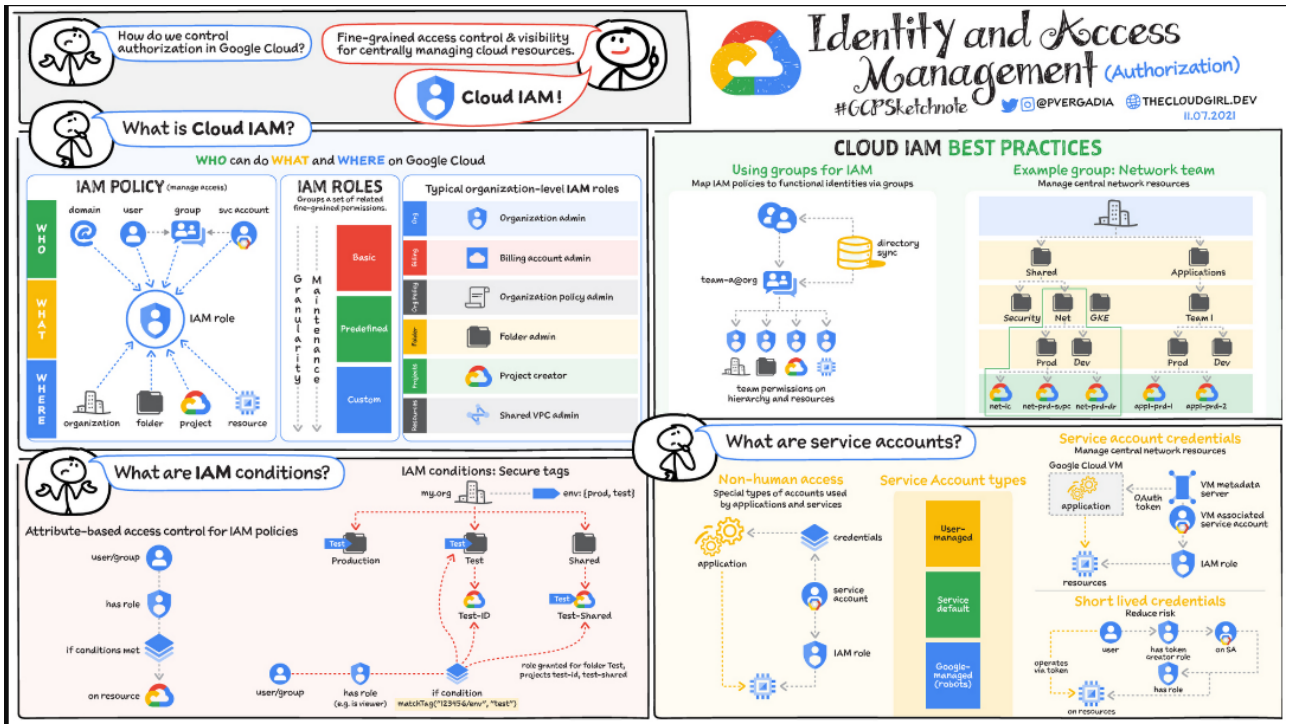
GCP IAM

- Overview



Cloud Identity: Managing Users

Cloud Identity Managing IdP and an HR system managing Users

- Organizations uses HRIS such as SAP, Successfactores or Workday to manage their users Refer Here

Cloud Identity delegates all IdP and user management to external provider (non-AD)

- Refer Here for details

Integrating Cloud Identity with Microsoft Active Directory

- AD Manages users and passwords on-premises, users are replicated to Google and Cloud Identity then acts as the IdP for access to Google cloud Refer Here
- AD manages users and passwords on-premises, users are replicated to Google and Cloud Identity then manages access to Google Cloud Refer Here
- AD Manages user and password onpremise, users are replicated to Google, and Cloud identity user on-premises ADFS for authentication
    - Refer Here for on-prem
    - Refer Here for office 365 integration.

Creating an intitial set of security groups

- The following groups are expected to be at bare miniumum in gcp as best practice
    - gcp-organization-admins:
        - Full control on logical structure
        - super users

        - there wont be many
    - gcp-network-admins
        - They manage vpc networks, shared vpcs, control network traffic, configure firewall rules
    - gcp-billing-admins:
        - pay attention to level of spending
    - gcp-developers:
        - they will be given permission to build, design, code and test apps in specific projects/environments
    - gcp-secuirty-admins:
        - They manage
    - gcp-devops:
        - they will be managing end to end CI/CD, infra provision on certain environments

Service Accounts (SA)

- They are used to provide non-human access to Google Cloud Services and they donot have any associated password and cannot login from browser
- Authentication is accomplished via public/private key pairs
- Unlike user accounts, Service Accounts dont belong to Google Workspace or Cloud Identity domain, they are create and managed inside GCP Project.
- There are three service account types
    - User managed service accounts:
        - create by us using CLI or API
        - By default a project can have 100 SA's (quota can be increased)
        - when we create a SA the name provided will be combine with project-id to create a SA email address `<your-name>@<project-id>.iam.gserviceaccount.com`
    - Default Service accounts:
        - Create by GCP to run some services
    - Google Managed service accounts
        - Created by Google in cojunction with Various services and when thoser service act on your behalf
        - Example:
            - These account setup behind K8s, compute engines etc..