



UNIVERSITÀ DI PARMA

AUTENTICAZIONE TRAMITE TOKEN IN
UN'ARCHITETTURA A MICROSERVIZI:
REALIZZAZIONE DI UN PLUGIN CUSTOM
PER L'API GATEWAY KONG

Relatore:
Prof. Roberto Alfieri

Anno Accademico
2022 – 2023

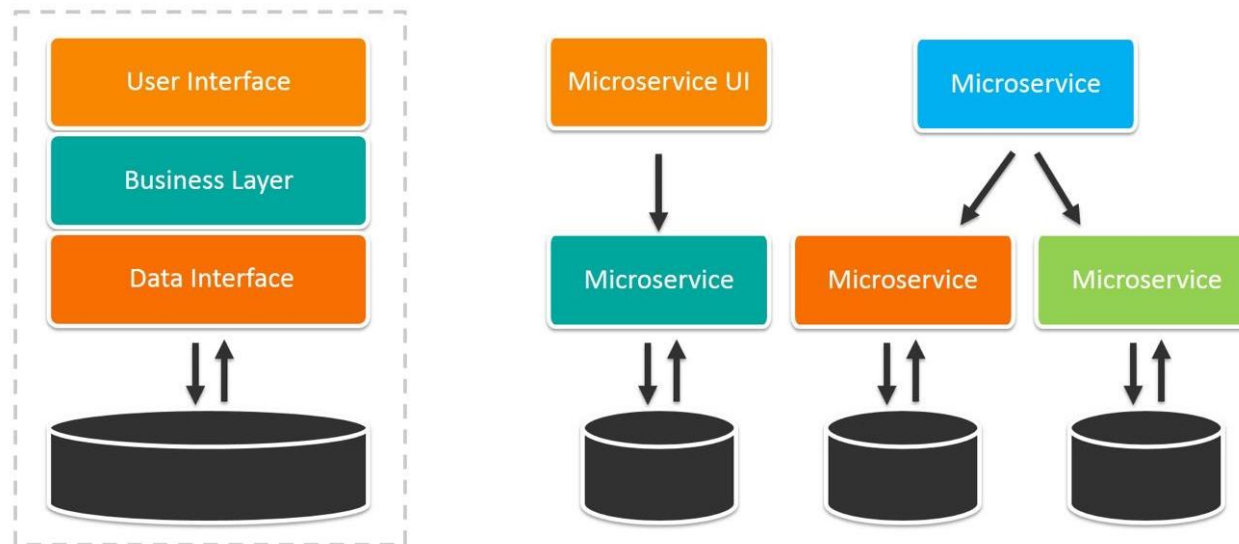
Candidato:
Valerio Desiati

MICROSERVIZI

Cosa sono i microservizi

Nelle architetture a microservizi l'obiettivo è quello di **scomporre l'applicazione** da realizzare nelle sue funzioni (**servizi**) di base.

Ogni servizio può essere compilato e distribuito in modo **indipendente**; quindi i singoli servizi possono funzionare o non funzionare senza compromettere gli altri.



