Aplicación Distribuida Segura En Todos Sus Frentes

Daniel Felipe Walteros Trujillo

12 de Marzo del 2021

Profesor:
Luis Daniel Benavides Navarro

Arquitecturas Empresariales

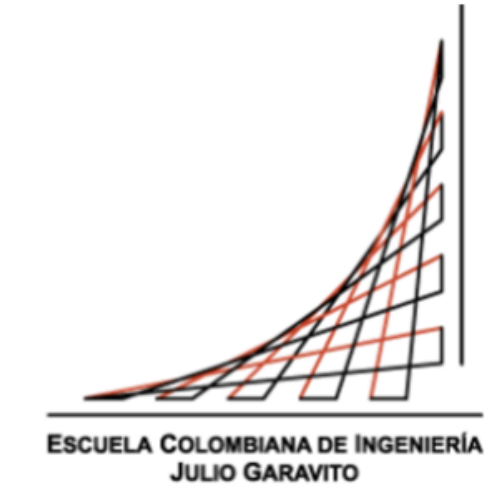


Tabla de Contenido

1 Prerrequisitos

Para el desarrollo del programa se utilizó Maven como una herramienta para la gestión del ciclo de vida del software, el código fue desarrollado con el lenguaje de programación Java, por lo tanto para su ejecución se requiere:

- Java versión 8 o superior.
- Maven versión 3.5 o superior.

2 Introducción

HTTPS (protocolo de Transferencia de Hiper-Texto) es un protocolo que permite establecer una conexión segura entre el servidor y el cliente, que no puede ser interceptada por personas no autorizadas, para esto encripta los datos para asegurar una transmisión de datos segura y además autnetica el servidor por medio de un certificado anstes de realizar la conexión[8].

Bajo los conceptos de esta asignatura, la seguridad se puede garantiza por medio de tres principios[6]:

- Autenticidad: Es la capacidad de un mensaje para mantener oculto su contenido de tal forma que si una tercera persona ve el mensaje no pueda interpretar su contenido.
- Integridad: Se refiere a que los elementos mensajes, datos, documentos, y otros formas de contenido no han sido modificados en tránsito o en reposo.
- Autorización: Se refiere a garantizar que el mensaje ha sido enviado por quien dice ser.

Keytool es una utilidad de administración de claves y certificados para generar y administrar claves y certificados SSL. Las claves y los certificados se almacenan en un archivo de almacén de claves. Puede utilizar un certificado autofirmado o firmado por una autoridad de certificación (CA). Para utilizar un certificado firmado por una CA, utilice keytool para generar una solicitud de firma de certificado (CSR) y solicitar un certificado de identidad digital de una CA [4].

La utilidad Keytool se incluye con Java. Puede encontrar la utilidad Keytool en el directorio /bin del directorio de JDK o JRE.

El algoritmo SHA-256 permte cifrar información de forma irreversible y única, su seguridad (y la de toda su familia de funciones SHA-2) se basa en la construcción de una serie de funciones criptográficas bien conocidas. Estas son las funciones hash de Merkle–Damgård creada por Ralph Merkle e Ivan Damgård en 1979, usando para ello una compresión one-way del tipo Davies–Meyer. Un método por el cual buscaban garantizar la resistencia a colisiones o repeticiones de hashes. Además de garantizar la mayor seguridad posible para la función[5].

Amazon Web Services (AWS) es la plataforma en la nube más adoptada y completa en el mundo, que ofrece más de 200 servicios integrales de centros de datos a nivel global. Millones de clientes, incluso las empresas emergentes que crecen más rápido, las compañías más grandes y los organismos gubernamentales líderes, están usando AWS para reducir los costos, aumentar su agilidad e innovar de forma más rápida [3].

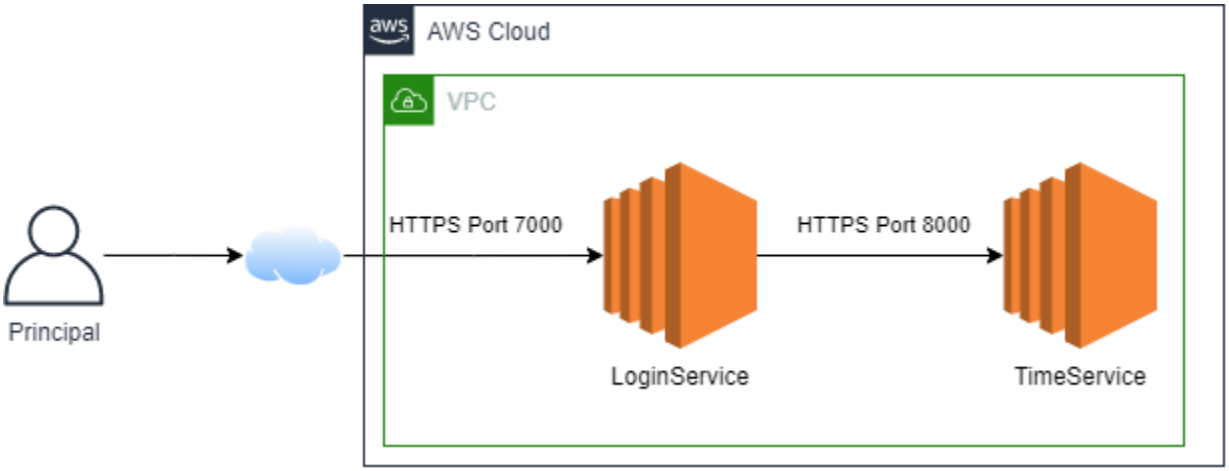
Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona capacidad informática en la nube segura y de tamaño modificable. Está diseñado para simplificar el uso de la informática en la nube a escala web para los desarrolladores. La sencilla interfaz de servicios web de Amazon EC2 permite obtener y configurar capacidad con una fricción mínima. Proporciona un control completo sobre los recursos informáticos y puede ejecutarse en el entorno informático acreditado de Amazon [2].

