

Proyecto fin de curso

ASIR



Sistema para la administración de aplicaciones web en Google Cloud

10/06/2019

Autor: Hisham Haitak Martínez

Tutor: Roberto García Altalaguerri

Índice

Índice	2
Introducción	3
Módulos que implica	3
Breve descripción del proyecto	3
Google Cloud	4
Preparación del servidor	6
Creación de la máquina con gcloud	6
Certificación	8
SDK Gcloud	10
Configurar SDK para que interactúe libremente con el servidor	11
Creación de las imágenes	12
Código	12
Página principal del proyecto	13
Creación de la máquina	14
Filtrado por usuario	16
Borrado y confirmación	17
Recursos	19
Conclusiones	20
Problemas encontrados	20
DNS	20
CÓDIGO	20
MAQUETADO Y ESTILOS	20
PRESUPUESTO	20
API GOOGLE CLOUD	20
CONFIRMACIÓN DEL BORRADO	20
Mejoras y ampliación	21
Referencias	21

Introducción

Módulos que implica

- Para realizar el proyecto, he usado los conocimientos adquiridos en los siguientes módulos:
- Para crear el servidor apache, establecer la conexión cifrada, el DNS así como trabajar con la consola de Google Cloud, Servicios en Red
- Para desarrollar los scripts de PHP y los estilos aplicados con Bootstrap 3, Aplicaciones web y Lenguaje de marcas
- Para hacer los comandos de bash usados en los scripts, Sistemas operativos

Breve descripción del proyecto

El proyecto consiste en una aplicación web alojada en un servidor remoto de Google Cloud, la aplicación es una herramienta para desplegar servidores de manera rápida, en mi proyecto he utilizado servidores web, pero podrían ser entornos preparados para otras finalidades.

<https://hgcloud.tk/>



- Que la aplicación permite crear y borrar los servidores.
- Acceder a los servidores por la ip pública, con usuario entregado al usuario, también por SSH
- Que permita identificar mediante un nombre los propietarios de las máquinas.
- Que se acceda desde internet, con un dominio propio

Google Cloud

Google cloud es una gran infraestructura de cloud computing con una gran variedad de servicios, pero los más importantes son estos 8

Compute Engine Máquinas virtuales escalables y de alto rendimiento.	Cloud Storage Almacenamiento de objetos en caché perimetral a nivel mundial.
App Engine Plataforma de aplicaciones sin servidor para aplicaciones y backends.	Cloud SQL Servicio de base de datos MySQL y PostgreSQL.
Transcripción de voz de Cloud Convierte voz en texto con la tecnología de aprendizaje automático.	BigQuery Almacén de datos totalmente gestionado y muy escalable con aprendizaje automático integrado.
Cloud Vision Consigue información valiosa a partir de imágenes con la tecnología de aprendizaje automático.	Uso obligatorio de llaves de seguridad Exige el uso de llaves de seguridad para prevenir la suplantación de identidad (phishing).

Yo para este proyecto usaré estas 2


Compute Engine Máquinas virtuales escalables y de alto rendimiento.
App Engine Plataforma de aplicaciones sin servidor para aplicaciones y backends.

- Compute Engine

Este servicio sirve para crear, borrar, importar y exportar máquinas virtuales online alojados en la nube

- App Engine

Tiene la posibilidad de desarrollar aplicaciones directamente sin preocuparte del servidor, es potente, nosotros solo usaremos la API del Compute Engine

 **Detalles**

Nombre
Compute Engine API

De
Google

Nombre del servicio
compute.googleapis.com

Información general
Creates and runs virtual machines on Google Cloud Platform.

Estado de activación
Habilitada

Preparación del servidor

Creacion de la maquina con gcloud

Para montar la infraestructura usaremos una Instancia Virtual de Google Cloud.

Configurar las reglas del cortafuego para que admitan http y https

Asignar una ip pública estática

He usado Debian 9, pero cualquier Linux nos serviría.

