CODELAB: APROVISIONAMIENTO DE INSTANCIAS DE COMPUTO

Desarrollo de Software

Estudiante:

Juan Sebastian Gomez – 2259474

Docente:

Alvaro Salazar

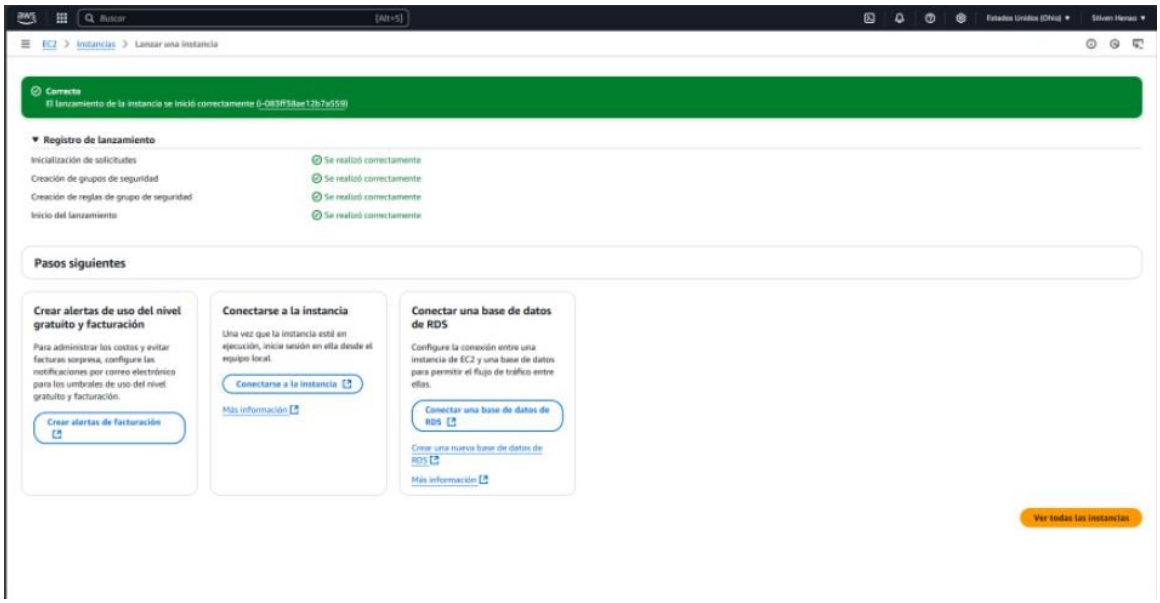
Tuluá, junio de 2025

Evidencias sobre el aprovisionamiento de infraestructura en Amazon EC2 para desarrollo

Lanzamiento de Instancia en Amazon EC2

La siguiente imagen corresponde al proceso exitoso de aprovisionamiento de una instancia en Amazon EC2, realizado a través de la consola de AWS. En ella se confirma que todos los pasos esenciales —incluyendo la inicialización de solicitudes, creación de grupos de seguridad y reglas, e inicio del lanzamiento— se completaron correctamente.

