GCP Assignment 1

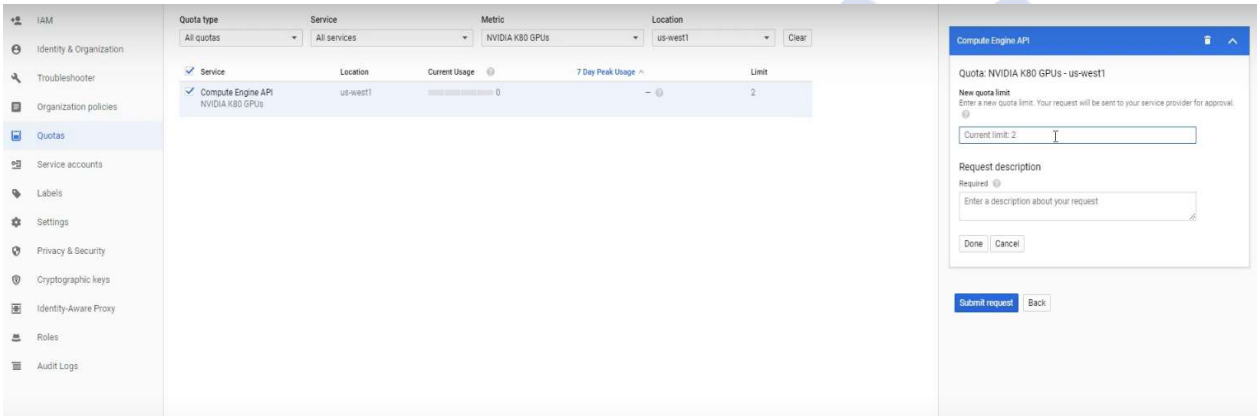
1. What is the GCP project quota? If necessary, how GCP quota can be increased?

   Project quotas protect Google Cloud users from unforeseen spikes in usage. However, as your usage of Google Cloud Platform increases, you can request an increase in your project quota. To request an increase to your quota, contact the Support team. project

   GCP Quota can be increased by –

   1. Go to the Quotas page.
   2. On the Quotas page, find the quota you want to increase in the Limit name column.
   3. Select the checkbox to the left of your quota.
   4. Click create EDIT QUOTAS.
   5. In the Quota changes form, enter the increased quota that you want for your project in the New limit field.

   For example in below screen shot , trying to increase quota for Compute Engine:



2. What is the definition of a virtual machine? Virtual machine types are offered in GCP. How to create a virtual computer in Google Cloud Platform.

A VM is a virtualized instance of a computer that can perform almost all the same functions as a computer, including running applications and operating systems. Virtual machines run on a physical machine and access computing resources from software called a hypervisor.

Virtual machine types that are offered in GCP –

- **Machine family**: A curated set of processor and hardware configurations optimized for specific workloads. When you create a VM instance, you choose a predefined or custom machine type from your preferred machine family.
- **Series**: Machine families are further classified by series and generation. For example, the N1 series within the general-purpose machine types is the older version of the N2 series. Generally, generations of a machine series use a higher number to describe the newer generation. For example, the N2 series is the newer generation of the N1 series.
- **Machine type**: Every machine series has predefined machine types that provide a set of resources for your VM. If a predefined machine type does not meet your needs, you can also create a custom machine type.

Creating a VM computer in GCP –

1. In the Google Cloud Console, go to the **VM instances** page.

   Go to VM instances
2. Select your project and click **Continue**.
3. Click **Create instance**.
4. Specify a **Name** for your VM.
5. Optional: Change the **Zone** for this VM. Compute Engine randomizes the list of zones within each region to encourage use across multiple zones.
6. Select a **Machine configuration** for your VM.
7. In the **Boot disk** section, click **Change**, and then do the following:
   a. On the **Public images** tab, choose the following:
      - Operating system
      - OS version

- Boot disk type
- Boot disk size

b. Optional: For advanced configuration options, click **Show advanced configuration**.

c. To confirm your boot disk options, click **Select**.

