

MANUAL TECNICO

Introducción

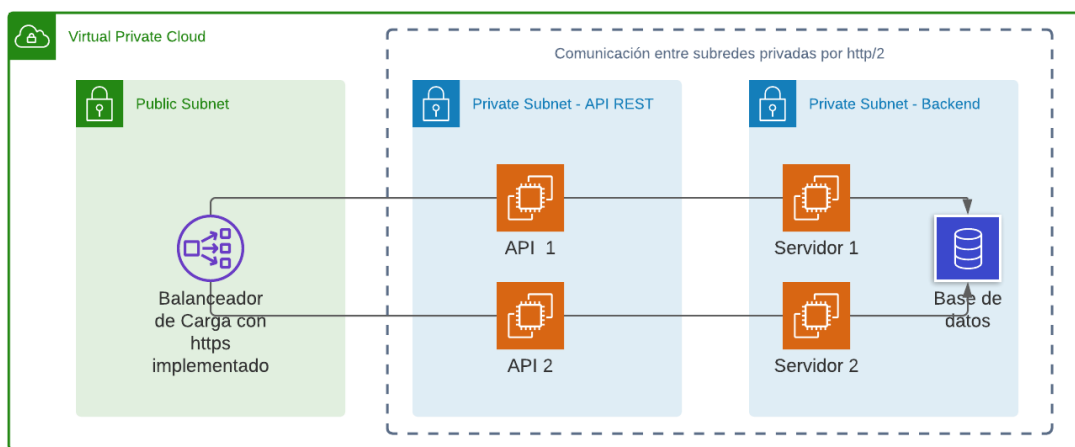
El siguiente documento es una guía sobre cómo está construida la herramienta y sus configuraciones, así como un diagrama de relación entre sus componente.

HTTPS: Hypertext Transfer Protocol Secure, este protocolo es de vital importancia debido a que permite una conexión segura entre servidor y cliente, el cual no puede ser interceptada por personas no autorizadas.

Nombre de dominio:

grupo17api.tk(principal)

grupo17api.ml(secundario)



El diagrama en la imagen anterior, muestra la construcción de la API. Como podemos observar se crea un módulo virtual en la nube, el cual tiene 2 subnets, una publica y una privada.

API, son las encargadas de comunicarse entre el servidor y la base de datos, el protocolo que se utiliza entre ambas es HTTP/2,

HTTP/2, es la nueva versión de HTTP, como podemos observar en la siguiente gráfica.



La razón de su uso en este proyecto es debido a que HTTP requiere de múltiples conexiones TCP, mientras que HTTP/2 se utiliza una única conexión para ofrecer múltiples solicitudes.

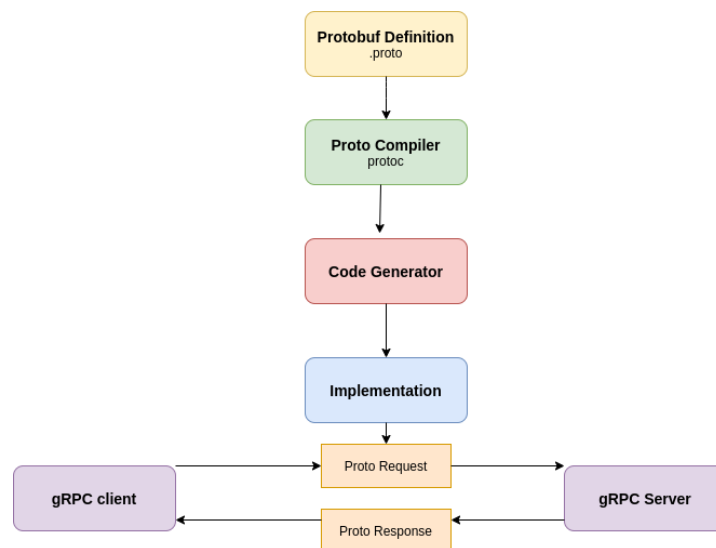
Características de HTTP/2

1. Una única conexión
2. Eliminación de redundancia
3. Multiplexación
4. Protocolo binario
5. Servicio server push
6. Compresión de cabeceras
7. Priorización de flujos

Se utilizará un gRPC en cliente y en servidor, gracias a sus características se utilizó

1. Transmisión bidireccional y autenticación conectable totalmente integrable con el tipo de protocolo HTTP/2.
2. Bajo consumo de CPU
3. Ofrece JSON encoding y serialización POTO3.

