Fecha:
Octubre 2024

Documentación de URL Shortener para Promociones

Propuesta de software

Realizado por:
Augusto Occhiuzzi

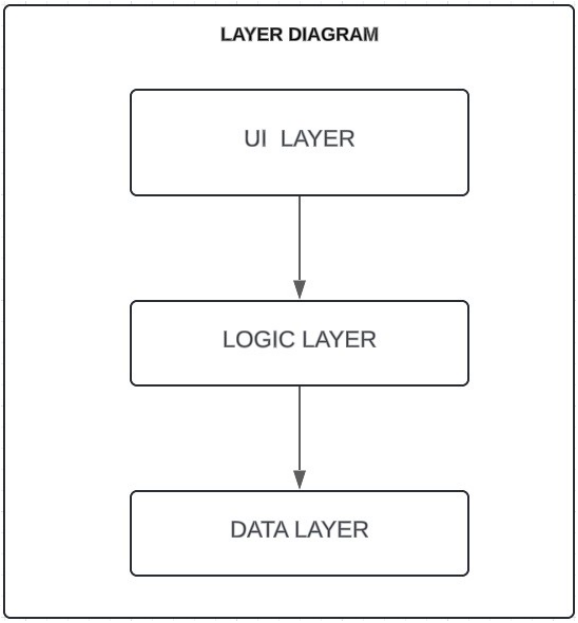
Introducción

El presente documento describe la arquitectura propuesta para un sistema de URL Shortener que permitirá generar enlaces cortos para ser utilizados en campañas de promoción en redes sociales como Twitter. La solución debe ser capaz de gestionar tráfico de hasta 1 millón de requests por minuto (RPM), operar con una disponibilidad del 99.98%, y ofrecer estadísticas de acceso casi en tiempo real. Además, las URLs generadas deben poder ser habilitadas o deshabilitadas y permitir la modificación de los componentes de su URL de destino.

El objetivo es garantizar la alta disponibilidad, escalabilidad, y eficiencia de costos, cumpliendo con los requerimientos funcionales y no funcionales exigidos para el proyecto.

Primeras aproximaciones:

El modelo esta basado en una arquitectura de capas, en la que tendremos un cliente como UI, el cual hara las peticiones a la capa logica y nuestra capa logica sera luego la encargada de ejecutar la persistencia en la capa de datos.



Arquitectura Propuesta

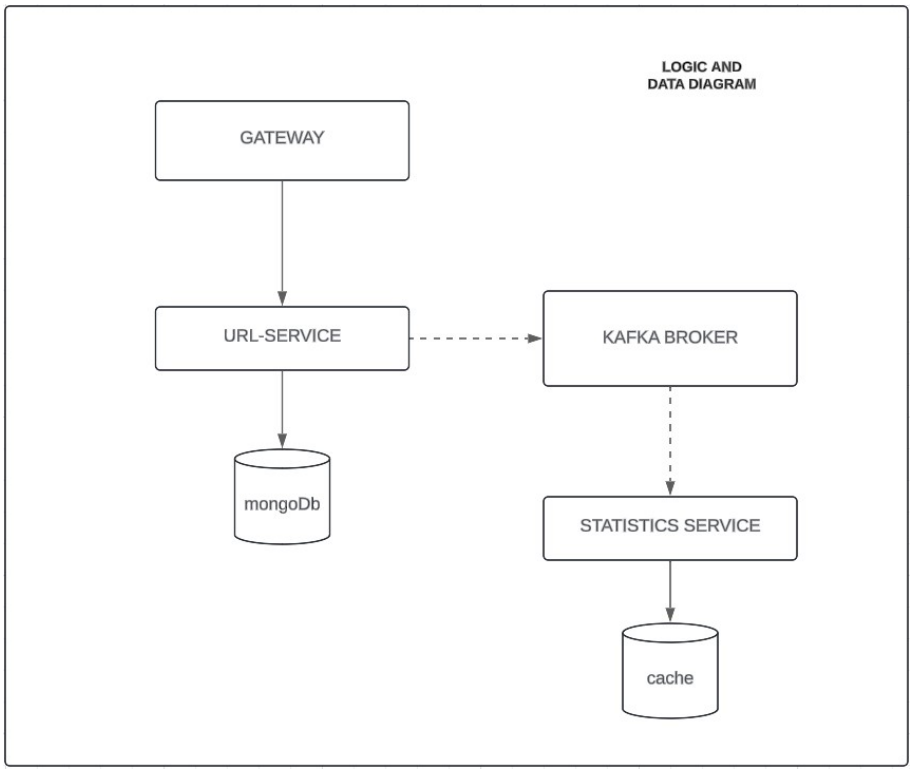
La solución está compuesta por una arquitectura de microservicios distribuida, con los siguientes componentes principales:

- **API Gateway**: Controla la autenticación y la autorización de los usuarios, permitiendo el acceso a los microservicios. Tambien se podria validar roles para ciertos recursos.

- **Microservicio UrlManager**: Responsable de la generación, modificación, habilitación/deshabilitación y resolución de las URLs cortas.

- **Microservicio StatisticsService**: Se encarga de recolectar, procesar y almacenar las métricas de acceso a las URLs.

Los microservicios se comunican a través de un bus de eventos asíncrono mediante **Kafka**, y se utilizan bases de datos **MongoDB** y **Redis** para la persistencia y caching, respectivamente.



Selección de Tecnologías y Justificación

Java 17 con Spring WebFlux

Elección: Para el desarrollo de la lógica de negocio de los microservicios se ha utilizado **Java 17** junto con **Spring WebFlux**, una librería reactiva de Spring que permite crear aplicaciones no bloqueantes.

Justificación:

Reactivo y no bloqueante: WebFlux está basado en un modelo reactivo, lo cual es crucial para manejar de forma eficiente grandes cantidades de tráfico concurrente. Con picos de hasta 1M RPM, se requiere una arquitectura no bloqueante para evitar cuellos de botella y garantizar tiempos de respuesta rápidos.

Soporte y madurez: Java es un lenguaje maduro y Spring WebFlux es ampliamente utilizado en aplicaciones de alto rendimiento. Ambas tecnologías cuentan con una comunidad sólida y soporte extendido.

Escalabilidad: WebFlux permite manejar de forma eficiente aplicaciones distribuidas que necesitan escalar horizontalmente, alineándose con el requisito de soportar grandes volúmenes de tráfico.

Microservicios UrlManager y StatisticsService

Elección: La lógica de negocio se ha dividido en dos microservicios:

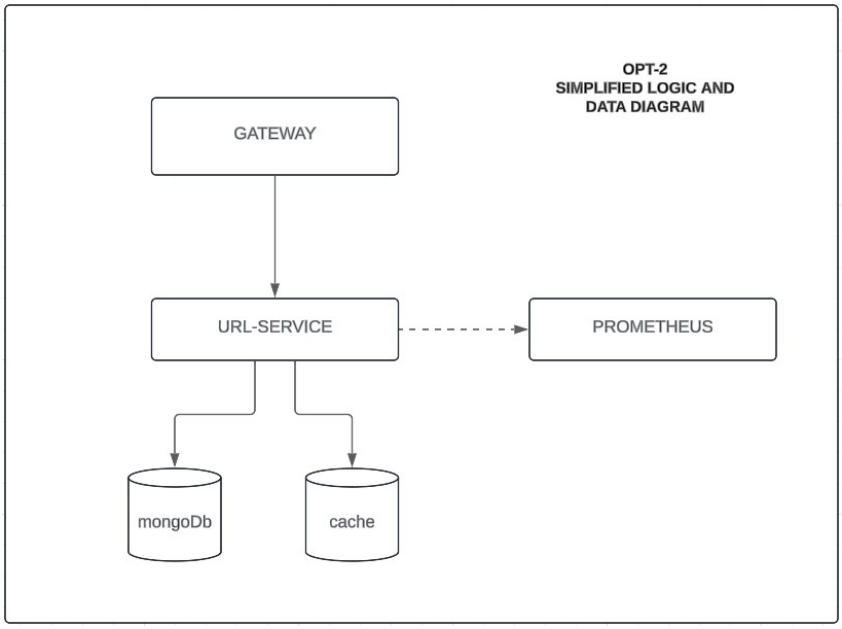
- **UrlManager**: Gestión de URLs cortas (crear, modificar, habilitar, deshabilitar).
- **StatisticsService**: Procesamiento y almacenamiento de estadísticas de acceso.