Abrimos una sesión desde la consola de Google Cloud

```
$ gcloud compute --project=pfc-hisham instances create srvsdk
--zone=europe-west4-a --machine-type=g1-small --subnet=default
--network-tier=PREMIUM --maintenance-policy=MIGRATE
--service-account=91227168306-compute@developer.gserviceaccount.com
--scopes=https://www.googleapis.com/auth/cloud-platform
--tags=http-server,https-server --image=debian-9-stretch-v20190326
--image-project=debian-cloud --boot-disk-size=15GB
--boot-disk-type=pd-standard --boot-disk-device-name=srvsdk
```

--project=pfc-hisham	Especifica el proyecto
--zone=europe-west4-a	La zona donde se encuentran los recursos de google
--machine-type=g1-small	tipo predefinido de maquina, esta tiene 0.5 CPU y 1.7 de RAM
--subnet=default	Selecciona la subred en nuestro caso predeterminada

--service-account=912...	La cuenta de servicio la mia del proyecto
--image=debian-9-stretch-v20190326	Imagen a utilizar, predeterminada debian 9 de google cloud.
--image-project=debian-cloud	El proyecto al que pertenece la imagen o familia de imágenes.
--boot-disk-size=15GB	Tamaño del disco virtual
--boot-disk-type=pd-standard	tipo de disco, disco estándar no ssd
--boot-disk-device-name=srvsdk	nombre del disco

La mayoría de los parámetros te los asigna por defecto, pero como es la primera máquina, los asignamos nosotros

```
Connected, host fingerprint: ssh-rsa 0 6F:D9:39:B6:51:DA:14:22:B2:17:A4:E6:44:75
:80:D2:45:E2:75:A3:F1:38:DD:B9:54:7D:42:F8:25:F4:D1:57
Linux srvsdk 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
```

Desde aquí, se maneja remotamente el servidor, desde la ventana de navegador que te abre Google Cloud.

Al ser un servidor pensado para producción tendrá que configurarse como tal.

```
GNU nano 2.7.4                               File: /etc/apache2/apache2.conf

LogFormat "%{User-agent}i" agent

# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

ServerName hgcloud.tk

ServerTokens Prod
MaxKeepAliveRequests 500
Timeout 300
LogLevel crit
```

Certificación

Usare Certbot con certificados de Lets encrypt.

Certbot

Certbot es un cliente automático fácil de usar que busca e implementa certificados SSL / TLS para su servidor web. Certbot fue desarrollado por EFF y otros como cliente de Let's Encrypt y anteriormente se conocía como "el cliente oficial de Let's Encrypt" o "el cliente de Let's Encrypt Python". Certbot también funcionará con cualquier otra CA que admita el protocolo ACME. [Externo](#)

Lets encrypt

Let's Encrypt es una autoridad de certificación (AC, o CA por sus siglas en inglés) gratuita, automatizada, y abierta, manejada para el beneficio público. Es un servicio proveído por el Internet Security Research Group (ISRG).

Le damos a las personas certificados digitales que necesitan en orden para habilitar HTTPS (SSL/TLS) para sitios web, gratuitamente, de la forma más fácil para el usuario en la que podemos. Hacemos esto porque queremos crear un web más seguro y respetuoso de privacidad. [Externo](#)


```
$ sudo apt-get install certbot python-certbot-apache -t stretch-backports
```

Una vez instalado lo iniciamos

```
$ sudo certbot --apache
```

```
Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
-----
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration.
-----
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 2
Enabled Apache rewrite module
Redirecting vhost in /etc/apache2/sites-enabled/000-default.conf to ssl vhost in /etc/apache2/sites-available/000-default-le-ssl.conf
-----
Congratulations! You have successfully enabled https://hgcloud.tk

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=hgcloud.tk
-----

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/hgcloud.tk/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/hgcloud.tk/privkey.pem
  Your cert will expire on 2019-07-22. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot again
  with the "certonly" option. To non-interactively renew *all* of
  your certificates, run "certbot renew"
- Your account credentials have been saved in your Certbot
  configuration directory at /etc/letsencrypt. You should make a
  secure backup of this folder now. This configuration directory will
  also contain certificates and private keys obtained by Certbot so
  making regular backups of this folder is ideal.
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF: https://eff.org/donate-le
```



Ya tenemos nuestro servidor cifrado con un certificado de confianza.

