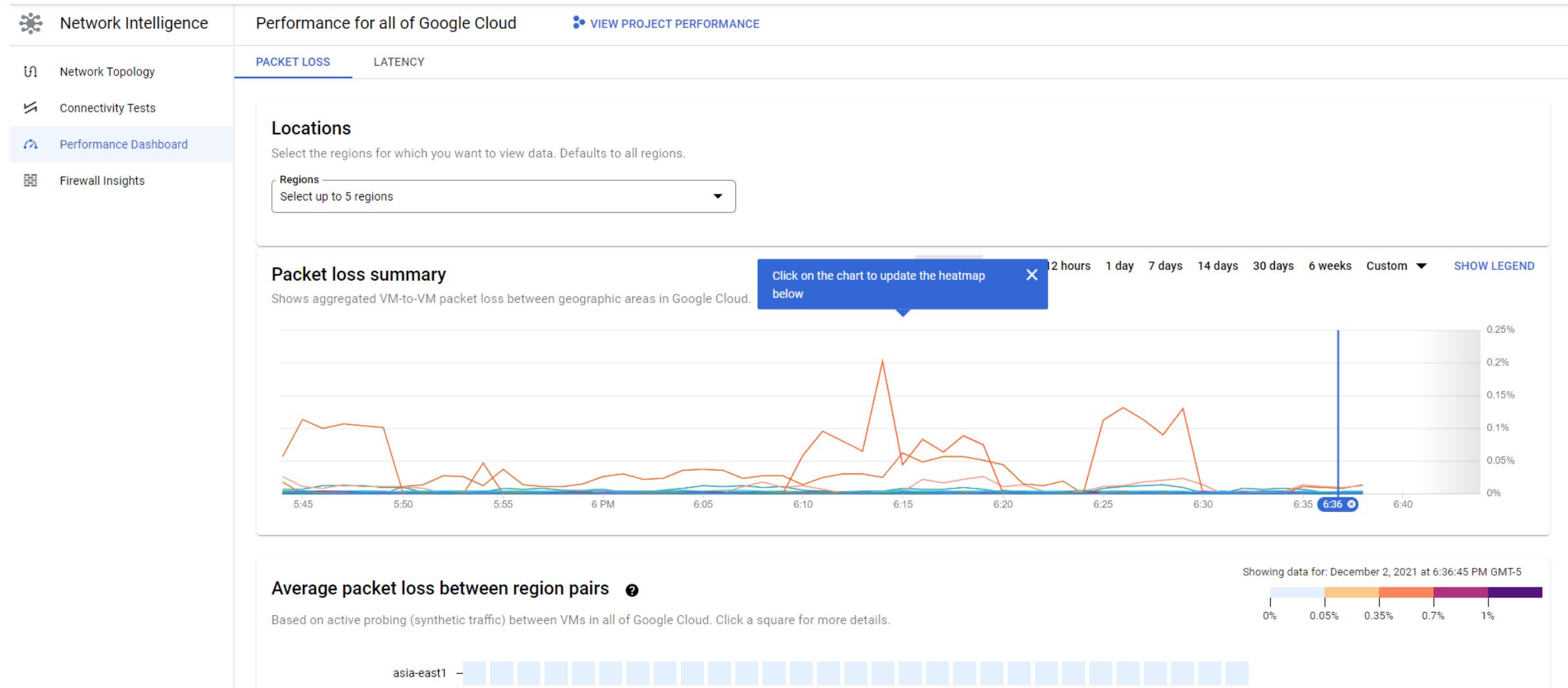
GCP Cloud Developer Overview

Multiple Projects

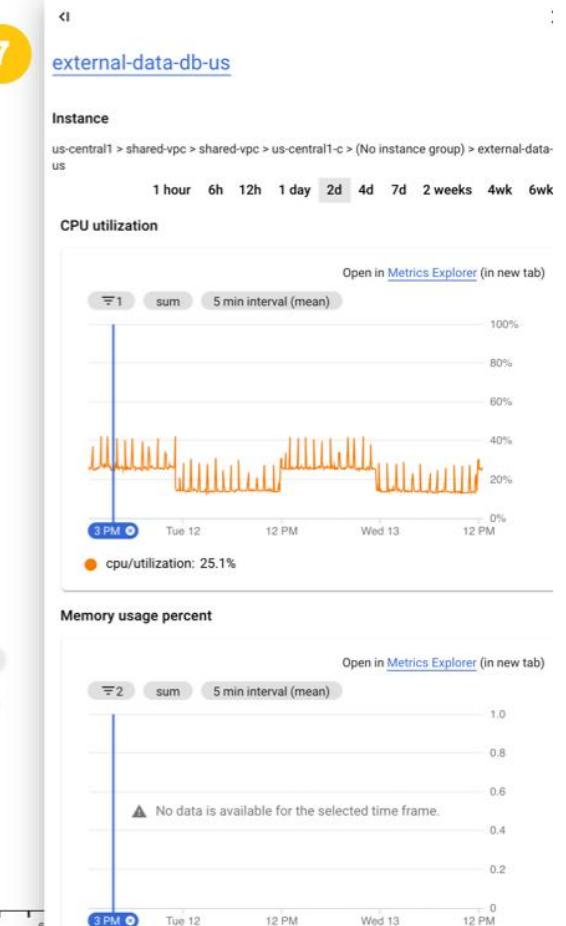
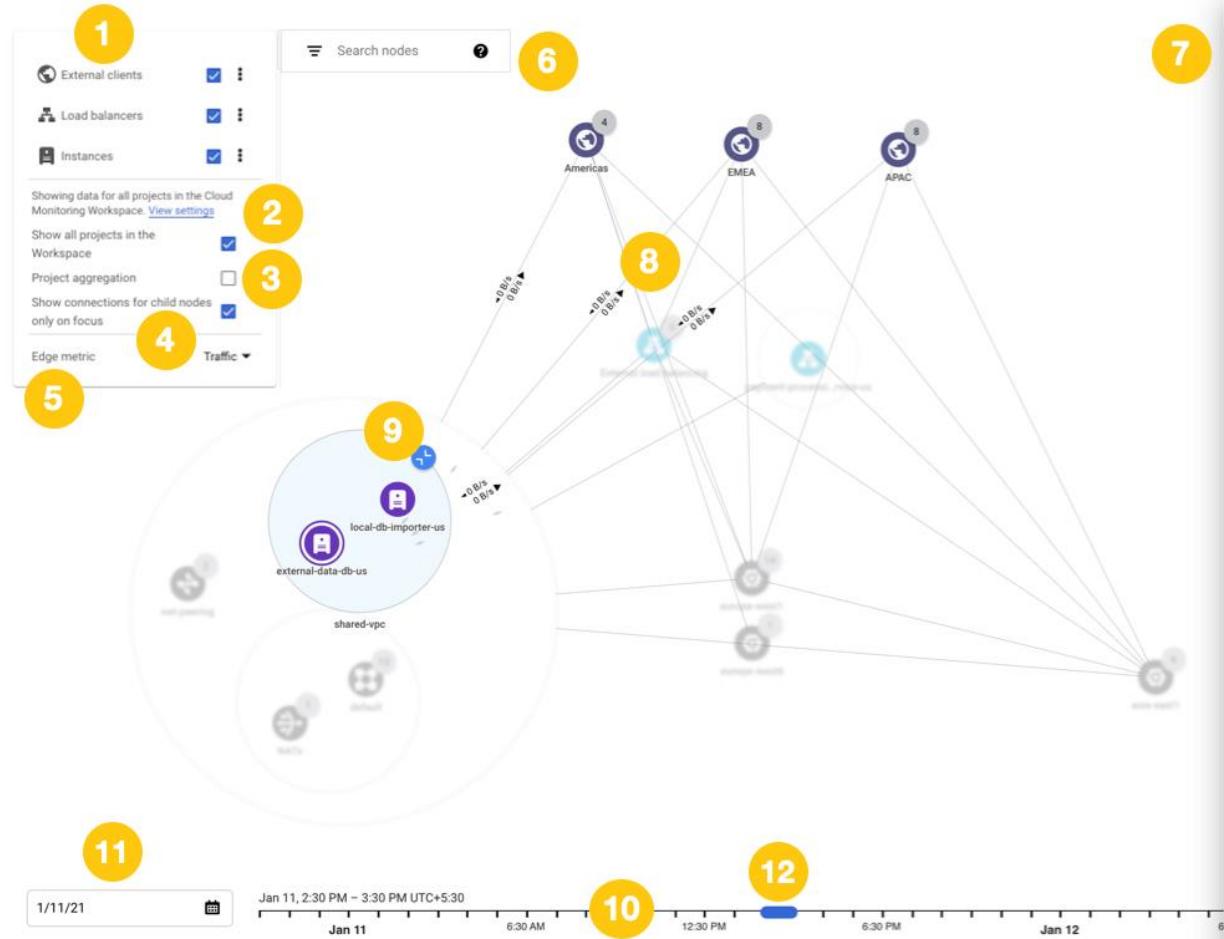
- Network Topology visualizes resources in your project, or you can use Cloud Monitoring, which can visualize metrics for multiple Google Cloud projects.
- Configure Cloud Monitoring to have access to the metrics for multiple projects, Network Topology can show network traffic that crosses multiple projects.
- Network Topology captures six weeks of history.
- The Network Topology history is divided into hourly segments, which start at the beginning of an hour

<https://cloud.google.com/network-intelligence-center/docs/network-topology/concepts/overview#ip-address-considerations>

GCP Cloud Developer Overview



GCP Cloud Developer Overview





6.4 Monitoring, maintaining, and troubleshooting latency and traffic flow.

Traffic

GCP Cloud Developer Overview

Considerations

- Network throughput and latency testing
- Routing issues
- Tracing traffic flow
- Optimizing network resources



Network throughput and latency testing

Understanding your traffic flow

GCP Cloud Developer Overview

Throughput and Latency

- Latency indicates how long it takes for packets to reach their destination.
- Throughput is the term given to the number of packets that are processed within a specific period of time.
- Throughput and latency have a direct relationship in the way they work within a network

GCP Cloud Developer Overview

Measuring Throughput and Latency

- ping, iperf, and netperf

```
ping <ip.address> -c 100
```

```
netperf -H <ip.address> -t TCP_RR -- \
-o min_latency,max_latency,mean_latency
```

PerfKit Benchmarker - <https://github.com/GoogleCloudPlatform/PerfKitBenchmarker>

GCP Cloud Developer Overview

Google Cloud Latency Dashboard

- For Google Cloud Inter-Region latency and throughput benchmarks.
- <https://datastudio.google.com/u/0/reporting/fc733b10-9744-4a72-a502-92290f608571/page/70YCB>



Routing Issues

Routing changes and troubleshooting

GCP Cloud Developer Overview

Routing

- Google Cloud routes define the paths that network traffic takes from a virtual machine (VM) instance to other destinations.
- In a VPC network, a route consists of a single destination prefix in CIDR format and a single next hop.
- When an instance in a VPC network sends a packet, Google Cloud delivers the packet to the route's next hop if the packet's destination address is within the route's destination range.