Justificación:

Desacoplamiento de responsabilidades: Separar las funciones en diferentes microservicios permite un mejor manejo de la escalabilidad y facilita el mantenimiento. Al tener servicios independientes, es posible escalar solo el microservicio que maneje la funcionalidad más demandada (por ejemplo, el UrlManager), evitando sobrecargar el sistema completo.

Disponibilidad y mantenibilidad: Esta división de responsabilidades también favorece la alta disponibilidad. Si uno de los microservicios experimenta problemas, el otro puede continuar funcionando, manteniendo la operatividad del sistema.

Alternativa evaluada (servicio unico): Una opción hubiera sido implementar toda la lógica en un solo servicio, pero esta opción generaría un acoplamiento excesivo, lo que dificultaría la escalabilidad y el mantenimiento del sistema, así como el manejo eficiente del tráfico elevado.



<u>MongoDB para almacenamiento de URLs</u>

Elección: Se ha elegido **MongoDB**, una base de datos NoSQL distribuida, para almacenar la información relacionada con las URLs generadas.

Justificación:

Escalabilidad horizontal: MongoDB es una base de datos diseñada para escalar horizontalmente, lo que significa que puede soportar grandes cantidades de tráfico distribuyendo la carga entre múltiples nodos.

Flexibilidad del esquema: Dado que las URLs pueden contener información variada, MongoDB permite la flexibilidad de almacenamiento con un esquema dinámico, lo que facilita el manejo de datos heterogéneos como las URLs cortas y sus componentes asociados.

Alternativa evaluada (SQL): Las bases de datos relacionales como MySQL o PostgreSQL también hubieran sido una opción. Sin embargo, estas bases de datos podrían haber presentado limitaciones en cuanto a la escalabilidad horizontal y flexibilidad, especialmente en un entorno con picos de

tráfico de 1M RPM. MongoDB, al ser NoSQL, soporta de manera más eficiente este tipo de carga distribuida.

Kafka para la comunicación asíncrona entre microservicios

Elección: Para la transmisión de eventos entre los microservicios, se ha seleccionado **Apache Kafka**.

Justificación:

Alta concurrencia y throughput: Kafka está diseñado para manejar grandes volúmenes de datos y alto throughput, lo que lo hace ideal para entornos con alta concurrencia de peticiones, como es el caso del acceso a estadísticas en tiempo real.

Desacoplamiento asíncrono: La comunicación asíncrona entre los microservicios mejora la eficiencia y reduce la latencia, ya que los servicios pueden procesar los eventos de manera independiente sin bloquear la ejecución de otros procesos.

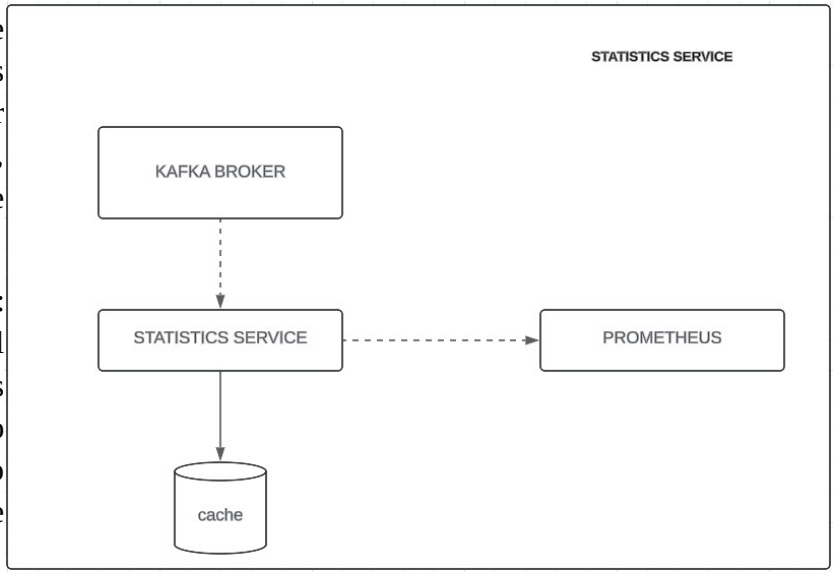
Alternativa evaluada (REST síncrono): La comunicación directa y síncrona entre los servicios hubiera generado un acoplamiento mayor, aumentando la latencia y reduciendo la escalabilidad. Kafka permite un desacoplamiento efectivo, garantizando que los servicios se puedan escalar de forma independiente.