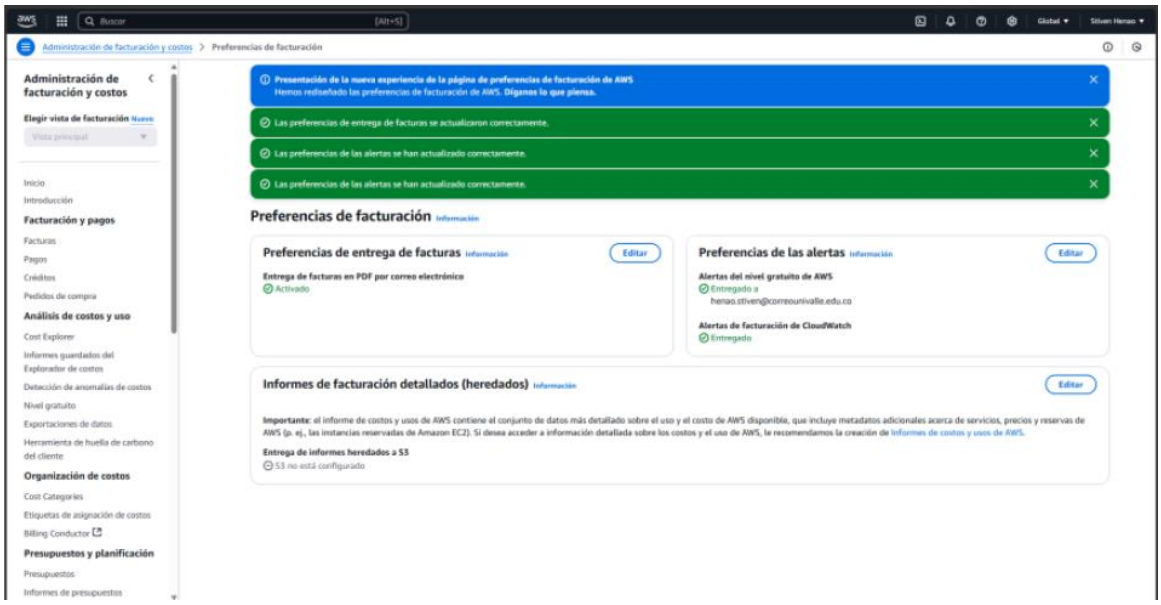
Este proceso constituye el primer paso para la creación de un entorno de desarrollo en la nube, permitiendo el despliegue de aplicaciones o servicios en una infraestructura escalable y controlada. Esta instancia puede ser posteriormente conectada mediante SSH y configurada para entornos de desarrollo backend, pruebas o despliegue continuo.



Configuración de Preferencias de Facturación y Alertas en AWS

La imagen muestra la sección de Administración de facturación y costos en la consola de AWS, donde se evidencian las preferencias de facturación y alertas correctamente actualizadas. Se activó la entrega de facturas en formato PDF al correo electrónico registrado y se configuraron las alertas de uso del nivel gratuito, así como las alertas de facturación mediante CloudWatch.

Esta configuración es clave para mantener el control financiero del entorno de desarrollo, permitiendo una gestión proactiva de los recursos y evitando sobrecostos inesperados. Es un paso fundamental dentro del aprovisionamiento responsable de infraestructura en la nube.