GCP Cloud Developer Overview

Routing

Review the Route Types - <https://cloud.google.com/vpc/docs/routes>

- System Generated Routes – When you create a VPC network, it includes a system-generated IPv4 default route (0.0.0.0/0).
- Subnet routes define paths to resources like VMs and internal load balancers in a VPC network.
- Static routes are defined using static route parameters and support static route next hops.

GCP Cloud Developer Overview

Dynamic routes are managed by Cloud Routers in the VPC network. (IP address ranges outside your VPC network, received from a BGP peer.)

- Dedicated Interconnect
- Partner Interconnect
- HA VPN tunnels
- Classic VPN tunnels that use dynamic routing

GCP Cloud Developer Overview

- Peering subnet routes define paths to resources using subnets in another VPC network connected using VPC Network Peering.
- Each instance has a set of applicable routes, which are a subset of all routes in the VPC network. Applicable routes are the possible egress paths that a packet can take when sent from the instance.

GCP Cloud Developer Overview

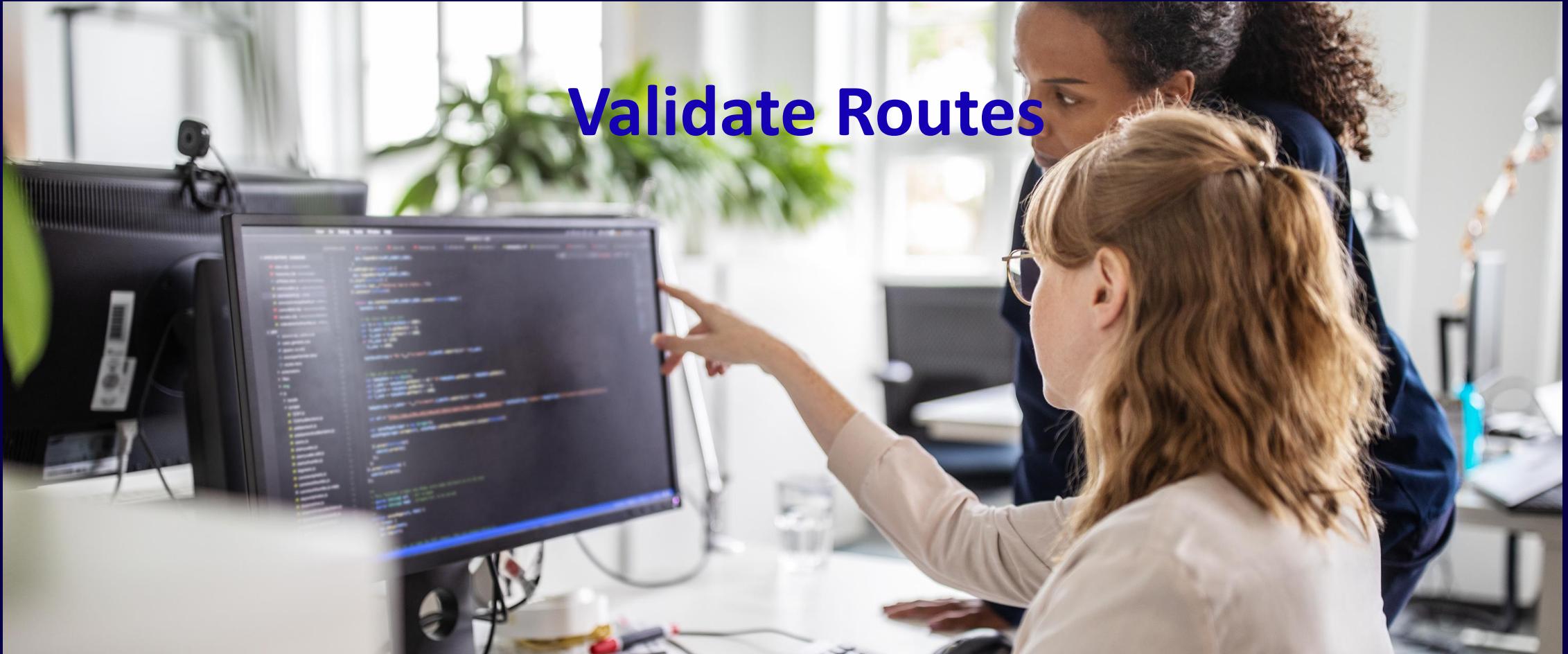
Routes							
		+ CREATE ROUTE	REFRESH	DELETE			
ALL		DYNAMIC	PEERING				
<input type="text"/> Filter Enter property name or value							...
<input type="checkbox"/>	Name ↑	Description	Destination IP range	Priority	Instance tags	Next hop	Network
<input type="checkbox"/>	default-route-0128f5a8d55cfbce	Default local route to the subnetwork 10.180.0.0/20.	10.180.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-1b4c688724bcc3fa	Default local route to the subnetwork 10.138.0.0/20.	10.138.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-2142390b5c02ab5b	Default local route to the subnetwork 10.146.0.0/20.	10.146.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-24566e483a7df689	Default local route to the subnetwork 10.192.0.0/20.	10.192.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-2fd24919de1cd615	Default route to the Internet.	0.0.0.0/0	1000	None	Default internet gateway	default
<input type="checkbox"/>	default-route-30916aa3c20f04b7	Default local route to the subnetwork 10.186.0.0/20.	10.186.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-30dbe1bc183ee8a2	Default local route to the subnetwork 10.148.0.0/20.	10.148.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-3461b9aa7b3aaa69	Default local route to the subnetwork 10.140.0.0/20.	10.140.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-3fe3262ec307d456	Default local route to the subnetwork 10.162.0.0/20.	10.162.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-40f8ce5733373c21	Default local route to the subnetwork 10.168.0.0/20.	10.168.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-44b88221db54cc63	Default local route to the subnetwork 10.150.0.0/20.	10.150.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-4d38944943dc9767	Default local route to the subnetwork 10.158.0.0/20.	10.158.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-4da4d2076cee80ec	Default local route to the subnetwork 10.178.0.0/20.	10.178.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-4e1543f1ed6f11ed	Default local route to the subnetwork 10.170.0.0/20.	10.170.0.0/20	0	None	Virtual network default	default
<input type="checkbox"/>	default-route-4fa373f8b6307c0c	Default local route to the subnetwork 10.156.0.0/20.	10.156.0.0/20	0	None	Virtual network default	default

