



# Kubernetes Workshop - GKE, Kubeflow

Date: Oct '14 2023

Instructor:  
Akash Agrawal  
<https://www.flaskd.in>



## Reference Links

- GitHub: <https://github.com/sky29/gdg-cloud-workshop-blr-oct-2023>
- [if required] Shared-doc-temp: <https://bit.ly/3PT5hIQ>
- [if required] Shared-sheet-temp: <https://bit.ly/3PN0HeQ>



# Objective

- GCP Project Level Access & Resource Hierarchy
- GKE Cluster
- Kubernetes Workloads
- Kubeflow



# About Me

- I have ~15 years of experience in IT Industry.
- Currently I work as an **[Independent] Consultant** (from last 4+ years).
- **Key Focus Area:** Cloud Infrastructure | Cloud Native Solutions | DevOps Automation | Big Data Ecosystem
- Previous to that, I worked [as Employee] with various global clients like Sabre Travel Technologies / Tangoe India Pvt. Ltd. / L&T Infotech (Clients: Citi Bank / Goldman Sachs) etc. (~ a decade)
- Get more details about me: <https://www.flaskd.in>



# Module-I:

## Google Cloud Platform (GCP) Access



# GCP Access - Scope

- Identity Onboarding:
  - GCP Resource Hierarchy
  - Identity & Access Management (IAM)



# Module-II:

**Google Kubernetes Engine (GKE)**



# GKE- Overview

- **Kubernetes** = [Open Source] Container Orchestration Platform
- **GKE** = [Managed] Kubernetes Service on Google Cloud
- Shared Responsibility Principle

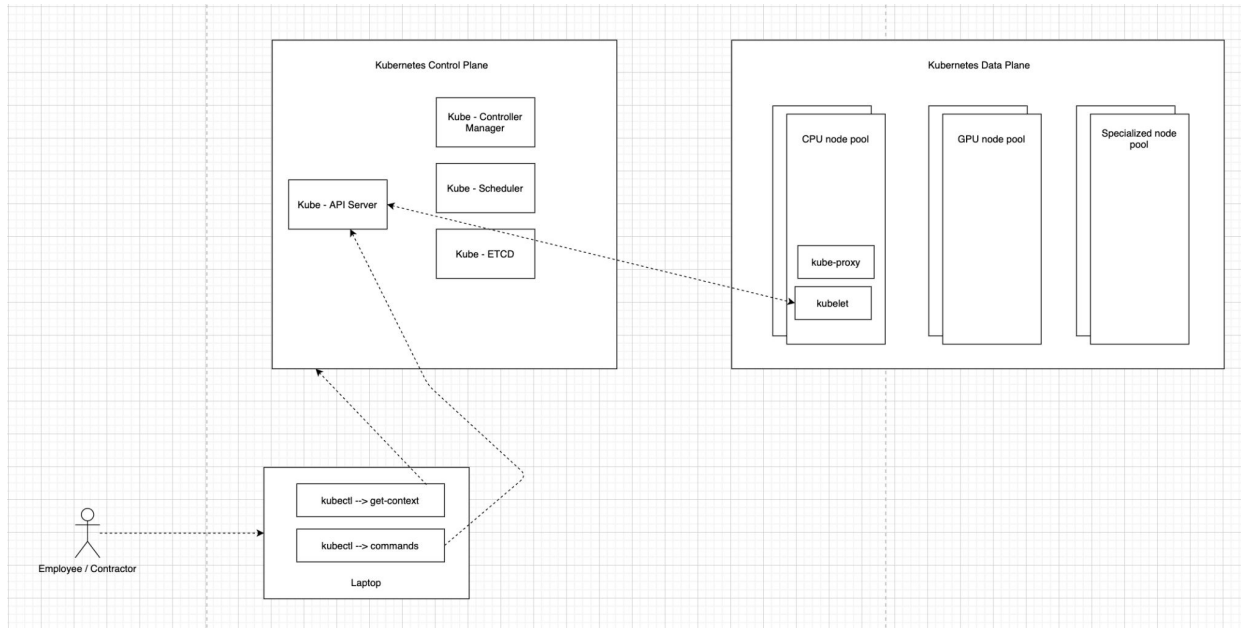




# GKE Cluster

- 3 angles:
  - Visibility:
    - GKE Public Cluster
    - GKE Private Cluster
  - Modes:
    - GKE Cluster in Standard Mode
    - GKE Cluster in Autopilot Mode
  - Zonal or Regional:
    - GKE Zonal Cluster
    - GKE Regional Cluster