SKD Gcloud

Para instalar el SDK de Google hay que crear primero una variable de entorno

```
exit
hishampzl@srvsdk:~$ export CLOUD_SDK_REPO="cloud-sdk-$(lsb_release -c -s)"
hishampzl@srvsdk:~$
```

Añadir el repositorio

```
hishampzl@srvsdk:~$ echo "deb http://packages.cloud.google.com/apt $CLOUD_SDK_REPO main" | sudo tee -a /etc/apt/sources.list.d/google-cloud-sdk.list
deb http://packages.cloud.google.com/apt cloud-sdk-stretch main
hishampzl@srvsdk:~$
```

Importamos la clave pública de la plataforma de google

```
hishampzl@srvsdk:~$ curl https://packages.cloud.google.com/apt/doc/apt-key.gpg | sudo apt-key add -
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1326 100 1326    0     0 45013      0 --:--:-- --:--:-- --:--:-- 45724
OK
hishampzl@srvsdk:~$
```

Y instalar el paquete después de actualizar los repositorios

```
hishampzl@srvsdk:~$ sudo apt-get update && sudo apt-get install google-cloud-sdk
Hit:1 http://security.debian.org stretch/updates InRelease
Ign:2 http://deb.debian.org/debian stretch InRelease
Get:3 http://deb.debian.org/debian stretch-updates InRelease [91.0 kB]
Get:4 http://deb.debian.org/debian stretch-backports InRelease [91.8 kB]
Hit:5 http://deb.debian.org/debian stretch Release
Hit:6 http://packages.cloud.google.com/apt cloud-sdk-stretch InRelease
Hit:7 http://packages.cloud.google.com/apt google-compute-engine-stretch-stable InRelease
Hit:9 http://packages.cloud.google.com/apt google-cloud-packages-archive-keyring-stretch InRelease
Fetched 183 kB in 0s (350 kB/s)
Reading package lists... Done
```

Configurar SDK para que interactúe libremente con el servidor

Como el servidor va a estar todo el rato en marcha, solo tenemos que hacer

```
hishampzl@srvsdk:~$ gcloud init
Welcome! This command will take you through the configuration of gcloud.

Settings from your current configuration [default] are:
compute:
  region: europe-west4
  zone: europe-west4-a
core:
  account: 91227168306-compute@developer.gserviceaccount.com
  disable_usage_reporting: 'True'
  project: pfc-hisham

Pick configuration to use:
[1] Re-initialize this configuration [default] with new settings
[2] Create a new configuration
Please enter your numeric choice: 1
```

escogemos cuenta asociada al proyecto, cuando creas tu cuenta de google cloud con la de gmail, automáticamente te crea esa id de arriba, como usuario con permisos.

```
Your current configuration has been set to: [default]

You can skip diagnostics next time by using the following flag:
  gcloud init --skip-diagnostics

Network diagnostic detects and fixes local network connection issues.
Checking network connection...done.
Reachability Check passed.
Network diagnostic passed (1/1 checks passed).

Choose the account you would like to use to perform operations for
this configuration:
[1] 91227168306-compute@developer.gserviceaccount.com
[2] Log in with a new account
Please enter your numeric choice: 1
```

```
Did not print [12] options.
Too many options [62]. Enter "list" at prompt to print choices fully.
Please enter numeric choice or text value (must exactly match list
item): 21

Your project default Compute Engine zone has been set to [europe-west3-a].
You can change it by running [gcloud config set compute/zone NAME].

Your project default Compute Engine region has been set to [europe-west3].
You can change it by running [gcloud config set compute/region NAME].

Your Google Cloud SDK is configured and ready to use!

* Commands that require authentication will use 91227168306-compute@developer.gserviceaccount.com by default
* Commands will reference project 'pfc-hisham' by default
* Compute Engine commands will use region 'europe-west3' by default
* Compute Engine commands will use zone 'europe-west3-a' by default

Run 'gcloud help config' to learn how to change individual settings

This gcloud configuration is called [default]. You can create additional configurations if you work with multiple
accounts and/or projects.
Run 'gcloud topic configurations' to learn more.

Some things to try next:

* Run 'gcloud --help' to see the Cloud Platform services you can interact with. And run 'gcloud help COMMAND' to
  get help on any gcloud command.
* Run 'gcloud topic --help' to learn about advanced features of the SDK like arg files and output formatting
```

y la zona, se suele elegir una zona cercana para evitar latencias altas, algunas zonas son más económicas que otras, pero al estar más alejadas el tiempo de respuesta puede ser peor.

