

ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

SCUOLA DI SCIENZE
Corso di Laurea in Informatica

TITOLO1
TITOLO2
TITOLO3

Relatore:
Prof. Ozalp Babaoglu

Presentata da:
Angelo Galavotti

Correlatore:
Prof. Francesco Giacomini

Sessione II
Anno Accademico 2021/2022

Dedica qui,
Dedica qui 2.

Sommario

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent sit amet lacus nulla. Proin quis nibh vel risus rutrum cursus quis ac dui. Integer nec mollis diam. Sed eget nisl sit amet sem maximus faucibus vel a sem. In hac habitasse platea dictumst. Vivamus a commodo ante. Aliquam erat volutpat. Suspendisse eu porttitor sem, nec porta mi. Etiam et risus euismod, gravida justo nec, pulvinar nulla. Pellentesque finibus tristique mauris, quis molestie nibh consequat nec.

Praesent pretium finibus turpis, sit amet sodales sem facilisis non. Nullam nisi eros, convallis in diam in, faucibus maximus justo. Mauris eu auctor erat, et tristique libero. Praesent pretium gravida magna, a faucibus neque posuere sit amet. Etiam tellus lacus, viverra sit amet dignissim in, eleifend vel diam. In hac habitasse platea dictumst. Nam ornare est nunc, ac interdum turpis rhoncus vitae. Aenean id neque diam. Nunc ac accumsan lectus. Ut vehicula luctus risus eget dignissim. Quisque sed justo non erat vestibulum consectetur vel a diam.

Fusce malesuada magna in odio vehicula, vel malesuada leo congue. Duis nec diam nunc. In hac habitasse platea dictumst. Vivamus vitae urna dignissim urna pharetra consequat. Aenean aliquam non sem et dictum. Proin sagittis tellus ex, a bibendum erat ornare ut. Nunc hendrerit maximus luctus. Etiam consequat vel velit sit amet ullamcorper. Interdum et malesuada fames ac ante ipsum primis in faucibus. Vestibulum vulputate dapibus orci eget laoreet. Sed non purus quis enim condimentum ultricies dapibus a tellus.

Aliquam erat volutpat. Sed non urna a quam pretium euismod viverra sed nisl. Integer egestas enim in nulla faucibus consequat. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum placerat quam nec ultrices vulputate. Sed sagittis quis leo ut ullamcorper. Nam id dui ac orci accumsan lobortis eget eu nunc. Aenean a

tempus mauris, nec accumsan sem. In imperdiet nisl ante, non cursus elit ornare vehicula. In posuere vulputate augue vitae efficitur. Suspendisse eu aliquet tellus.

Vivamus sed maximus ex, ac placerat est. Sed accumsan laoreet nunc. Phasellus finibus mauris velit, eu finibus tellus ullamcorper a. Ut lobortis sagittis nisl, eget eleifend dolor viverra et. Phasellus vitae pellentesque nibh. Ut quis posuere nisl. Donec mattis rhoncus orci vitae vestibulum. Pellentesque tempus at libero ut placerat. Nulla facilisi.

Indice

| | | |
|----------|--------------------------------------------|----------|
| 1 | Introduzione | 1 |
| 1.1 | Struttura del documento | 1 |
| 1.2 | Autorizzazione e autenticazione | 1 |
| 1.3 | Open Policy Agent | 2 |
| 2 | Progettazione | 3 |
| 2.1 | Componenti | 3 |
| 2.1.1 | Reverse Proxy | 4 |
| 2.1.2 | Sistema di politiche | 4 |
| 2.1.3 | Service server | 4 |
| 2.2 | Topologia finale | 5 |
| 3 | Implementazione | 7 |
| 3.1 | Software stack | 7 |
| 3.1.1 | OpenPolicyAgent | 7 |
| 3.1.2 | NGINX | 7 |
| 3.1.3 | Docker | 7 |
| 3.2 | Implementazioni delle componenti | 7 |
| 3.2.1 | Reverse proxy | 7 |
| 3.2.2 | Sistema di politiche | 7 |
| 3.2.3 | Service server | 7 |
| 3.3 | Testing | 8 |
| 4 | Gestione dell'autenticazione | 9 |

| | | |
|----------|--------------------------------------------|-----------|
| 5 | Interfacciamento con Storm-Tape API | 11 |
| 6 | Conclusioni e sviluppi futuri | 13 |
| | Bibliography | 15 |

Elenco delle figure

| | | |
|-----|----------------------------------------------------|---|
| 2.1 | Rappresentazione concettuale del sistema | 5 |
|-----|----------------------------------------------------|---|

Elenco delle tabelle

Capitolo 1

Introduzione

1.1 Struttura del documento

In questa tesi verrà esposta una leggera introduzione su alcuni concetti chiave sul contesto e sulle tecnologie in uso. Dopodiché, sarà mostrerà l'implementazione vera e propria dell'intera infrastruttura, aumentando il numero di features andando avanti con i capitoli. Infine, verrà illustrata un'analisi delle performance e verranno fatte le ultime conclusioni.