Componentes principales

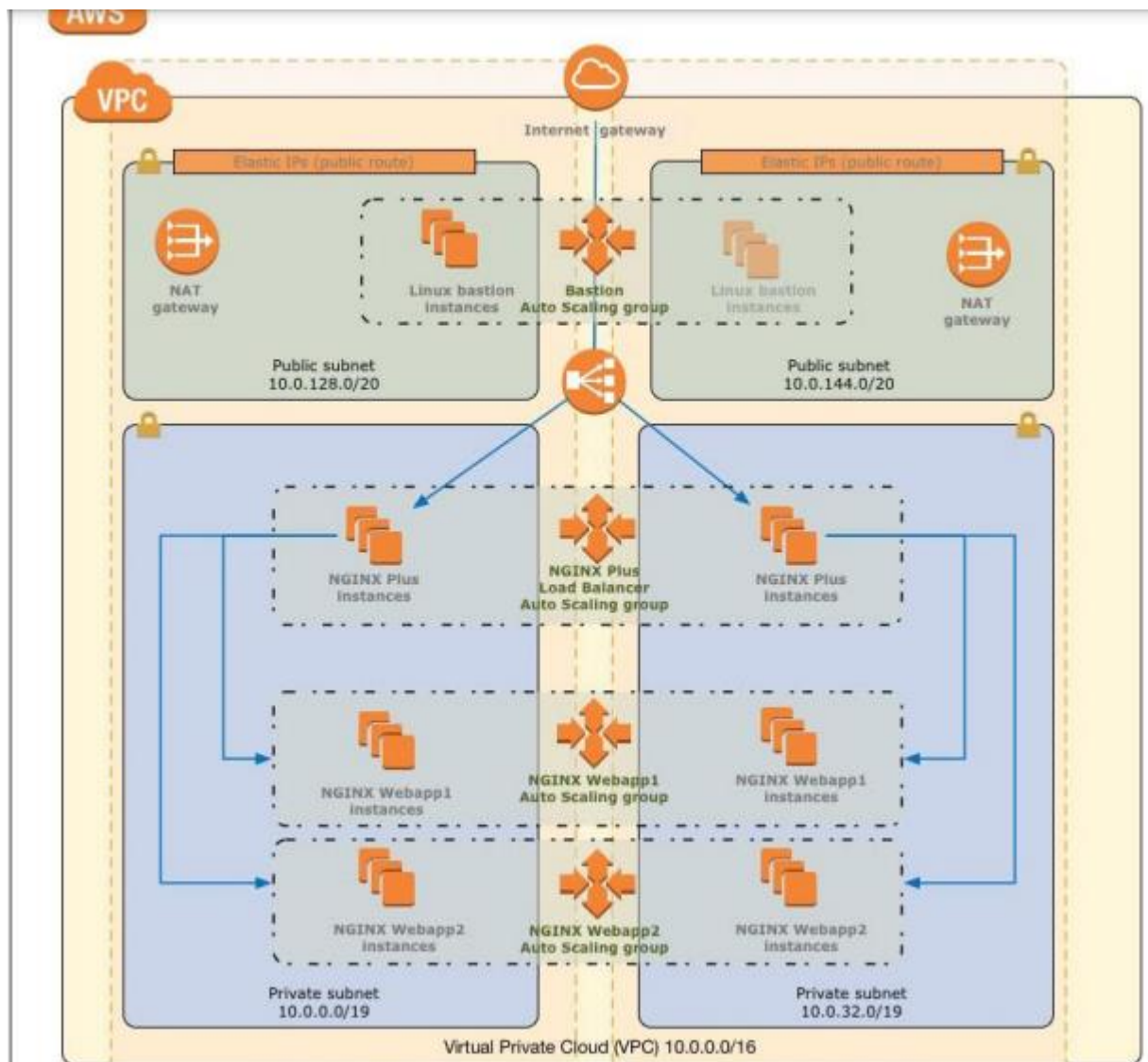


Balanceo de carga:

