Google Cloud for Network and Security Engineer

Course Overview

A Network Engineer configures, maintains, and troubleshoots network components of their cloud-based infrastructure and also develops, implements, and monitors their organization's security infrastructure to protect sensitive information. This learning path guides you through a curated collection of concepts and labs that provide you with real-world, hands-on experience using Google Cloud technologies essential to the Network and Security Engineer role.

Duration: 08 days / 64 hours

Level: Professional

Prerequisites: There is no prerequisite for this learning path. Basic knowledge of Linux and Network administration is helpful but not mandatory.

Course Outcome: Learner can take **Google Cloud Certified Professional Cloud Network Engineer** exam and **Google Cloud Certified Professional Cloud Security Engineer** exam

Table of Content

Google Cloud Fundamentals: Core Infrastructure

- Introducing Google Cloud
- Resources and Access in the Cloud
- Virtual Machines and Networks in the Cloud
- Storage in the Cloud
- Containers in the Cloud
- Applications in the Cloud
- Prompt Engineering

Networking in Google Cloud: Fundamentals

- Welcome to Networking in Google Cloud
- VPC Networking Fundamentals
- Sharing VPC Networks
- Network Monitoring and Logging

Networking in Google Cloud: Routing and Addressing

- Welcome to Networking in Google Cloud
- Network Routing and Addressing in Google Cloud
- Private Connection Options

Managing Security in Google Cloud

- Foundations of Google Cloud Security
- Securing Access to Google Cloud
- Identity and Access Management (IAM)
- Configuring Virtual Private Cloud for Isolation and Security

Security Best Practices in Google Cloud

- Welcome to Security Best Practices in Google Cloud
- Securing Compute Engine: Techniques and Best Practices
- Securing Cloud Data: Techniques and Best Practices
- Application Security: Techniques and Best Practices
- Securing Google Kubernetes Engine: Techniques and Best Practices

Mitigating Security Vulnerabilities on Google Cloud

- Protecting against Distributed Denial of Service Attacks (DDoS)
- Content-Related Vulnerabilities: Techniques and Best Practices
- Monitoring, Logging, Auditing and Scanning

Logging and Monitoring in Google Cloud

- Introduction to Google Cloud Operations Suite
- Monitoring Critical Systems
- Alerting Policies
- Advanced Logging and Analysis
- Working with Audit Logs

Observability in Google Cloud

- Configuring Google Cloud Services for Observability
- Monitoring Google Cloud Network
- Investigating Application Performance Issues
- Optimizing the Costs for Google Cloud Observability