8. In the **Firewall** section, to permit HTTP or HTTPS traffic to the VM, select **Allow HTTP traffic** or **Allow HTTPS traffic**. When you select one of these, Compute Engine adds a network tag to your VM, which associates the firewall rule with the VM. Then, Compute Engine creates the corresponding ingress firewall rule that allows all incoming traffic on tcp:80 (HTTP) or tcp:443 (HTTPS).
9. Optional: If you chose an OS image that supports Shielded VM features, you can modify the Shielded VM settings. To modify shielded VM settings, expand the **Security** section in the **Networking, disks, security, management, sole tenancy** section and do the following, as required:

- To turn on Secure Boot, select **Turn on Secure Boot**. Secure Boot is disabled by default.
- To turn off vTPM, clear the **Turn on vTPM** checkbox. vTPM is enabled by default. Disabling vTPM also disables integrity monitoring because integrity monitoring relies on data gathered by Measured Boot.
- To turn off integrity monitoring, clear the **Turn on Integrity Monitoring** checkbox. Integrity monitoring is enabled by default.

10. To create and start the VM, click **Create**.

We can create VM using gcloud command as well:

1. Select a public image. Make a note of the name of the image or image family and the name of the project containing the image.
2. Use the gcloud compute instances create command to create a VM from an image family or from a specific version of an OS image.

   If you specify the optional --shielded-secure-boot flag, Compute Engine creates a VM with all three of the Shielded VM features enabled:

   - Virtual trusted platform module (vTPM)
   - Integrity monitoring
   - Secure Boot

   After Compute Engine starts your VM, you must stop the VM to modify Shielded VM options.

gcloud compute instances create *VM_NAME* \
[--image=*IMAGE* | --image-family=*IMAGE_FAMILY*] \
--image-project=*IMAGE_PROJECT*
--machine-type=*MACHINE_TYPE*

Replace the following:

- *VM_NAME*: name of the new VM
- *IMAGE* or *IMAGE_FAMILY*: specify one of the following:
  - *IMAGE*: a specific version of a public image

    For example, --image=debian-10-buster-v20200309.
  - *IMAGE_FAMILY*: an image family.

    This creates the VM from the most recent, non-deprecated OS image. For example, if you specify --image-family=debian-10, Compute Engine creates a VM from the latest version of the OS image in the Debian 10 image family.
- *IMAGE_PROJECT*: project containing the image
- *MACHINE_TYPE*: machine type, predefined or custom, for the new VM

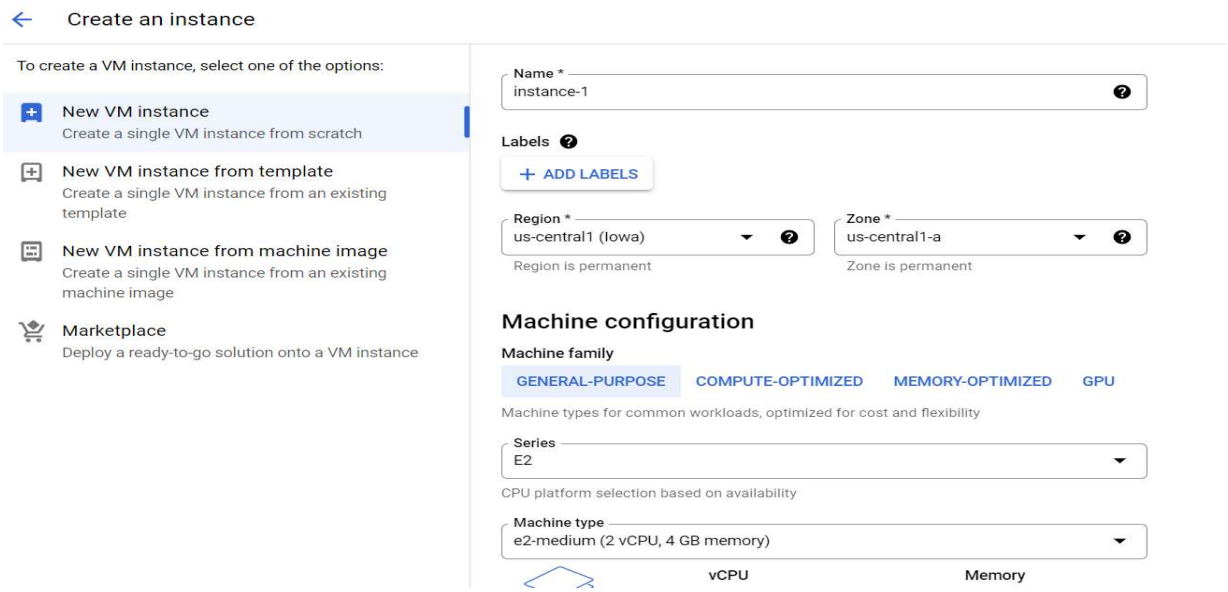
  To get a list of the machine types available in a zone, use the gcloud compute machine-types list command with the --zones flag.

