Analisi e implementazione di un sistema di autorizzazione compatibile con token OAuth 2.0 e certificati VOMS

Presentata da Angelo Galavotti
Relatore: Ozalp Babaoglu
Correlatore: Francesco Giacomini

Corso di Laurea in Informatica
Alma Mater Studiorum Università di Bologna

12 Ottobre 2022

Sommario

Background

- Il Worldwide LHC Computing Grid (**WLCG**) è una collaborazione mondiale di **centri di calcolo** finalizzata all'**analisi** e all'**elaborazione** dei dati generati dall'**acceleratore di particelle** del **CERN** di Ginevra.
- Uno di questi centri di calcolo è situato alla sede CNAF di Bologna dell'INFN, e si occupa anche dello **sviluppo del middleware** dell'infrastruttura **WLCG**.
- Molte componenti di tale middleware necessitano di un **sistema di autorizzazione**.

Obiettivo

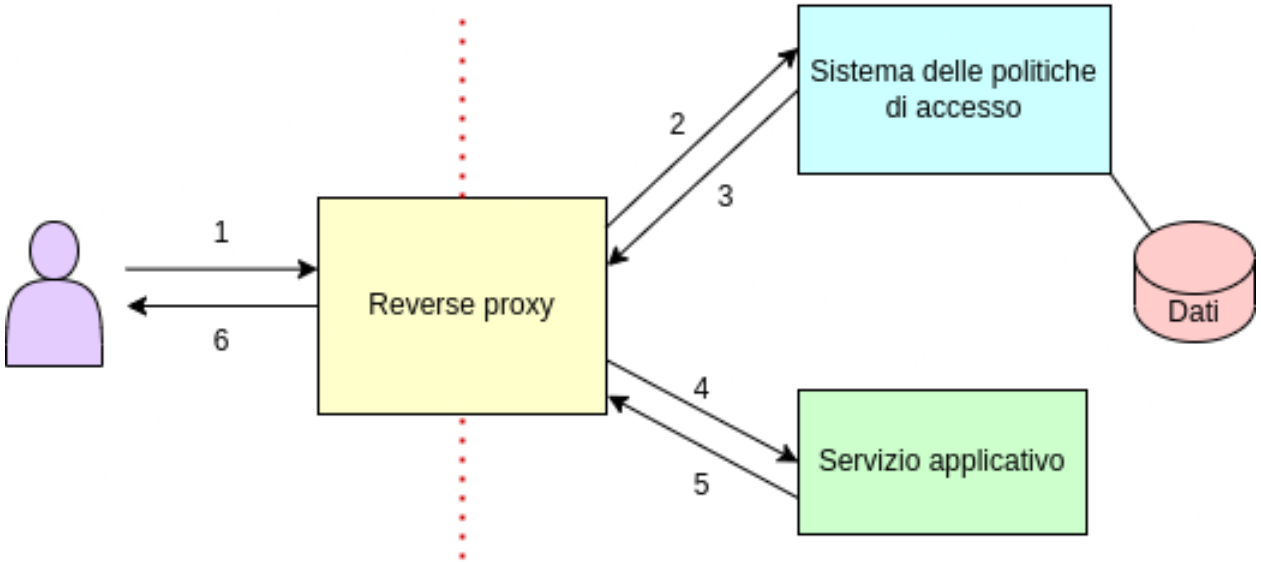
L'obiettivo del progetto consiste nella creazione di un PoC di un **sistema di autorizzazione** che sia **versatile** e **compatibile** con i **metodi di autenticazione** attualmente adottati dal WLCG.

Struttura

L'infrastruttura presenta tre componenti principali, ciascuno in esecuzione all'interno di un container **Docker**:

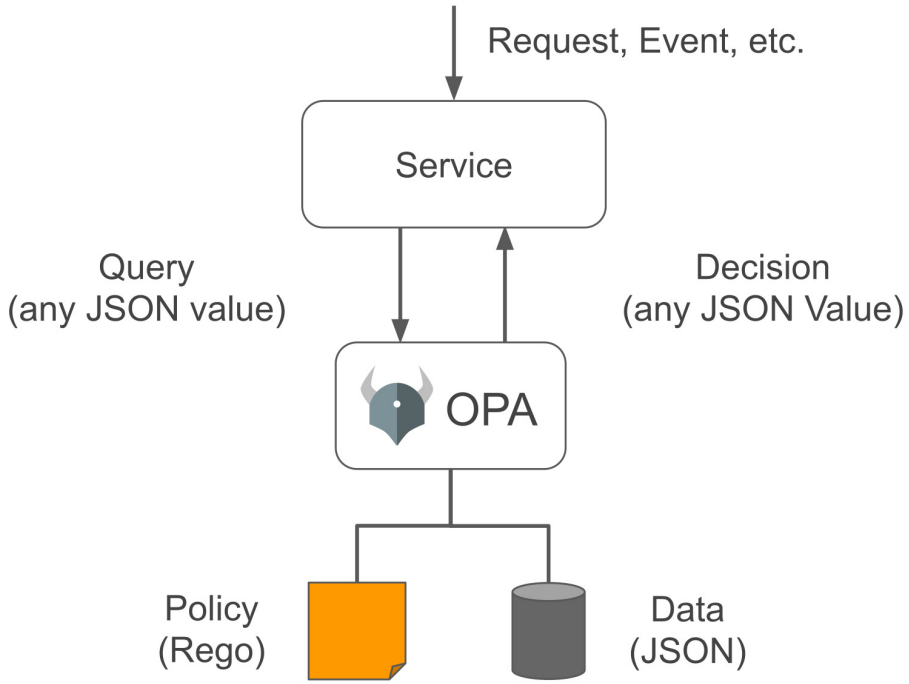
- **Sistema delle politiche di accesso**
- **Reverse proxy**
- **Servizio applicativo**

La separazione in componenti permette di **evitare ambiguità** durante il controllo degli accessi e di garantire la **manutenibilità**.



OpenPolicyAgent

- **OpenPolicyAgent** è il sottosistema software alla base del **sistema delle politiche** di accesso.
- È un **policy engine** che permette l'**applicazione di politiche** e regole scritte in linguaggio Rego.
- Le regole implementate in questo progetto attuano un **modello RBAC** per il controllo degli accessi.



NGINX

- **NGINX** è il software utilizzato per l'implementazione del **reverse proxy** e del **servizio applicativo**.
- È conosciuto per la sua **stabilità**, **efficienza** e **semplicità** di configurazione.
- Contiene direttive built-in che facilitano l'implementazione del reverse proxy e l'**interrogazione del sistema delle politiche** di accesso.
- Le sue funzionalità possono essere estese tramite la scrittura di **procedure** in **linguaggio NJS**.

Gestione dei metodi di autenticazione

- Un requisito chiave del sistema è la compatibilità con i **metodi di autenticazione** attualmente adottati dal **WLCG**.
- Le procedure di autenticazione del WLCG sono in **fase di transizione**:
  - attualmente si basano su **certificati VOMS Proxy** ed evolveranno verso l'uso di **JSON Web Token**.
- È necessario che il PoC sia compatibile con entrambi i metodi.

JSON Web Token

- I JSON Web Token (**JWT**) definiscono un metodo **compatto** e **sicuro** per la trasmissione di dati in **formato JSON**.
- Sono alla base dallo standard **OpenID Connect**, basato sul protocollo di autorizzazione **OAuth 2.0**.
- Si definiscono come una stringa di caratteri, in cui si riconoscono **tre parti separate da un punto**.

`[header].[payload].[signature]`

- OpenPolicyAgent fornisce delle **funzioni built-in** per la decodifica e la verifica dei JWT.

Certificati proxy VOMS

- I certificati **VOMS Proxy** hanno lo stesso formato di un certificato **X.509**, ma aggiungono il campo **Attribute Certificate**.
- Questo campo contiene il certificato di una **Virtual Organization** (VO), in modo da poter **delegare** ad essa le operazioni da svolgere.

- È disponibile un **modulo di NGINX** per l'**estrazioni dei dati** da un VOMS Proxy.

StoRM-Tape

- Per dimostrare le qualità del PoC, si è deciso di **interfacciare** il sistema con un **componente middleware** attualmente in sviluppo al CNAF.

- **StoRM-Tape** è un'implementazione della specifica della WLCG Tape REST API, che offre un'**interfaccia comune** per la gestione della **residenza dei dati** mantenuti negli **storage** dei grid computazionali.

Interfacciamento

Le **modifiche** necessarie per interfacciare il sistema con StoRM-Tape sono **minime**:

- **Modifica dei permessi** in modo che siano correlate con le funzionalità offerte da StoRM-Tape.
- **Ridenominazione** degli **endpoint** nel **reverse proxy** in modo che coincidano che quelle dell'API.

Conclusioni e sviluppi futuri

Il PoC realizzato **soddisfa tutti i requisiti** e si interfaccia con servizi di diverso carattere in modo **trasparente**, richiedendo **poche modifiche**.
Alcune possibili evoluzioni:

- Possibilità di **modificare le policy** collegandosi dall'**esterno** dell'infrastruttura.
- Modifica delle regole per permettere un controllo degli accessi **capability-based**.
- Variazione delle topologia in modo che il **servizio applicativo** possa comunicare **direttamente** con **OpenPolicyAgent**.