Redis para caching de estadísticas

Elección: Se ha optado por **Redis** como capa de caching para almacenar temporalmente las estadísticas de acceso antes de su persistencia y publicación.

Justificación:

Bajo tiempo de respuesta: Redis es conocido por ser extremadamente rápido gracias a que almacena datos en memoria, lo que permite acceder a las estadísticas casi en tiempo real, cumpliendo con el requerimiento de latencia mínima.



Eficiencia en la lectura de datos: Redis mejora significativamente el tiempo de acceso a datos frecuentemente consultados, como las estadísticas de URLs, reduciendo la carga sobre el microservicio de estadísticas y MongoDB.

Alternativa evaluada (almacenamiento directo en MongoDB): Almacenar las estadísticas directamente en MongoDB hubiera incrementado los tiempos de lectura/escritura, generando una latencia mayor. Redis actúa como una capa intermedia eficiente, disminuyendo la latencia y mejorando la performance general del sistema.

Prometheus para monitorización de métricas

Elección: Para la recopilación y visualización de métricas en tiempo real, se ha utilizado **Prometheus**.

Justificación:

Monitoreo eficiente: Prometheus es una de las soluciones más populares para monitorear aplicaciones distribuidas y microservicios. Es capaz de manejar grandes volúmenes de datos y ofrece flexibilidad para recopilar y visualizar estadísticas en tiempo real.

Integración sencilla con Redis y Kafka: Prometheus se integra fácilmente con Redis y Kafka para capturar métricas, lo que facilita la instrumentación del sistema sin añadir complejidad adicional.