3. Verify that Compute Engine created the VM:
4. gcloud compute instances describe *VM_NAME*

   Replace *VM_NAME* with the name of the VM.

We can use terraform and API as well to create VM.

For reference, please find below screen shot of creating VM from console.



3. What is Google Big Query, and how does it work? Replicate certain instances to demonstrate a use case.

   BigQuery is a fully managed enterprise data warehouse that helps you manage and analyze your data with built-in features like machine learning, geospatial analysis, and business intelligence. BigQuery's serverless architecture lets you use SQL queries to answer your organization's biggest questions with zero infrastructure management. BigQuery's scalable, distributed analysis engine lets you query terabytes in seconds and petabytes in minutes.

   BigQuery maximizes flexibility by separating the compute engine that analyzes your data from your storage choices. You can store and analyze your data within BigQuery or use BigQuery to assess your data where it lives. Federated queries let you read data from external sources while streaming supports continuous data updates. Powerful tools like BigQuery ML and BI Engine let you analyze and understand that data.

   BigQuery interfaces include Google Cloud Console interface and the BigQuery command-line tool. Developers and data scientists can use client libraries with familiar programming including Python, Java, JavaScript, and Go, as well as BigQuery's REST API and RPC API to transform and manage data. ODBC and JDBC drivers provide interaction with existing applications including third-party tools and utilities.

As a data analyst, data engineer, data warehouse administrator, or data scientist, the BigQuery ML documentation helps you discover, implement, and manage data tools to inform critical business decisions.

USE CASES

Use cases

USE CASE

Migrating data warehouses to BigQuery

Solve for today’s analytics demands and seamlessly scale your business by moving to Google Cloud’s modern data warehouse. Streamline your migration path from Netezza, Oracle, Redshift, Teradata, or Snowflake to BigQuery and accelerate your time to insights. Learn more and get started with our comprehensive data warehouse migration guides.

