DIPLOMA IN CLOUD SECURITY

Project Assignment 4: Google Cloud

By

Juan José Para Catalá

01st December 2018

Table of Contents:

	Page(s)
Background	3
Introduction to Google Cloud	4
1- Setting up a cloud environment in Google Cloud	4
2- Creating a VM Instance	6
3- Setting up our VM Instance as a Web-Server	8
4- Browsing our VM	10
5- Creating a simple JAVA app for CARS to deploy in the Cloud	11
Feasibility report	13 - 14
Recommendations	14

Background

The Department of Transportation is composed of a number of different agencies, including the Office of the Secretary of Transportation (OST) and the National Highway Traffic and Safety Administration (NHTSA), but also encompasses aviation, rail, maritime and even pipeline administrations. On June 24, 2009, President Obama signed the Consumer Assistance to Recycle and Save (CARS) Act, which directed the Secretary of Transportation (acting through NHTSA) to establish and administer what would come to be popularly known as the "cash for clunkers" program. The Car Allowance Rebate System, was a $3 billion U.S. federal scrappage program intended to provide economic incentives to U.S. residents to purchase a new, more fuel-efficient vehicle when trading in a less fuel-efficient vehicle. The program was promoted as providing stimulus to the economy by boosting auto sales, while putting safer, cleaner and more fuel-efficient vehicles on the roadways. NHTSA was called on to lead the CARS program at the implementation level. Given the sheer size and scope – and just a 30 day timeline – everyone who could be spared within the DOT was pulled onto the project. That meant leveraging as many existing resources and services as possible, as well as working closely with DOT partners, systems and networks to make this mandate happen. Cloud computing was one obvious way to realize the kind of scale and speed that was required. However, at the time, cloud computing seemed to offer more problems than solutions, presenting security challenges that appeared to be incompatible with the government's certification and accreditation process. There was also the issue of the extensive eligibility requirements for consumers to trade in their cars.

They were the following: ▪ Vehicle must be less than 25 years old on the trade-in date. ▪ Only the purchase or 5-year minimum lease of new vehicles qualify. ▪ Generally, trade-in vehicles must get a weighted combined average rating of 18 or fewer miles per gallon (some very large pickup trucks and cargo vans have different requirements). ▪ Trade-in vehicles must be registered and insured continuously for the full year preceding the trade-in. ▪ Trade-in vehicles must be in drivable condition. ▪ The program ran from July 1, 2009 until August 24, 2009. ▪ The program requires the scrapping of the eligible trade-in vehicle and that the dealer disclose to the customer an estimate of the scrap value of the trade-in. The scrap value, however minimal, will be in addition to the rebate, and not in place of the rebate. ▪ The new car bought under the plan must have a suggested retail price of no more than $45,000, and for passenger automobiles, the new vehicle must have a combined fuel economy value of at least 22 mpg. The CARS program will be administrated through a central system that will be accessible by car dealers involved in the program and centrally managed by the NHTSA. The system will track the incoming and outgoing vehicles, as well as consumer information and eligibility requirements. The program will need to be central so as to track vehicles and consumers. The 'clunkers', that the car dealer received were not allowed be resold. To ensure that vehicles traded-in under were not resold by dealers, the program outlines a procedure for destructively disabling the engine. You have been contracted by the company as IT security manager to assess the security concerns surrounding the CARS program being hosted in the cloud. Your findings will form a security report.

You will also be required to test current cloud solutions offered by Google and Microsoft.

Introduction to Google Cloud:

Google Cloud Platform, offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search and YouTube. Alongside a set of management tools, it provides a series of modular cloud services including computing, data storage, data analytics and machine learning. Registration requires a credit card or bank account details.

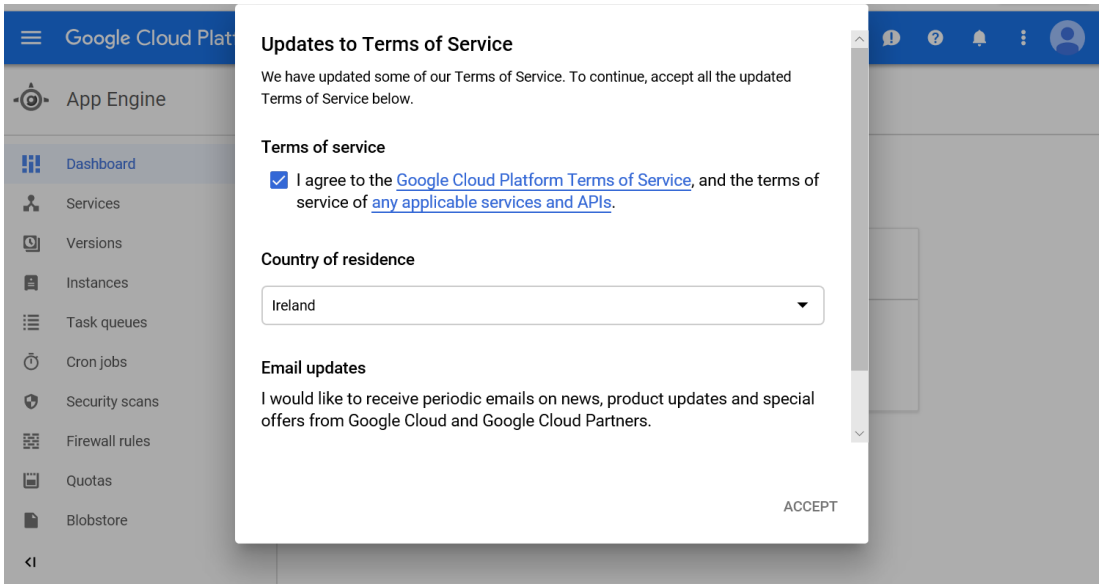
Google Cloud Platform provides Infrastructure as a service, Platform as a service, and Serverless computing environments.

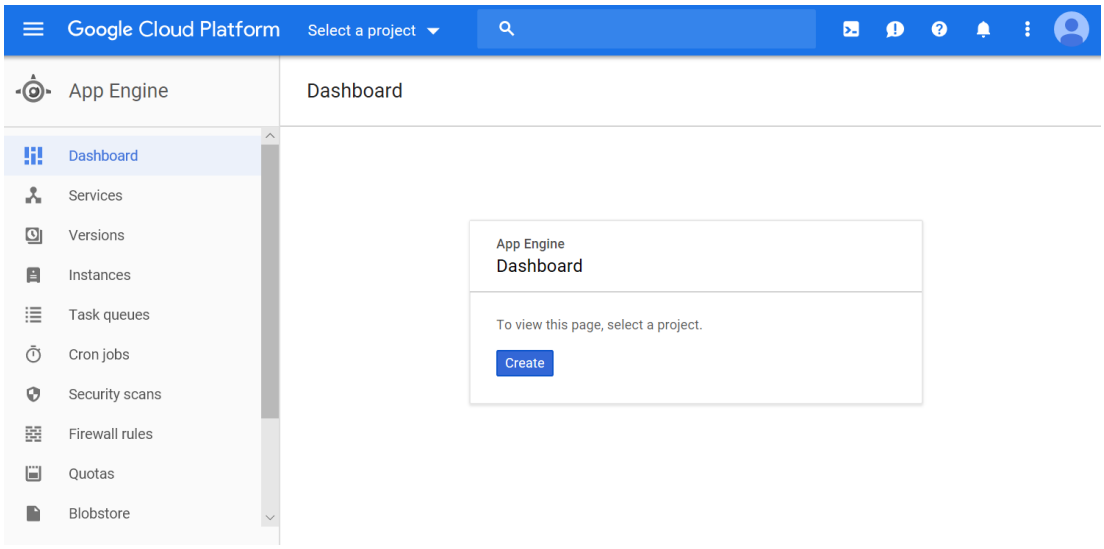
https://en.wikipedia.org/wiki/Google_Cloud_Platform