Escalabilidad y Orquestación con Kubernetes

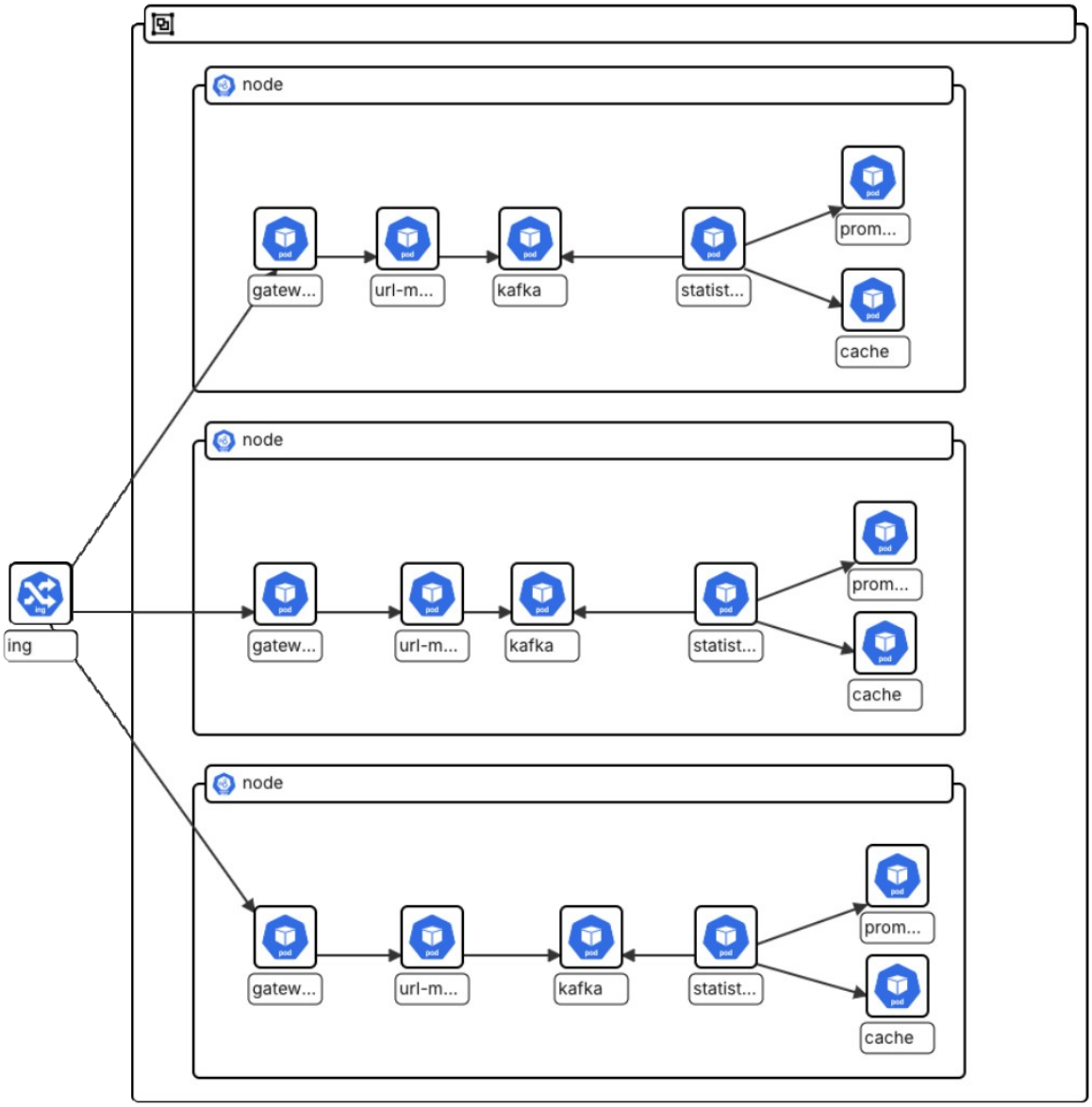
Para garantizar que la arquitectura de microservicios sea **escalable de forma eficiente** y pueda manejar el tráfico masivo con elasticidad, la propuesta incluye el uso de **Kubernetes** como plataforma de orquestación de contenedores. Kubernetes proporciona una manera flexible y eficiente de escalar automáticamente los microservicios según la demanda, manteniendo la estabilidad y la disponibilidad del sistema.

Se implementará un **LoadBalancer** que distribuya el tráfico entrante hacia el **API Gateway**. Este componente será responsable de gestionar el acceso a los microservicios y balancear la carga de manera eficiente. El uso de un LoadBalancer asegura que el tráfico se distribuya de manera equitativa entre las réplicas del **API Gateway**, garantizando una respuesta rápida y un manejo óptimo del tráfico, especialmente durante picos de tráfico.

Cada microservicio, tanto el **UrlManager** como el **StatisticsService**, se desplegará en pods independientes. Estos pods tendrán réplicas configuradas para escalar automáticamente según la carga del sistema. Separar los microservicios en pods independientes asegura que un fallo en un microservicio no afecte al resto del sistema.

En un principio, seria ideal tener un Kafka cluster externo, al igual que el cache, pero como eso podria incrementar los costos y ademas es dificil teniendo en cuenta para la aplicación de esta demo, se opta por hacer el deploy dentro de un pod de K8s. Los servicios de Kafka estarán desplegados entonces en pods dentro de Kubernetes, con réplicas que aseguren la disponibilidad y el manejo eficiente de la comunicación asíncrona. En cuanto a redis, se utilizaria la herramienta de Helm que nos provee un HA (High Availability) Redis Sentinel. Ver: https://www.baeldung.com/ops/redis-sentinel-kubernetes-high-availability