Escojo la europe-3-a, porque durante el proyecto, puse europe-4-a y en cierto momento del proyecto, no le quedaban recursos para mis maquinas así que me tocó cambiarla.

Creación de las imágenes

En este apartado use Bitnami con GCloud para crear la imagen básica de Wordpress, moodle y prestashop, tras hacer eso, aplique reglas de cortafuegos permitiendo ssh, http y https y cree la imagen a partir de esa máquina, me guardé los usuarios predeterminados de la máquina para administrar el servidor web, y los añadí a el script.php para que dependiendo de la imagen usada, saliera unos usuarios o otros.

Bitnami

Bitnami es el líder de la industria en empaquetado de aplicaciones. Desde nuestras raíces en la creación de instaladores de Windows y Linux para miles de ISV en Bitrock hasta ayudar a los usuarios a implementar más de 1 millón de aplicaciones al mes como el principal proveedor de máquinas virtuales listas para ejecutar e imágenes en la nube para los proveedores de nube líderes del mundo, Bitnami nunca ha renunciado a nuestra misión de poner a disposición de todos un software increíble. Bitnami continúa esa misión hoy al reducir la barrera de adopción para que cualquiera pueda implementar y mantener un espectro completo de aplicaciones de servidor, pilas de desarrollo y aplicaciones de infraestructura en prácticamente cualquier formato que deseen. Desde usuarios no técnicos que buscan lanzar una aplicación empresarial o un entorno de alojamiento web hasta desarrolladores empresariales que buscan acelerar el desarrollo o automatizar la migración a la nube. [Externo](#)

Código

El proyecto consta de 4 archivos principalmente que adjuntare en la entrega:

index.html	Todo html, es el formulario que apunta a los scripts php
script.php	Este fichero tiene la creación de las máquinas

script.php	Este fichero contiene el código para la consulta de máquinas
script3.php	Este fichero contiene el script de borrado de máquinas

Página principal del proyecto

Este fichero es la cara del proyecto su nombre es index.html, tiene dos formularios en html con bootstrap 3 para maquetar y poner estilos.

Web Server Creator

Consultar

Usuario
Usuario propietario de las maquinas
[a-z]

Consulta

Cancelar

Crear

Usuario
Identificador de cada usuario
[a-z]
Nombre de la instancia
Nombre que recibirá la instancia
[a-z,0-9]
Selecciona la imagen

Moddle ▼

Usuario propietario de la clave
Nombre exacto del usuario propietario de la imagen, dejar null si no se va a utilizar

Solo rellenar si utilizaras conexion SSH

Crear

Borrar

Creación de la máquina

Este script es el grande de el proyecto ya que es este el que interactúa con gcloud para crear las máquinas

```
$salida = shell_exec('gcloud compute instances create "'.$name.'"
--zone europe-west 3-a --description "'.$user.'" --image "'.$image.'" |
tail -n+2 | tr -s " " | cut -d " " -f5');
```

Para añadir las claves públicas de ssh y que se pueda conectar a la máquina, es necesario añadirla por fichero creado en el host, para ello con esta línea, se crea un fichero en local con el usuario de la clave y con la clave en si, el label descripción es para añadir usuario a la máquina, y luego poder filtrar por el mismo,

```
shell_exec('echo "'.$sshuser.'":"'.$clave.'" > keys');
```

shell_exec	Ejecuta comandos en el servidor mediante php
echo "'.\$sshuser.'":"'.\$clave.'"> keys	Imprime esas dos variables en el fichero keys

El fichero keys contendrá el usuario y la clave pública de ssh del propietario de la máquina.

