**Interoperabilità e Cooperazione Applicativa delle Regioni**

*Azione di transizione ai nuovi standard*

# ICAR Playground

*Installazione*

**Task: INF-1 (Regione Toscana)**
**Seconda annualità**

**Versione 1.0**

# Indice

# 1 Introduzione

Questo documento descrive i passi necessari per l'installazione e il corretto avvio dello strumento **ICAR Playground** realizzato nell'ambito delle attività evolutive previste nel progetto ICAR per la transizione ai nuovi standard in materia di interoperabilità.

# 2 Composizione del Playground

ICAR Playground è stato realizzato integrando container di tipo **Docker** (https://www.docker.com) in un ambiente integrato tramite il tool "docker-compose". Per supportare i pattern di interoperabilità che prevedono interazioni tra servizi in accordo alle specifiche tecniche di riferimento, è stato selezionato un set di componenti minimo per consentirne l'esecuzione. A livello generale si tratta dei seguenti componenti:

- API Gateway
- Authorization Server
- Reverse Proxy
- Database Server
- Servizi di infrastruttura per il monitoraggio degli SLA

L'ambiente Docker Compose contiene quindi un'istanza di ciascuno di tali componenti per i quali sono state fatte le seguenti scelte:

- **Traefik** (https://docs.traefik.io)

  Fornisce le funzionalità di reverse proxy e load balancer al fine di garantire la gestione del frontend HTTP, le comunicazioni SSL e l'inoltro delle richieste in ingresso verso il corrispondente nodo dell'API Gateway.

- **KeyCloak** (https://www.keycloak.org)

  Fornisce le funzionalità di identity management necessarie al supporto dell'autenticazione di utenti e applicazioni. Nel contesto del modello di riferimento, KeyCloak è utilizzato, nello scenario Oauth2, come Authorization Server allo scopo di gestire le fasi di rilascio e validazione degli access token.

- **GovWay** (https://govway.org)

  un API gateway che include il supporto completo delle nuove linee guida di interoperabilità e che permette quindi di esplorare i diversi pattern proposti da AGID in ModiPA. Oltre a ModiPA, Govway supporta tutte le classiche funzionalità di API Gateway quali: controllo degli accessi, tracciatura dei flussi in ingresso e uscita, rate limiting, ...

- **PostgreSQL** (https://postgresql.org)

  il database utilizzato per le configurazioni e i log di Govway e KeyCloak.

- **Sla-Api**

  Microservizio realizzato nell'ambito delle attività del task INF-2 del progetto, che mette a disposizione delle API per il monitoraggio delle performance dei servizi.

Per consentire un rapido utilizzo dell'ambiente viene fornito, insieme alla piattaforma di interoperabilità, un set di interazioni preconfigurate che permettono di avviare gli scenari supportati tramite l'applicativo **Postman** (https://www.postman.com). Le interazioni sono raccolte in una collection di Postman che, oltre a consentire l'esecuzione dei pattern, permette di verificare le modalità di integrazione degli applicativi alla piattaforma di interoperabilità ed eventualmente procedere con estensioni a proprio piacimento.

ICAR Playground è quindi uno strumento che ciascun ente può installare nel proprio ambiente dopo aver acquisito i due elementi che lo compongono, che sono:

- L'**Ambiente Docker Compose (icar-playground.zip)**, che costituisce la piattaforma demo di interoperabilità.
- La **Collection Postman ICAR-Playground.postman_collection.json**, che contiene le interazioni preconfigurate per eseguire i pattern di interoperabilità.
- La **Collection Postman ICAR-Playground-SLA-API.postman_collection.json**, che contiene le interazioni preconfigurate per la creazione di misure e indici per il recupero delle performance di un servizio.

Come prerequisito per l'esecuzione degli scenari previsti, è necessaria l'installazione iniziale dei software Docker, lato server, e Postman lato client, reperibili agli indirizzi forniti in precedenza.