GCP Professional Cloud Network Engineer Crash Course



Hands-on exercise

Validate Routes



Section Summary

Section 6 : Managing and Monitoring Network Operations



6

Section

Section Summary

- Cloud Operations is a hybrid Monitoring, logging, and diagnostics for applications on Cloud Platform and AWS.
- GCP ensures communication is secure at the transport layer, through secure TLS connection management and front-end controls to prevent DoS attacks
- Cloud Endpoints is OAuth 2.0 & Firebase NGINX-based proxy & distributed
- Firewall rules apply to a given project and network, and connections are allowed or denied on a per-instance basis.
- Network Topology is a visualization tool that shows the topology of your Virtual Private Cloud (VPC) networks, hybrid connectivity to and from your on-premises networks, connectivity to Google-managed services, and the associated metrics.
- Google Cloud routes define the paths that network traffic takes from a virtual machine (VM) instance to other destinations.
- In a VPC network, a route consists of a single destination prefix in CIDR format and a single next hop.

Section Review Questions

Section 6 : Managing and Monitoring Network Operations



Review Questions

Your enterprise has migrated the entire application stack to Google Cloud Platform. Your enterprise is running thousands of instances across multiple projects managed by different departments. You want to have a historical record of what was running in Google Cloud Platform at any point in time. What should you do? (Choose One)

- Use Forseti for inventory snapshots
- Use IAM to set up permissions for Splunk
- Use Cloud Operations logging to view records
- Use Security Command Center to view records



Section 7 : Optimize Network Resources

Understanding the domain testable objectives



Domain Objectives

What are the exam objectives covered?

Domain Overview

- Optimize Traffic Flow
- Optimize for Cost and Efficiency



7.1 Optimizing traffic flow

GCP Cloud Developer Overview

Optimizing traffic is critical to maintain performance and also reducing cloud costs.