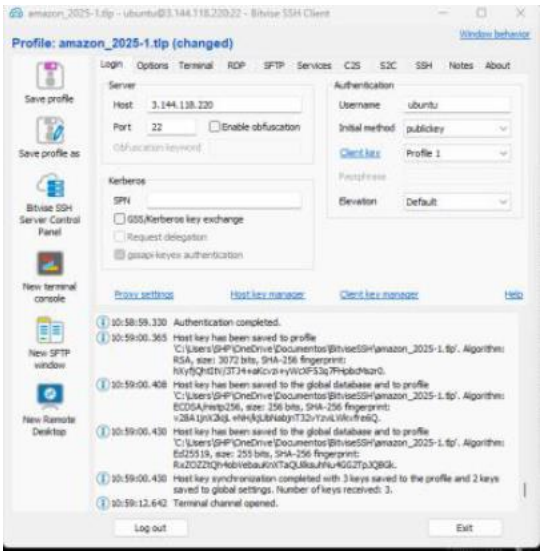


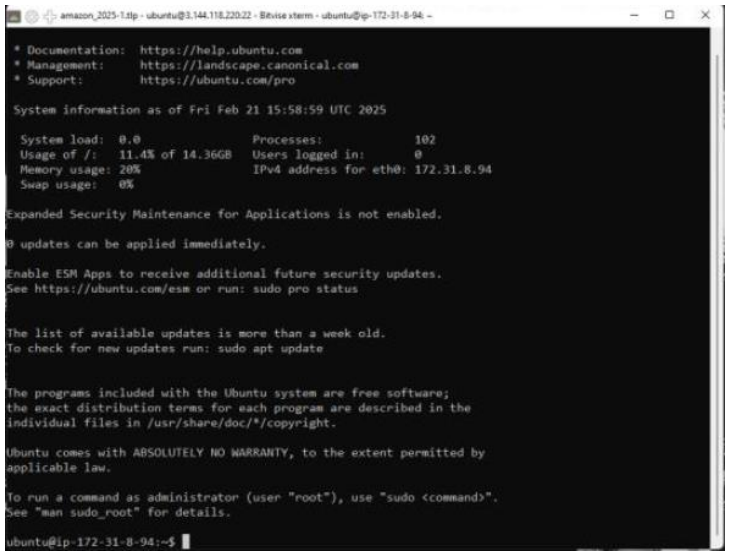
Configuración de acceso a la instancia mediante Bitvise SSH Client

Las imagenes muestran la conexión exitosa a una instancia EC2 de Amazon mediante el cliente **Bitvise SSH**, utilizando autenticación por clave pública. Se ha configurado el perfil de conexión especificando:

- **Dirección IP pública** de la instancia (ej. 3.144.118.220).
- **Puerto 22** para conexión SSH.
- **Nombre de usuario**: ubuntu.
- **Autenticación** mediante clave .ppk generada previamente desde la consola de AWS.

Tambien, se visualiza la terminal con la sesión activa en el sistema operativo **Ubuntu Server**, confirmando el acceso al entorno de desarrollo en la nube. Esta configuración permite la administración remota de la instancia para instalar software, desplegar aplicaciones o ejecutar tareas de mantenimiento.



