Bitácora y Configuración de Seguridad Servidor GCP

Tabla de contenido

[1. Resumen del Proyecto y Estado Actual 3](#_Toc208173990)

[2. Características de la Infraestructura (Google Cloud Compute Engine) 3](#_Toc208173991)

[3. Configuración de la Red y Firewall 4](#_Toc208173992)

[4. Servicios Adicionales del Servidor 4](#_Toc208173993)

[5. Configuración de la Base de Datos (PostgreSQL) 5](#_Toc208173994)

[6. Conexión y Acceso 5](#_Toc208173995)

# 1. Resumen del Proyecto y Estado Actual

Este documento detalla la configuración de un servidor en la nube y su base de datos relacional, diseñado para soportar una aplicación estudiantil. La infraestructura se aloja en Google Cloud Platform (GCP) utilizando una instancia de Compute Engine. El sistema fue comprometido inicialmente debido a vulnerabilidades de seguridad, lo que ha llevado a una reconfiguración completa con un enfoque prioritario en la seguridad.

# 2. Características de la Infraestructura (Google Cloud Compute Engine)

* **Proveedor:** Google Cloud Platform (GCP)
* **Servicio:** Compute Engine
* **Nombre de la Instancia:** server-capstone-g3
* **Tipo de Máquina:** e2-micro. Esta instancia de nivel gratuito está configurada con 2 vCPUs y 1 GB de RAM, ideal para entornos de desarrollo y pruebas.
* **Sistema Operativo:** Distribución de Linux (Debian/Ubuntu).
* **Región y Zona:** us-central1-a
* **Dirección IP Externa Actual:** 34.67.243.255. Esta dirección IP es dinámica y cambia cada vez que la instancia se reinicia. Sirve como el punto de acceso público actual para todos los servicios del servidor.
* **Autenticación de Acceso:** El acceso SSH por contraseña ha sido **deshabilitado**. La autenticación al servidor ahora se realiza exclusivamente a través de **claves SSH** para garantizar una conexión segura.

# 3. Configuración de la Red y Firewall

Las reglas del firewall de GCP han sido reevaluadas para una mayor seguridad. La regla anterior de acceso irrestricto al puerto 5432 fue eliminada.

* **Regla de Firewall - Tráfico Web (HTTP):**
  + **Nombre de la Regla:** default-allow-http
  + **Prioridad:** 1000
  + **Acción:** Permitir
  + **Protocolo y Puertos:** tcp:80
  + **Rangos de IP de Origen:** 0.0.0.0/0 (acceso público)
  + **Propósito:** Habilita el acceso al servidor web Nginx.
* **Regla de Firewall - Tráfico de Base de Datos (PostgreSQL):**
  + **Nombre de la Regla:** allow-postgres-5432
  + **Prioridad:** 1000
  + **Acción:** Permitir
  + **Protocolo y Puertos:** tcp:5432
  + **Rangos de IP de Origen:** **Restringido a un rango de IP específico**. La configuración anterior de 0.0.0.0/0 fue eliminada para evitar nuevas vulnerabilidades.

# 4. Servicios Adicionales del Servidor

* **Servidor Web Nginx:** Instalado y configurado en el servidor para servir contenido estático y para actuar como un **proxy inverso** para las aplicaciones de backend. El archivo index.html de prueba está alojado en /var/www/html/.
* **Plataforma de Backend (Futuro):** Se ha definido una arquitectura segura donde el procesamiento de documentos con la API de Gemini se realizará en un servidor de backend (usando Java/Kotlin) que se comunicará con la base de datos de forma local, evitando exponer la clave de la API. Se recomienda el despliegue de esta aplicación en **Google Cloud Run** para mayor seguridad, escalabilidad y eficiencia de costos.

# 5. Configuración de la Base de Datos (PostgreSQL)

La base de datos fue reinstalada y configurada desde cero para corregir problemas y reforzar la seguridad.

* **Motor:** PostgreSQL
* **Versión:** 15.13
* **Método de Inicio:** El servicio no se gestiona con systemd. Se debe iniciar manualmente con el siguiente comando SSH:

*sudo -u postgres /usr/lib/postgresql/15/bin/pg\_ctl start -D /var/lib/postgresql/15/main*

* **Usuario de la Aplicación:** Se ha creado un nuevo usuario seguro: cvalencia.
* **Contraseña:** Una contraseña fuerte y aleatoria fue asignada al usuario cvalencia para evitar vulneraciones.
* **Base de Datos de la Aplicación:** Se ha creado una base de datos exclusiva: DB\_CAPSTONEG3.
* **Configuración de Conexión Remota:**
  + postgresql.conf: La directiva listen\_addresses se ha establecido en '\*' para permitir la conexión remota.
  + pg\_hba.conf: Se ha configurado una entrada para el usuario cvalencia que exige autenticación de contraseña mediante el método seguro **scram-sha-256** para todas las conexiones remotas a la base de datos DB\_CAPSTONEG3.

# 6. Conexión y Acceso

Para conectarse a la base de datos desde un cliente externo o la aplicación móvil, se deben usar los siguientes parámetros:

* **Host/Dirección IP:** 34.67.243.255
* **Puerto:** 5432
* **Usuario:** cvalencia
* **Base de Datos:** DB\_CAPSTONEG3
* **Contraseña:** La contraseña fuerte que se configuró para el usuario cvalencia.