La base de datos **MongoDB** se desplegará externamente a Kubernetes. En el caso de Prometheus, podria estar securitizado mediante una **VPN** en un entorno externo para garantizar que solo los componentes autorizados puedan acceder a sus métricas. Al igual que antes, Mantener Prometheus fuera del clúster de Kubernetes y securitizado mediante una VPN tiene beneficios clave como mayor seguridad y carga reducida en el cluster, pero como complijiza la solucion para esta demo, se pondra el prometheus ejecutandose internamente en Kubernetes,



Conclusión

La arquitectura diseñada está alineada con los requisitos de **alta disponibilidad**, **escalabilidad**, y **bajo costo**. Las decisiones tecnológicas fueron tomadas tras una cuidadosa evaluación de las alternativas disponibles, priorizando la capacidad de manejar picos de tráfico y la eficiencia en la resolución de URLs y la recolección de estadísticas. La implementación basada en **Java 17 con WebFlux**, **microservicios desacoplados**, **MongoDB**, **Kafka**, **Redis**, y **Prometheus** asegura un rendimiento óptimo, flexibilidad para adaptarse a nuevos requisitos, y un fácil mantenimiento del sistema.

DOCUMENTACION API-REST
Microservicio UrlManager

Pasos previos:

Previa a cualquier interaccion con el Api, **debemos tener un token de acceso.** Si bien esta hecho a fines demostrativos como podra verse en el codigo, el gateway nos provee un token. Este token luego se utilizara en las subsiguientes solicitudes para poder acceder al API. **Este enfoque es erroneo, ya que el gateway no deberia proveer un token, sino que deberiamos utilizar proveedores externos o un flujo de autenticacion aparte.** Sin embargo, para fines demostrativos, embebi la generacion dentro del gateway. Cabe destacar que la generacion de token es un “dummy class” ya que da token de acceso a cualquiera que se lo pida.

Generar Token:

Tipo	Req. Header	Endpoint
POST	----	/authenticate

Rquest-body:

```
{
   “username”: “random-email.com”
}
```

Response:

```
{
 "token":"eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJhdWd1c3RvLm9jY2hAZ21haWwuY29tIiwiaWF0IjoxNzI3Nzg4Njg0LCJleHAiOjE3Mjc4MjQ2ODR9.ou6HnYmh43nak1CkSyHZxgl7ZZ5hTEnSaYgjq9uaHjc"
}
```

Con ese token, ya podemos ponerlo en los **requests subsiguientes. Sin ese token, respondera con status 401 (Unauthorized)**

1 - CREAR URL

Descripcion: Hace un create, guardandolo en la base de datos. Se debe enviar un body en el que se pone el nuevo url a colocar. Si ya existe no se crea y responde error.

Tipo	Req. Header	Endpoint
POST	Authentication Bearer + token	`/url/management`

Rquest-body:

```
{
   “url”: “https://random-url.com”
}
```

Response:


```
{
   "id": "66fbf936c66d17598c24209a",
   "shortUrl": "meli.ly/1727789365991",
   "originalUrl": "https://random-url.com",
   "enabled": true,
   "createdAt": "2024-10-01T10:29:25.991893618",
   "updatedAt": "2024-10-01T10:29:25.991909107"
}
```


Si el URL ya existe, respondera con codigo de error HTTP Status: Conflict

2 - UPDATE URL

Descripcion: Hace un update de lo guardado en la base de datos. Se le debe enviar como param “id” el short-url. Ademas en el body, se pone el nuevo url a colocar. Se actualiza el updatedAt luego de la modificacion.

Tipo	Req. Header	Endpoint
PUT	Authentication Bearer + token	/url/management?id=meli.ly/1727541701011

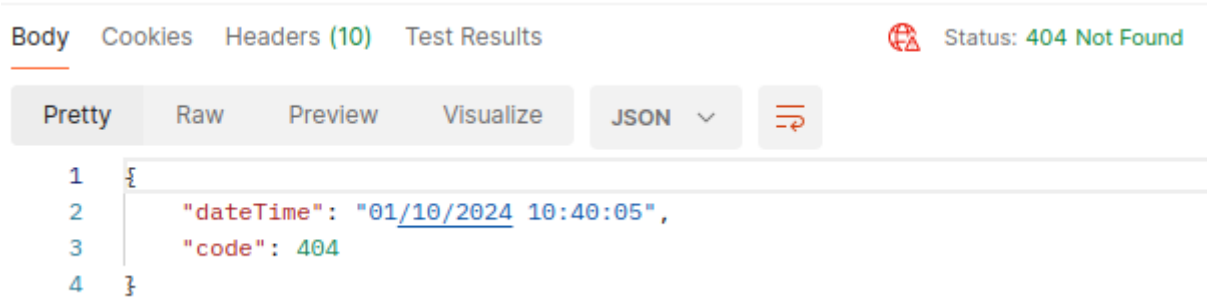
Rquest-body:

```
{
   “url”: “https://new-random-url.com”
}
```