Tras eso, hay que añadir la clave a la máquina, para ello he usado este otro comando de gcloud

```
shell_exec('gcloud compute instances add-metadata "'.$name.'" --zone
europe-west3-a --metadata-from-file ssh-keys="/var/www/html/keys"');
```

gcloud compute instances add-metadata	Añade metadatos a la máquina a nivel de instancia
--metadata-from-file	Coge los metadatos de un fichero en nuestro caso

ssh-keys="/var/www/html/keys"	el fichero keys
-------------------------------	-----------------

Cuando se ejecuta la salida del script.php entrega el nombre de la máquina, comando a ejecutar para conectarte por ssh y los datos web de la máquina para poder administrar la web.

Tu máquina virtual

Nombre de tu maquina
prueba

SSH:null@35.246.255.199

Tu web estará disponible en un maximo de 2 minutos.[Direccion a tu web](#)
Username: user
Password: QG200JaEFyOs

Se recomienda cambiar la contraseña genérica por seguridad

Atras

NOTA: Si pones null, no te sale usuario, lo desactive para hacer la captura, la salida de dejar el campo en null es la siguiente captura.

Tu máquina virtual

Nombre de tu maquina
preuba2

No añadiste clave SSH

Tu web estará disponible en un maximo de 2 minutos.[Direccion a tu web](#)
Username: user
Password: joVpjH2U0Xn1

Se recomienda cambiar la contraseña genérica por seguridad

Atras

Filtrado por usuario

Este apartado sucede en el script2.php, que recibe los datos del index.html con post

Con este comando, filtra las máquinas usando la descripción que se añadió antes como usuario

```
$img = shell_exec('gcloud compute instances list
--filter="description:"'. $user. '"' | tail -n+2 | tr -s " " | cut -d " "
-f1,5,6');
```

gcloud compute instances list	Lista todas las máquinas del proyecto
--filter="description:\$user"	Filtra por la descripción añadida en este caso usuario
tail -n+2	Imprime sólo a partir de la segunda línea
tr -s " "	Elimina espacios extras
cut -d " " -f1,5,6	Imprime sólo los campos 1 5 y 6 con delimitador "espacio"

Le especificas el nombre usuario, y el filtra por un nombre en la descripción

Estas son tus maquinas

prueba 35.198.100.141 RUNNING

Borrar

Nombre de la máquina

Nombre de la máquina que desea borrar

Borrar

Cancelar

Atras

Borrado y confirmación

Este script contiene los comandos de borrado y confirmación del mismo

```
$del = shell_exec('gcloud compute instances delete "'. $mach.'"
--delete-disks all --zone europe-west 3-a --quiet || hostname');
```

gcloud compute instances delete	Borra una máquina
--delete-disks all	Si la maquina tiene mas discos puedes elegir que tipo de discos borrar, de arranque o de datos, en nuestro caso todos
--quiet	Para evitar interacciones en el prompt
hostname	Si la salida es errónea, ejecuta hostname Más información del motivo del comando

la salida de \$del, se lleva a un if que si ha dado ok, confirma con el nombre y si no, te dice que la máquina introducida no existe.