# 3 Avvio e configurazione

Per avviare l'ambiente il primo passo consiste nell'attivare i container che costituiscono l'ambiente Docker. I passi da eseguire sono i seguenti:

1. Scompattare l'archivio **icar-playground.zip** e trasferire i file in esso contenuti nella directory preferita per ospitare l'ambiente.
2. Configurare l'ambiente globale editando il file *env.sh*, presente al primo livello dell'archivio scompattato. Questo file si occupa di inizializzare le seguenti due variabili d'ambiente:
   - *SERVER_FQDN*

     Rappresenta l'hostname con il quale risulteranno raggiungibili i componenti del playground. Il valore di default è *gw.icar*. Modificare eventualmente questo valore con uno adatto alle proprie esigenze e prevedere un metodo di risoluzione del nome, come ad esempio la registrazione sul file "hosts" del sistema operativo ospitante.

   - *LOCAL_DATA*

Path della directory che sarà utilizzata come area di storage dai container che costituiscono l'ambiente. Il valore di default è *./data* che riferisce una cartella già presente nell'archivio.

3. Avviare Docker Compose eseguendo lo script *starttest.sh* nella directory di destinazione scelta. Saranno così avviati i quattro componenti che fanno parte dell'ambiente.

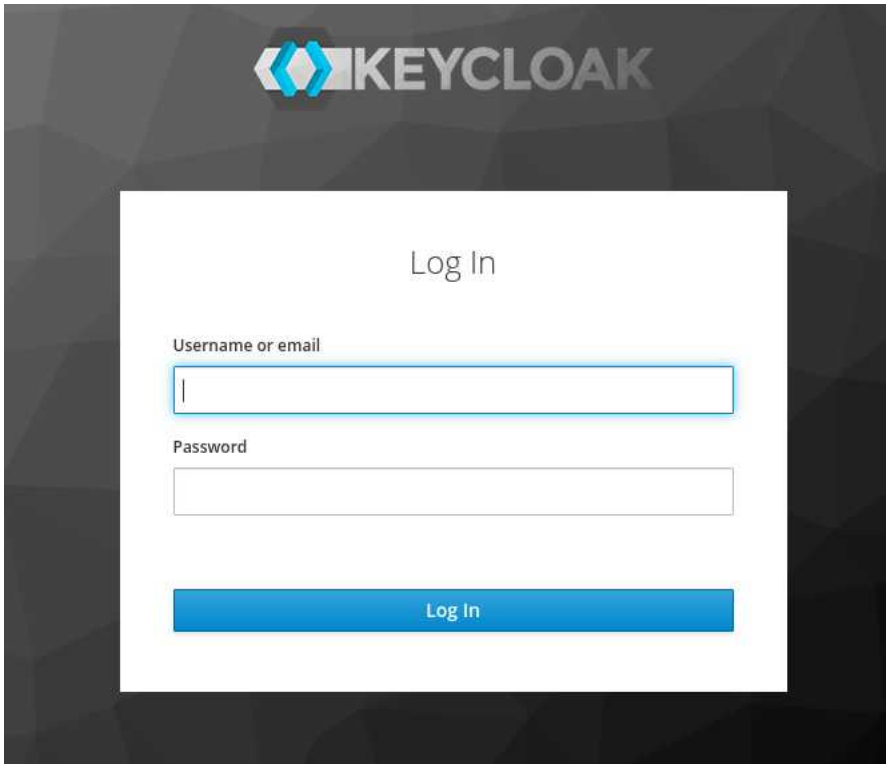
```
[root@poli-nb18 AmbienteDocker]# ./starttest
Starting govauth ...
Starting spid_testenv ...
Starting govauth
Starting ambientedocker_init_1 ...
Starting ambientedocker_init_1
Starting ambientedocker_init_1 ... done
Starting PGSQL95 ...
Starting gatewaystenv ... done
Starting PGSQL95 ... done
Starting keycloak ...
Starting keycloak ... done
Starting traefik ...
Starting traefik ... done
```

Dopo aver effettuato l'avvio dei Docker container sarà possibile effettuare le prime verifiche sulla raggiungibilità delle console di gestione degli applicativi di base:

- **Govway Console** – cruscotto grafico per la gestione delle configuazioni dell'API Gateway
  - URL: https://gw.icar/govwayConsole
  - username: amministratore
  - password: 123456


- **Govway Monitor** – cruscotto grafico per il monitoraggio del traffico sull'API Gateway
  - URL: https://gw.icar/govwayMonitor
  - username: operatore
  - password: 123456


- **Keycloak** – Cruscotto di gestione delle configurazioni dell'authorization server
  - URL: https://gw.icar/auth
  - username: admin
  - password: admin




4 Importare la Collection Postman "ICAR Playground" fornita con tutte le interazioni preconfigurate. Dall'interfaccia di Postman selezionare la funzione "Import" e scegliere il file *scenari-postman.json*.