1.2 Autorizzazione e autenticazione

[aggiungeer roba sulla storia?] I concetti di "*autorizzazione*" e "*autenticazione*" rappresentano due nuclei fondamentali nell'ambito della sicurezza informatica. Con *autorizzazione* si intende la funzione che specifica i privilegi di accesso a determinate risorse o servizi. L'*autenticazione*, invece, rappresenta l'atto di confermare la verità dell'identità di un utente. Essenzialmente, il processo di autorizzazione fa uso dei dati provenienti dal processo di autenticazione, e in base a questi stabilisce i permessi che un utente possiede.

1.3 Open Policy Agent

[\[Migliorare coesione dei concetti\]](#) Open Policy Agent è un motore di policy open-source, che si occupa principalmente di definire e imporre le politiche di autorizzazione attraverso lo stack una applicazione. Grazie a questo sistema, il processo di decision making nella fase di autorizzazione viene spostato dall'applicazione ad una componente esterna.

Le politiche vengono specificate attraverso un linguaggio dichiarativo di alto livello chiamato *Rego*. Attraverso Rego, le richieste di autorizzazione vengono

Capitolo 2

Progettazione

Durante la progettazione di un sistema di autorizzazione, è necessario considerare alcuni parametri fondamentali che ci permettono di valutarlo nel contesto in cui ci si trova. Quelli che hanno influito maggiormente sulle scelte progettuali sono state la *versatilità* (la capacità di interfacciarsi con sistemi di funzionalità e struttura diversa) e la *manutenibilità* (la facilità di apportare modifiche a sistema realizzato).

Attraverso la divisione in più componenti, modificare le regole d'accesso non richiede un'alterazione del codice del complesso. Inoltre, la separabilità totale dal servizio che si intende proteggere permette di facilitare la compatibilità con altre tecnologie.

2.1 Componenti

L'architettura dell'infrastruttura presenta uno scheletro formato da tre componenti di principali: il *reverse proxy*, il *sistema di politiche* e il *service server*. Ciascuna di esse veste un ruolo importante nella gestione della richiesta, tuttavia solo le prime due influenzano il processo di autorizzazione.

2.1.1 Reverse Proxy

Il reverse proxy rappresenta l'entry-point dell'intero sistema di autorizzazione. Il compito di questo componente è di mediare la comunicazione tra client e service server: ogni richiesta che viene fatta da un utente dovrà prima attraversare il reverse proxy. In questo modo, al client apparirà di comunicare direttamente con il server, nonostante le richieste siano dirette al proxy e da esso propriamente gestite.

La mediazione fornita da questo elemento incorpora un aspetto decisionale, attraverso il quale viene espresso effettivamente il concetto di autorizzazione. Infatti, il reverse proxy inoltra o ignora le richieste al service server, basandosi sull'output di un sistema di politiche.

2.1.2 Sistema di politiche

Il sistema di politiche è la parte che determina come la richiesta dovrà essere gestita.

Per adempiere al suo ruolo, sfrutta le informazioni di identità dell'utente contenute nella richiesta, che devono essere propriamente formattate per essere comprese correttamente. Dopodiché, le confronta con dati quali politiche e permessi, ai quali ha accesso diretto. Infine, restituisce in output una decisione, che stabilisce se l'accesso è consentito.

2.1.3 Service server

Con service server si intende il servizio che sfrutta il sistema di autorizzazione. Come tale, il suo ciclo d'esecuzione consiste nel gestire le richieste provenienti dagli utenti tramite il reverse proxy e formulare una risposta. Questa viene indirizzata al mittente iniziale, senza che sia filtrata o analizzata, ma attraversando comunque il proxy.

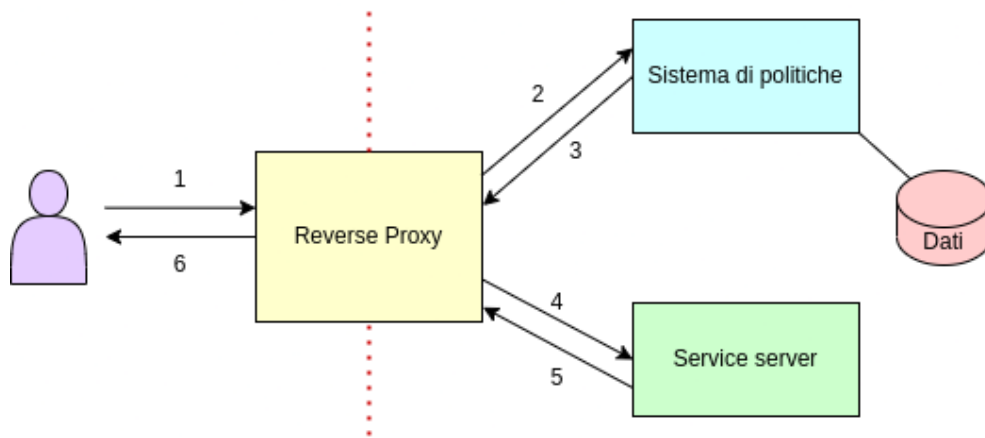


Figura 2.1: Rappresentazione concettuale del sistema

2.2 Topologia finale

In base a quanto è stato esposto nei paragrafi precedenti, si ottiene una struttura topologica simile a quanto mostrato nella Figura 2.1. I numeri su ogni freccia indicano l'ordinamento temporale delle trasmissioni di dati tra ogni elemento.