Estas son tus maquinas

haitak 35.198.97.59 RUNNING

Borrar

Nombre de la máquina

haitak2

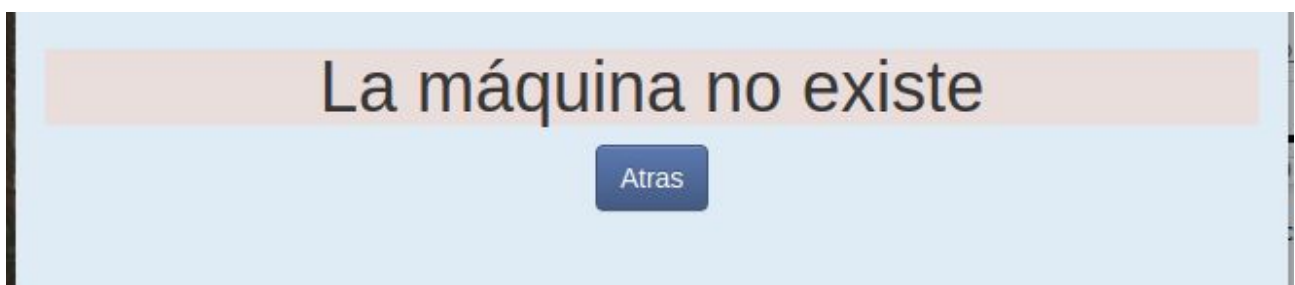
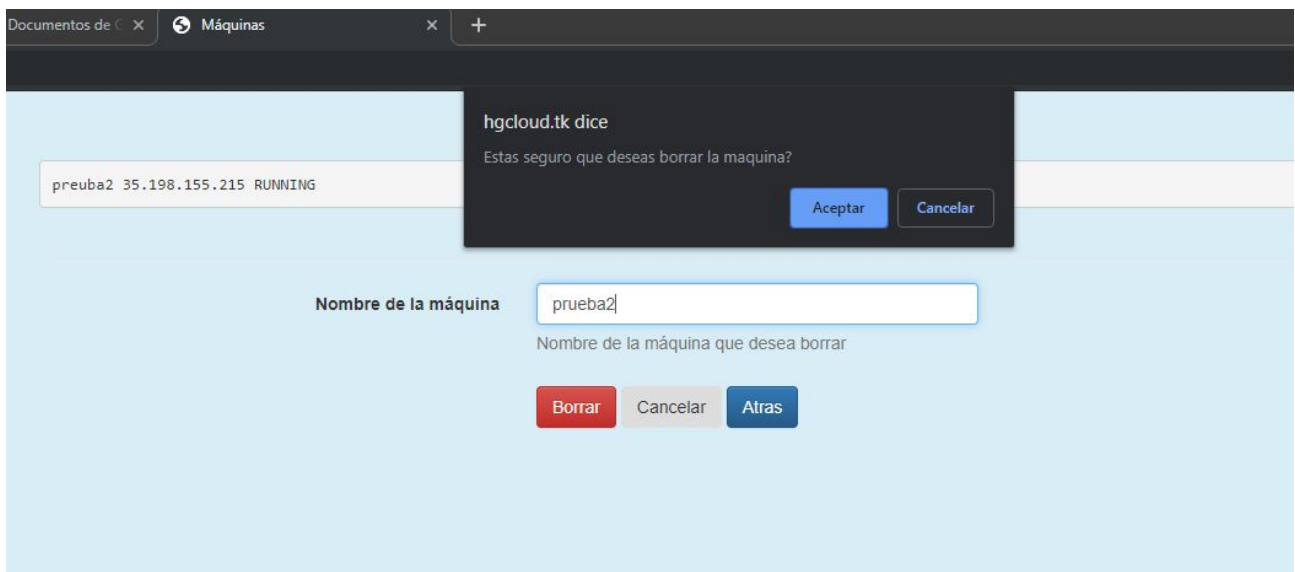
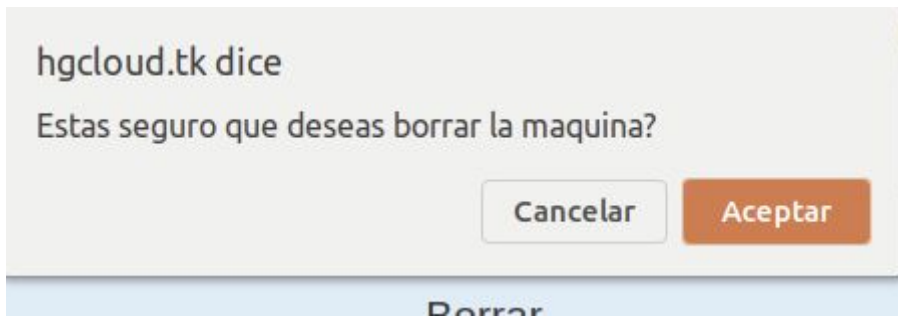
Nombre de la máquina que desea borrar

