

Boot Camp - Professional Cloud Network Engineer

Course#: BC-CN
Duration: 1 Day
Price: 0.00

Course Description

This course provides basic information about the Professional Cloud Network certification exam, including sample questions. Its designed to eliminate any confusion or misunderstandings about the process and nature of the exam itself. Youll also explore additional training resources that can help you prepare for the exam.

Objectives

Position the Professional Cloud Network Engineer Certification.

Provide information, tips, and advice on taking the exam.

Review each section of the exam covering highest-level concepts sufficient to build confidence in what is known by the candidate and indicate skill gaps/areas of study if not known by the candidate.

Connect candidates to appropriate target learning.

Audience

Cloud professionals who intend to take the Professional Cloud Network engineer certification exam.

Prerequisites

Knowledge and experience with GCP, equivalent to GCP Architecting Infrastructure.

At least 1 year of hands-on experience working with Google Cloud Platform and may work on networking or cloud teams with architects who design the infrastructure.

Content

The course includes presentations, demonstrations, and hands-on labs.

Module 1: Designing, planning, and prototyping a GCP network

Failover and disaster recovery strategy

Options for high availability

DNS strategy (e.g., on-premises, Cloud DNS, GSLB)

Meeting business requirements

Choosing the appropriate load balancing options

Optimizing for latency (e.g., MTU size, caches, CDN)

Understanding how quotas are applied per project and per VPC

Hybrid connectivity (e.g., Google private access for hybrid connectivity)

Container networking

Module 2: Implementing a GCP Virtual Private Cloud (VPC)

Configuring GCP VPC resources (CIDR range, subnets, firewall rules, etc.)

Configuring VPC peering

Creating a shared VPC and explaining how to share subnets with other projects

Configuring API access (private, public, NAT GW, proxy)

Configuring VPC flow logs

Configuring internal static/dynamic routing

Configuring routing policies using tags and priority

Configuring NAT (e.g., Cloud NAT, instance-based NAT)

Module 3: Configuring network services

Creating backend services

Firewall and security rules

HTTP(S) load balancer: including changing URL maps, backend groups, health checks, CDN, and SSL certs

- TCP and SSL proxy load balancers
- Network load balancer
- Internal load balancer
- Session affinity
- Capacity scaling
- Enabling and disabling Cloud CDN
- Using cache keys
- Cache invalidation
- Signed URLs
- Managing zones and records
- Migrating to Cloud DNS
- DNS Security (DNSSEC)
- Global serving with Anycast
- Cloud DNS
- Internal DNS
- Integrating on-premises DNS with GCP

Module 4: Implementing hybrid interconnectivity

- Partner (e.g., layer 2 vs. layer 3 connectivity)
- Virtualizing using VLAN attachments
- Bulk storage uploads
- Configuring Cloud Router for reliability.

Module 5: Implementing network security

- Viewing account IAM assignments
- Assigning IAM roles to accounts or Google Groups
- Defining custom IAM roles
- Using pre-defined IAM roles (e.g., network admin, network viewer, network user)
- IP-based access control
- Configuring third-party device insertion into VPC using multi-nic (NGFW)
- Managing keys for SSH access

Module 6: Managing and monitoring network operations

Logging and monitoring with Stack driver or GCP Console

Firewalls (e.g., cloud-based, private)

Diagnosing and resolving IAM issues (shared VPC, security/network admin)

Identifying traffic flow topology (e.g., load balancers, SSL offload, network endpoint groups)

Draining and redirecting traffic flows

Cross-connect handoff for interconnect

Monitoring ingress and egress traffic using flow logs

Monitoring firewall logs

Managing and troubleshooting VPNs

Troubleshooting Cloud Router BGP peering issues

Network throughput and latency testing

Routing issues

Tracing traffic flow

Module 7: Optimizing network resources

Load balancer and CDN location

Global vs. regional dynamic routing

Expanding subnet CIDR ranges in service

Accommodating workload increases (e.g., autoscaling vs. manual scaling)

Cost optimization (Network Service Tiers, Cloud CDN, autoscaler [max instances]) Automation VPN vs. interconnect

Bandwidth utilization (e.g., kernel sys tuning parameters)

Module 8: Next Steps

Present Qwiklabs Challenge Quest for the Professional cloud Network Engineer

Identify Instructor Led Training courses and what they cover that will be helpful based on skills that might be on the exam

Connect candidates to individual Qwiklabs, and to Coursera individual courses and specializations.