USE CASE

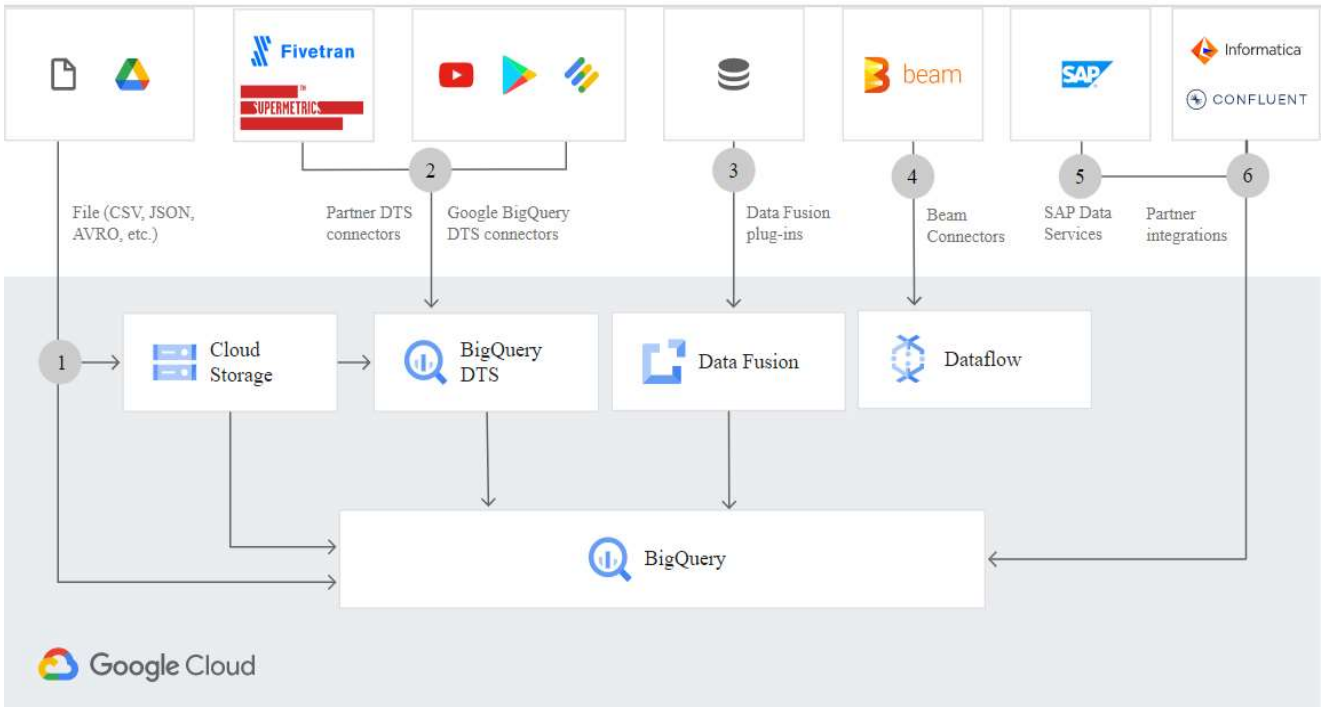
Predictive analytics

Predictive analytics helps you predict future outcomes more accurately and discover opportunities in your business. Our smart analytics reference patterns are designed to reduce time-to-value for common analytics use cases with sample code and technical reference guides.

USE CASE

Bring any data into BigQuery

Make analytics easier by bringing together data from multiple sources in BigQuery, for seamless analysis. You can upload data files from local sources, Google Drive, or Cloud Storage buckets, take advantage of BigQuery Data Transfer Service (DTS), Data Fusion plug-ins, or leverage Google's industry-leading data integration partnerships. You have ultimate flexibility in how you bring data into your data warehouse.



4. What exactly is the Google Cloud SDK? List the numerous Google cloud SDK installation options.

   Google Cloud SDK (Software Development Kit), in simple terms, is a set of tools that are used to manage applications and resources that are hosted on the Google Cloud Platform.

   It is composed of the **gsutil**, **gcloud**, and **bqcommand** line tools. The gcloudtool is automatically downloaded with the Cloud SDK.

   There are some stipulations or the system **necessities** for the installation of Google Cloud SDK.

   Google Cloud SDK run on specific platforms – Windows, Linux, and macOS and requires Python 2.7.x.

   Some specific tools within the Google Cloud
   SDK might have further necessities like Java tools used for the development of Google App Engine needs Java 1.7 or the later one.

   INSTALLATION:

   There are four different ways for the installation of the Google Cloud SDK. As per the necessity, the user will choose any of the following to install Google Cloud Software Development Kit.

- Using Cloud SDK with scripts or continuous integration or continuous deployment – during this case, the user will install google cloud SDK by downloading a versioned archive for a non-interactive installation of a specific version of Cloud SDK.
- By running Red Hat Enterprise Linux 7/CentOS 7 – YUM is used to get the latest released version of the Google Cloud SDK in the package format.
- Through running Ubuntu/Debian – APT-GET is employed to get the most recent free version of the Google Cloud SDK in the package format.
- For all the other use cases, the user will run the interactive installer to install the latest version of the Google Cloud SDK.

5. List the many cloud computing deployment models.

   There are **four cloud** deployment models: public, private, community, and hybrid.

   • Public Cloud
   The public cloud model is the most widely used cloud service. This cloud type is a popular option for web applications, file sharing, and non-sensitive data storage. The service provider owns and operates all the hardware needed to run a public cloud. Providers keep devices in massive data centers.
   The public cloud deliverynmodel plays a vital role in development and testing. Developers often use public cloud infrastructure for development and testing purposes. Its virtual environment is cheap and can be configured easily and deployed quickly, making it perfect for test environments.