Borrar

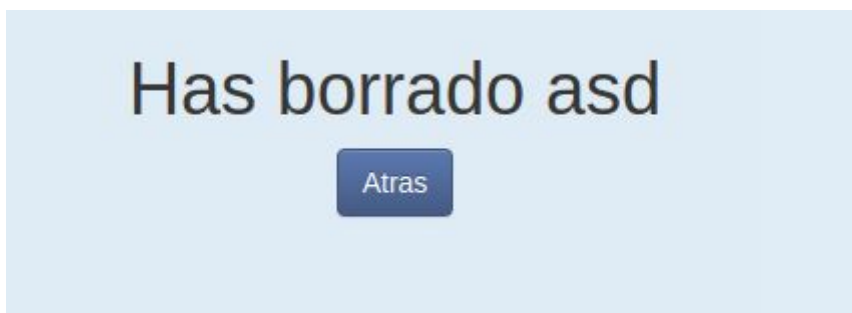
Cancelar

Atras

Si introduzco un nombre inexistente, y le damos a borrar, te pedirá confirmación al aceptar con un nombre erróneo



Pero si la máquina existe, la borra y nos confirma cuál es la máquina borrada.



Recursos

Los recursos de los que dispongo son una cuenta con 300\$ gratuitos de Google Cloud, y un portátil HP Probook G3 con 8 GB de ram y un i5, el portátil iba a ser utilizado para montar el servidor en el, pero al final se usó para trabajar por ssh en el servidor.

Conclusiones

Problemas encontrados

DNS

Cuando empecé en el proyecto, lo hice en un portátil de la empresa, pero cuando fui a darle un dominio propio a la web, al estar en la red del trabajo no pude ponerlo.

CÓDIGO

No conseguía hacer que el php metiera las variables dentro de los shell_exec, me tocó documentarme bien, y sobre todo en las condiciones, a la hora de hacer los formularios, me tocó informarme bien de el bootstrap ya que no he estudiado eso, sobre todo con los caracteres especiales de html ya que hay que tratarlos de otra forma con el php.

En el último script, hice un if que trataba la salida del borrado, y no conseguía hacer que la condición se cumpliera y mostrará lo que quería, por lo que al final hice un doble tubería, y puse un comando, el cual la salida fuera siempre fija, hostname, y en la condición especifiqué que cuando fuera hostname diera fallo de borrado y el else diera comando correcto.

MAQUETADO Y ESTILOS

Tuve que informarme y hacer bastantes pruebas hasta que quedara como quise, en los estilos, muchas clases no se cargaban, y no hacían lo que yo quería eso desencadenó más pruebas.

PRESUPUESTO

Como la cuenta es gratuita, no he podido acceder a todas las opciones de Google Cloud, y no pude hacer la parte de exportador de maquinas, porque requería almacenamiento de google y no tenía acceso al mismo.

API GOOGLE CLOUD

Cuando intenté crear las máquinas desde el script php, y no me dejaba, si me dejaba listar, pero cuando intentaba crearlas, no me dejaba, como ya he mencionado arriba, investigue un poco, ya que con las mismas variables, un comando funcionaba y otro no, miré los logs, y encontré un aviso de un API, lo active

en la consola de google cloud, y tras eso el comando funcionaba sin ningun problema.

CONFIRMACIÓN DEL BORRADO

La salida del comando de Gcloud para borrar, es interactiva, y para que no lo sea hay que añadirle el parámetro `--quiet`, la salida que da al poner ese parámetro es nula, hayas borrado la máquina, o no exista, así que tuve que poner que al dar error en la salida con un `||` ejecutará `hostname` en el shell y me entregara algo legible por el `if`.

Mejoras y ampliación

Se puede añadir más seguridad en cuanto a la autenticación, una base de datos y un formulario de registro, sería una opción a contemplar.

Con el Storage de Google se puede realizar un apartado que exporte la maquina y te permita llevarla a la plataforma que quieras.

Se pueden añadir muchisimas mas imagenes para crear máquinas sin mucho esfuerzo.

Referencias

<https://letsencrypt.org/es/getting-started/>

<https://certbot.eff.org/lets-encrypt/debianstretch-apache>

<https://cloud.google.com/sdk/docs/>

<https://www.w3schools.com/>

<https://php.net/manual/es/intro-what-is.php>

<https://bitnami.com/>