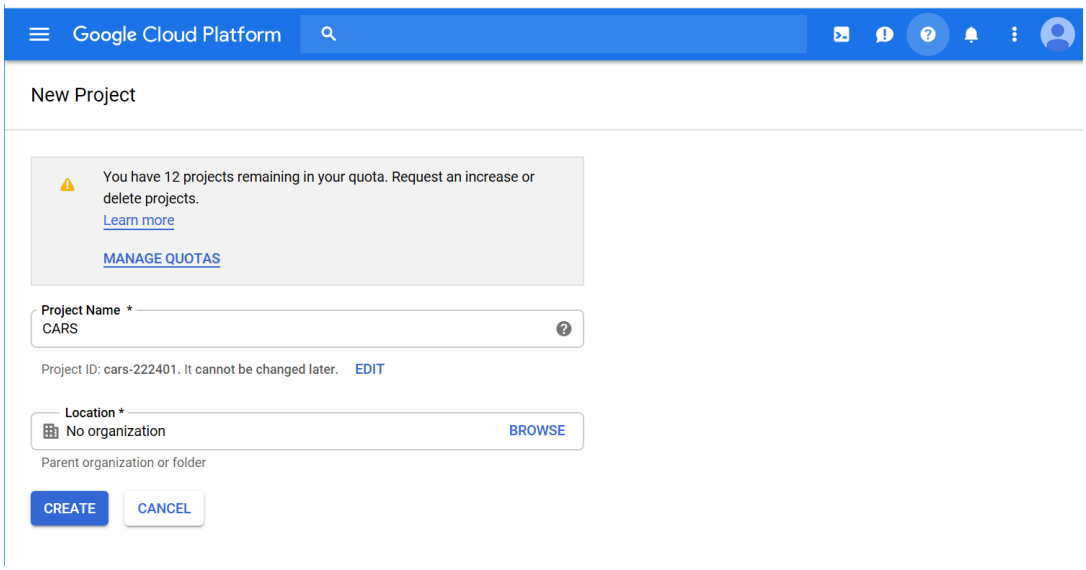
In our case, CARS program is a project which use Platform as a Service (PaaS).

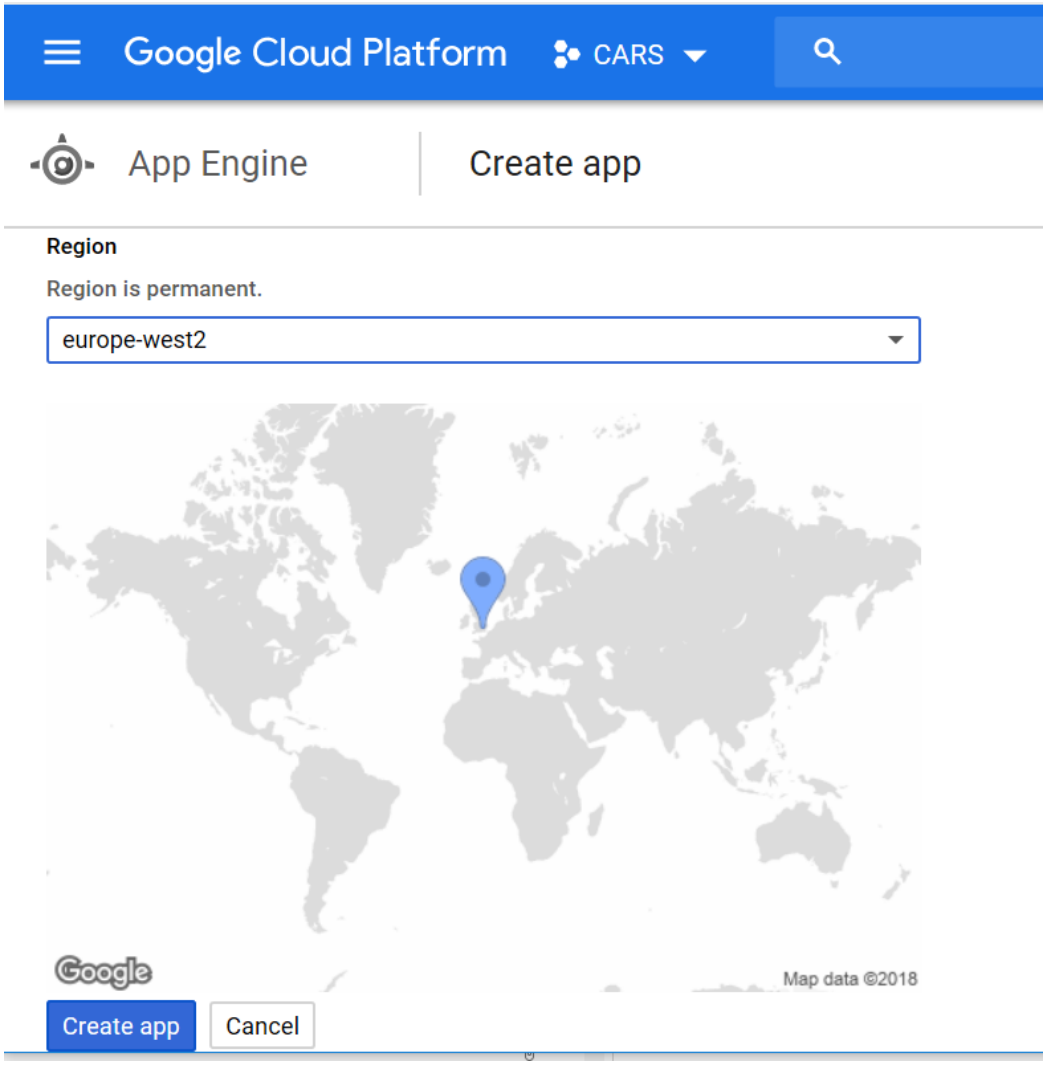
We are going to create an instance or VM and use it as a web server where CARS program is going to be hosted.