Response:


```
{
   "id": "66fbf936c66d17598c24209a",
   "shortUrl": "meli.ly/1727541701011",
   "originalUrl": "https://new-random-url.com",
   "enabled": true,
   "createdAt": "2024-09-30T10:29:25.991893618",
   "updatedAt": "2024-10-01T10:29:25.991909107"
}
```


Si el URL no existe, respondera con codigo de error HTTP Status: Not Found



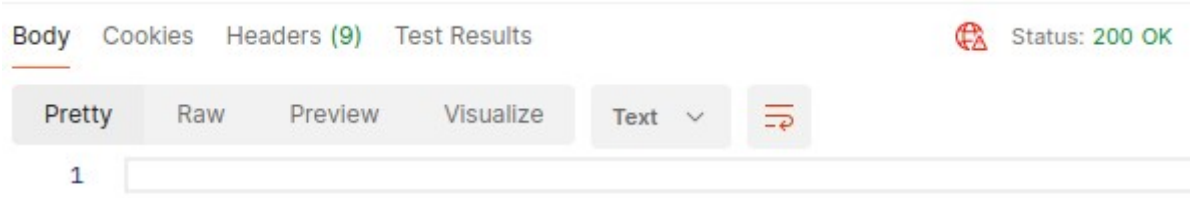
3 - ENABLE URL

Descripcion: Habilita el URL. Si se quiere redireccionar luego de habilitarla, se permitira acceder al recurso. Se manda como param “id” el short-url.

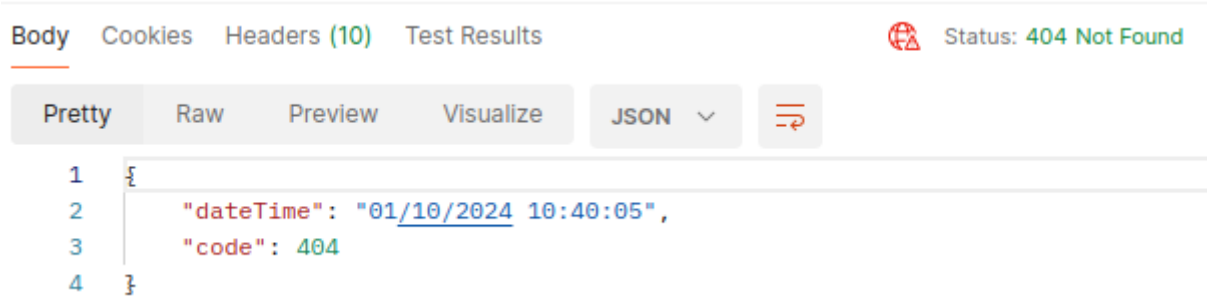
Tipo	Req. Header	Endpoint
PATCH	Authentication Bearer + token	`/url/management/enable?id=meli.ly/1727541701011`

Response:

Si el URL existe, respondera con codigo de error HTTP Status: OK



Si el URL no existe, respondera con codigo de error HTTP Status: Not Found



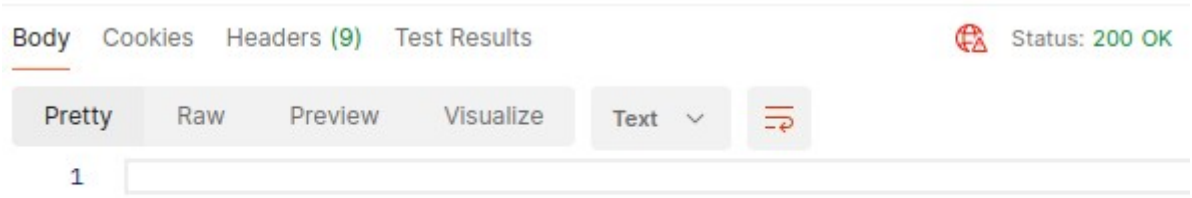
4 - DISABLE URL

Descripcion: Deshabilita el URL. Si se quiere redireccionar luego de deshabilitarla, no se dejara acceder al recurso. Se manda como param “id” el short-url.