Confronto tra architettura monolitica e a microservizi

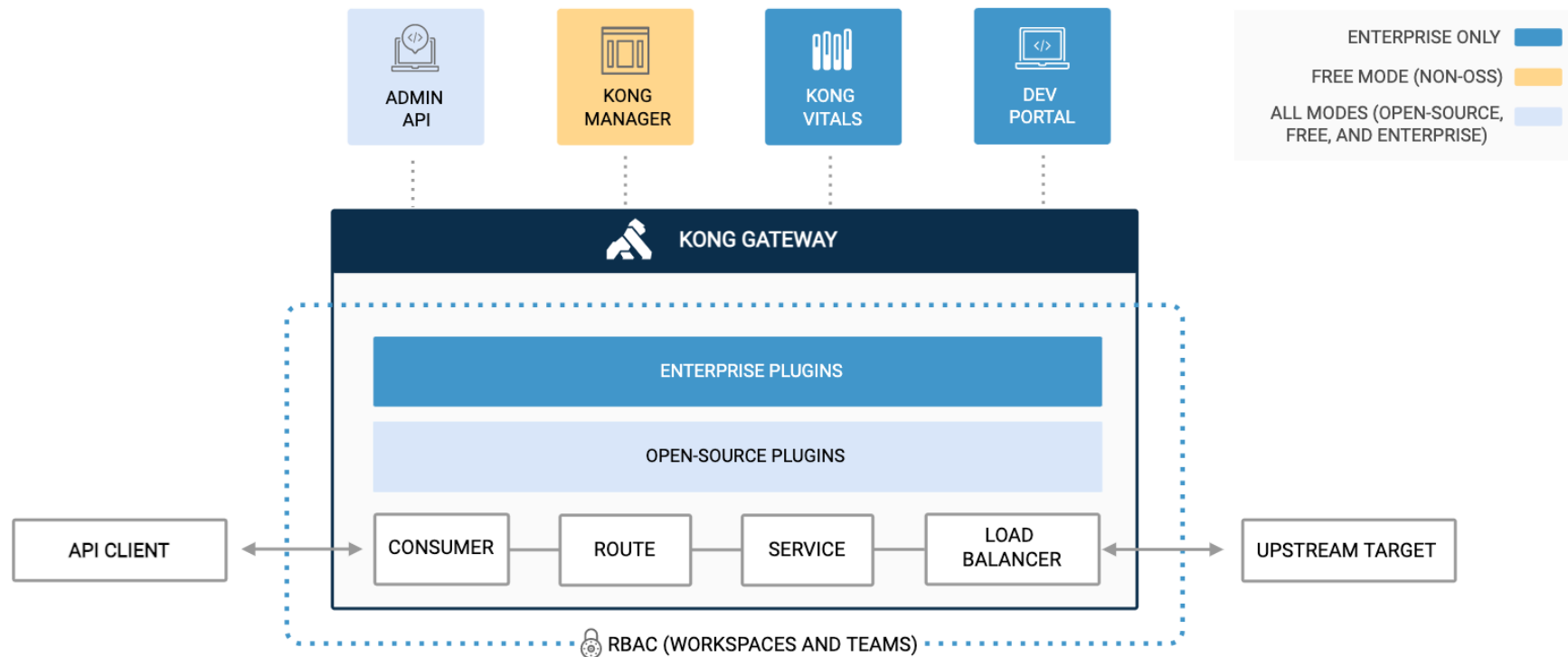
Caratteristiche dei microservizi



KONG GATEWAY

Cos'è Kong Gateway API?

Kong Gateway è un API gateway cloud-native che si interpone tra un client e un back – end per la **gestione delle API** che si comporta come un **proxy inverso** accettando tutte le richieste indirizzate alle API gestite, consentendo di configurare **services, routes e plugin**.