1- Setting up a cloud environment in Google Cloud



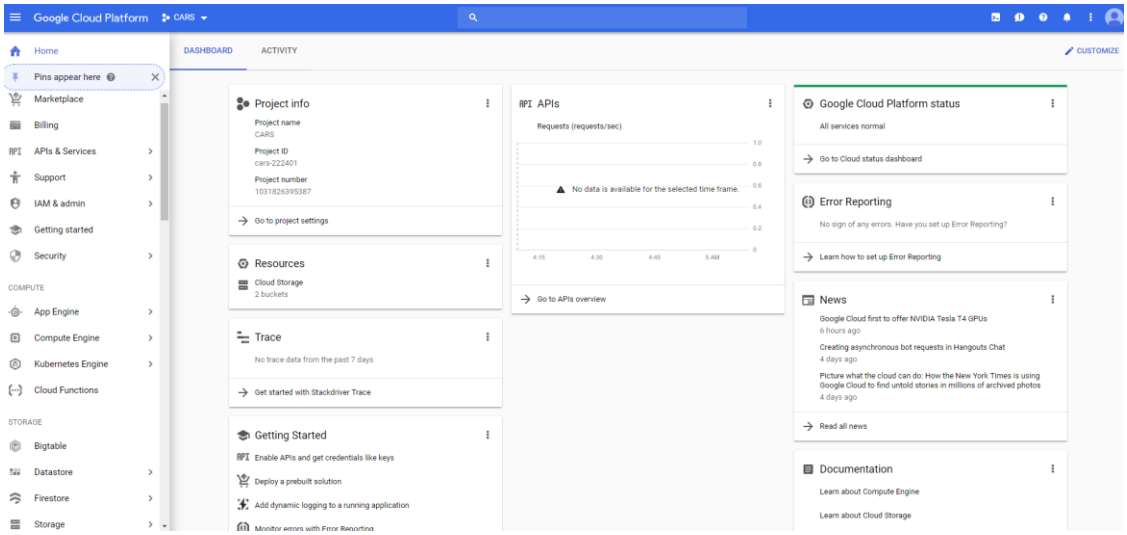




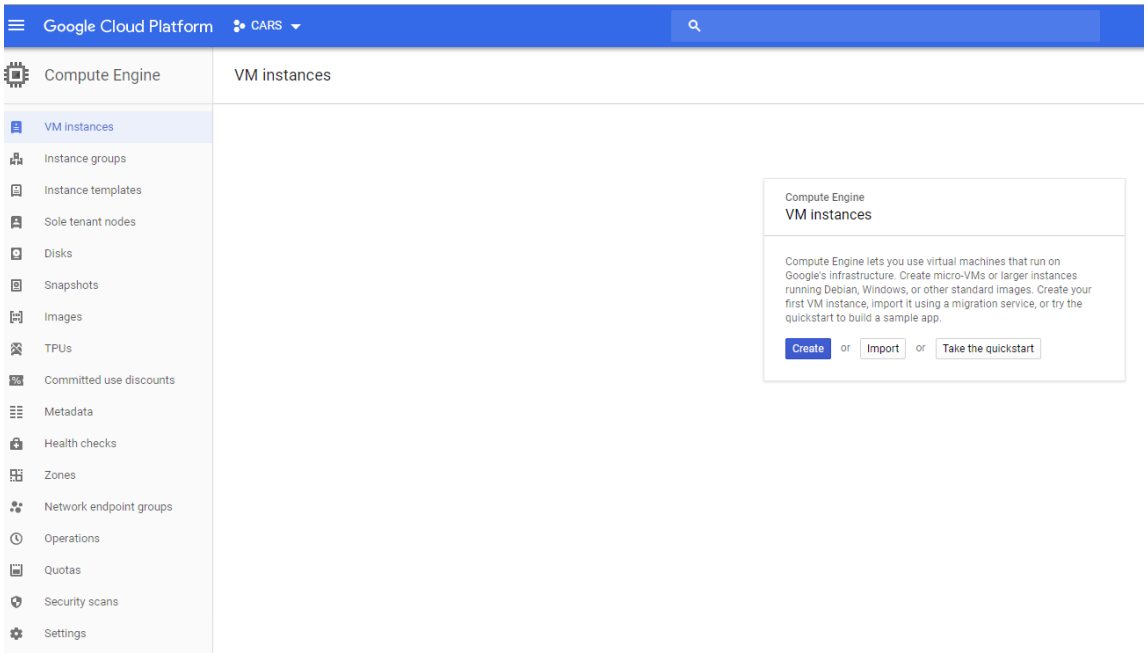


In the screenshots above we can see the process of creating an account. First we login with our own google account, then we access cloud.google.com and create a project, we select the area where we are.
We can see below our Dashboard, with our project which at the moment does not contains anything.

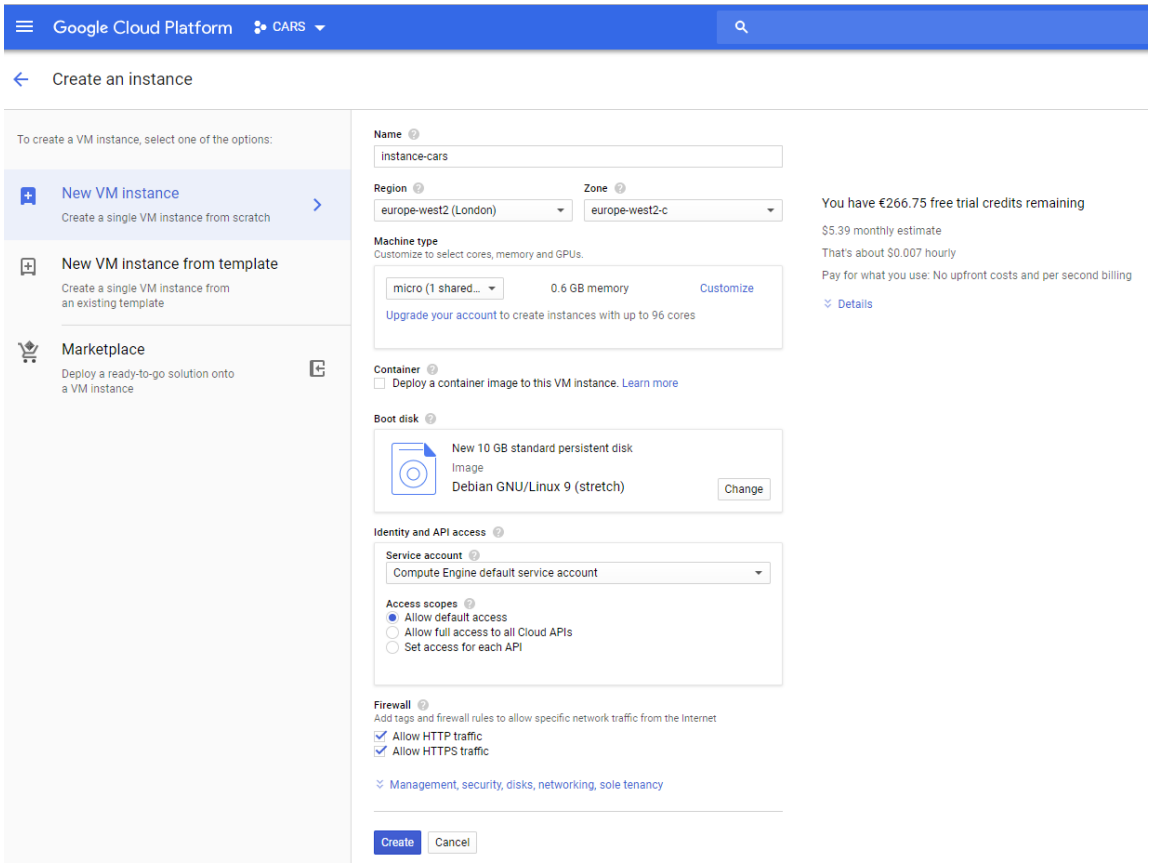
2- Creating a VM Instance

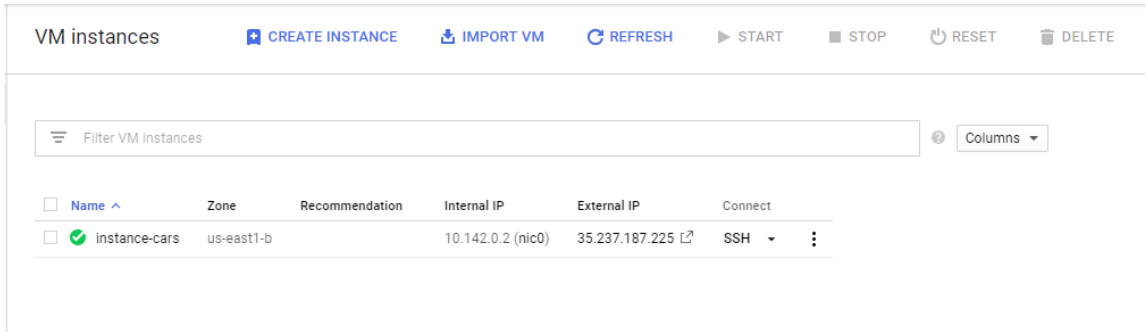


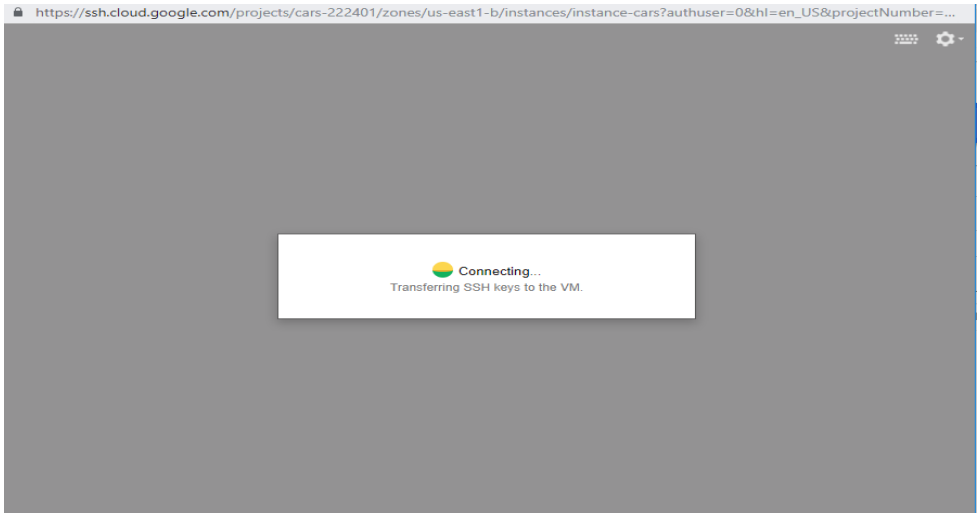
To create a VM instance, we go the left panel and select Compute Engine, then we select VM instances, and it gives us the option to Create, Import or Take a quickstart. Here we Create.