Services to consider

CDN

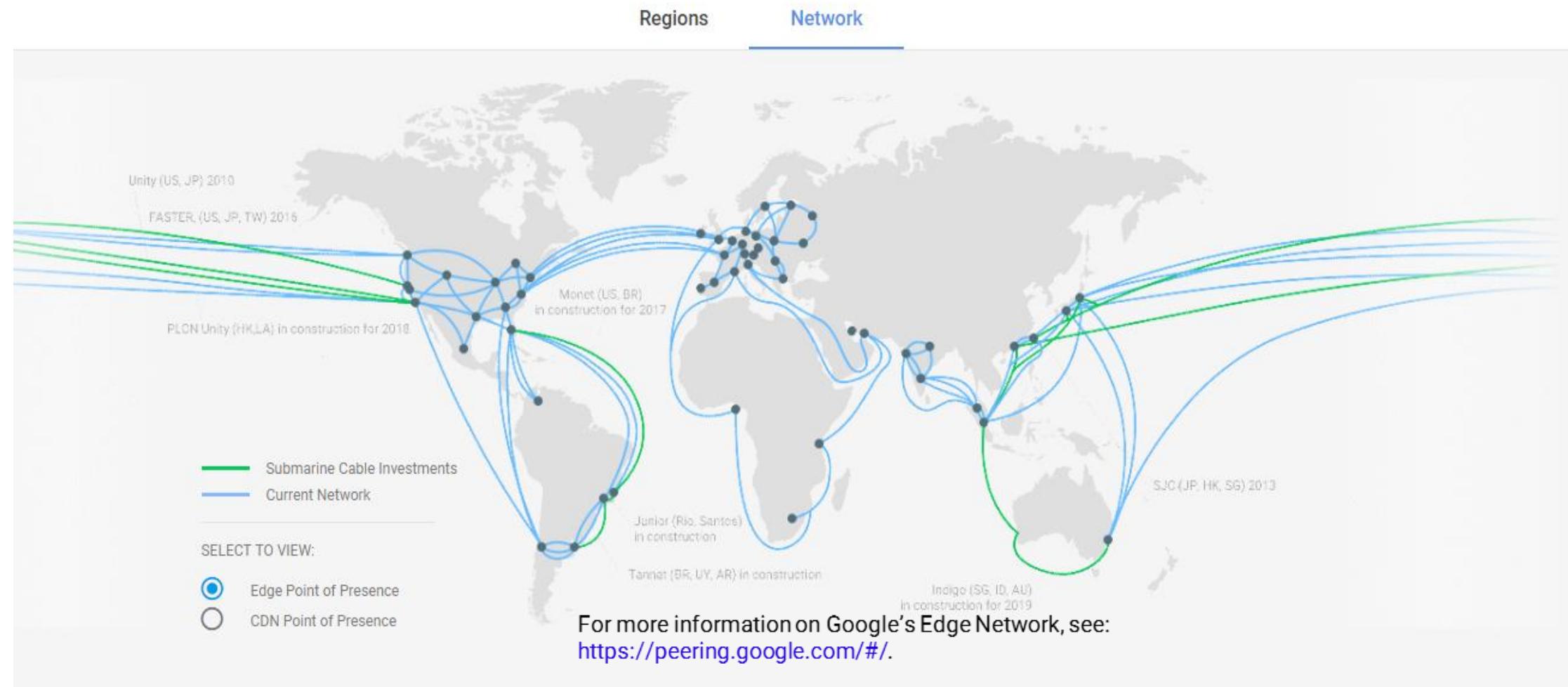
Load Balancing



Load balancer and CDN location

Locality

GCP Cloud Developer Overview



GCP Cloud Developer Overview

≡ Google Cloud Platform PearsonTestEnv ▾

App Engine | Create app

Region
Region is permanent.

