

KF6013: CLOUD COMPUTING AND WEB APIs

PART 1 CLOUD SOLUTION SPECIFICATION

STUDENT: MARTINA PANI W19020174

Introduction

This report details the scope of implementing a cloud solution for Living Planet which is provided by Google Cloud computing services. It covers key aspects including ethical and sustainability considerations, security and privacy measures, and compliance with legal requirements.

Furthermore, it provides Handover Plans in detail with roles and responsibilities for managing the cloud infrastructure, and a comparison between Google VM and Google Kubernetes Engine (GKE).

The main aim of this report is to ensure an efficient, secure, and environmentally friendly cloud solution that aligns with Living Planet's objectives.

Ethical Concerns

CLIENT SUSTAINABILITY TARGETS.

Living Planet's goal of becoming climate positive by 2030 is supported by the chosen solution using Google Cloud Platform (GCP). GCP has robust sustainability initiatives, including commitments to carbon neutrality and using renewable energy. This aligns with Living Planet's targets by ensuring that the IT infrastructure has minimal environmental impact.

GCP data centres are highly efficient and use renewable energy.

Furthermore, GCP offsets its carbon footprint, contributing to reduce environmental impact.

In terms of resource optimisations, the use of a general-purpose e2-micro VM instance helps minimise resource waste.

All these specific aspects can have a favourable impact on the Client's targets.

SECURITY AND PRIVACY CONCERNS.

The selected solution handles security and privacy concerns in numerous ways.

Identity and Access Management (IAM) ensures that only authorised users have access to the project's resources. The roles of Owner and Editor are clearly specified to regulate access levels.

Shielded VMs improve virtual machine security with secure boot, vTPM, and integrity monitoring.

The firewall settings are adjusted to allow only necessary traffic (HTTP and HTTPS), lowering the danger of unauthorised access.

The Google Maps APIs will be encrypted by API keys, allowing only authenticated requests.

LEGAL REQUIREMENTS.

The solution is hosted in Oregon (us-west1), which was chosen for its low cost and GDPR compliance. Hosting the web application in a respected region with strong data protection legislation helps to ensure GDPR compliance.

Oregon zone offers competitive pricing, reducing operational costs while maintaining legal compliance.

GCP's data centres adhere to strict privacy and security guidelines, ensuring that user data is protected.

Handover plan

Two handover plans for the solution may be proposed to Living Planet:

1. The Client takes over full management.
2. The organisation offers a management service for an additional fee.

PLAN 1

In the case the Client prefers to take over the management, information for managing the cloud solution will be provided.

Access and Management.

Login credentials and necessary permissions will be provided to access the Google Cloud Console, along with documented roles and their associated responsibilities and permissions. API Keys will be securely stored and shared for accessing Google Maps and weather APIs.

Billing and Subscription.

Instructions for transferring billing details to Living Planet will be provided with appropriate guidelines for monitoring usage and costs within the GPC Console.

Basic Cloud and security management will be offered to the Living Planet operators that will take over administrator. It will be guaranteed that they will have knowledges and skills on starting, stopping, and managing VM instances, IAM roles, firewalls settings, and security configurations.

PLAN 2

For an additional fee, the Client will have the option to benefit of the management service offers from the organisation.

A formal Service Level Agreement (SLA) will be established for outlining uptime levels and availability for any issues, support hours and maintenance schedules, as well as performance metrics that will be monitored and reported.

Roles and Responsibilities

The organisation will manage the Cloud infrastructure, IAM roles, firewall settings, and security configurations.

Updates, maintenance, and system health checks will be regularly performed to report system performance, costs, and any incidents.

Living Planet will be expected to provide user feedback on system performance and any issues encountered.

Access and Management

To ensure security, user accounts will be created and managed with appropriated roles with defined access levels.

Billing and cost management

The organisation will also handle billing and cost management efficiently.

Billing details will be kept updated ensuring that charges are transparent and agreed upon with the Client.

Usage and costs will be monitored as regular basis using GCP's cost management tools; budget alerts will be set up on the previously discussed and agreed upon budget to avoid unexpected costs.

