GCP version 2 Assignment 1

1. What is Google Cloud Platform Document AI?
   Answer:
   Document AI is a service from Google Cloud Platform that helps you extract data from documents using machine learning. You can use it to automate processes, classify documents, and search and store data.

2. What are the database services offered by Google's cloud platform?
   Answer:
   Google Cloud Platform offers three types of database services: relational, non-relational, and in-memory

   Some examples of relational database services are Cloud SQL, Cloud Spanner, and Bare Metal Solution

   Some examples of non-relational database services are Firestore, Bigtable, and Cloud Storage

   Some examples of in-memory database services are Memorystore and BigQuery

3. What is the difference between cloud search and cloud identity? Prepare a list of the applications for cloud search and cloud identity.
   Answer:
   Cloud Search and Cloud Identity are two different services offered by Google Cloud Platform.

   Cloud Search is a service that allows you to search across your company's data in Google Workspace, such as Gmail, Drive, Docs, Sheets, Slides, Calendar, and more1. You can also use Cloud Search to index and search data from third-party sources, such as Salesforce, SAP, or SharePoint.
   Cloud Identity is a service that allows you to centrally manage users and groups in your organization. You can use Cloud Identity to provide single sign-on (SSO) and

multi-factor authentication (MFA) for your cloud applications, as well as device management and endpoint security for your devices.
Some of the applications for Cloud Search and Cloud Identity are:

Cloud Search: You can use Cloud Search to find information faster and easier, such as documents, emails, contacts, events, etc. You can also use Cloud Search to create custom search applications for your specific needs, such as intranet portals, knowledge bases, or customer support systems.
Cloud Identity: You can use Cloud Identity to simplify user management and access control for your cloud applications, such as Google Workspace, Salesforce, Dropbox, etc. You can also use Cloud Identity to protect your devices and data from unauthorized access or theft, by enforcing policies such as password strength, screen lock, encryption, etc.

4. What is conversational AI, and how does it work? List and Explain various GCP Conversation AI services.
   Answer:
   Conversational AI is a type of artificial intelligence (AI) that can simulate human conversation. It is made possible by natural language processing (NLP), a field of AI that allows computers to understand and process human language12.
   Conversational AI systems are trained on large amounts of data, such as text and speech, and use machine learning (ML) to learn from the data and improve their performance.

   Some of the benefits of conversational AI are:

   It can provide faster and more convenient service to customers, such as answering queries, booking appointments, or placing orders.
   It can reduce operational costs and increase efficiency, by automating repetitive and mundane tasks, or providing 24/7 support.
   It can enhance customer satisfaction and loyalty, by providing personalized and engaging experiences, or offering proactive suggestions and recommendations.
   Google Cloud Platform (GCP) offers a range of conversational AI services that you can use to build and deploy chatbots, virtual agents, voice assistants, or speech applications. Some of the GCP conversational AI services are:

Dialogflow: A developer platform for building conversational agents that can understand natural language and respond accordingly. You can use Dialogflow to create chatbots or voice assistants for various platforms, such as websites, mobile apps, messaging apps, or smart devices.
Contact Center AI: A solution for enhancing customer service in contact centers, by using conversational AI to automate interactions, provide agent assistance, or analyze customer feedback. You can use Contact Center AI to improve customer satisfaction, reduce wait times, or optimize agent performance.
Cloud Speech-to-Text: An API for converting speech to text in real time or asynchronously. You can use Cloud Speech-to-Text to transcribe audio files, enable voice commands, or create speech applications.
Cloud Text-to-Speech: An API for converting text to natural-sounding speech in various languages and voices. You can use Cloud Text-to-Speech to synthesize speech for voice applications, narrate audiobooks, or generate voice prompts.

5. Give an example of GCP's Media Translation service.
   Answer:
   Media Translation API is a service that delivers real-time speech translation to your content and applications directly from your audio data. You can use Media Translation API to stream translation output as you supply audio from a microphone or prerecorded audio file.

   An example of using Media Translation API is to create a live captioning system for multilingual audiences. You can use Media Translation API to transcribe and translate the speech from a video or audio source, and display the captions on the screen in different languages. This can help you reach a wider and more diverse audience, and improve accessibility and engagement.

6. Explain how to use Google Cloud Platform's cloud logging and monitoring features.
   Answer:

Google Cloud Platform (GCP) offers cloud logging and monitoring features that allow you to store, search, analyze, monitor, and alert on log data and events from your GCP services, applications, and infrastructure. You can use cloud logging and monitoring to troubleshoot issues, optimize performance, and ensure security and compliance.

To use GCP's cloud logging and monitoring features, you need to:

Enable the Cloud Logging API for your project, which allows you to collect and ingest log data from various sources, such as Google Cloud services, applications running on Google Cloud or elsewhere, or third-party services1.
Use the Cloud Logging UI or the gcloud command-line tool to view, filter, export, or delete your log entries. You can also use the Logs Explorer to query your logs using advanced filters and expressions.
Create log-based metrics, which are custom metrics based on the content or volume of your log entries. You can use log-based metrics to create charts, dashboards, or alerts for your logs.
Enable the Cloud Monitoring API for your project, which allows you to collect and ingest metrics, events, and metadata from Google Cloud services, hosted uptime probes, application instrumentation, and a variety of common application components including Cassandra, Nginx, Apache Web Server, Elasticsearch, and many others.
Use the Cloud Monitoring UI or the gcloud command-line tool to view, filter, analyze, or visualize your metrics. You can also use the Metrics Explorer to query your metrics using advanced filters and aggregations.
Create dashboards, which are collections of charts that display metrics and log-based metrics for your resources and services. You can use dashboards to monitor the health and performance of your system.
Create alerting policies, which are rules that specify the conditions under which you want to be notified of an issue. You can use alerting policies to monitor your metrics and log-based metrics for anomalies or errors.
Configure notification channels, which are mechanisms that deliver notifications to you or your team when an alerting policy is triggered. You can use notification channels such as email, SMS, Slack, PagerDuty, etc.

7. How to use Cloud Identity to generate and manage user IDs in the cloud?
   Answer:
   Cloud Identity is a service that centrally manages users and groups in the cloud. You can use Cloud Identity to create and manage user IDs, assign roles and permissions, enforce security policies, and federate identities with other identity providers.

   To use Cloud Identity to generate and manage user IDs in the cloud, you need to:

   Sign up for Cloud Identity, either as a standalone product or as part of Google Workspace or Google Cloud Platform.
   Create users and groups in the Cloud Identity admin console, or sync them from an existing directory service such as Active Directory or Azure Active Directory.
   Assign roles and permissions to users and groups, either using predefined roles or creating custom roles. You can also use organizational units to apply different policies to different subsets of users.
   Enforce security policies such as password strength, multi-factor authentication, device management, and phishing prevention. You can also use security reports and alerts to monitor user activity and detect anomalies.
   Federate identities with other identity providers, such as SAML or OpenID Connect, to enable single sign-on (SSO) to thousands of cloud applications. You can also use Cloud Identity-Aware Proxy (IAP) to secure access to your own applications hosted on Google Cloud.