us-central ▾

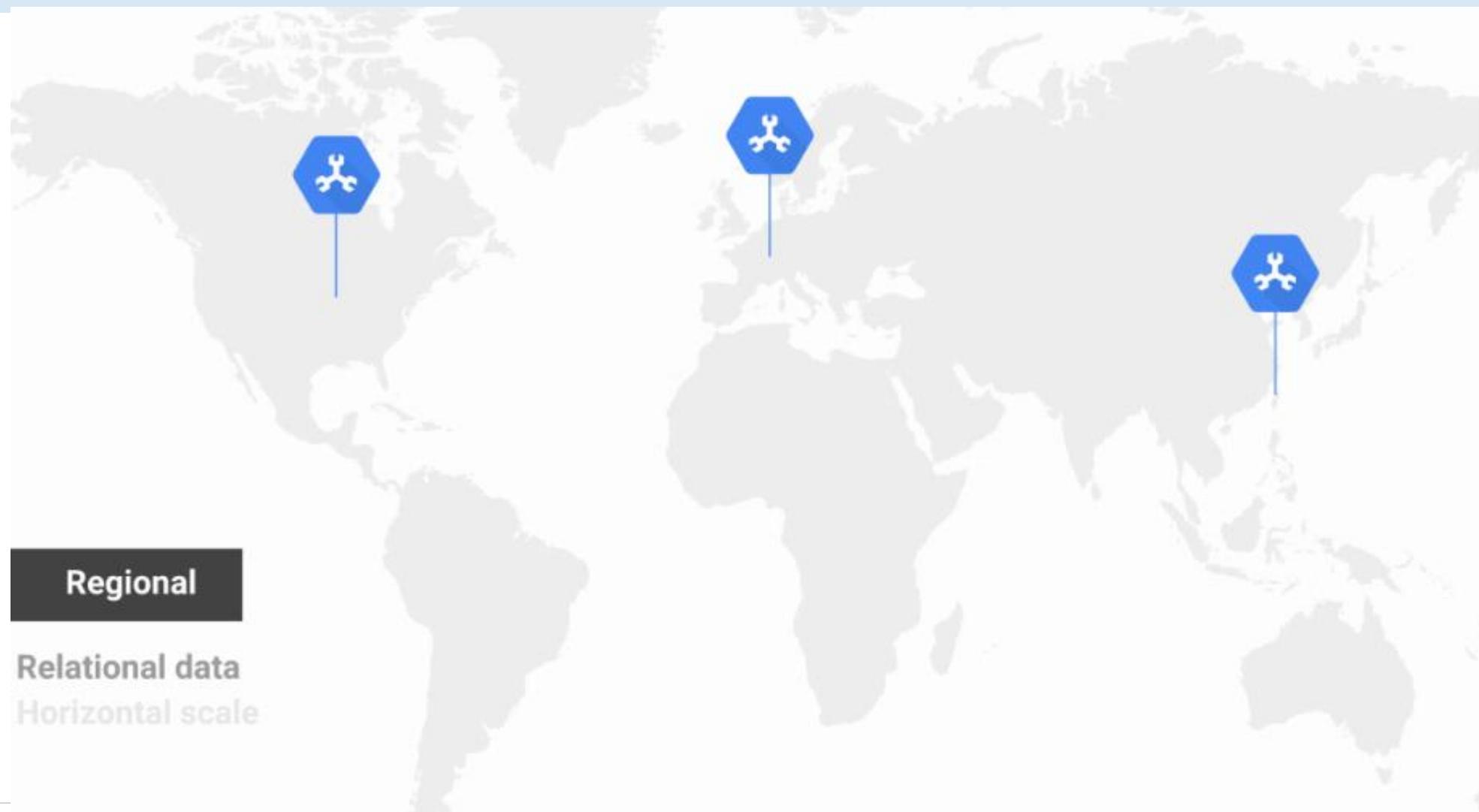


Map data ©2019

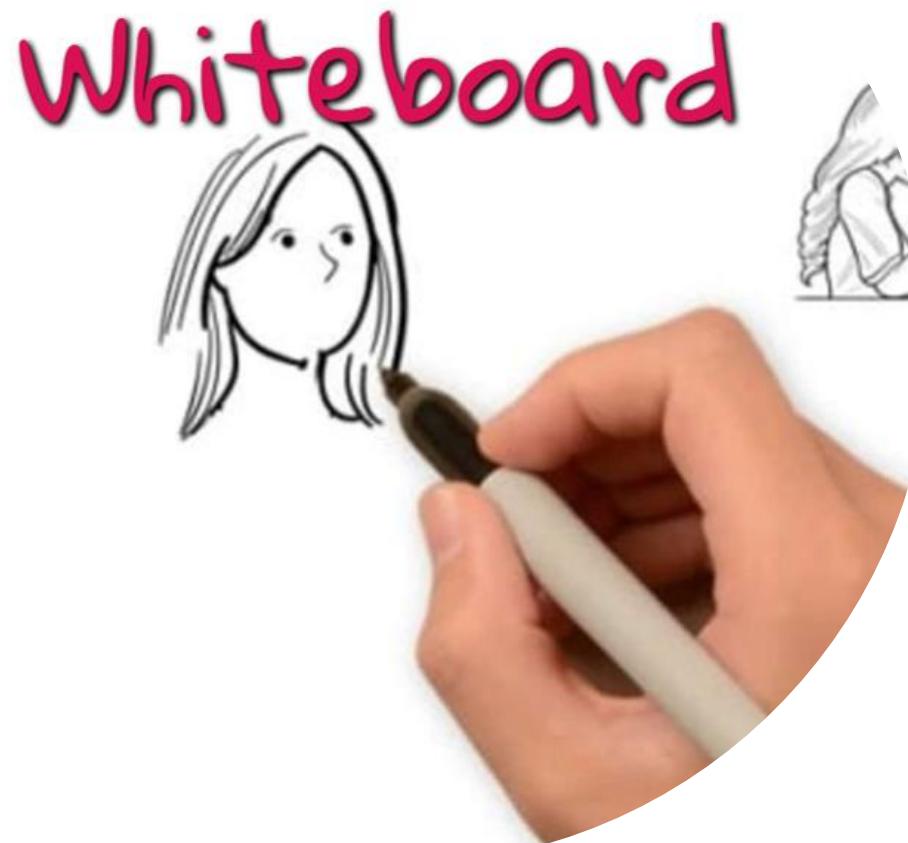
Google

Create app Cancel

GCP Cloud Developer Overview



Designing Locality



- User Distribution

Test Tip



Locality reduces latency and complexity

- SQL is a regional service
- Cloud Spanner is multiregional
- Deploy services as close to your user base.
- App Engine is a regional service.
- Cloud Storage is cached at edge locations

Global vs regional dynamic routing

Locality

GCP Cloud Developer Overview

Cloud Router is a fully distributed and managed Google Cloud service that uses the Border Gateway Protocol (BGP) to advertise IP address ranges.

- It programs custom dynamic routes based on the BGP advertisements that it receives from a peer.
- Instead of a physical device or appliance, each Cloud Router is implemented by software tasks that act as BGP speakers and responders.
- A Cloud Router also serves as the control plane for Cloud NAT.

GCP Cloud Developer Overview

Cloud Router provides BGP services for the following Google Cloud products:

- Dedicated Interconnect
- Partner Interconnect
- HA VPN
- Supported router appliances

GCP Cloud Developer Overview

- The dynamic routing mode of a VPC network—either regional or global—determines which subnet routes the Cloud Routers in that network advertise.
- The dynamic routing mode also controls how each Cloud Router applies learned prefixes as custom dynamic routes in a VPC network.
- When you create a Cloud Router, you choose the Google-side ASN for all BGP sessions used by the Cloud Router.

GCP Cloud Developer Overview

Custom Route

- Custom route advertisement mode gives you control over the routes that a Cloud Router advertises.
- You can specify custom route advertisements for all BGP sessions on a Cloud Router or for individual BGP sessions



Expanding subnet CIDR ranges in service

Network Expansion

GCP Cloud Developer Overview

Primary Range Expansion

- Go to the VPC networks page in the Google Cloud Console. Go to the VPC networks page. ...
- To focus on subnets for a particular network, click the name of a network.
- Click Edit.
- Enter a new, broader CIDR block in the IP address range field. ...
- Click Save.

GCP Cloud Developer Overview

Primary Range Expansion

- When you create a subnet, you must define a primary IP address range.
- You can optionally define one or more secondary ranges
- CIDR range mask length must not be greater than 29, which means that the minimum allowed is /29, while the maximum is /9.

GCP Cloud Developer Overview

Primary Range Expansion - gcloud

Expand IP range of a subnet

- `gcloud compute networks subnets expand-ip-range`

Review this page.

<https://cloud.google.com/sdk/gcloud/reference/compute/networks/subnets/expand-ip-range>

GCP Cloud Developer Overview

Primary Range Expansion

- When you create a subnet, you must define a primary IP address range.
- You can optionally define one or more secondary ranges
- CIDR range mask length must not be greater than 29, which means that the minimum allowed is /29, while the maximum is /9.