IL PROGETTO

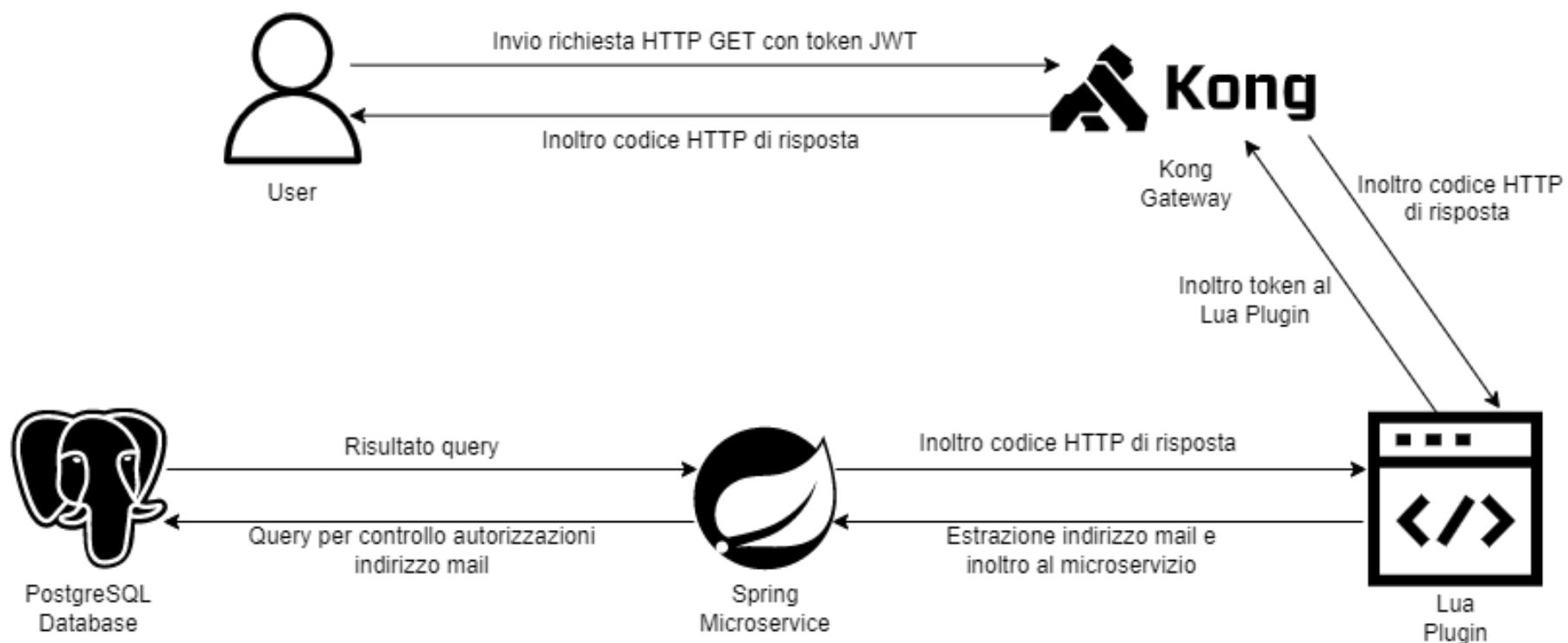
Scopo del progetto

L'obiettivo del progetto è quello di realizzare un software che consenta l'autenticazione di un utente all'interno di una piattaforma generica tramite un token da includere all'interno della richiesta inviata, senza quindi l'utilizzo di password o altri strumenti di autenticazione.

Il progetto è strutturato in 4 macro – componenti:

- Database
- Microservizio in Java utilizzando Spring Framework
- Kong Gateway
- Plugin custom per Kong Gateway in Lua

Schema delle comunicazioni



DATABASE

Struttura del Database PostgreSQL

Contiene due tabelle:

- **users**
Contiene le informazioni di tutti gli utenti abilitati ad accedere ad un determinato servizio.
- **email**
Contiene gli indirizzi e-mail di tutti gli utenti della piattaforma, quindi non è garantito che tutti avranno accesso a tutti i servizi.

| email | |
|-------|-----------------------------------|
| PK | <u>id integer SERIAL NOT NULL</u> |
| | email text NOT NULL |

| users | |
|-------|-----------------------------------|
| PK | <u>id integer SERIAL NOT NULL</u> |
| | email text NOT NULL |
| | name text |
| | surname text |

Modello Entità – Relazione del Database

MICROSERVIZIO CheckEmail

Obiettivi del microservizio

Lo scopo principale del microservizio è quello di ricevere una richiesta HTTP con all'interno del body un indirizzo e-mail.

Si effettua una query all'interno del Database per controllare che l'indirizzo sia presente nella tabella degli utenti abilitati all'utilizzo del servizio.

Si restituisce infine il codice HTTP adatto.

| Codice HTTP | Significato |
|-------------|--------------------------|
| 200 | OK |
| 402 | PAYMENT REQUIRED |
| 500 | INTERNAL SERVER ERROR |
| 503 | SERVICE UNAVAILABLE |



La classe main

La classe principale del progetto è composta da un solo comando, che si occupa di avviare l'applicazione.

Il metodo `run()` è il metodo principale di Spring Framework, serve ad avviare tutti i processi necessari per l'esecuzione dell'applicazione.

```
package com.aesys.valeriodesiati.mail;

import org.springframework.boot.SpringApplication;
import org.springframework.boot.autoconfigure.SpringBootApplication;

@SpringBootApplication
public class EmailApplication {

    public static void main(String[] args) {
        SpringApplication.run(EmailApplication.class, args);
    }

}
```

Le classi @Entity

Una classe annotata come @Entity indica che questa servirà per la creazione di una tabella all'interno del Database specificato, utilizzando come campi gli attributi della classe.