Para ello se utiliza NGINX en una instancia EC2

Paso 1

1. Primero debemos tener una cuenta de AWS, el cual se puede registrar en el siguiente enlace, <https://aws.amazon.com/>
2. Suscríbase a la [Imagen de máquina de Amazon \(AMI\) para NGINX Plus](#) en AWS Marketplace.
3. [Lance el Quick Start](#). La implementación toma alrededor de 25 minutos.
4. Para probar la implementación, equilibre la carga de las aplicaciones web y revise los archivos de configuración.



Paso 2:

1. Iniciar sesión en tu cuenta AWS <https://aws.amazon.com/marketplace/pp/B00UU272MM>
2. Abrir NGINX Plus – Amazon Linux AMI en la tienda de AWS y seleccionar continuar.
3. Revise los términos y condiciones y luego aceptar.
4. Luego de esto se enviará un correo de confirmación a tu buzón de correo indicado, el cual deberás confirmar.

La comunicación entre front(web) y la API se realiza por medio del protocolo HTTPS

Para implementar el protocolo https, primero se necesita de conseguir un certificado para el sitio web, esto desplegado por el host



Para obtener uno, siga estos pasos:

1. Establecer la variable de entorno de configuración de OpenSSL (opcional).
2. Generar un archivo de claves.
3. Crear una solicitud de firma de certificado (CSR).
4. Enviar la CSR a una autoridad emisora de certificados (CA) para obtener un certificado SSL.
5. Utilizar la clave y el certificado para configurar Tableau Server para poder utilizar SSL.

Gestor de base de datos

MongoDB

1. Inscribirse en AWS si no posee cuenta, de lo contrario iniciar sesión.
2. Lance la plantilla AWS CloudFormation en su cuenta AWS.

Opción 1	Opción 2
Implementar MongoDB en una VPC nueva en AWS	Implementar MongoDB en una VPC existente en AWS
<div>Launch Quick Start (for new VPC)</div> 	<div>Launch Quick Start (for existing VPC)</div> 

3. Conectarse a los nodos de MongoDB a través de la instancia NAT debido a que los nodos se encuentran en una subnet privada.

Connect To Your Instance

I would like to connect with ☒ A standalone SSH client
☐ A Java SSH Client directly from my browser (Java required)

To access your instance:

1. Open an SSH client. (find out how to [connect using PuTTY](#))
2. Locate your private key file (home.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:

```
chmod 400 home.pem
```
4. Connect to your instance using its Elastic IP:

```
54.149.135.237
```

Example:

```
ssh -i home.pem ec2-user@54.149.135.237
```

Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

Close

Nota:

inicie sesión en la instancia de bastión con el reenvío de agentes SSH habilitado.
Consulte los siguientes ejemplos:

Inicie sesión en el host de bastión con el reenvío de agentes SSH habilitado:

```
ssh -A ec2-user@Bastion-public-ip
```

Agregue una clave privada al agente SSH:

```
ssh-add -K mykey.pem
```

Crear un ACL web

Para crear una ACL web

1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS WAF en <https://console.aws.amazon.com/wafv2/>.
2. Elija **Web ACLs (ACL web)** en el panel de navegación y, a continuación, elija **Create web ACL (Crear ACL web)**.
3. En **Name (Nombre)**, escriba el nombre que desea utilizar para identificar esta ACL web.

nota

No se puede cambiar el nombre después de crear la ACL web.

4. (Opcional) En **Description - optional (Descripción: opcional)**, introduzca una descripción más larga para la ACL web si lo desea.