Autoscaling

Workload Expansion

GCP Cloud Developer Overview

Primary Range Expansion

- Autoscaling is a tool that allows your apps to efficiently handle increases in traffic by dynamically adding compute capacity but also reduce capacity and costs in periods of low traffic and resource demand.
- Google Compute Engine uses managed instance groups (MIGs), or a collection of common VM instances created from the same API resource known as a template, to automatically add or remove instances based on traffic and demand to your application

7.2 Optimizing for cost and efficiency.

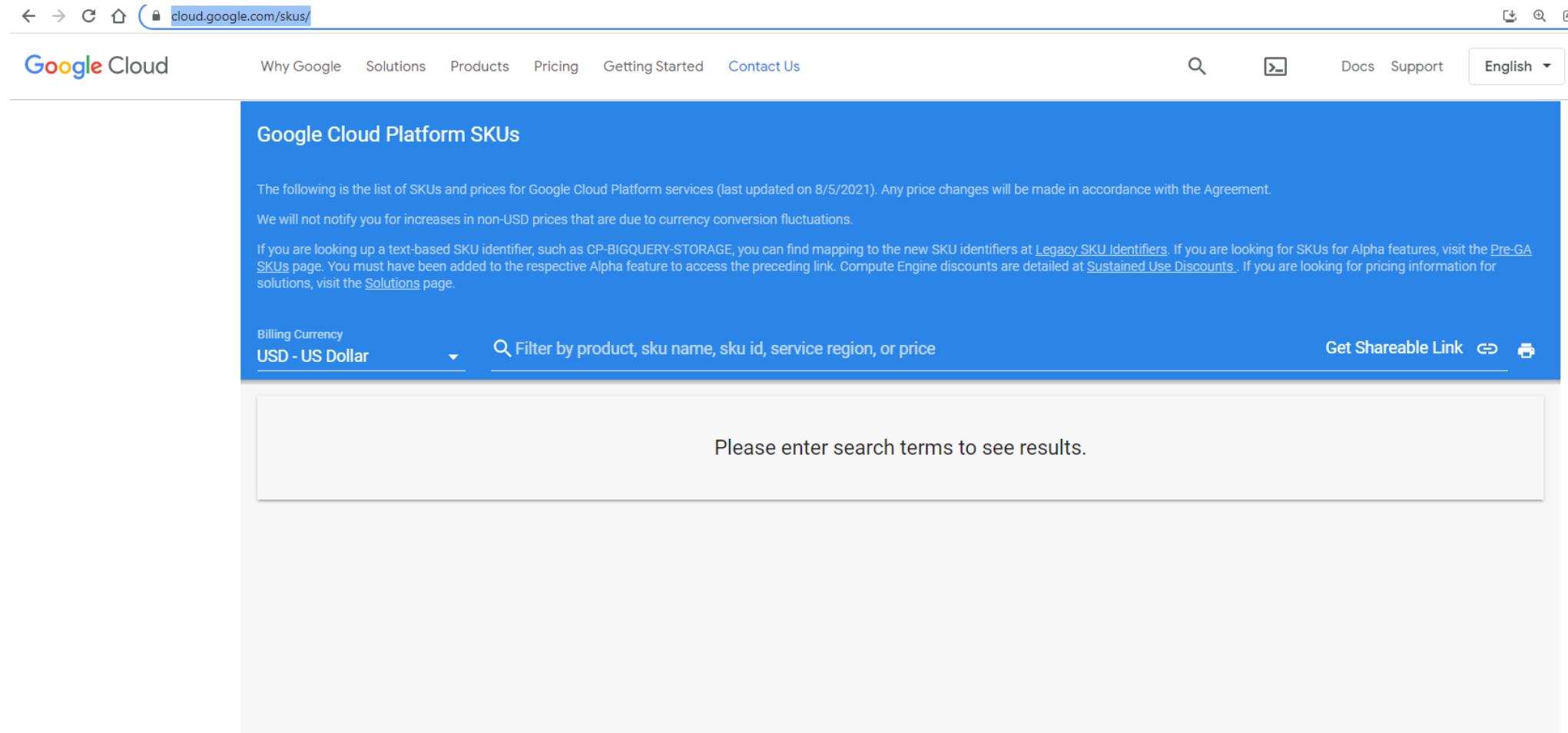
Managing costs

GCP Cloud Developer Overview

Optimization can take many forms

- Identify idle VMs (and disks)
- Schedule VMs to auto start and stop
- Use the right tools to manage costs
- Leverage preemptible VMs
- Rightsized VMs
- Use best storage classes
- Use Lifecycles (storage)
- Dedupe
- Controls

GCP Cloud Developer Overview



The screenshot shows the Google Cloud Platform SKUs page. At the top, there is a navigation bar with links for Why Google, Solutions, Products, Pricing, Getting Started, Contact Us, a search icon, a share icon, Docs, Support, and a language selector set to English. The main title is "Google Cloud Platform SKUs". Below the title, a message states: "The following is the list of SKUs and prices for Google Cloud Platform services (last updated on 8/5/2021). Any price changes will be made in accordance with the Agreement." It also mentions that "We will not notify you for increases in non-USD prices that are due to currency conversion fluctuations." A note for legacy SKU identifiers and alpha features is provided. A dropdown menu for "Billing Currency" is set to "USD - US Dollar". A search bar with placeholder text "Filter by product, sku name, sku id, service region, or price" is present. A "Get Shareable Link" button is located on the right. A large central area displays a message: "Please enter search terms to see results."