El desarrollo de este trabajo fue una aplicación Web segura con los siguientes requerimientos:

- Permite un acceso seguro desde el browser a la aplicación garantizando autenticación, autorización e integridad de usuarios.
- Tiene dos computadores comunicandose entre ellos y el acceso de servicios remotos también garantiza autenticación, autorización e integridad. Nadie puede invocar los servicios si no está autorizado..
- Es fácil escalarla para incorporar nuevos servicios.

3 Diseño

3.1 Diagrama de Despliegue



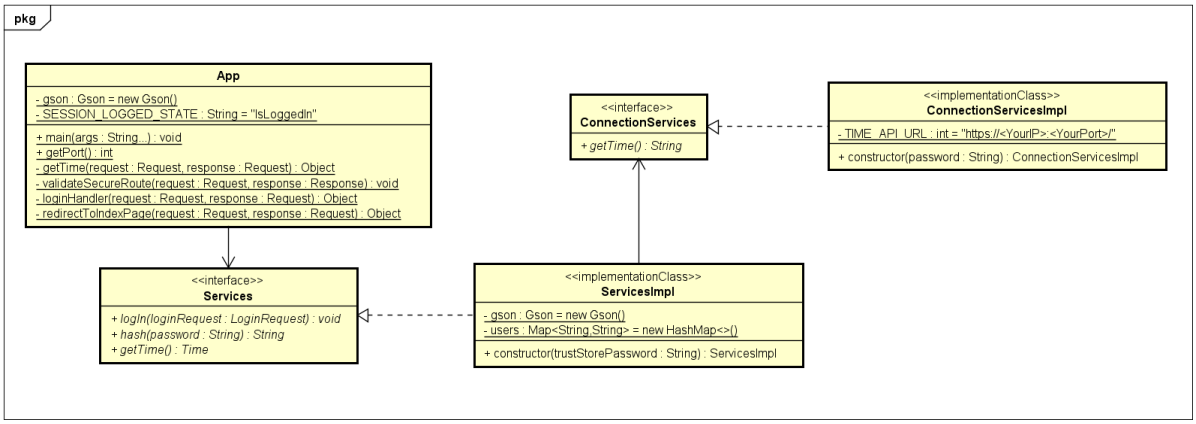
El usuario Principal se conecta por medio del internet y del protocolo HTTPS al servicio de Login que se esta ejecutando en una instancia de Amazon EC2 por el puerto 7000 (puerto por defecto); una vez accede a ella debe proveer credenciales para garantizar su autenticidad.

De ser efectivo el proceso de autenticación, el servicio de Login se conectará por medio de HTTPS al servicio de tiempo para informarle al Principal el tiempo actual del servidor.

Al realizar todas las conexiones por medio de HTTPS y de certificados encriptados, se garantiza la integridad y autorización del sistema.