Below we can see the process to configurate our VM, we gave it a name, we selected the region to take the resources from. First I selected Europe-west2(London), however that location did not have the resources available at the time I created my VM, so I ended up selecting us-east1-b.
We had to select the machine type, I selected a Debian Linux machine with 0.6 GB memory, because for this example is enough and as bigger the memory, storage and CPUs Google will charge more.
Identity and Access mode we leave them as default, however very important to select in the Firewall “Allow HTTP and HTTPS traffic” to be able to connect via web browser.
Management, security, disks, networking, sole tenancy we left the default as well.
Then we Create and give us an Internal and External IP which we will use to browse and connect to our new VM via SSH.

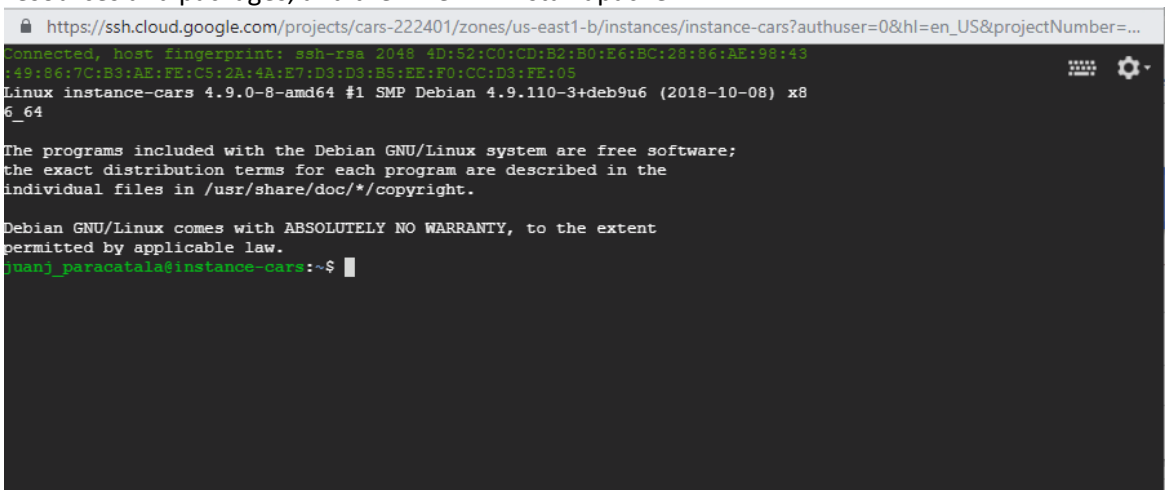

Google Cloud Platform
CARS
Create an instance
To create a VM instance, select one of the options:
New VM instance
Create a single VM instance from scratch
New VM instance from template
Create a single VM instance from an existing template
Marketplace
Deploy a ready-to-go solution onto a VM instance
Name
instance-cars
Region
europe-west2 (London)
Zone
europe-west2-c
Machine type
Customize to select cores, memory and GPUs.
micro (1 shared...
0.6 GB memory
Customize
Upgrade your account to create instances with up to 96 cores
Container
Deploy a container image to this VM instance. Learn more
Boot disk
New 10 GB standard persistent disk
Image
Debian GNU/Linux 9 (stretch)
Change
Identity and API access
Service account
Compute Engine default service account
Access scopes
Allow default access
Allow full access to all Cloud APIs
Set access for each API
Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
Allow HTTP traffic
Allow HTTPS traffic
Management, security, disks, networking, sole tenancy
Create
Cancel
You have €266.75 free trial credits remaining
$5.39 monthly estimate
That's about $0.007 hourly
Pay for what you use: No upfront costs and per second billing
Details


VM instances
CREATE INSTANCE
IMPORT VM
REFRESH
START
STOP
RESET
DELETE
Filter VM instances
Columns
Name
Zone
Recommendation
Internal IP
External IP
Connect
instance-cars
us-east1-b
10.142.0.2 (nic0)
35.237.187.225
SSH

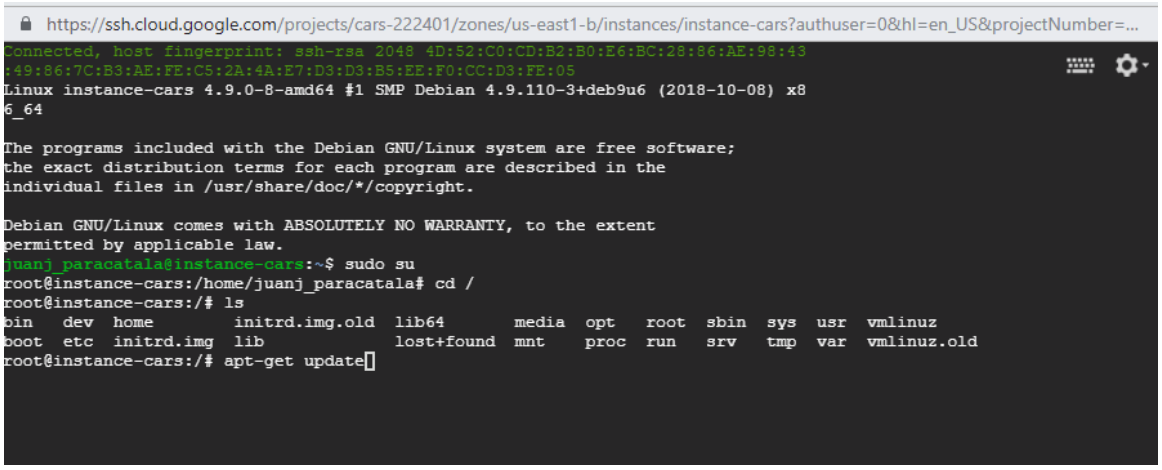

https://ssh.cloud.google.com/projects/cars-222401/zones/us-east1-b/instances/instance-cars?authuser=0&hl=en_US&projectNumber=...
Connecting...
Transferring SSH keys to the VM.

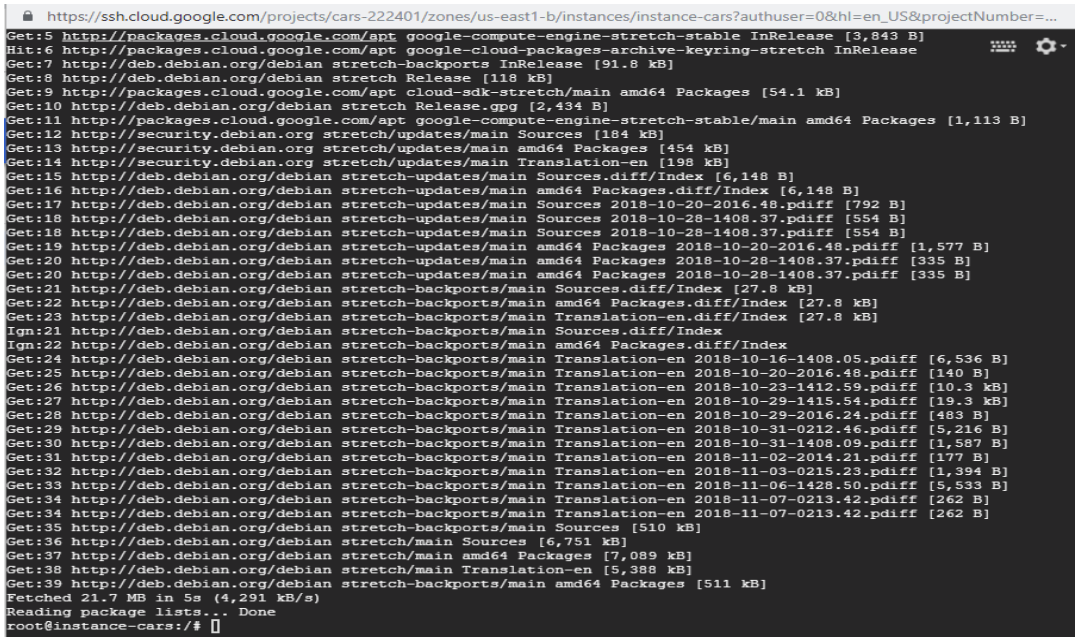
3- Setting up our VM Instance as a Web-Server

Now that we have our VM, we are going to use it as a web server, so we will start updating the resources and packages, and then we will install apache2.