## 3.1 Gli aspetti di sicurezza

Per la gestione dei diversi livelli di sicurezza relativi alle comunicazioni previste dai flussi di esempio, il playground è stato dotato di un kit di certificati SSL utilizzati a vari livelli. I certificati utilizzati riguardano i seguenti ambiti:

- Il livello trasporto HTTPS sul quale avvengono le comunicazioni da e verso i componenti applicativi coinvolti: API Gateway, Authorization Server, API Implementations.
- I certiticati per la gestione della sicurezza sul canale. Tali certificati sono necessari per identificare e autenticare il dominio di provenienza di una richiesta, ad esempio: Ente, EnteEsterno, ecc.
- I certificati per la gestione della sicurezza sul messaggio. Tali certificati sono necessari per identificare e autenticare l'applicativo mittente e per gestire la firma a garanzia dell'integrità e non ripudio dei contenuti delle comunicazioni.

Il kit di certificati di esempio è presente nella directory di destinazione dell'ambiente ed è così composto:

- */data/govway/pki/CA_icar/ca/certs*

  sono presenti tutti i certificati utilizzati in formato PEM
- */data/govway/pki/CA_icar/ca/private*

  sono presenti tutte le chiavi private utilizzate in formato PEM
- */data/govway/keys*

  sono presenti le coppie di chiavi in formato PKCS12 e il truststore di default utilizzato dall'API Gateway
- */data/traefik*

  sono presenti i certificati utilizzati dal reverse proxy per la terminazione delle connessioni HTTPS.

L'utilizzatore del Playground può utilizzare il kit esistente per eseguire gli scenari preconfigurati senza necessità di alcun intervento. Può eventualmente sostituire i certificati con quelli relativi al proprio dominio, in questo caso sarà necessario intervenire sulla configurazione dell'API Gateway per aggiornare i certificati utilizzati.

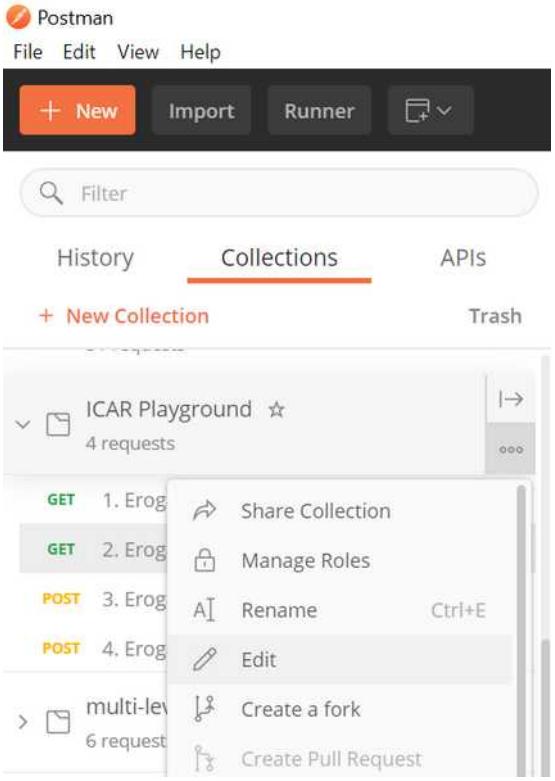
## 3.2 Configurazione di Postman

La collection importata dentro Postman comprende alcune interazioni preconfigurate che consentono di riprodurre rapidamente i pattern architetturali previsti dal progetto ICAR.