Monitoring and Reporting

A robust monitoring and reporting system will be implemented.

The Client will receive regular reports on performance, metrics, uptime, incidents, and cost analysis, which are tracked using GCP's monitoring tools.

The organisation will conduct regular performance reviews to identify areas for improvement, as well as look for resource usage optimisation and reduce costs.

Plan 1 would be potentially more convenient for the Client, having also full control and flexibility over their cloud resources. However, high technical expertise and responsibility for monitoring and security management are required, which may aggravate on costs in terms of hiring human resource with advance knowledge.

Comparative consideration

Deciding on the best appropriate cloud infrastructure for the Living Planet web application required careful consideration of specific requirements and constraints of the project, particularly sustainability and cost-effectiveness.

Major cloud services' providers have been analysed and compared in terms of sustainability, not dwelling only on the cloud services themselves, but also on environmental impact that Google, Microsoft, and Amazon have in all their various domains as the world's three largest and most influential tech companies.

Google has consistently been a leader in sustainability, being carbon-neutral since 2007 and achieving 100% renewable energy since 2017. Their goal on 100% carbon-free energy by 2030. However, Microsoft and Amazon are also making significant strides investing in renewable energy and technologies as part of their commitments to addressing climate change.

Overall, Google stands out for its early and comprehensive commitments, innovative use of technology, and ongoing achievement in operating sustainability.

Once Google Cloud was chosen, Google VM (compute engine) and Google Kubernetes Engine (GKE) were compared to determinate which was more suitable for hosting a web application that features a Google Maps and OpenWeather APIs, and Google OAuth integration.

The table below summarises the features analysed.

	Google VM	GKE
Management Complexity	Low, direct control over a single VM	High, requires managing Kubernetes configurations
Resource Efficiency	Limited by instance size, manual optimization	Efficient resource utilization, scales with demand
Setup and Deployment	Simple setup with direct environment control	Complex setup with Kubernetes configurations
Control	Full control over the VM environment	Abstracted control, managed by Kubernetes

Flexibility	High flexibility for custom configurations	Flexibility within Kubernetes constraints
Usability	Easy to manage for small applications	More suitable for microservices and larger applications
Security	VM-level security, manage OS patches manually	Managed security updates and policies by GKE
Suitability for Free Tier	Highly suitable for small, low-resource applications	May exceed free tier limits quickly with additional resource use
Sustainability	Simplified management, reduced over-provisioning, aligns well with sustainability goals for small-scale apps	Efficient resource use at scale, but complexity might lead to over-provisioning for small apps

GKE is a managed Kubernetes service that simplifies the deployment of containerised applications. It offers robust tools for automation, scaling, and managing containerised applications, being particularly suitable for microservices architectures and applications that demand frequent updates and scaling.

Google VM offers a straightforward setup and management process, suitable for smaller applications, providing direct control over the environment. In contrast, GKE introduces additional complexity with Kubernetes configurations, which might be unnecessary for Living Planet web application.

The Free Tier for Google VM provided sufficient resources for small-scale applications without incurring additional costs. GKE could quickly exceed Free Tier limits due to its underlying resource requirements. In fact, the Free Tier for GKE includes a single Autopilot cluster, but additional resources used by the workloads would incur costs.

For Living Planet solution is more practical and cost-effective to manage a single VM instance, reducing also energy consumption from administrative overhead.

Both services use Google's carbon-neutral data centres. Kubernetes' ability to dynamically scale resource helps in resource usage optimisation, which can be more sustainable for larger and high-traffic applications than the Living Planet web application.

Google VM's simplicity, cost-effectiveness, and sufficient capabilities make it an ideal solution for hosting the Living Planet web application on a Free Tier plan. While GKE offers powerful features for larger and more complex application, it introduces unnecessary complexity and potential additional costs for the specific use case.

Furthermore, the more straightforward management and reduced risk of overprovisioning with Google VM align well with sustainability goals for small-scale applications.

