Servicios profesionales para:

LEFEBVRE EL DERECHO

PROPUESTA DESARROLLO DE API EXTERNA CON AUTENTICACIÓN JWT PARA JITSI MEET

Propuesta Tecnológica

CONTENIDO

1 CONTROL DE VERSIONES 3

2 SERVICIO 4

2.1 INTRODUCCIÓN 4
2.2 OBJETIVOS 4
2.3 ALCANCE 4
2.4 CRITERIOS DE ACEPTACIÓN 4
2.5 RECURSOS HUMANOS 5

3 TECNOLOGÍA A TRABAJAR 5

4 ARQUITECTURA DE LA SOLUCIÓN 6

1 CONTROL DE VERSIONES

FECHA	VERSIÓN	OBSERVACIONES	AUTOR
23-08-2020	Versión inicial v01	Definición de alcance	Kelvin Castillo

2 SERVICIO

2.1 Introducción

El propósito de este documento es detallar el plan de trabajo de Dominion para desarrollar un API Externa con autenticación JWT para la aplicación de Jitsi Meet.

Por nuestra amplia experiencia, estamos convencidos que podemos aportar en un solo equipo, expertos en las tecnologías de este aplicativo; a continuación, describiremos en los siguientes apartados de este documento el alcance de esta propuesta.

2.2 Objetivos

- Implementar la configuración requerida en el proveedor de autenticación Prosody que verifica la conexión del cliente según el token JWT
- Desarrollar un API rest que implementara un controlador para generar el token JWT como se describe en el RFC, con la finalidad de que una vez se conecte con un token válido, el sistema jitsi-meet lo considere autenticado.
- Configurar el ID de la aplicación que identifica al cliente y un secreto compartido tanto por el servidor prosody como por el generador de tokens JWT.

2.3 Alcance

El propósito de este proyecto es aportar personal técnico profesional que desarrolle el API Externa con autenticación JWT para poder generar llamadas en la herramienta de Jitsi Meet de manera segura.

El Desarrollo del API conlleva:

- Configuración de variables de entorno en el servidor prosody.
- Desarrollo de API rest.
- Implementar un controlador para generar tokens de acceso.
- Configuraciones en servidor prosody para definir id y secreto compartido como generador de tokens JWT.

2.4 Criterios de aceptación

- Debe de darse visto bueno del alcance para iniciar el desarrollo.
- La aplicación de Jitsi Meet debe estar funcionando de manera estable y permitir realizar configuraciones en el servidor prosody para modificar el tipo de autenticacion de internal a JWT
- Definición de objetivos del API rest (crear salas, autenticar usuarios, ver estadisticas de llamadas realizadas, etc.)
- Contar con acceso al ambiente donde se encuentra desplegada la aplicación de Jitsi Meet para realizar las configuraciones y validaciones correspondientes.

2.5 Recursos Humanos

Para el desarrollo del API rest e implementacion de autenticación JWT se utilizará 1 recurso con los siguientes detalles:

Recurso	Horas	Precio / Hora	Total
Recurso 1	18		

Desglose de horas:

Funcionalidad	Horas invertidas
Configuración entorno servidor prosody	3
Desarrollo API rest	5
Desarrollo controlador de autenticación	4
Pruebas y validaciones	3
Documentación API	3
Total horas invertidas	18

Funcionalidad	Horas invertidas
Configuración local external api de jitsi (crear llamadas, autenticar usuarios, modificar parametros en cada llamada)	2
Configuración local api estadisticas jitsi (configuracion de imagen prosody, jvb y web de jitsi)	2
Creacion de Apis de prueba de manera local (api de pruebas creada con javascript y tokens generados con el debugger de jwt)	2
Pruebas y validaciones	2
Configuración local imagen jibri jitsi (permite grabar y transmitir llamadas)	**3**
Analisis y propuesta con el tema de seguridad en jitsi	**1**
Elaboración de informe	2
Total horas invertidas	14

3 Tecnología a Trabajar

A continuación, listamos a modo de resumen de las tecnologías detectadas de aplicación y para esta solución:

- ✓ Spring Boot

4 Arquitectura de la solución