We can see below the use of “sudo su” to become root.

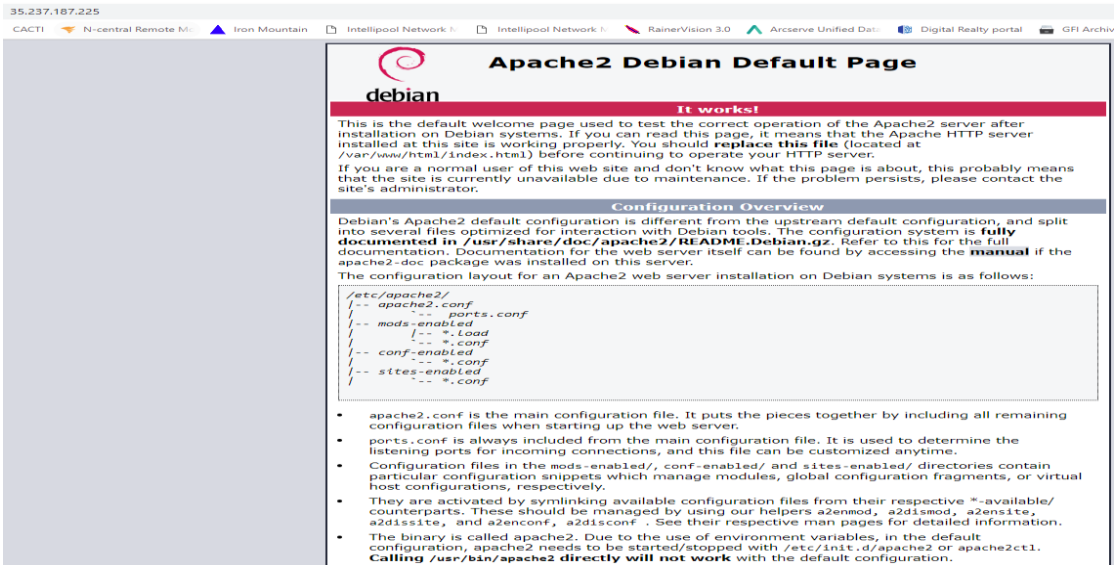




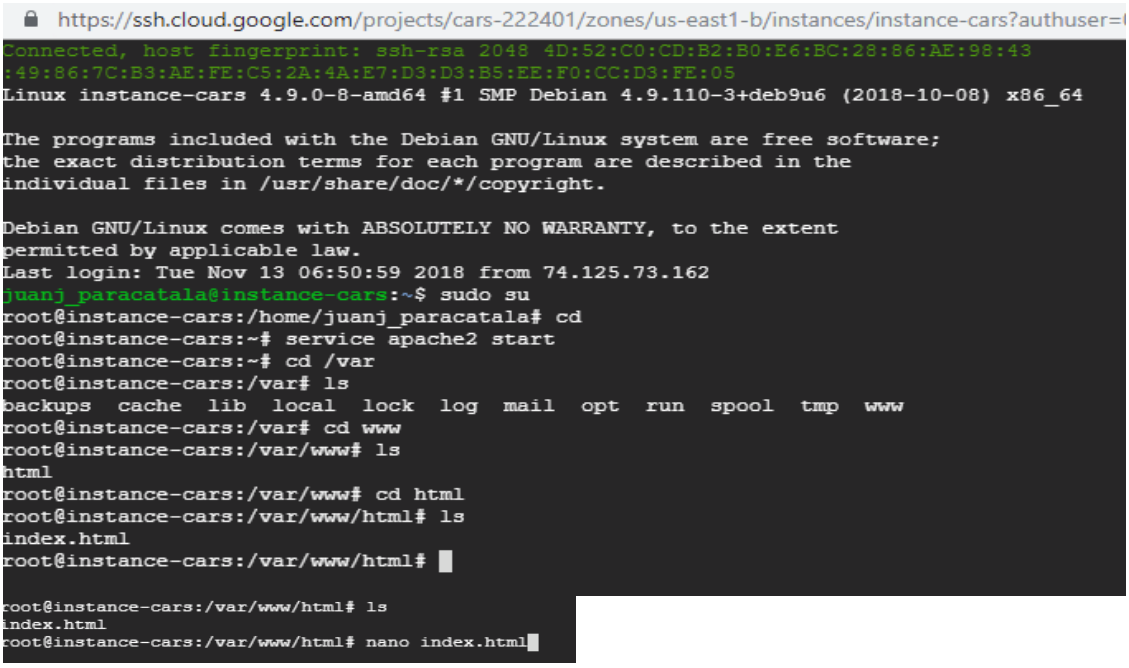
```
Get:5 http://packages.cloud.google.com/apt google-compute-engine-stretch-stable InRelease [3,843 B]
Hit:6 http://packages.cloud.google.com/apt google-cloud-packages-archive-keyring-stretch InRelease
Get:7 http://deb.debian.org/debian stretch-backports InRelease [91.8 kB]
Get:8 http://deb.debian.org/debian stretch Release [118 kB]
Get:9 http://packages.cloud.google.com/apt cloud-sdk-stretch/main amd64 Packages [54.1 kB]
Get:10 http://deb.debian.org/debian stretch Release.gpg [2,434 B]
Get:11 http://packages.cloud.google.com/apt google-compute-engine-stretch-stable/main amd64 Packages [1,113 B]
Get:12 http://security.debian.org stretch/updates/main Sources [184 kB]
Get:13 http://security.debian.org stretch/updates/main amd64 Packages [454 kB]
Get:14 http://security.debian.org stretch/updates/main Translation-en [198 kB]
Get:15 http://deb.debian.org/debian stretch-updates/main Sources.diff/Index [6,148 B]
Get:16 http://deb.debian.org/debian stretch-updates/main amd64 Packages.diff/Index [6,148 B]
Get:17 http://deb.debian.org/debian stretch-updates/main Sources 2018-10-20-2016.48.pdiff [792 B]
Get:18 http://deb.debian.org/debian stretch-updates/main Sources 2018-10-28-1408.37.pdiff [554 B]
Get:18 http://deb.debian.org/debian stretch-updates/main Sources 2018-10-28-1408.37.pdiff [554 B]
Get:19 http://deb.debian.org/debian stretch-updates/main amd64 Packages 2018-10-20-2016.48.pdiff [1,577 B]
Get:20 http://deb.debian.org/debian stretch-updates/main amd64 Packages 2018-10-28-1408.37.pdiff [335 B]
Get:20 http://deb.debian.org/debian stretch-updates/main amd64 Packages 2018-10-28-1408.37.pdiff [335 B]
Get:21 http://deb.debian.org/debian stretch-backports/main Sources.diff/Index [27.8 kB]
Get:22 http://deb.debian.org/debian stretch-backports/main amd64 Packages.diff/Index [27.8 kB]
Get:23 http://deb.debian.org/debian stretch-backports/main Translation-en.diff/Index [27.8 kB]
Ign:21 http://deb.debian.org/debian stretch-backports/main Sources.diff/Index
Ign:22 http://deb.debian.org/debian stretch-backports/main amd64 Packages.diff/Index
Get:24 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-10-16-1408.05.pdiff [6,536 B]
Get:25 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-10-20-2016.48.pdiff [140 B]
Get:26 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-10-23-1412.59.pdiff [10.3 kB]
Get:27 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-10-29-1415.54.pdiff [19.3 kB]
Get:28 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-10-29-2016.24.pdiff [483 B]
Get:29 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-10-31-0212.46.pdiff [5,216 B]
Get:30 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-10-31-1408.09.pdiff [1,587 B]
Get:31 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-11-02-2014.21.pdiff [177 B]
Get:32 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-11-03-0215.23.pdiff [1,394 B]
Get:33 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-11-06-1428.50.pdiff [5,533 B]
Get:34 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-11-07-0213.42.pdiff [262 B]
Get:34 http://deb.debian.org/debian stretch-backports/main Translation-en 2018-11-07-0213.42.pdiff [262 B]
Get:35 http://deb.debian.org/debian stretch-backports/main Sources [510 kB]
Get:36 http://deb.debian.org/debian stretch/main Sources [6,751 kB]
Get:37 http://deb.debian.org/debian stretch/main amd64 Packages [7,089 kB]
Get:38 http://deb.debian.org/debian stretch/main Translation-en [5,388 kB]
Get:39 http://deb.debian.org/debian stretch-backports/main amd64 Packages [511 kB]
Fetched 21.7 MB in 5s (4,291 kB/s)
Reading package lists... Done
root@instance-cars:/# apt-get install apache2
```

```
https://ssh.cloud.google.com/projects/cars-222401/zones/us-east1-b/instances/instance-cars?authuser=0&hl=en_US&projectNumber=...
Setting up apache2 (2.4.25-3+deb9u6) ...
Enabling module mpm_event.
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apach
e-htcacheclean.service.
Processing triggers for libc-bin (2.24-11+deb9u3) ...
Processing triggers for sgml-base (1.29) ...
Processing triggers for systemd (232-25+deb9u4) ...
root@instance-cars:/# ls
bin   dev  home        initrd.img.old  lib64       media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib             lost+found  mnt    proc  run   srv   tmp  var  vmlinuz.old
root@instance-cars:/# cd var
root@instance-cars:/var# ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
root@instance-cars:/var# cd www
root@instance-cars:/var/www# ls
html
root@instance-cars:/var/www# service apache2 start
root@instance-cars:/var/www#
```