# Kubernetes (Open Source) - Architecture





# Kubernetes Workloads

- **Sample:**
  - Ingress-nginx
  - External-dns
  - Cert-manager
  - Cert-issuer
  - Demo app



# Module-II:

Kubeflow



# Kubeflow - Scope

- Kubeflow Overview
- Kubeflow Installation
- Kubeflow - Experimentation & Notebooks
- Kubeflow - Multi User Access
- Kubeflow - Pipeline



# Kubeflow - Overview

- **Machine Learning Toolkit for Kubernetes**
  - ML Workflows / Pipelines
  - Composable, Portable, Scalable ML Stack
  - MLOPs



# Kubeflow - Installation

- **Using Manifests:**
  - Create a Kubernetes Cluster
  - Install Kustomize (specific version)
  - Clone the Kubeflow Manifest Repository
  - Deploy Kubeflow
  - Access Kubeflow UI by port forwarding (HTTP)...



# Kubeflow - Installation

- **Using Packaged Distributions:**
  - DeployKF
  - Kubeflow on Google Cloud
  - ...





# Understanding ML Workflow

- Experimentation
- Pipelining
- Training
- Inference
- Others



# Kubeflow - Notebooks

- **Notebooks**
  - Use:
    - EDA / Rapid Data Analysis / Prototyping / Experimentation
    - Also well suited for smaller datasets:
      - EDA + Train + Serve
  - Native support for JupyterLab, RStudio, and Visual Studio Code (code-server).
  - Web-based development environments + running as pods
  - External Volumes / PV & PVCs
  - Accelerators - GPUs
  - Custom Images + Admins can provide standard notebook images for their organization with required packages pre-installed



# Kubeflow - Multi Tenancy + Multi Users

- **Configured by Kubeflow Administrators**
- **Goal:**
  - Users only have necessary and minimal access, which is configured by Administrator
- **Kubeflow Components that supports multi user isolation:**
  - Central Dashboard, Notebooks, Pipelines, AutoML (Katib), KFServing
  - Resources created by the notebooks (for example, training jobs and deployments) also inherit the same access



# Kubeflow - Multi Tenancy + Multi Users

- **Key Concepts:**
  - **Administrator:**
    - someone who creates and maintains the Kubeflow cluster.
    - configures permissions (i.e. view, edit) for other users
  - **User:**
    - A User is someone who has access to some set of resources in the cluster.
    - User's access privileges - defined by the Administrator
  - **Profile:**
    - A Profile is a unique configuration for a user, which determines their access privileges
    - defined by the Administrator



# Kubeflow - Multi Tenancy + Multi Users

- **Key Concepts:**
  - **Isolation:**
    - Isolation uses Kubernetes Namespaces.
    - Namespaces isolate users or a group of users
  - **Authentication:**
    - Authentication is provided by an integration of Istio and OIDC and is secured by mTLS
  - **Authorization:**
    - Authorization is provided by an integration with Kubernetes RBAC



# Kubeflow Pipelines

- Deploying ML workflows
- Components:
  - UI - Experiments, Jobs, Runs
  - Engine - for scheduling workflows (Argo Workflow based)
  - Python SDK - DSL, Defining Pipelines programmatically
  - Notebooks



# Thanks

**Akash Agrawal**

**Website:** <https://www.flaskd.in>

**LinkedIn:** <http://www.linkedin.com/in/akash-agrawal-58a97813>