Understanding how access management works on Google Cloud is key to making the following decisions as you plan your SAP implementation:

- How to organize your resources on Google Cloud.
- Which team members can access and work with resources.
- Exactly which permissions each team member needs to have to conform to the *least privileges* (/iam/docs/using-iam-securely) principle for resource access.
- Which services and applications need to use which service accounts, and what level of permissions to grant in each case.

ant: Google Cloud recommends that you follow the best practices for enterprise-grade access control provided in izational setup (/docs/enterprise/best-practices-for-enterprise-organizations#organizational_setup), and Identity a s management (/docs/enterprise/best-practices-for-enterprise-organizations#identity-and-access-management) in ractices for Enterprise Organizations guide.

For a high-level overview of authentication on Google Cloud, see Authentication overview (/docs/authentication/).

The Cloud Platform Resource Hierarchy (/resource-manager/docs/cloud-platform-resource-hierarchy#organizations) defines the various resource containers on Google Cloud, how they relate to each other, and what the access scopes are.

Access control policies applied to a parent resource, such as an organization or project, are inherited by the children of that resource, such as the Compute Engine virtual machines or Cloud Storage buckets in the organization or project.

Cloud Identity and Access Management (Cloud IAM) provides unified control over permissions for Google Cloud resources. You can manage access control by defining who has what access to resources. For example, you can control who can perform control-plane operations on your SAP instances, such as creating and modifying VMs, persistent disks, and networking.

Cloud IAM *service accounts* provide a way for you to give permissions to applications and services. It's important to understand how service accounts work in Compute Engine. For details, see Service Accounts (/compute/docs/access/service-accounts).

Cloud IAM *roles* grant permissions to users. For a reference about roles and which permissions they provide, see Identity and Access Management Roles (/iam/docs/overview#roles).

For more details about Cloud IAM, see the Overview of Cloud IAM (/iam/docs/overview).

For each resource that your SAP systems use, such as a Compute Engine resource, you need understand how Cloud IAM implements authentication and access management for the resource and what predefined roles Cloud IAM provides for the resource.

For information about how some resources that are commonly used by SAP systems implement Cloud IAM, see:

- BigQuery predefined roles and permissions (/bigquery/docs/access-control)
- Compute Engine access control options (/compute/docs/access/)
- Deployment Manager access control options (/deployment-manager/docs/access-control)
- Stackdriver Logging access control guide (/logging/docs/access-control)
- Stackdriver Monitoring access control (/monitoring/access-control)