   • Private Cloud
   Whereas a public model is available to anyone, a private cloud belongs to a specific organization. That organization controls the system and manages it in a centralized fashion. While a third party (e.g., service provider) can host a private cloud server (a type of colocation), most companies choose to keep the hardware in their on-premises data center. From there, an in-house team can oversee and manage everything. The private cloud deployment model is also known as the internal or corporate model.

   • Community Cloud
   The community cloud deployment model operates as a public cloud. The difference is that this system only allows access to a specific group of users with shared interests and use cases.
   This type of cloud architecture can be hosted on-premises, at a peer organization, or by a third-party provider. A combination of all three is also an option.

Typically, all organizations in a community have the same security policies, application types, and legislative issues.

• Hybrid Cloud
A hybrid cloud is a combination of two or more infrastructures (private, community, VPC, public cloud, and dedicated servers). Every model within a hybrid is a separate system, but they are all a part of the same architecture.
A typical deployment model example of a hybrid solution is when a company stores critical data on a private cloud and less sensitive information on a public cloud. Another use case is when a portion of a firm's data cannot legally be stored on a public cloud.
The hybrid cloud model is often used for cloud bursting. Cloud bursting allows an organization to run applications on-premises but "burst" into the public cloud in times of heavy load. It is an excellent option for organizations with versatile use cases.

6. Describe the Google cloud platform's security features.

GOOGLE CLOUD PLATFORM SECURITY INFRASTRUCTURE

The Google Cloud platform infrastructure uses multiple layers of security. Because redundancy is built into the progressive layers of security, no one incident can take down the Google Cloud infrastructure. Google Cloud security layers includes everything from physical security at data centers to some of the most advanced cybersecurity technology and professionals available in the world.

GOOGLE CLOUD PLATFORM INFRASTRUCTURE SECURITY FEATURES INCLUDE:

- 24/7/365 operations, device security detection and response from both internal and external threats
- Data in-transit encrypted communication to and from Google's public cloud, including layered defense redundancies to protect customers from denial-of-service (DoS) attacks
- Identity protection and management through multiple authentication factors
- Data at-rest storage security using encryption against unauthorized access and distribution for reliability
- An entire hardware infrastructure created, built, controlled, and secured by Google including servers, networking equipment, and security chips

GOOGLE CLOUD PLATFORM SECURITY PRODUCTS

Google has not only built the most secure cloud platform available as a service, but also provides security products to customers. These security products help any type of organization secure operations and communication in the cloud. Some Google Cloud security products are provided through G Suite licenses, while others are purchased separately.

GOOGLE CLOUD PLATFORM SECURITY PRODUCTS FEATURES INCLUDE:

- **Infrastructure Security:** Google's "secure-by-design" infrastructure security product includes features such as hardening, configuration management, and vulnerability management for Google Cloud customers.
- **Network Security:** Google Cloud's network security products include Virtual Private Cloud, Cloud Load Balancing, Encryption, and Application Layer Transport Security to help customers define, enforce, and secure their perimeter.
- **Endpoint Security:** The number of endpoints in districts has exploded over recent years! Google Cloud Platform can help secure endpoints with device management, patch and vulnerability management, and device hardening for Chromebooks, Chrome OS, Chrome Browser, and G Suite Device Management.
- **Data Security:** Google Cloud provides a wide range of data security features at different license levels to support discovery G Suite data loss prevention, data governance, and more.
- **Identity & Access Management:** Identity and Google Cloud access security features authentication and identity management in G Suite, system access management and more. Add-on Google Cloud security products include Cloud Identity, Cloud Identity-Aware Proxy, and Security Keys.
- **Application Security:** Google Cloud application security is a necessity for any school district storing sensitive student, faculty, staff, and/or financial information in Google Cloud (including G Suite applications such as Gmail, Drive, and Shared Drives).