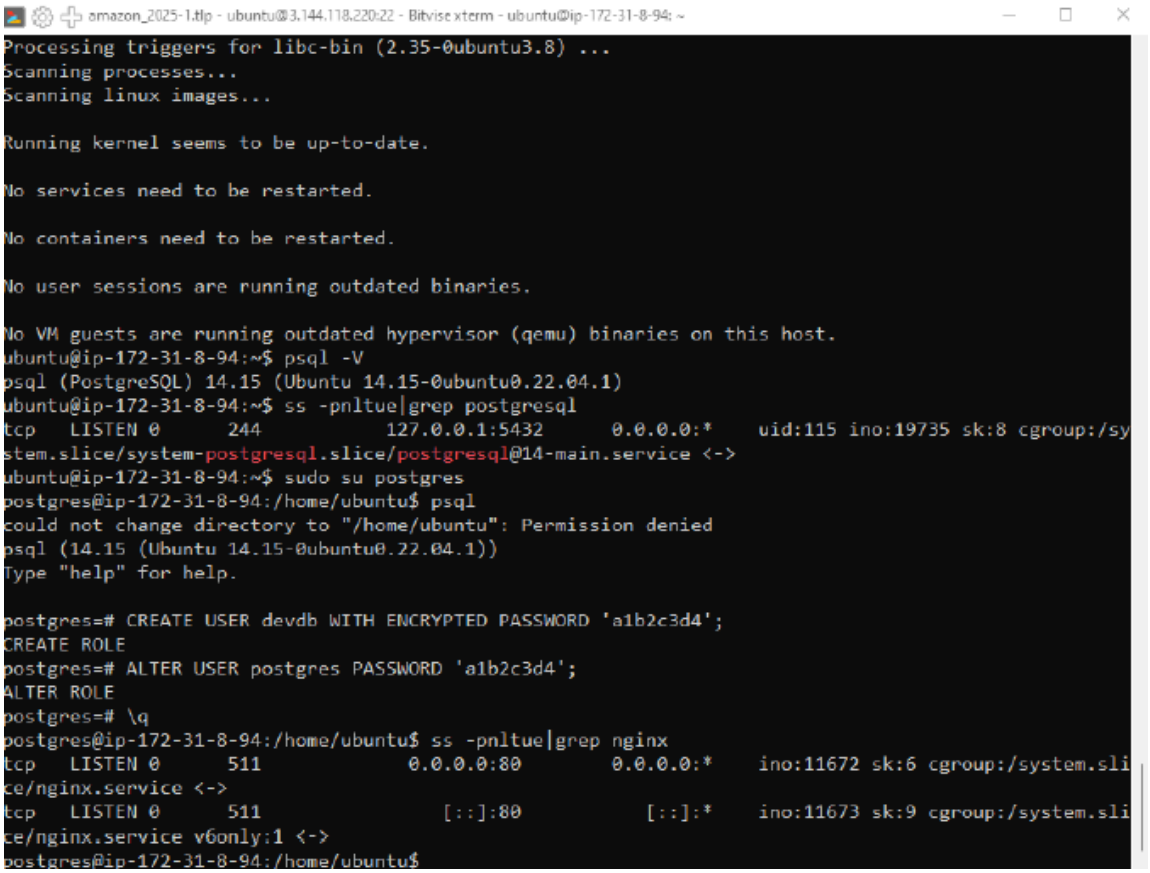


Configuración inicial y uso de PostgreSQL en consola (EC2 - Ubuntu)

La imagen evidencia el uso de **PostgreSQL** desde la terminal de una instancia EC2 con Ubuntu, accediendo mediante **Bitvise SSH**. En esta sesión se realizaron los siguientes pasos:

- Verificación de la versión instalada: PostgreSQL 14.15 sobre Ubuntu 22.04.
- Comprobación del servicio PostgreSQL en ejecución y escuchando en el puerto 5432.
- Acceso al cliente psql como el usuario postgres.
- Creación de un nuevo usuario devdb con contraseña cifrada.
- Modificación de la contraseña del usuario postgres utilizando comandos SQL estándar (ALTER USER).
- Además, se comprobó que el servicio **nginx** se encuentra activo, lo cual indica la coexistencia de múltiples servicios en la misma instancia.

Este avance demuestra que PostgreSQL está correctamente instalado, configurado y operativo, listo para utilizarse como base de datos en aplicaciones backend desplegadas en esta infraestructura.