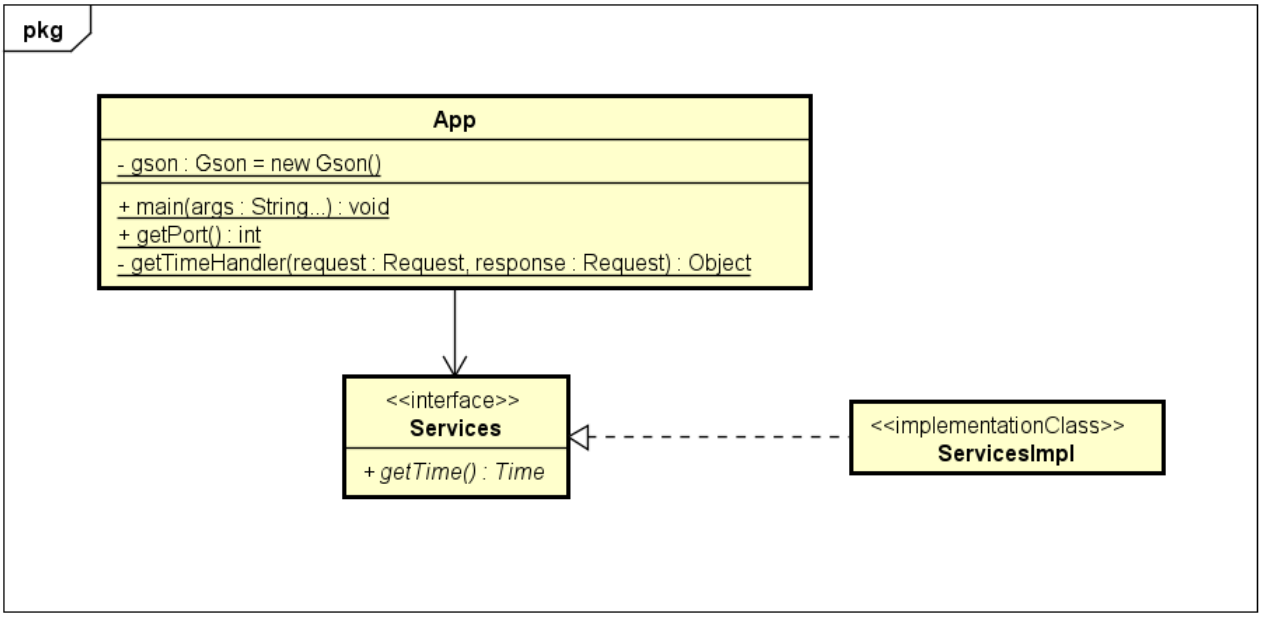
Debido a que la aplicación no esta dockerizada, requiere que en las instancias de EC2[2] se instale Maven[9] y Java[1]; en el caso de java es posible que ya este instalado pero en la versión erronea, para esto se usa el comando alternatives[7].

3.2 Diagrama de Clases Login Service



El programa Login Service posee un certificado para la conexión por HTTPS, utiliza la interfaz Services para realizar el login con un usuario cuya contraseña esta cifrada por medio una función hash, la implementación de esta interfaz utiliza el cifrado SHA256; además esta clase consulta el tiempo actual del servidor por medio de la interfaz ConnectionService, la implementación de esta interfaz se conecta por medio de una URI y de una TrustStore al servicio de tiempo.

3.3 Diagrama de Clases Time Service



El programa Time Service posee un certificado para la conexión por HTTPS y además utiliza la interfaz Services para consultar el tiempo actual en el servidor, la implementación de esta clase maneja las posibles excepciones y consulta el tiempo directamente.

4 Conclusiones

- El sistema garantiza los tres principios de seguridad en cada conexión.
- El uso de interfaces para generalizar comportamientos dentro de la aplicación permite la extensión o cambio de código sin la necesidad de alterar múltiples archivos.
- El despliegue de una aplicación web por medio de EC2 permite el uso comercial de la misma en todos los sitios que tengan conexión a Internet sin incurrir en altos costos por administración y soporte de servidores, esto se debe a que esta plataforma utiliza tecnologías en la nube.
- La incorporación de nuevos servicios desplegados en nuevos servidores requiere la creación de pares de llaves y de certificados para su integración, garantizando que la incorporación de nuevos sistemas mantiene su seguridad.

5 Referencias

[1] Amazon. *Amazon Corretto 8 Installation Instructions for Amazon Linux 2*. URL: https://docs.aws.amazon.com/es_es/corretto/latest/corretto-8-ug/amazon-linux-install.html. (entered: 12-03-2021).

[2] Amazon. *Amazon EC2*. URL: https://aws.amazon.com/es/ec2/?ec2-whats-new.sort-by=item.additionalFields.postDateTime&ec2-whats-new.sort-order=desc. (entered: 26-02-2021).

[3] Amazon. *Informática en la nube con AWS*. URL: https://aws.amazon.com/es/what-is-aws/. (entered: 26-02-2021).

[4] Informatica. *Utilidad Keytool*. URL: https://docs.informatica.com/es_es/data-security-group/test-data-management/10-2-1/_guia-de-instalacion_test-data-management_10-2-1_ditamap/antes_de_instalar_tdm/antes_de_instalar_tdm_en_unix/configurar_un_archivo_de_almacen_de_claves/utilidad_keytool.html#:~:text=Keytool%20es%20una%20utilidad%20de,archivo%20de%20almac%C3%A9n%20de%20claves.. (entered: 09-06-2018).

[5] José Maldonado. *¿Qué es SHA-256? El algoritmo criptográfico usado por Bitcoin*. URL: https://es.cointelegraph.com/explained/what-is-sha-256-the-cryptographic-algorithm-used-by-bitcoin. (entered: 28-04-2020).

[6] oblancarte. *Seguridad – Confidencialidad, Integridad y Autenticidad en mensajes*. URL: https://www.oscarblancarteblog.com/2015/02/22/confidencialidad-integridad-y-autenticidad-en-mensajes/. (entered: 22-02-2015).

[7] Rahul. *How to Install Java 11/8 on Amazon Linux*. URL: https://tecadmin.net/install-java-on-amazon-linux/. (entered: 31-10-2020).

[8] Ryte. *HTTPS*. URL: https://es.ryte.com/wiki/HTTPS. (entered: 12-03-2021).

[9] Sebsto. *Install Maven with Yum on Amazon Linux*. URL: https://gist.github.com/sebsto/19b99f1fa1f32cae5d00. (entered: 12-03-2021).