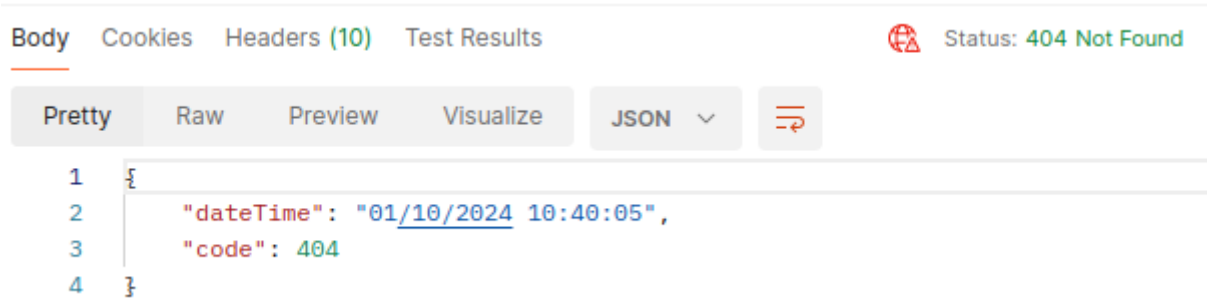
Tipo	Req. Header	Endpoint
PATCH	Authentication Bearer + token	`/url/management/disable?id=meli.ly/1727541701011`

Response:

Si el URL existe, respondera con codigo de error HTTP Status: OK



Si el URL no existe, respondera con codigo de error HTTP Status: Not Found



5 - REDIRECT URL

Descripcion: busca el el URL. **Si existe el recurso y esta habilitado,** nos devuelve el url original, redireccionandonos alli. Si no existe o esta deshabilitado, respondera error. Se manda como param “id” el short-url.

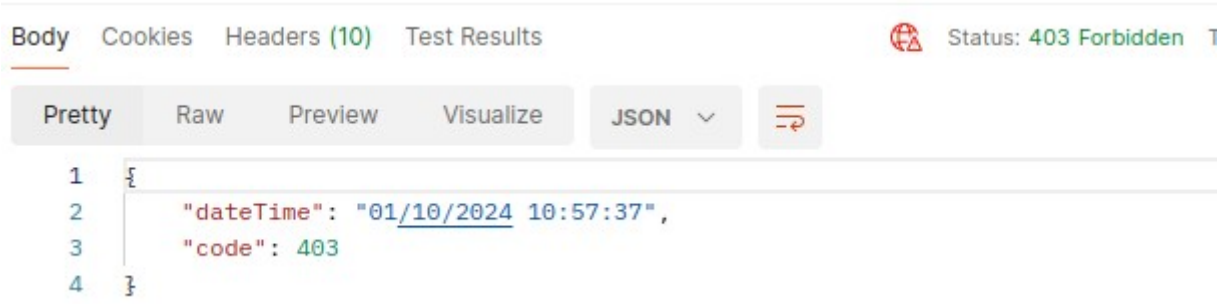
Tipo	Req. Header	Endpoint
GET	Authentication Bearer + token	`/api/short/url?id=meli.ly/1727541701011`

Response:

Si el URL **existe y esta habilitada,** respondera con codigo de error HTTP Status OK y el URL original.

```
{
   "originalUrl": "https://new-random-url.com"
}
```

Si el URL **existe pero esta deshabilitada,** respondera con codigo de error HTTP Status: Forbidden



Si no existe, por el contrario nos retornara un codigo de error HTTP Status: Not Found