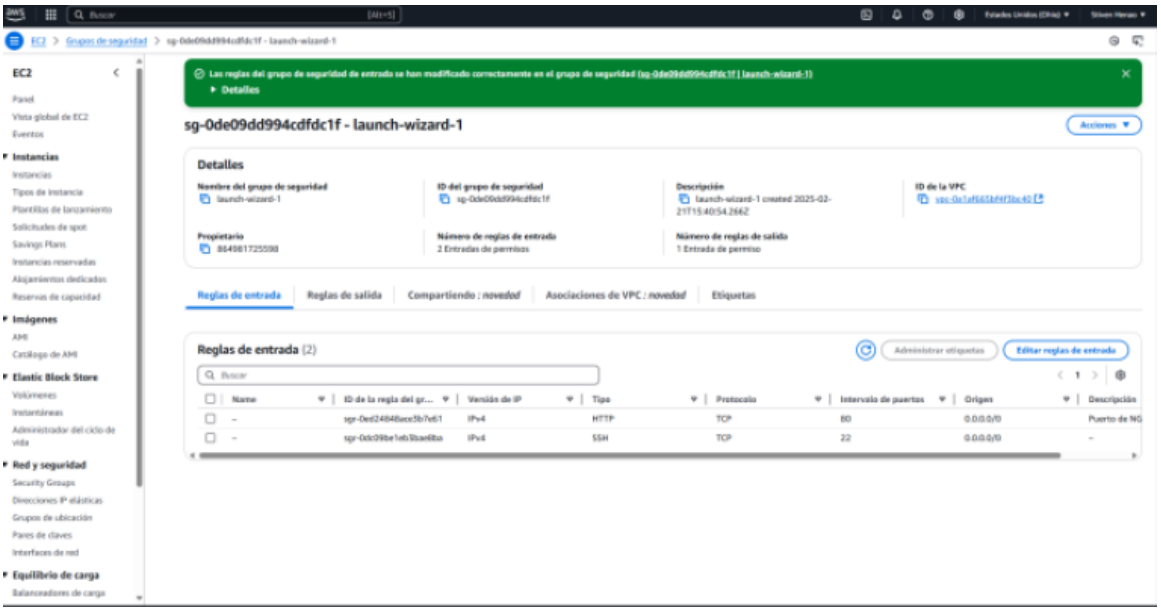


Creación de regla de seguridad para habilitar el puerto HTTP (NGINX)

La imagen muestra la configuración del **grupo de seguridad** asociado a la instancia EC2, en la cual se ha creado una **regla de entrada para el puerto 80 (HTTP)**. Esta configuración permite el acceso público al servicio NGINX desde cualquier dirección IP (0.0.0.0/0), facilitando la entrega del frontend desplegado en la instancia.

También se observa la regla previa del **puerto 22 (SSH)**, que garantiza el acceso remoto para administración mediante terminal.
La apertura del puerto 80 es esencial para exponer aplicaciones web a usuarios finales y habilitar la navegación desde navegadores web externos.

Esta regla garantiza que el frontend alojado en la instancia sea accesible públicamente a través del protocolo HTTP.



Creación de túnel C2S para acceso remoto a PostgreSQL

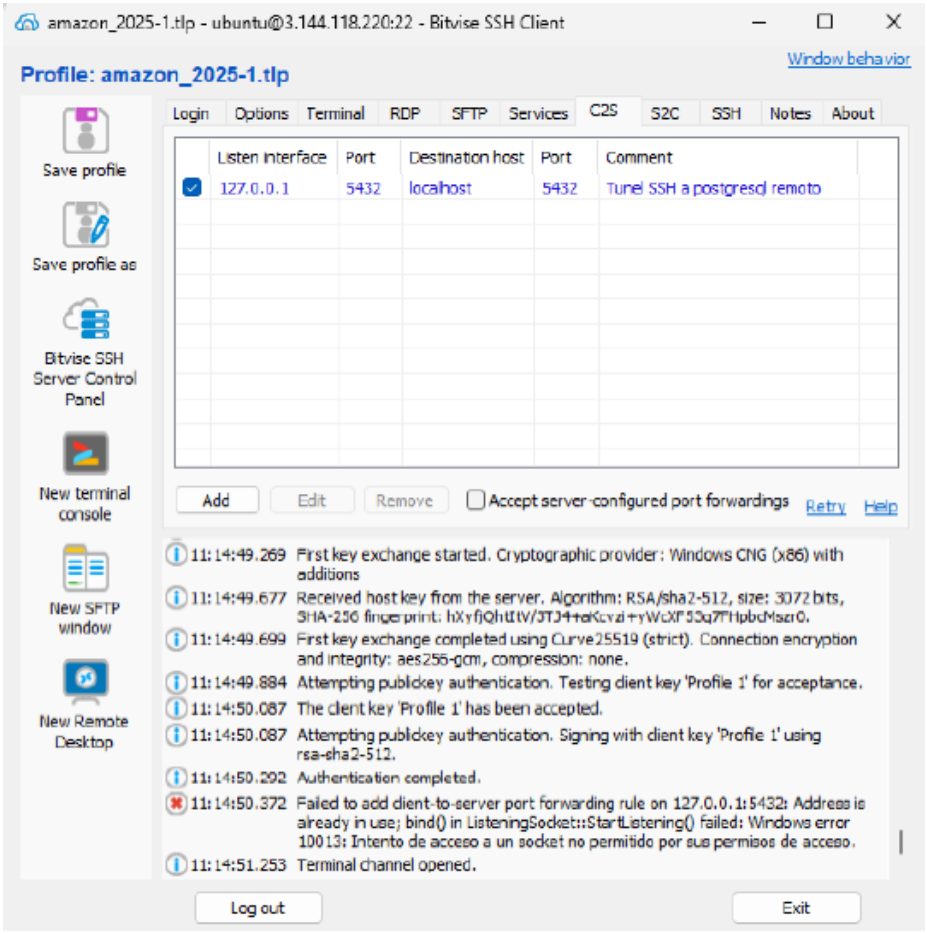
La imagen muestra la configuración de un **túnel SSH de tipo C2S (Client to Server)** en **Bitvise SSH Client**, con el objetivo de permitir el acceso remoto y seguro a la base de datos PostgreSQL alojada en una instancia EC2.