Cost optimization

Managing costs

GCP Cloud Developer Overview

Consider

- Network Service Tiers
- Cloud CDN
- Autoscaling



Cost optimization

Managing costs

GCP Cloud Developer Overview

- Network Service Tiers
- Cloud CDN
- Autoscaling

 Network Service Tiers Network Service Tiers

Network Service Tiers enable you to optimize network quality and performance vs. cost for your resources and projects. [Learn more](#)

Project Network Service Tier [?](#)
Premium (recommended) [?](#)

[CHANGE TIER](#)

[Which Network Service Tier is right for me?](#)

Resource Network Service Tiers

Your project resources and the Network Service Tier that they use. You can set the Network Service Tier at the resource level in case you need some resources to use a different Network Service Tier.

Resource Type ↑	Premium tier counts	Standard tier counts
 Static external IP address	0	0
 Load balancer forwarding rule	0	0
 Network Interface	0	0

GCP Cloud Developer Overview

Network Service Tiers

- For GCP Choose between two network service tiers: premium and standard.
- For excellent performance around the globe, you can choose Premium tier
- Standard tier offers a lower performance, but may be a suitable alternative for some cost-sensitive workloads.
- Premium Tier uses Global Load Balancing, while the Standard Tier offers only Regional Load Balancing

<https://cloud.google.com/network-tiers/docs/overview>

GCP Cloud Developer Overview

Network Service Tiers

- Premium Tier Network, users can take advantage of the global fiber network, with globally distributed Points of Presence.
- All the ingress (inbound) traffic from the customer to Google's data centers gets routed to the nearest Point of Presence, which are distributed globally, and then the request is routed 100% over Google's private backbone.
- Premium tier packets spend more time on Google's network, with less bouncing around, and thus perform better (but cost more).

Section Summary

Section 7 : Optimize Network Resources



7

Section

Section Summary

- Cloud Router is a fully distributed and managed Google Cloud service that uses the Border Gateway Protocol (BGP) to advertise IP address ranges
- Google Compute Engine uses managed instance groups (MIGs), or a collection of common VM instances created from the same API resource known as a template, to automatically add or remove instances based on traffic and demand to your application
- It's a best practice to deploy services as close to your user base.
- Autoscaling is a tool that allows your apps to efficiently handle increases in traffic by dynamically adding compute capacity but also reduce capacity and costs in periods of low traffic and resource demand.

Section Review Questions

Section 7 : Optimize Network Resources



Review Questions

Which service provides a cost-effective solution to cache the static content and reduce the load on the origin servers in Google Cloud? (Select One)

- Cloud DNS
- Load Balancing
- Cloud CDN
- Cloudflare

Review Questions

Which service provides a cost-effective solution to cache the static content and reduce the load on the origin servers in Google Cloud? (Select One)

- Cloud DNS
- Load Balancing
- **Cloud CDN**
- Cloudflare

Review Questions

Which of the following two statements are true about Edge locations in GCP?
(Select Two)

- Edge Locations are GCP endpoints that cache content locally
- Services Supported are Amazon CloudFront, S3, Amazon Route 53, GCP Firewall Manager, GCP Shield, and GCP WAF
- Edge Locations are Regions that cache content locally.
- Services Supported are only compute and storage services.

Review Questions

Which of the following two statements are true about Edge locations in GCP?
(Select Two)

- Edge Locations are GCP endpoints that cache content locally
- Services Supported are Amazon CloudFront, S3, Amazon Route 53, GCP Firewall Manager, GCP Shield, and GCP WAF
- Edge Locations are Regions that cache content locally.
- Services Supported are only compute and storage services.



Course Closeout

Let's review and closeout the course

Section Overview

Summary
Review

Resources

Exam
Overview

Course
Closeout



Preparation Summary

Let's Summarize before closing out.

What is a Professional Cloud Network Engineer ?

- This is a certification geared towards people with a technical understanding of both IT security and Google Cloud security best practices.
- Google states that a Professional Cloud Network Engineer has an understanding of security best practices and industry security requirements, this individual designs, develops, and manages a secure infrastructure leveraging Google security technologies.
- The Professional Cloud Network Engineer can manage compliance and cloud security operations.

Preparation Summary

- We must know the basics of cloud security
- We must have hands experience conjuring GCP Services.
- This exam is not an introductory exam and the expectations that GCP sets are high.
- The exam expects you to know GCP Cloud Security services in detail
- The exam expects you to know GCP security best practices
- The exam expects you to determine the best option on the exam. One or more exam questions could be correct.



Resources

Where to find resources and more help

GCP Professional Cloud Network Engineer Crash Course

Learn More



- Google Free Practice Exam
- Use Qwiklabs for hands on practice
- Review GCP Document Library
- Google Next Videos (YouTube)
- O'Reilly Resources



Exam Experience

What to Expect taking the exam and after.

Exam Experience

- Sign up for the exam via Kryterion. <https://www.kryteriononline.com/Locate-Test-Center> (Online or In Person proctored)
- Cost is \$200 at time of writing.
- On the Exam we will have multiple choice questions.
- There are a few Command Line Questions to know
- You will know if you fail or pass when you submit the exam. No score is provided.
- Within 6 weeks you will receive your certificate. (Possibly Swag Kit)

GCP Professional Cloud Network Engineer Crash Course



GCP Professional Cloud Network Engineer Crash Course

Thank You



- Thank you for joining the course
- Please reach out if I can help in anyway.



- Contact me on LinkedIn
- Contact me on YouTube
- Contact me on Steemit
- Contact me on Twitter
- Contact me at Techcommanders



WEBSITE

www.techcommanders.com