Ciascun componente è interpretabile come un processo separato in esecuzione sullo stesso server o su server diversi.

Capitolo 3

Implementazione

bho.

3.1 Software stack

3.1.1 OpenPolicyAgent

3.1.2 NGINX

3.1.3 Docker

3.2 Implementazioni delle componenti

3.2.1 Reverse proxy

3.2.2 Sistema di politiche

3.2.3 Service server

Come descritto nel Capitolo 2, con service server si intende un servizio qualsiasi che sfrutta l'infrastruttura di autorizzazione. Siccome questa fase del progetto si focalizza sullo sviluppo corretto delle componenti dedicate al filtraggio delle richieste, il service server è dato da una API abbastanza

elementare.

L'API in questione ritorna 200 se si accede correttamente all'endpoint `/operation`, mentre una richiesta a `/operation/image_request` permette lo scaricamento di un'immagine. Siccome queste locazioni presentano il prefisso "operation", il loro accesso comporta l'uso del sistema di autorizzazione.

Per implementare quando appena descritto, si è utilizzato nuovamente il software NGINX, sfruttando la sua modalità webserver.

```
1      # invia 200 se si esegue l'operazione con successo
2      location /operation {
3          return 200;
4      }
5
6      # simula la richiesta di una risorsa al server
7      location /operation/image_request {
8          try_files $uri /test.jpg;
9      }
```

Codice 3.1: sda

Questa scelta ha facilitato lo sviluppo, permettendo di definire una API funzionante in poche righe di codice.

3.3 Testing

Capitolo 4

Gestione dell'autenticazione

Capitolo 5

Interfacciamento con Storm-Tape API

Capitolo 6

Conclusioni e sviluppi futuri

Bibliografia

- [1] Linux's Contributors, *Linux Kernel*, <https://www.kernel.org/>.
- [2] Free Software Foundation, Inc., *GNU General Public License Version 3*, <https://www.gnu.org/licenses/gpl-3.0.en.html>.

Ringraziamenti

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent sit amet lacus nulla. Proin quis nibh vel risus rutrum cursus quis ac dui. Integer nec mollis diam. Sed eget nisl sit amet sem maximus faucibus vel a sem. In hac habitasse platea dictumst. Vivamus a commodo ante. Aliquam erat volutpat. Suspendisse eu porttitor sem, nec porta mi. Etiam et risus euismod, gravida justo nec, pulvinar nulla. Pellentesque finibus tristique mauris, quis molestie nibh consequat nec.

Praesent pretium finibus turpis, sit amet sodales sem facilisis non. Nullam nisi eros, convallis in diam in, faucibus maximus justo. Mauris eu auctor erat, et tristique libero. Praesent pretium gravida magna, a faucibus neque posuere sit amet. Etiam tellus lacus, viverra sit amet dignissim in, eleifend vel diam. In hac habitasse platea dictumst. Nam ornare est nunc, ac interdum turpis rhoncus vitae. Aenean id neque diam. Nunc ac accumsan lectus. Ut vehicula luctus risus eget dignissim. Quisque sed justo non erat vestibulum consectetur vel a diam.

Fusce malesuada magna in odio vehicula, vel malesuada leo congue. Duis nec diam nunc. In hac habitasse platea dictumst. Vivamus vitae urna dignissim urna pharetra consequat. Aenean aliquam non sem et dictum. Proin sagittis tellus ex, a bibendum erat ornare ut. Nunc hendrerit maximus luctus. Etiam consequat vel velit sit amet ullamcorper. Interdum et malesuada fames ac ante ipsum primis in faucibus. Vestibulum vulputate dapibus orci eget laoreet. Sed non purus quis enim condimentum ultricies dapibus a tellus.

Aliquam erat volutpat. Sed non urna a quam pretium euismod viverra sed nisl. Integer egestas enim in nulla faucibus consequat. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum placerat quam nec ultrices vulputate. Sed sagittis quis leo ut ullamcorper. Nam id dui ac orci accumsan lobortis eget eu nunc. Aenean a tempus mauris, nec accumsan sem. In imperdiet nisl ante, non cursus elit ornare vehicula. In posuere vulputate augue vitae efficitur. Suspendisse eu aliquet tellus.

Vivamus sed maximus ex, ac placerat est. Sed accumsan laoreet nunc. Phasellus finibus mauris velit, eu finibus tellus ullamcorper a. Ut lobortis sagittis nisl, eget eleifend dolor viverra et. Phasellus vitae pellentesque nibh. Ut quis posuere nisl. Donec mattis rhoncus orci vitae vestibulum. Pellentesque tempus at libero ut placerat. Nulla facilisi.