En esta configuración:

- **Listen interface:** 127.0.0.1 (localhost del equipo cliente).
- **Port:** 5432 (puerto local en el cliente).
- **Destination host:** localhost (dentro de la instancia remota).
- **Port:** 5432 (puerto donde PostgreSQL está escuchando).
- **Comentario:** "Túnel SSH a PostgreSQL remoto".

Este túnel permite a herramientas locales (como PgAdmin o DBeaver) conectarse de manera segura al servidor PostgreSQL remoto **como si estuviera alojado localmente**, sin exponer el puerto 5432 en el firewall público de AWS.

Además, en los logs de la conexión se observa que el túnel fue iniciado pero hubo un intento fallido de establecer el puerto por estar ocupado o restringido, lo cual requiere liberar el puerto o elegir otro diferente para finalizar la configuración con éxito.



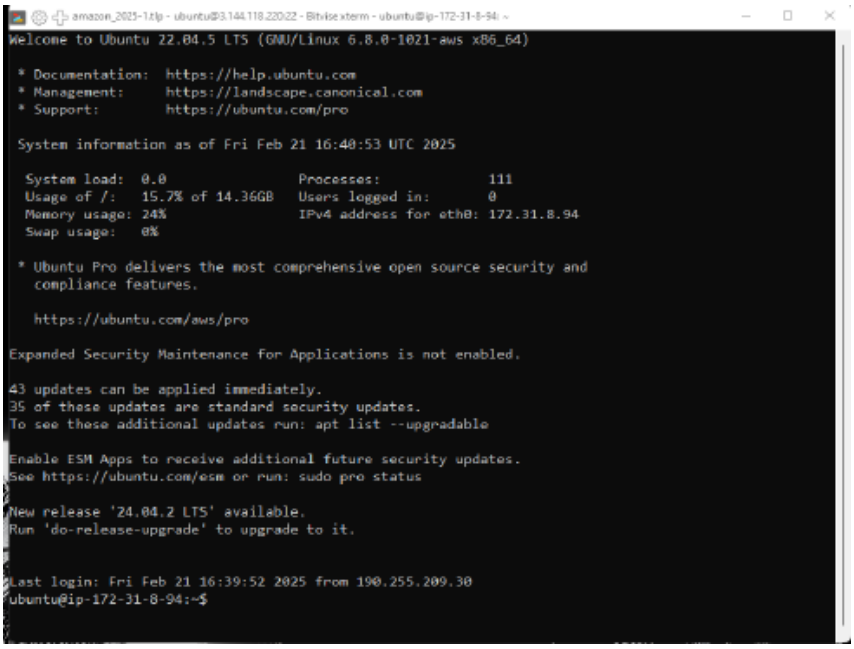
Acceso al servidor AWS 2025-1 utilizando clave privada con passphrase