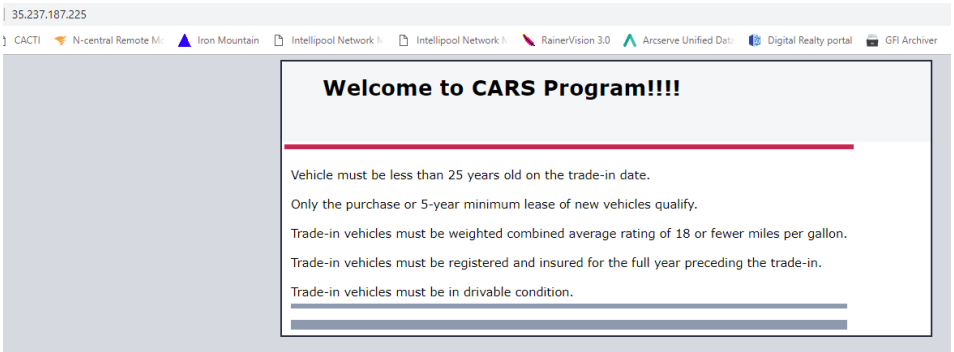
Once we have installed apache2, it creates a folder called www, we make sure apache2 has started, so we browsed the External IP and we see It Works!



Within the folder www, there is another folder called html and in there we see the file index.html, so with a simple word editor as nano we have edited the content of our basic website for the CARS program as an example.



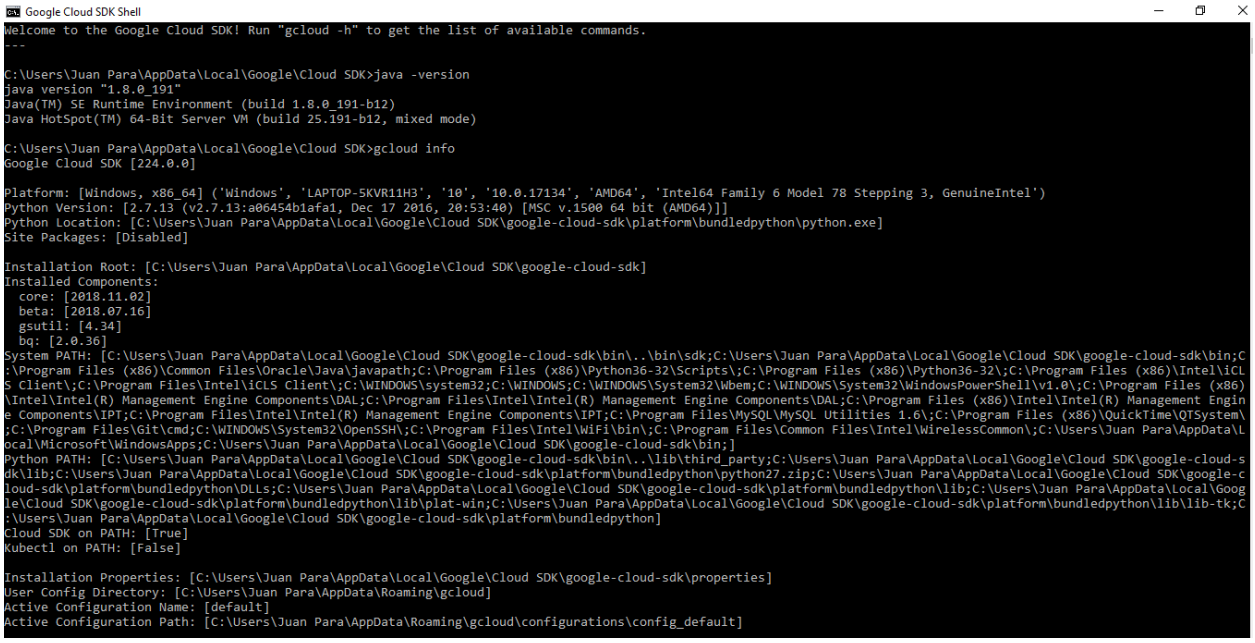
4- Browsing our VM



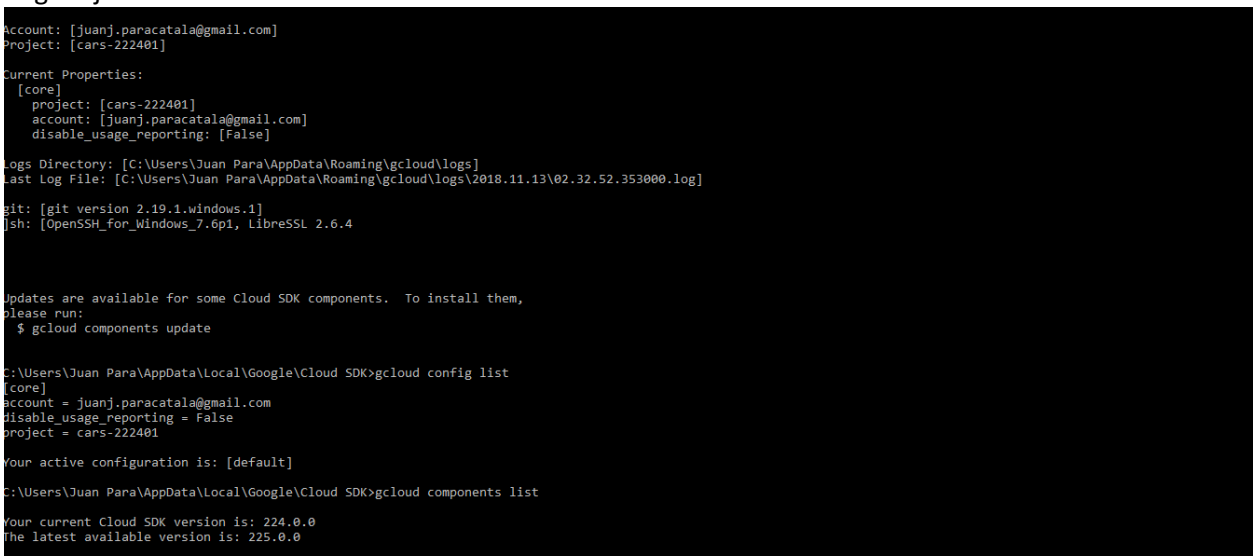
5- Creating a simple JAVA app for our CARS program to Deploy it in the Cloud

Another way to Deploy our Application with Google Cloud is using programming languages as Python or Java. In this example we will use a simple Java instance to deploy in Google Cloud.
We need to Download the Eclipse IDE for Java Developers, Java SE 8 SDK and Google cloud SDK.