5. En **Nombre de la méCloudWatch** Cambie el nombre predeterminado de, si procede. Siga las instrucciones de la consola para ver los caracteres válidos. El nombre no puede contener caracteres especiales, espacios en blanco ni se pueden utilizar nombres de métricas reservados para AWS WAF, como «All» y «Default_Action».

nota

No se puede cambiar el nombre de las métricas de CloudWatch después de crear la ACL web.

6. En **Tipo de recurso**, elija la categoría de recurso de AWS que desea asociar a esta ACL web. Para obtener más información, consulte [Asociar o disociar una ACL web con un recurso de AWS](#).
7. En **Región** Si ha elegido un tipo de recurso regional, elija la región donde desea que AWS WAF almacene la ACL web.

Solo tiene que elegir esta opción para los tipos de recursos regionales. Para las distribuciones de CloudFront, la región está codificada para la región EE. UU. Este (Norte de Virginia), us-east-1, para aplicaciones globales (CloudFront).

8. (Opcional) Para **Recursos asociados de AWS: opcional**, elija **Adición de recursos de AWS**. En el cuadro de diálogo, elija los recursos que desea asociar y, a continuación, elija **Add**. AWS WAF le devuelve al **Describir ACL web y los recursos asociados de AWS** (Se ha creado el certificado).
9. Seleccione **Next (Siguiente)**.
10. (Opcional) Si desea agregar grupos de reglas administrados, en la página **Add rules and rule groups (Añadir reglas y grupos de reglas)**, seleccione **Add rules (Añadir reglas)** y, a continuación, haga clic en **Add managed rule groups (Añadir grupos de reglas administrados)**. Realice lo siguiente para cada grupo de reglas administrado que desee agregar:
 - a. En la página **Agregar grupos de reglas administrados por**, amplíe la lista de grupos de reglas administrados por AWS o para el vendedor de AWS Marketplace de su elección.
 - b. En el grupo de reglas que desea agregar, active la opción **Add to web ACL (Añadir a la ACL web)** en la columna **Action (Acción)**.

Si desea configurar las acciones de todas las reglas del grupo de reglas para que solo cuenten, elija **Edit (Editar)** y, a continuación, active el **Establecer todas las acciones de reglas para contar** y elija **Regla de guardado**. Para obtener más información acerca de esta opción, consulte [Invalidar las acciones de un grupo de reglas o de sus reglas](#).

11. Seleccione **Add rules (Añadir reglas)** para terminar de agregar reglas administradas y volver a la página **Add rules and rule groups (Añadir reglas y grupos de reglas)**.

12. (Opcional) Si desea agregar su propio grupo de reglas, en la página **Add rules and rule groups (Añadir reglas y grupos de reglas)**, elija **Add rules (Añadir reglas)** y, a continuación, seleccione **Add my own rules and rule groups (Añadir mis propias reglas y grupos de reglas)**. Realice lo siguiente para cada grupo de reglas que desee agregar:

- a. En la página **Add my own rules and rule groups (Añadir mis propias reglas y grupos de reglas)**, elija **Rule group (Grupo de reglas)**.
- b. Elija el grupo de reglas de la lista y, a continuación, elija **Agregar regla**.

13. (Opcional) Si desea agregar su propia regla, en la página **Add rules and rule groups (Añadir reglas y grupos de reglas)**, elija **Add rules (Añadir reglas)**, **Add my own rules and rule groups (Añadir mis propias reglas y grupos de reglas)**, **Rule builder (Generador, de reglas)** y, a continuación, **Rule visual editor (Editor visual de reglas)**.

- a. En **Name (Nombre)**, introduzca el nombre que desea utilizar para identificar esta regla.
- b. Introduzca la definición de la regla en función de sus necesidades. Puede combinar reglas dentro de **AND** y **OR** Instrucciones de reglas de. El asistente le guía a través de las opciones para cada regla según el contexto. Para obtener información sobre las opciones de reglas, consulte [Reglas de AWS WAF](#).
- c. En **Action (Acción)**, seleccione la acción que desea que realice la regla cuando coincida con una solicitud web. Para obtener más información acerca de sus opciones, consulte [Acción de la regla de AWS WAF](#) y [Evaluación de reglas de ACL web y grupos de reglas](#).