7. What exactly is vertex AI? With some usage scenarios, implement vertex AI.

Vertex AI brings AutoML and AI Platform together into a unified API, client library, and user interface. AutoML lets you train models on image, tabular, text, and video datasets without writing code, while training in AI Platform lets you run custom training code. With Vertex AI, both AutoML training and *custom training* are

available options. Whichever option you choose for training, you can save models, deploy models, and request predictions with Vertex AI.

Where Vertex AI fits in the ML workflow

You can use Vertex AI to manage the following stages in the ML workflow:

- Create a dataset and upload data.
- Train an ML model on your data:
  - Train the model
  - Evaluate model accuracy
  - Tune hyperparameters (custom training only)
- Upload and store your model in Vertex AI.
- Deploy your trained model to an endpoint for serving predictions.
- Send prediction requests to your endpoint.
- Specify a prediction traffic split in your endpoint.
- Manage your models and endpoints.

Components of Vertex AI

This section describes the pieces that make up Vertex AI and the primary purpose of each piece.

Model training

You can train models on Vertex AI by using AutoML, or if you need the wider range of customization options available in AI Platform Training, use custom training.

In custom training, you can select from among many different machine types to power your training jobs, enable distributed training, use hyperparameter tuning, and accelerate with GPUs.

Model deployment for prediction

You can deploy models on Vertex AI and get an endpoint to serve predictions on Vertex AI whether or not the model was trained on Vertex AI.

Vertex AI Data Labeling

Data Labeling jobs let you request human labeling for a dataset that you plan to use to train a custom machine learning model. You can submit a request to label your video, image, or text data.

To submit a labeling request, you provide a representative sample of labeled data, specify all the possible labels for your dataset, and provide some instructions for how to apply those labels. The human labelers follow your instructions, and when the labeling request is complete, you get your annotated dataset that you can use to train a machine learning model.

Vertex AI Feature Store

Vertex AI Feature Store is a fully managed repository where you can ingest, serve, and share ML feature values within your organization. Vertex AI Feature Store manages all the underlying infrastructure. For example, it provides storage and compute resources for you and can easily scale as needed.

Vertex AI Workbench

Vertex AI Workbench is a Jupyter notebook-based development environment for the entire data science workflow. Vertex AI Workbench lets you access data, process data in a Dataproc cluster, train a model, share your results, and more, all without leaving the JupyterLab interface.