Si noti come ad una normale classe Java siano aggiunte solo le annotazioni Spring:

- @Id e @GeneratedValue() per definire l'attributo come id autogenerato
- @Column() per definire il nome di un campo (colonna) della tabella ed eventuali altre proprietà

```
package com.aesys.valeriodesiati.mail.model;
//imports..
@Entity
@Table (name="users")
public class Users {

    @Id
    @GeneratedValue(strategy=GenerationType.IDENTITY)
    private int id;
    @Column(name = "email", nullable = false)
    private String email;
    @Column(name = "name")
    private String name;
    @Column(name = "surname")
    private String surname;

    public Users(int id, String email, String name, String surname) {
        this.id = id;
        this.email = email;
        this.name = name;
        this.surname = surname;
    }

    //setters, getters, toString()...
}
```

Le classi @Controller

Una classe annotata come `@RestController` è utilizzata per la gestione di richieste HTTP. I metodi che possono essere utilizzati con questa tipologia di Controller sono `@RequestMapping`, `@GetMapping`, `@PostMapping`, `@PutMapping`, `@DeleteMapping` ecc., si devono sempre specificare l'URL e il tipo di richiesta da gestire.

In un'architettura REST le risorse sono rappresentate in modo da essere compatibili con le operazioni **CRUD** (Create, Read, Update, Delete).

La classe JoinController.java

```
package com.aesys.valeriodesiati.mail.controller;
//imports..
@RestController
public class JoinController {
    @Autowired
    EntityManagerFactory emf;

    @Transactional
    @GetMapping("/join/checkemail/{mail}")
    public ResponseEntity<Integer> checkEmail(@PathVariable("mail") String mail) {
        EntityManager em = emf.createEntityManager();
        em.getTransaction().begin();
        String result = null;

        try {
            result = (String) em.createQuery("SELECT u.email FROM Users u, Email e WHERE u.email = e.email AND u.email = :email")
                .setParameter("email", mail).getSingleResult();
        }
        catch (NoResultException | NullPointerException e) {
            return ResponseEntity.status(HttpStatus.PAYMENT_REQUIRED).body(402);
        }
        if (result == null)
            return ResponseEntity.status(HttpStatus.PAYMENT_REQUIRED).body(402);
        else
            return ResponseEntity.status(HttpStatus.OK).body(200);
    }
}
```

PLUGIN checkemail

Obiettivi del plugin Lua

È richiesto il seguente comportamento dal plugin:

1. Analizzare il token ricevuto

```
local function SplitToken(token)
    local segments = {}
    for str in string.gmatch(token, "([^\.\.]+)") do
        table.insert(segments, str)
    end
    return segments
end
```

Obiettivi del plugin Lua

È richiesto il seguente comportamento dal plugin:

1. Analizzare il token ricevuto
2. Parse del token

```
local function ParseToken(token)
    local segments = SplitToken(token)
    if #segments ~= 3 then
        return nil, nil, nil, "Invalid token"
    end

    local header, err = cJSON_safe.decode(basexx.from_url64(segments[1]))
    if err then
        return nil, nil, nil, "Invalid header"
    end

    local body, err = cJSON_safe.decode(basexx.from_url64(segments[2]))
    if err then
        return nil, nil, nil, "Invalid body"
    end

    local sig, err = basexx.from_url64(segments[3])
    if err then
        return nil, nil, nil, "Invalid signature"
    end

    return header, body, sig
end
```

Obiettivi del plugin Lua

È richiesto il seguente comportamento dal plugin:

1. Analizzare il token ricevuto
2. Parse del token
3. Inviare una richiesta HTTP al microservizio CheckEmail

```
local body, code, headers, status =  
    http.request("http://restservice-springid.azurewebsites.net  
                /join/checkemail/"..bodyTok.email)
```

Obiettivi del plugin Lua

È richiesto il seguente comportamento dal plugin:

1. Analizzare il token ricevuto
2. Parse del token
3. Inviare una richiesta HTTP al microservizio CheckEmail
4. Ottenere risposta dal microservizio e inoltrarla al Gateway

```
if code == 200 then
    return kong.response.exit(200, "Success")
end

if code == 402 then
    return kong.response.error(402, "Payment Required")
end

--response codes 500 and 503...
```