References

Google Cloud. (2023) Google Environmental Report 2023. Available at: <https://cloud.google.com/sustainability>

Google Cloud. (2023) Google Cloud's Commitment to Sustainability. Available at: <https://cloud.google.com/sustainability/commitment>

Microsoft. (2023) Microsoft Sustainability Report 2023. Available at: <https://www.microsoft.com/en-us/sustainability/emissions-impact-dashboard>

Microsoft. (n.d.) Sustainability at Microsoft. Available at: <https://www.microsoft.com/en-us/sustainability>

Amazon. (2023) Amazon Sustainability Report 2023. Available at: <https://sustainability.aboutamazon.com>

Amazon. (n.d.) Sustainability in the Cloud. Available at: <https://aws.amazon.com/sustainability/>

Google Cloud. (n.d.) Identity and Access Management (IAM). Available at: <https://cloud.google.com/iam/docs>

Google Cloud. (n.d.) Google Cloud and GDPR. Available at: <https://cloud.google.com/security/gdpr>

Google Cloud. (n.d.) Billing and Cost Management. Available at: <https://cloud.google.com/billing/docs>

Google Cloud. (n.d.) Google Compute Engine (VMs). Available at: <https://cloud.google.com/compute>

Google Cloud. (n.d.) Google Kubernetes Engine (GKE). Available at: <https://cloud.google.com/kubernetes-engine>

Appendices

Cloud service provider	Google Cloud Platform (GCP)
Details of the virtual machine and any other cloud services you will be using in your solution	GENERAL-PURPOSE Virtual Machine Series: E2 Machine type: e2-micro
Subscription details of cloud solution: a. Subscription cost b. Length of current subscription c. Date current subscription expires. d. Size/details of data storage included with subscription. e. Number of hours per month (if applicable) within subscription f. Any user limits associated with the subscription e.g. can only use so many hours a month, can only have so many VMs running at once, only have x amount of credits to use, details of limited user accounts etc.	Google Cloud Free Program <ul style="list-style-type: none"> a. Free Tier b. NA c. No end date, but it is subject to change. d. <ul style="list-style-type: none"> • 30 GB-months standard persistent disk. • • 5 GB-month snapshot storage in the following regions: <ul style="list-style-type: none"> - Oregon: <code>us-west1</code> - Iowa: <code>us-central1</code> - South Carolina: <code>us-east1</code> • 1 GB network from North America to all region destinations (excluding China and Australia) per month. e. N/A f. <ul style="list-style-type: none"> - 1-non preemptible e2-micro VM instance per month. - No limit for e2-micro instances; free access until exceeds the total usage hours in the current month. - External IP addresses are not included. - GPUs and TPUs are not included; extra charge if added in VM. - \$300 credits included to use for a 90-days free trial.

The region that your solution is hosted on	Oregon: <code>us-west1</code>
Technical architecture e.g. LAMP/WAMP/MAMP stack	LAMP stack
Security provision e.g. identity and access management, user accounts, user roles, permissions, firewall settings:	<p>By default, the project can be accessed by a single user that matches with the original user project creator. No other users can access to the project and its Cloud Engine resources.</p> <p>Identity Access Management (IAM) permits to add new users to the project or specific resources and grant them permissions assigning roles.</p> <p>It is possible to give access to any user with a valid Google Account, a Google Group, a service account, or a Google Workplace domain.</p> <p>User accounts:</p> <ul style="list-style-type: none"> - Compute Engine default service account. Role: Editor Type: service account - Google APIs Service Agent Role: Editor Type: service account - Martina Pani Roles: Owner, Compute Instance Admin(v1) Type: User <p>Editor: permissions for read and modify actions; permissions to create and delete resources for most Google Cloud Services but not to perform all actions for all services.</p> <p>Owner: All editor permissions in addition to manage roles and permissions for the project and all resources within it, and to set up billing for the project.</p>

	<p>Security:</p> <ol style="list-style-type: none">1. Shielded VM:<ul style="list-style-type: none">- Secure Boot- vTPM- Integrity monitoring2. VM access: SSH keys are generated automatically when connecting to the VM. <p>Firewall settings: Allow HTTP and HTTPS traffic.</p>
--	---