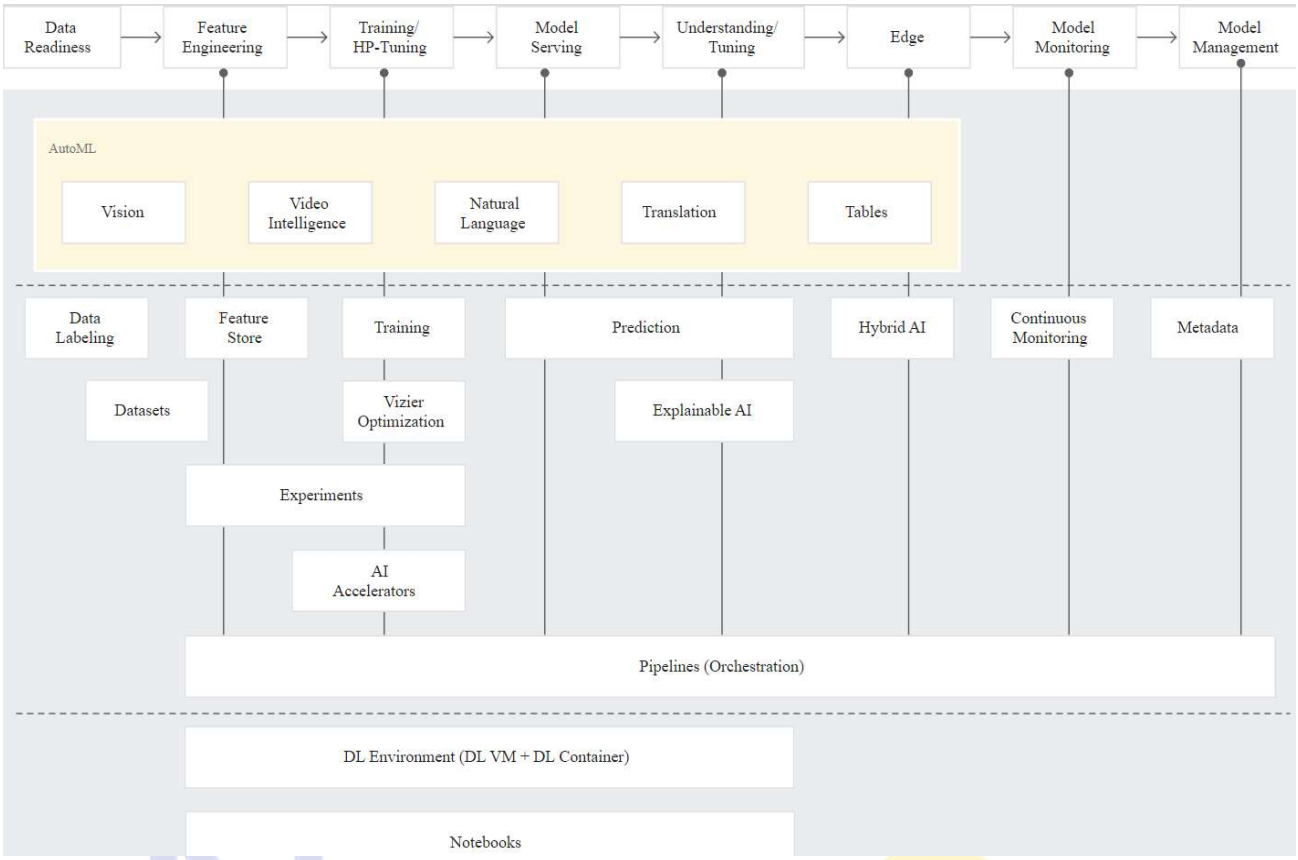
USE CASES

Explore common ways to take advantage of Vertex AI

USE CASE

Data readiness

Vertex AI supports your data preparation process. You can ingest data from BigQuery and Cloud Storage and leverage Vertex AI Data Labeling to annotate high-quality training data and improve prediction accuracy.



USE CASE

Feature engineering

Use Vertex AI Feature Store, a fully managed rich feature repository, to serve, share, and reuse ML features; Vertex AI Experiments to track, analyze, and discover ML experiments for faster model selection; Vertex AI TensorBoard to visualize ML experiments; and Vertex AI Pipelines to simplify the MLOps process by streamlining the building and running of ML pipelines.

USE CASE

Training and hyperparameter tuning

Build state-of-the-art ML models without code by using AutoML to determine the optimal model architecture for your image, tabular, text, or video-prediction task, or build custom models using Notebooks. Vertex AI Training offers fully managed training services, and Vertex AI Vizier provides optimized hyperparameters for maximum predictive accuracy.

USE CASE

Model serving

Vertex AI Prediction makes it easy to deploy models into production, for online serving via HTTP or batch prediction for bulk scoring. You can deploy custom models built on any framework (including TensorFlow, PyTorch, scikit or XGB) to Vertex AI Prediction, with built-in tooling to track your models' performance.

USE CASE

Model tuning and understanding

Get detailed model evaluation metrics and feature attributions, powered by Vertex Explainable AI. Vertex Explainable AI tells you how important each input feature is to your prediction. Available out of the box in AutoML Forecasting, Vertex AI Prediction, and Vertex AI Workbench.

USE CASE

Edge

Vertex AI Edge Manager (in experimental phase) is designed to facilitate seamless deployment and monitoring of edge inferences and automated processes with flexible APIs, to allow you to distribute AI across your private and public cloud infrastructure, on-premises data centers, and edge devices.

USE CASE

Model monitoring

Continuous monitoring offers easy and proactive monitoring of model performance over time for models deployed in the Vertex AI Prediction service. Continuous monitoring monitors signals for your model's predictive performance and alerts when the signals deviate, diagnose the cause of the deviation, and trigger model-retraining pipelines or collect relevant training data.

USE CASE

Model management

Vertex ML Metadata enables easier auditability and governance by automatically tracking inputs and outputs to all components in Vertex Pipelines for artifact, lineage, and execution tracking for your ML workflow. Track custom metadata directly from your code and query metadata using a Python SDK.