CONFIGURAZIONE KONG GATEWAY

Script di configurazione

Tutta la configurazione è effettuata tramite lo script bash `addplugin` che ha i seguenti compiti:

1. Avviare il container
2. Copiare al suo interno i file relativi ai plugin custom
3. Riavviare il container
4. Eseguire il comando `curl` per tutti i file JSON presenti relativi a tutte le altre configurazioni necessarie

```
sudo docker exec -it --user root $container rm -rf
    /usr/local/share/lua/5.1/kong/plugins/$dir
sudo docker exec -it --user root $container mkdir
    /usr/local/share/lua/5.1/kong/plugins/$dir
sudo docker cp . $container:/usr/local/share/lua/5.1/kong/plugins/$dir/
curl -s -X POST -H "Content-Type: application/json"
    -d @./config/checkemail/services.json
    http://checkemail.westeurope.cloudapp.azure.com:8001/services > /dev/null
```


TESTING

Test con Postman

Postman è una piattaforma API per la creazione, sviluppo e testing di APIs.

È stato utilizzato per la fase di testing dato che permette di effettuare delle **richieste HTTP/S**, offrendo la possibilità di **configurare il body** della stessa e di ricevere la risposta.

Il software risulta molto intuitivo, si seleziona il metodo di richiesta (HTTP GET), si inserisce l'URL e, se necessario, si configurano i campi della richiesta, in questo caso si aggiunge al body della richiesta il **token JWT**.



Risultati – OK

The screenshot displays a REST client interface with the following components:

- Request Bar:** Method `GET`, URL `http://checkemail.westeurope.cloudapp.azure.com:8000/join/checkemail/valerio.desiati@aesys.tech`, and a `Send` button.
- Request Tabs:** `Params`, `Authorization` (active), `Headers (7)`, `Body`, `Pre-request Script`, `Tests`, `Settings`, and `Cookies`.
- Authorization Section:**
 - Type:** `Bearer Token`.
 - Token:** `eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InB1WmZhcWZLRzBPV3M4Z0x6NmVDUjZkZ2g3QmRkeXBKIn0.eyJlbWFpbCI6InZhbGVyaW8uZGVzaWF0aUBhZXN5cy50ZWNoZiZlZjoxMTEuMTExMTExOX0uZDRI8-MNIL4YRnZlYd0Xk2Jqd1Ga7fCfV2EcMIAR-E`
- Response Section:** Tabs for `Body` (active), `Cookies`, `Headers (10)`, and `Test Results`.
 - Response Bar:** Status `200 OK`, Time `531 ms`, Size `389 B`, and a `Save Response` button.
 - Response Format:** `Pretty` (selected), `Raw`, `Preview`, `Visualize`, and `JSON`.
 - Response Content:** A list of response items, with the first item labeled `1` and a value of `200`.

Risultati – Unauthorized

The screenshot shows a REST client interface with a GET request to `http://checkemail.westeurope.cloudapp.azure.com:8000/join/checkemail/valerio.desiati@aesys.tech`. The 'Authorization' tab is active, showing 'Bearer Tok...' as the type and 'Token' as the value. Below this, a message states: 'The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)'. The 'Body' tab is also active, displaying a JSON response: `{ "message": "Unauthorized" }`. The status bar at the bottom indicates 'Status: 401 Unauthorized', 'Time: 376 ms', and 'Size: 284 B'. A 'Save Response' button is visible on the right.

GET ⌵ `http://checkemail.westeurope.cloudapp.azure.com:8000/join/checkemail/valerio.desiati@aesys.tech` Send ⌵

Params Authorization ● Headers (6) Body Pre-request Script Tests Settings Cookies

Type Bearer Tok... ⌵ Token Token

The authorization header will be automatically generated when you send the request.
[Learn more about authorization](#) ➤

Body Cookies Headers (7) Test Results 🌐 Status: 401 Unauthorized Time: 376 ms Size: 284 B Save Response ⌵

Pretty Raw Preview Visualize JSON ⌵ ☰

```
1 {  
2   "message": "Unauthorized"  
3 }
```



UNIVERSITÀ DI PARMA

GRAZIE PER L'ATTENZIONE!