Once we have download Google cloud SDK, we can install and configure Google´s plugins for our Eclipse IDE.
First we check a list of available commands “gcloud –h” and then our java version “java –version”, “gcloud info”.



“gcloud components update”, “gcloud components list”, “gcloud components install app-engine-java”.



```
                                                  Components
+------------------+-----------------------------------------------------+------------------------+-----------+
|      Status      |                        Name                         |           ID           |    Size   |
+------------------+-----------------------------------------------------+------------------------+-----------+
| Update Available | BigQuery Command Line Tool                          | bq                     |   < 1 MiB |
| Update Available | Cloud SDK Core Libraries                            | core                   |   8.9 MiB |
| Update Available | gcloud Beta Commands                                | beta                   |   < 1 MiB |
| Not Installed    | App Engine Go Extensions                            | app-engine-go          |  56.9 MiB |
| Not Installed    | Cloud Bigtable Command Line Tool                    | cbt                    |   6.2 MiB |
| Not Installed    | Cloud Bigtable Emulator                             | bigtable               |   4.2 MiB |
| Not Installed    | Cloud Datalab Command Line Tool                     | datalab                |   < 1 MiB |
| Not Installed    | Cloud Datastore Emulator                            | cloud-datastore-emulator |  17.7 MiB |
| Not Installed    | Cloud Datastore Emulator (Legacy)                   | gcd-emulator           |  38.1 MiB |
| Not Installed    | Cloud Pub/Sub Emulator                              | pubsub-emulator        |  33.4 MiB |
| Not Installed    | Cloud SQL Proxy                                     | cloud_sql_proxy        |   3.5 MiB |
| Not Installed    | Emulator Reverse Proxy                              | emulator-reverse-proxy |  14.5 MiB |
| Not Installed    | Google Container Registry's Docker credential helper | docker-credential-gcr  |   1.8 MiB |
| Not Installed    | gcloud Alpha Commands                               | alpha                  |   < 1 MiB |
| Not Installed    | gcloud app Java Extensions                          | app-engine-java        | 108.8 MiB |
| Not Installed    | gcloud app PHP Extensions                           | app-engine-php         |  19.1 MiB |
| Not Installed    | gcloud app Python Extensions                        | app-engine-python      |   6.2 MiB |
| Not Installed    | gcloud app Python Extensions (Extra Libraries)      | app-engine-python-extras |  28.5 MiB |
| Not Installed    | kubectl                                             | kubectl                |   < 1 MiB |
| Installed        | Cloud Storage Command Line Tool                     | gsutil                 |   3.5 MiB |
+------------------+-----------------------------------------------------+------------------------+-----------+
To install or remove components at your current SDK version [224.0.0], run:
  $ gcloud components install COMPONENT_ID
  $ gcloud components remove COMPONENT_ID

To update your SDK installation to the latest version [225.0.0], run:
  $ gcloud components update


C:\Users\Juan Para\AppData\Local\Google\Cloud SDK>gcloud components install app-engine-java

Restarting command:
  $ gcloud components install app-engine-java


C:\Users\Juan Para\AppData\Local\Google\Cloud SDK>
```

