**Resources and access in the cloud**

- (Google Cloud resouce hieracgy) In Google Cloud, the resource hierarchy consists of four levels: resources, projects, folders, and the organization node. Resources represent virtual machines, Cloud Storage buckets, etc. Projects are entities under the organization node, enabling the use of Google Cloud services. Each project has a unique project ID assigned by Google and can have different owners and users. Folders sit at the third level and allow policies to be applied to resources within them, providing granularity. Folders can contain projects or other folders and help group resources based on departments or teams. The organization node is at the top level, encompassing all projects, folders, and resources in the organization. It allows for the management and application of policies at various levels and enables administrative control, including project creation and spending. The organization node can be automatically created for Google Workspace customers or generated using Cloud Identity for others.

- (Identity and Access Management (IAM) ) In Google Cloud, Identity and Access Management (IAM) allows administrators to control access and permissions for resources. IAM policies define "who" (principals) can do "what" (permissions) on resources. Principals can be Google accounts, Google groups, service accounts, or Cloud Identity domains, each with its identifier (usually an email address). IAM roles are collections of permissions. When a role is granted to a principal, they receive all the permissions within that role. IAM policies apply to the chosen element and all elements below it in the resource hierarchy. Deny policies can prevent certain principals from using specific permissions, overriding allow policies. There are three types of roles: basic (broad in scope, such as owner, editor, viewer, and billing administrator), predefined (specific roles offered by Google Cloud services), and custom (tailored roles with specific permissions). Custom roles require managing permissions and can only be applied at the project or organization level, not folders. Companies often use a "least-privilege" model, assigning minimal privilege needed for each job role.

- (Service accounts) Service accounts in Google Cloud are used to grant permissions to applications or virtual machines instead of individual users. They use cryptographic keys for authentication and can access resources based on assigned roles. Service accounts are managed as resources, allowing IAM policies to be attached to them, providing flexibility in assigning roles to different users. They provide a secure and controlled way to authorize applications without revealing sensitive credentials to individual users.

- (Cloud Identity) Cloud Identity is a tool that enables organizations to centrally manage user identities and access to Google Cloud resources. It allows admins to define policies, manage users and groups, and control access. When someone leaves the organization, their account can be disabled and removed from groups. It comes in free and premium editions, and Google Workspace customers already have access to these features in the Google Admin Console.

- (Interacting with Google Cloud) Briefly, there are four ways to access and interact with Google Cloud:

1. Google Cloud Console: A web-based graphical user interface for deploying, managing, and diagnosing production issues.
2. Cloud SDK and Cloud Shell: A set of command-line tools for managing resources and applications on Google Cloud, with Cloud Shell providing browser-based command-line access.
3. APIs: Services on Google Cloud offer APIs that allow developers to control them programmatically.
4. Cloud Console Mobile App: An app that allows users to manage Google Cloud resources, view logs, administer applications, and receive billing information on mobile devices.

- (Getting started with GCP and Qwiklabs) In Google Cloud training, labs are completed through the hands-on lab platform, which gives limited time access to Google Cloud resources with temporary login credentials. To start a lab, click 'Start Lab' and access the temporary environment. The lab page will display student login credentials, project details, a timer, and an 'Open Google Console' button. Open the Google Console in an incognito window to avoid login errors. Login using the temporary credentials and agree to the terms. Progress through the lab, switch between the lab page and console as needed, and complete tasks to increase your score. Remember to finish before the timer runs out or click 'End Lab' to delete the temporary login and content. Provide feedback and return to the course once you complete the lab successfully.