Si desea personalizar la solicitud o respuesta, elija las opciones para ello y rellene los detalles de su personalización. Para obtener más información, consulte [Personalización de solicitudes y respuestas web en AWS WAF](#).

Si desea que su regla agregue etiquetas a las solicitudes web coincidentes, elija las opciones para ello y rellene los detalles de su etiqueta. Para obtener más información, consulte [Etiquetas de AWS WAF en solicitudes web](#).








- d. Seleccione **Add rule**.

14. Elija la acción predeterminada para ACL web. Esta será la acción que AWS WAF ejecutará cuando una solicitud web no coincida con alguna de las reglas de la ACL web. Para obtener más información, consulte [Decidir sobre la acción predeterminada para una ACL web](#).

Si desea personalizar la acción predeterminada, elija las opciones para ello y rellene los detalles de su personalización. Para obtener más información, consulte [Personalización de solicitudes y respuestas web en AWS WAF](#).

15. Seleccione **Next (Siguiente)**.
16. En la **Establecer prioridad de regla**, seleccione y coloque las reglas y los grupos de reglas al orden que desee que AWS WAF los procese. Para obtener más información, consulte [Evaluación de reglas de ACL web y grupos de reglas](#).
17. Seleccione **Next (Siguiente)**.
18. En la **Configurar métricas**, actualice sus métricas y opciones de muestreo según sea necesario. Puede combinar métricas de varios orígenes proporcionando la misma **Nombre de la métrica** para ellos.
19. Seleccione **Next (Siguiente)**.
20. Revise las definiciones en la página **Review and create web ACL (Revisar y crear ACL web)**. Si desea cambiar cualquier área, elija el área y seleccione **Edit (Editar)**. Esto le devuelve a la página en el asistente de ACL web. Realice los cambios y, a continuación, haga clic en **Next (Siguiente)** para pasar las páginas hasta volver a la página **Review and create web ACL (Revisar y crear ACL Web)**.
21. Elija **Create web ACL (Crear ACL web)**. La nueva ACL web aparece en la página **Web ACLs**.

El proyecto esta creado en las siguientes fases

 gomzalo last changes		
..		
	API	last changes
	API_1	last changes
	Backend	last changes
	Backend_1	last changes
	db	last changes
	docker-compose.yml	last changes

✓

main [REDES2_1S2021_GRUPO17](#) / [Proyecto1](#) / [Server](#) / [API](#) /

gomzalo last changes		
..		
datapb		grpc y mongo
Dockerfile		grpc y mongo
data.proto		backend proto actualizado
docker-compose.yml		last changes
go.mod		grpc y mongo
go.sum		grpc y mongo
main.go		grpc y mongo

main [REDES2_1S2021_GRUPO17](#) / [Proyecto1](#) / [Server](#) / [API_1](#) /

gomzalo last changes		
..		
datapb		last changes
Dockerfile		last changes
data.proto		last changes
docker-compose.yml		last changes
go.mod		last changes
go.sum		last changes
main.go		last changes

main ▾

[REDES2_1S2021_GRUPO17](#) / [Proyecto1](#) / [Server](#) / **Backend** /



gomzalo last changes

..



datapb

grpc y mongo



Dockerfile

grpc y mongo



data.proto

protos



docker-compose.yml

last changes



go.mod

grpc y mongo




go.sum

grpc y mongo



main.go

grpc y mongo

 main ▾

[REDES2_1S2021_GRUPO17](#) / [Proyecto1](#) / [Server](#) / **Backend_1** /



gomzalo last changes

..



datapb

last changes



Dockerfile

last changes



data.proto

last changes



docker-compose.yml

last changes



go.mod

last changes




go.sum

last changes



main.go

last changes

 main ▾

[REDES2_1S2021_GRUPO17](#) / [Proyecto1](#) / [Server](#) / **db** /



gomzalo last changes

..



db

last changes



docker-compose.yml

last changes