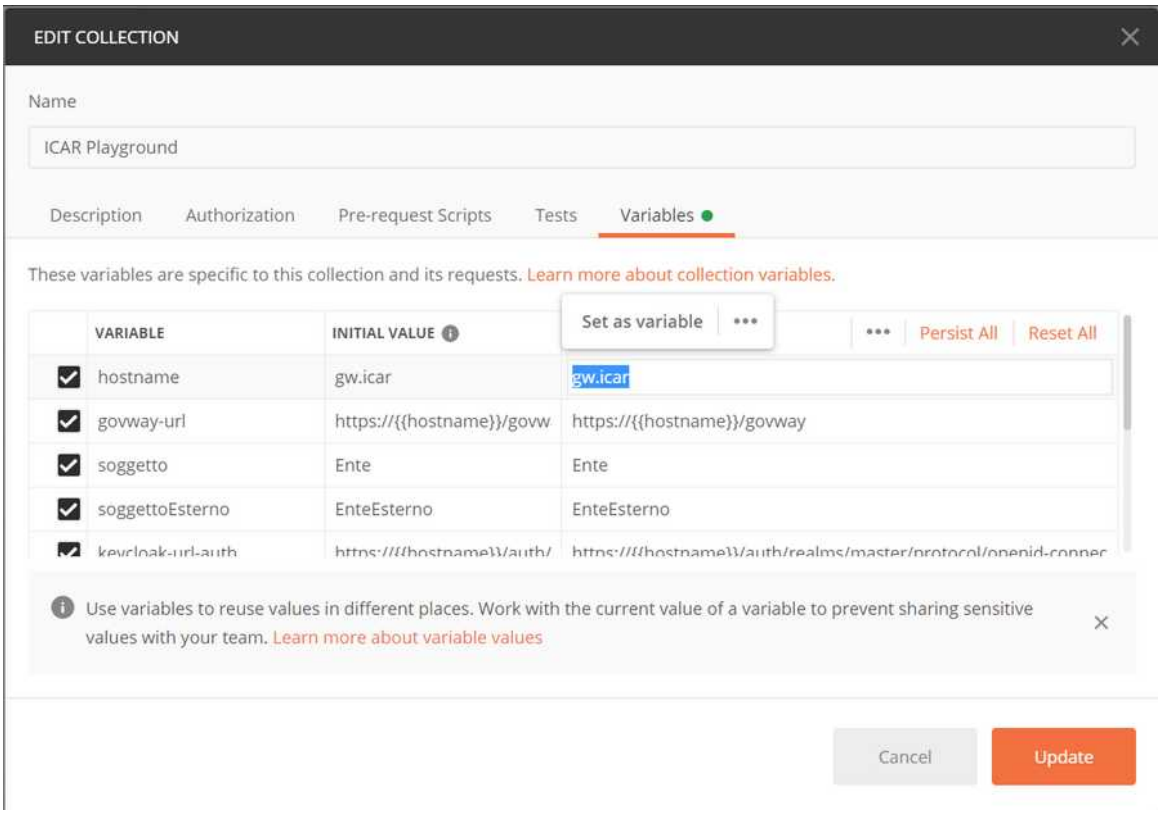
La figura seguente mostra la composizione della collection Postman. La descrizione delle interazioni contenute sarà fornita più avanti.


Le configurazioni delle interazioni sono incluse nella collection, è però necessario apportare alcune modifiche relative all'ambiente specifico:

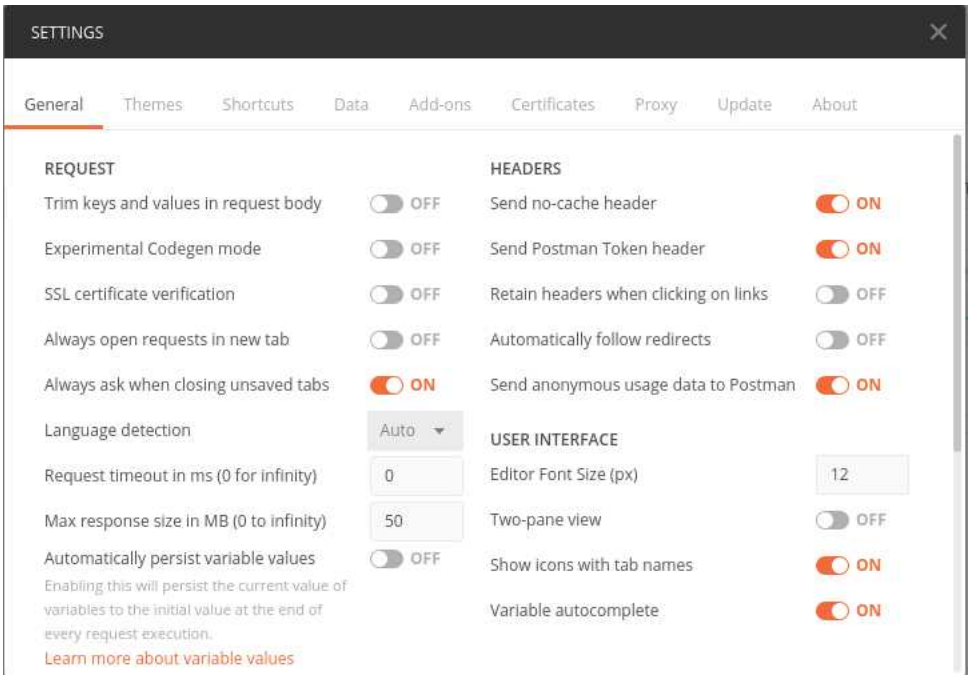
- Modificare le variabili della collection al fine di impostare l'hostname relativo all'ambiente in cui è stata attivata l'esecuzione dei docker.



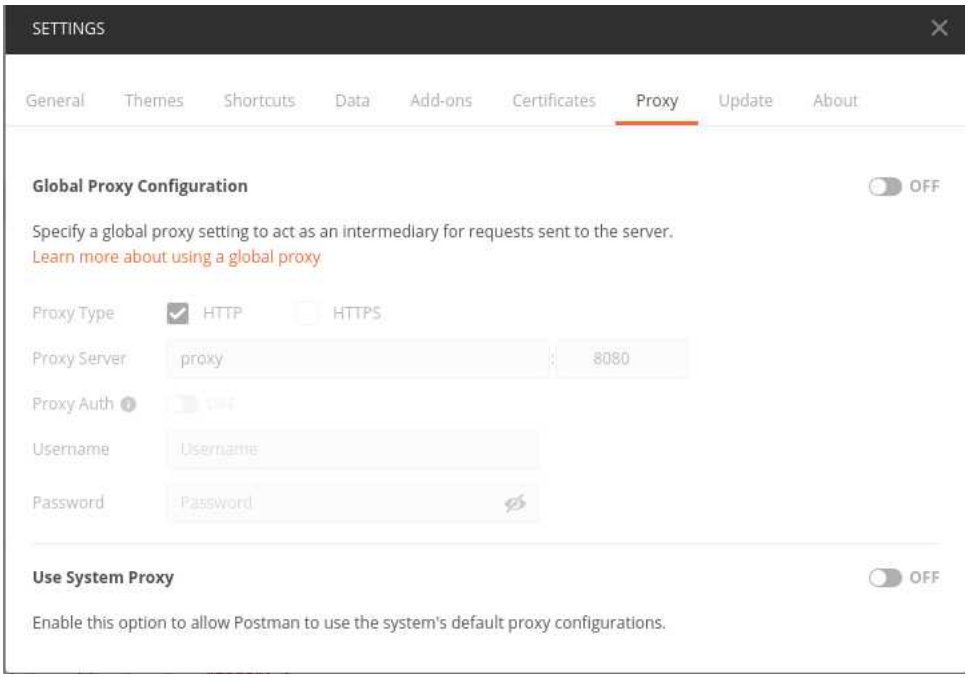

Selezionare "Edit" dal menu della collection e quindi inserire il valore corretto per la variabile "hostname". Il valore di default è *gw.icar*.




- Accedere alla configurazione globale di Postman (File > Settings) ed assicurarsi che:
  - la voce “SSL Certificate Verification” nella maschera “General” sia disabilitata




  - Nel tab "Proxy" non sia stato impostato alcun proxy




- Caricare nel tab "Certificates" la CA Icar utilizzata per gli scopi del playground e disponibile nella directory di destinazione dell'ambiente al path:

  /data/govway/pki/CA_icar/ca/certs/ca_icar.cert.pem