Security & Identity Fundamentals

Fundamental 8 Steps 1 day 40 Credits

Security is an uncompromising feature of Google Cloud services, and Google Cloud has developed specific tools for ensuring safety and identity across your projects. In this fundamental-level quest, you will get hands-on practice with Google Cloud's Identity and Access Management (IAM) service, which is the go-to for managing user and virtual machine accounts. You will get experience with network security by provisioning VPCs and VPNs, and learn what tools are available for security threat and data loss protections. Looking for a hands on challenge lab to demonstrate your skills and validate your knowledge? On completing this quest, enroll in and finish the additional challenge lab at the end of this quest to receive an exclusive Google Cloud digital badge.

Infrastructure Security

Prerequisites:

Although this quest will teach you the fundamentals of Identity and Access Management (IAM) and Security in Google Cloud, you will still need hands-on experience with the platform's core tools and services. It is recommended that the student have at least earned a Badge by completing the Google Cloud Essentials and/or the Baseline: Infrastructure Quests before beginning.

Quest Outline

Cloud IAM: Qwik Start

Google Cloud IAM unifies access control for Cloud Platform services into a single system to present a consistent set of operations. Watch the short video Manage Access Control with Google Cloud IAM.

45 minutes | Introductory | 1 Credit

IAM Custom Roles

Cloud IAM provides the right tools to manage resource permissions with minimum fuss and high automation. You don't directly grant users permissions. Instead, you grant them roles, which bundle one or more permissions. This allows you to map job functions within your company to groups and roles.

1 hour | Fundamental | 5 Credits

Service Accounts and Roles: Fundamentals

In this hands-on lab, you will learn how to create and manage Service Accounts

1 hour | Fundamental | 5 Credits

VPC Network Peering

Google Cloud Platform (GCP) Virtual Private Cloud (VPC) Network Peering allows private connectivity across two VPC networks regardless of whether or not they belong to the same project or the same organization.

45 minutes | Advanced | 7 Credits

User Authentication: Identity-Aware Proxy

Learn how to restrict access selected authenticated users with Identity-Aware Proxy without special programming. Discover how to retrieve user identity information from IAP.

1 hour | Fundamental | 5 Credits

Getting Started with Cloud KMS

In this lab you'll work with advanced features of Google Cloud Security and Privacy APIs, including setting up a secure Cloud Storage bucket, managing keys and encrypted data using Key Management Storage, and viewing Cloud Storage audit logs.

30 minutes | Fundamental | 5 Credits

Google Cloud Packet Mirroring with OpenSource IDS

This lab demonstrates a common enterprise use case for Google Cloud's Packet Mirroring in conjunction with an Open Source Intrusion Detection System.

1 hour 30 minutes | Fundamental | 5 Credits

Setting up a Private Kubernetes Cluster

Hands-on lab for creating a private cluster in the cloud environment. In a private cluster, nodes do not have public IP addresses, so your workloads run in an environment that is isolated from the Internet. Prerequisites: Experience with Kubernetes Clusters, and CIDR-range IP address.

1 hour 30 minutes | Advanced | 7 Credits

Quest Complete!

Congrats! You completed this quest and earned a badge. Become a cloud expert and start another.