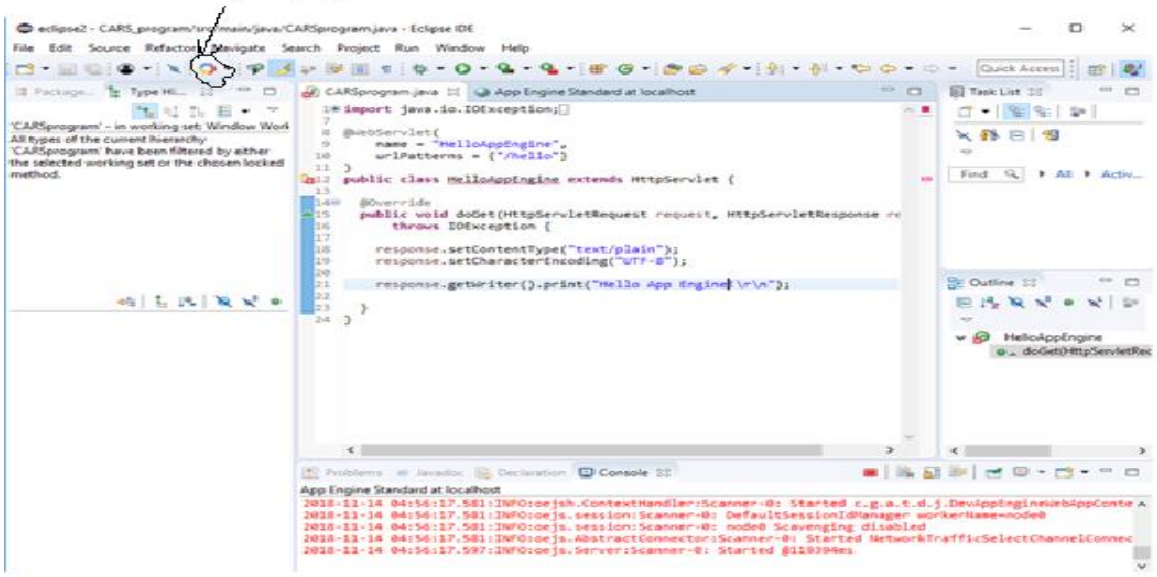
```
Your current Cloud SDK version is: 224.0.0
The latest available version is: 225.0.0

                                                  Components
+------------------+-----------------------------------------------------+------------------------+-----------+
|      Status      |                        Name                         |           ID           |    Size   |
+------------------+-----------------------------------------------------+------------------------+-----------+
| Update Available | BigQuery Command Line Tool                          | bq                     |   < 1 MiB |
| Update Available | Cloud SDK Core Libraries                            | core                   |   8.9 MiB |
| Update Available | gcloud Beta Commands                                | beta                   |   < 1 MiB |
| Update Available | gcloud app Python Extensions                        | app-engine-python      |   6.2 MiB |
| Not Installed    | App Engine Go Extensions                            | app-engine-go          |  56.9 MiB |
| Not Installed    | Cloud Bigtable Command Line Tool                    | cbt                    |   6.2 MiB |
| Not Installed    | Cloud Bigtable Emulator                             | bigtable               |   4.2 MiB |
| Not Installed    | Cloud Datalab Command Line Tool                     | datalab                |   < 1 MiB |
| Not Installed    | Cloud Datastore Emulator (Legacy)                   | gcd-emulator           |  38.1 MiB |
| Not Installed    | Cloud Pub/Sub Emulator                              | pubsub-emulator        |  33.4 MiB |
| Not Installed    | Cloud SQL Proxy                                     | cloud_sql_proxy        |   3.5 MiB |
| Not Installed    | Emulator Reverse Proxy                              | emulator-reverse-proxy |  14.5 MiB |
| Not Installed    | Google Container Registry's Docker credential helper | docker-credential-gcr  |   1.8 MiB |
| Not Installed    | gcloud Alpha Commands                               | alpha                  |   < 1 MiB |
| Not Installed    | gcloud app PHP Extensions                           | app-engine-php         |  19.1 MiB |
| Not Installed    | gcloud app Python Extensions (Extra Libraries)      | app-engine-python-extras |  28.5 MiB |
| Not Installed    | kubectl                                             | kubectl                |   < 1 MiB |
| Installed        | Cloud Datastore Emulator                            | cloud-datastore-emulator |  17.7 MiB |
| Installed        | Cloud Storage Command Line Tool                     | gsutil                 |   3.5 MiB |
| Installed        | gcloud app Java Extensions                          | app-engine-java        | 108.8 MiB |
+------------------+-----------------------------------------------------+------------------------+-----------+
To install or remove components at your current SDK version [224.0.0], run:
  $ gcloud components install COMPONENT_ID
  $ gcloud components remove COMPONENT_ID

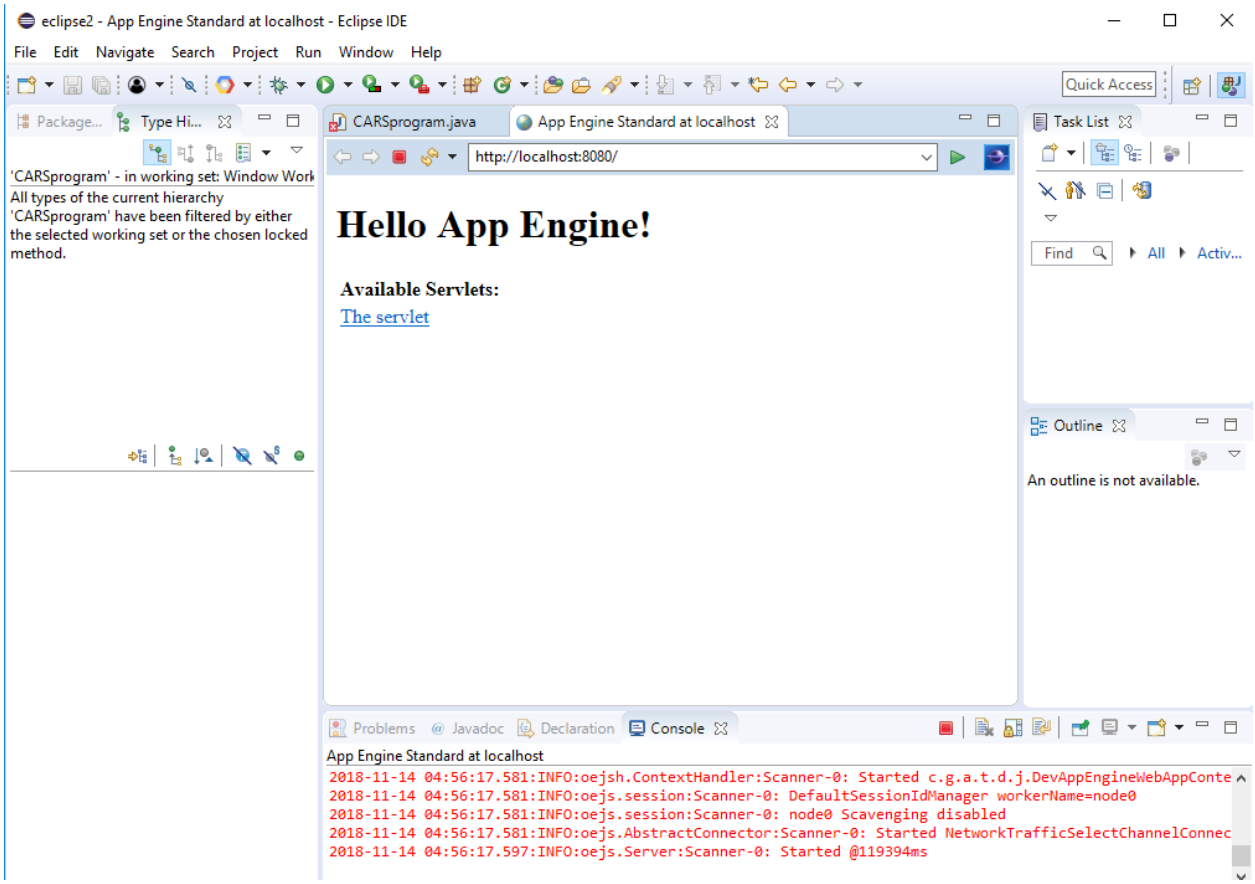
To update your SDK installation to the latest version [225.0.0], run:
  $ gcloud components update

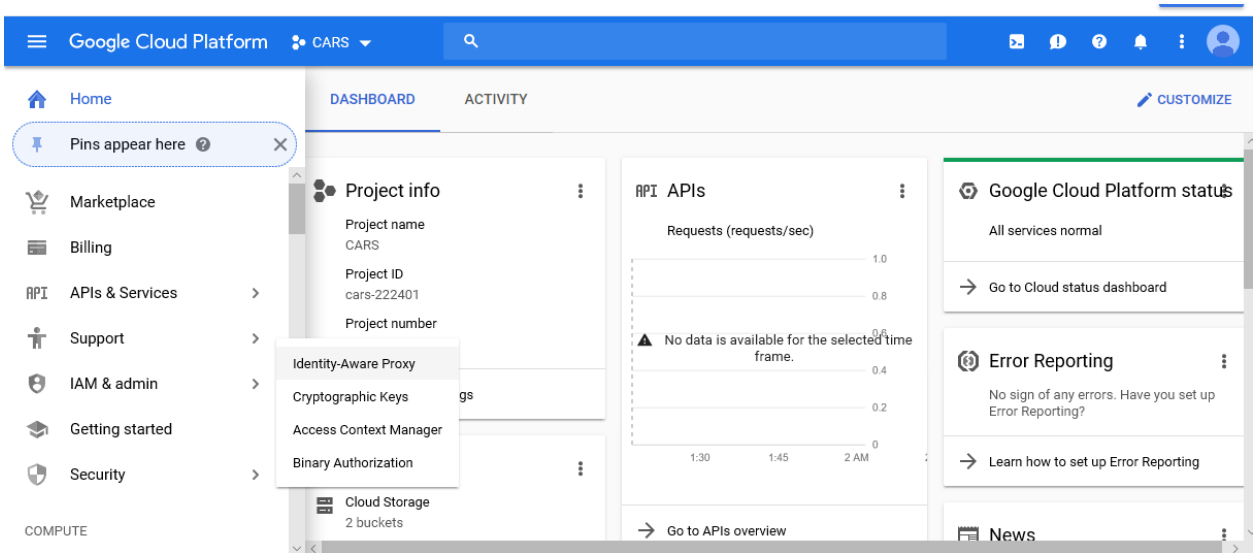

C:\Users\Juan Para\AppData\Local\Google\Cloud SDK>
```

Google's plugins



After that we can create our project as Google web app.





Feasibility report on using Google Cloud:

GCP provides the same flexibility, namely the sustained-use discounts, after merely a month of usage, and the discount can be applied to any other package, should the need for configuration adjustment arise. This makes long-term discount policy from GCP a viable and feasible alternative to what to any other Cloud Provider offers, and rather an investment, not an item of

expenditure. Besides, you avoid vendor lock-in and are free to change the provider if need be, without losing all the money paid in advance.

GCP, offers per-second billing as an option for ALL their virtual machines, regardless of the OS's they run on, and their instances are fully configurable, so the customers can order 1 CPU and 3.25GB RAM, or 4.5GB, or 2.5GB….

Google has full-scale encryption of all their data and communication channels. Even the stored data is encrypted, and so the traffic between data centers.

GCP already provides all the needed functionality and offers competitive pricing and configuration models, backed up by serious traffic privacy and security measures.

https://hackernoon.com/aws-vs-google-cloud-platform-which-cloud-service-provider-to-choose-94a65e4ef0c5

Recommendations regarding Google Apps for the CARS system:

CARS program will have to monitors Daily APIs Quota Consumption, it's also needs to implement Back off Retry Strategy for HTTP 4xx and 5xx errors.

The Application will need to follow Google OAuth, OpenID, Google APIs and SSO best practices if deployed on Google App Engine and Compute Engine.

Supports deployment on several browsers and devices and develops a rollback plan for any major deployment, in case of any incompatibility issue.

The application also needs to maintain a staging environment for testing and debugging as it is possible the application will grow and implement more features.

Implements a deployment strategy that can scale 10x of its current user base, as it is hard to guess how many car dealers will agree to take onboard the CARS program and it will require a lots of work, time and commitment to work under this legislation.

It will be important to maintain an on call rotation of engineers in the event of customer deployments, product errors, failures, and outages.

Implements an Information Security policy that is periodically reviewed, approved by the provider's Senior Management, and communicated to all employees.

Implements an Incident Response & Risk Management policy that is periodically reviewed, approved by the provider's Senior Management, and communicated to all employees.

Engages accredited third-parties to periodically audit internal security controls.

Since the application is reviewed on an annual basis, application providers and customers should conduct an internal or external network and web-application vulnerability scan prior to the release of any major upgrade of the application.

https://support.google.com/a/answer/6067029?hl=en