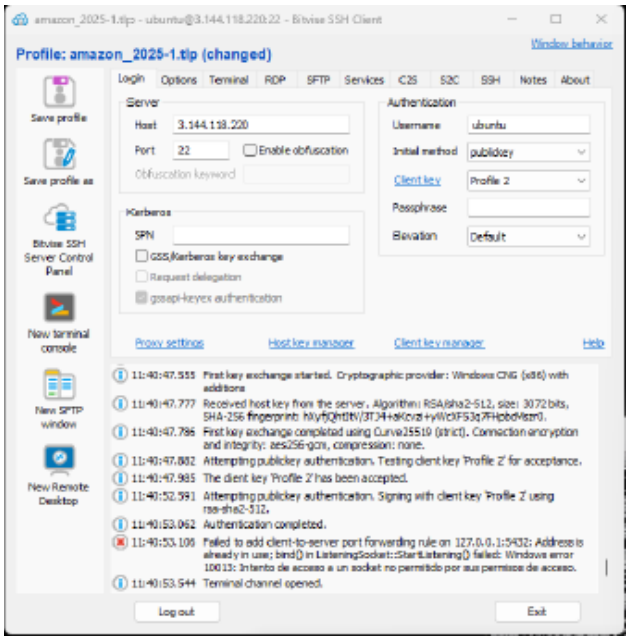
Las imagenes muestran la conexión exitosa al servidor remoto "AWS 2025-1" mediante **Bitvise SSH Client**, empleando una **clave privada protegida con passphrase** para autenticar al usuario ubuntu.

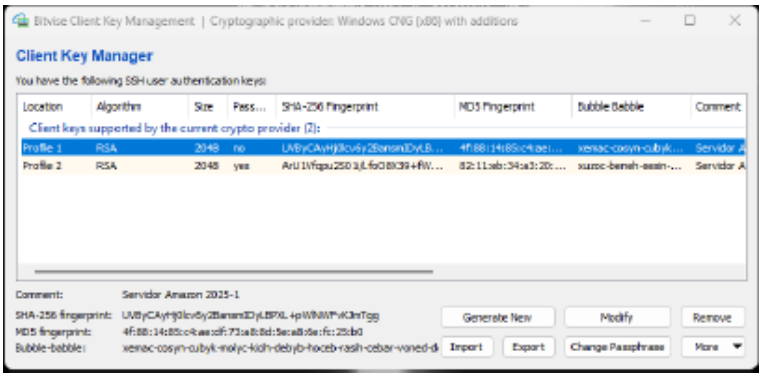
La evidencia incluye tres ventanas:

1. **Perfil de conexión en Bitvise**, donde se especifica la IP pública (3.144.118.220), el puerto 22, y el uso de la clave almacenada en el perfil seguro.
2. **Terminal activa**, confirmando el ingreso al sistema operativo **Ubuntu 22.04.5 LTS**, con detalles del sistema cargados y conexión establecida.
3. **Client Key Manager**, donde se visualiza la clave utilizada para el acceso (Profile 1), con algoritmo RSA, longitud de 2048 bits, y protección mediante passphrase, lo cual mejora la seguridad ante intentos de uso no autorizado.

Esta configuración garantiza un acceso robusto al servidor, cumpliendo buenas prácticas de seguridad en el manejo de claves SSH mediante cifrado con passphrase.







Conclusión General

El proceso documentado demuestra el aprovisionamiento exitoso y seguro de una instancia EC2 en Amazon Web Services, habilitada como entorno de desarrollo y despliegue de servicios backend y frontend. Se evidenció la creación y configuración correcta de:

- La **instancia EC2** y su grupo de seguridad, con apertura de puertos esenciales (SSH, HTTP).
- La conexión **segura mediante Bitvise SSH Client**, utilizando claves privadas con passphrase.
- La **configuración de túneles C2S** para acceder de forma local a servicios remotos como PostgreSQL.
- La **instalación y uso de PostgreSQL por consola**, creación de roles y validación de servicios.
- La **habilitación de NGINX** para servir el frontend a través del puerto 80.
- El monitoreo de uso y alertas mediante la **activación de preferencias de facturación** y control de recursos.

Cada paso siguió buenas prácticas de seguridad y administración en la nube, asegurando un entorno funcional, escalable y controlado. Este tipo de implementación es esencial para proyectos académicos y profesionales que requieren ambientes virtualizados con alta disponibilidad, acceso remoto y servicios distribuidos.