Autenticazione implementata mediante IAM per i Servizi Nazionali: test iniziali e sviluppi futuri

Giovanni Zizzi

Workshop CCR, Rimini, 11-15 Giugno 2018

Indice

Istituto Nazionale di Fisica Nucleare

- Questioni aperte da studiare per i Servizi Nazionali
- Per approfondire i temi tecnici abbiamo studiato INDIGO-DataCloud IAM
- Cosa è stato fatto
  - RocketChat (devel)
- Conclusioni e prossimi passi

Necessità dei Servizi Nazionali

Istituto Nazionale di Fisica Nucleare

- Non tutte le applicazione gestite dai Servizi Nazionali hanno connettori SAML o Shibboleth, tali da poter essere utilizzati con l'Idp dell'INFN (e.g. in nostro sistema di cloud storage Pandora), in tale caso si deve ricorrere ad altri tool come il Central Authentication Service (CAS) per effettuare la conversione dei protocolli
  - sarebbero utili i connettori OAuth o OpenID

- Abbiamo anche richieste – lato scientifico – di permettere il login ad utenti esterni all'INFN senza dover registrarli in AAI, di cui vorremmo studiare le implicazioni tecniche

Perché INDIGO IAM

Istituto Nazionale di Fisica Nucleare

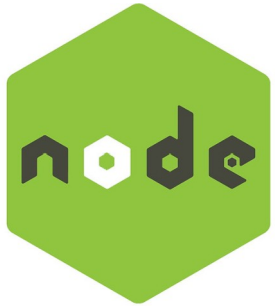
Si è pensato di testare il servizio IAM di INDIGO-DataCloud per avere spunti tecnici da valutare

- Disponibilità di connettori Oauth e OpenID
- Facile aggiungere utenti non INFN
- Possibilità di fare login tramite eduGAIN
- Prossime release:
  - poter specificare metodi di autenticazioni diversi per applicazioni diverse
  - in caso di IAM federato autorizzare solo alcuni enti
  - integrazione con LDAP (per utilizzare gli uid di AAI)

INDIGO - DataCloud

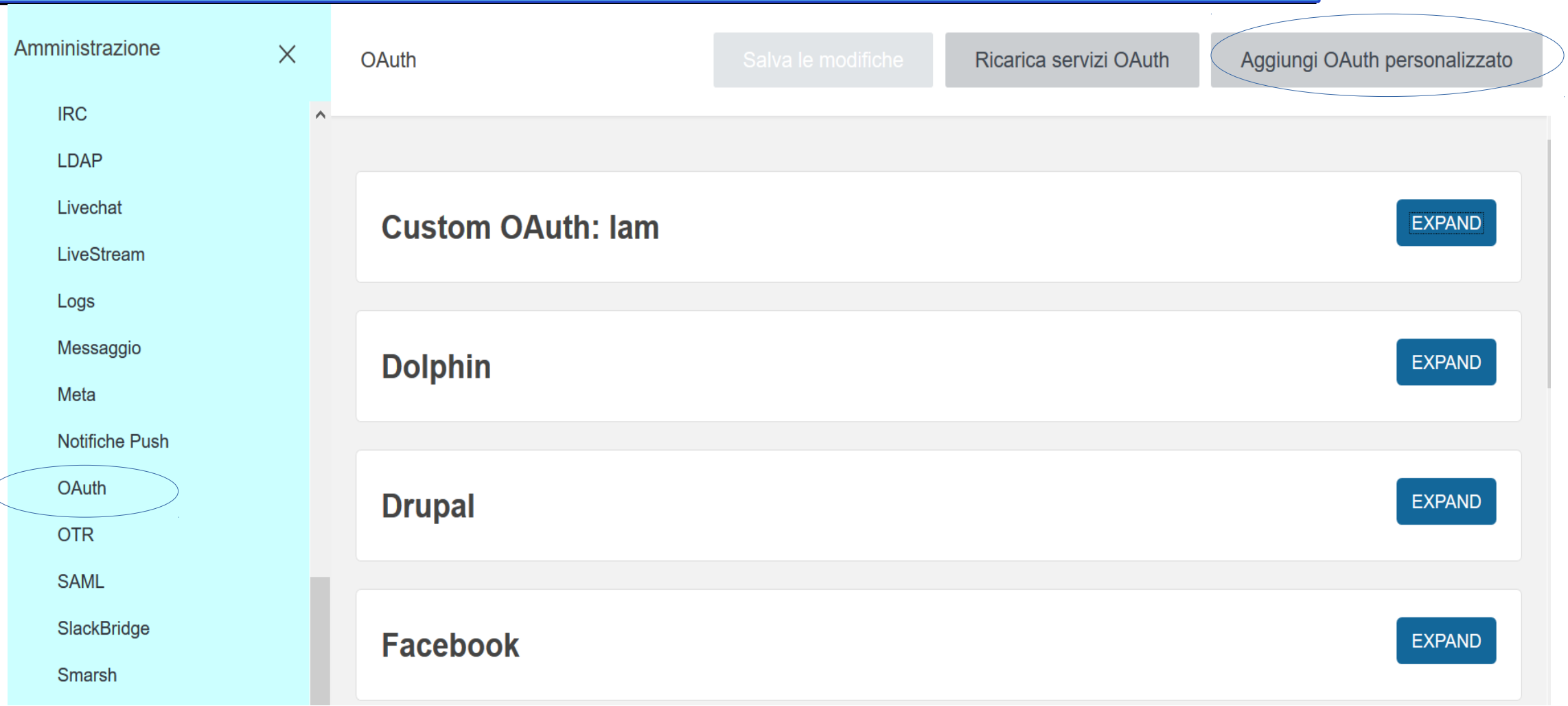
Test: RocketChat

- Opensource
- Basato su WebRTC
- Non necessita di client (basta un browser)
- Ricezione di notifiche da parte dei sistemi di monitoring
- Supporta i canali
- Si può avere un server locale
- Integrabile con l'idp INFN
- https://chat.infn.it



Test con RocketChat 1/3

Istituto Nazionale di Fisica Nucleare



Test con RocketChat 2/3

Istituto Nazionale di Fisica Nucleare

OAuth | Salva le modifiche | Ricarica servizi OAuth | Aggiungi OAuth personalizzato

Custom OAuth: Iam

COLLAPSE

Quando si imposta l'OAuth Provider, è necessario impostare un URL Callback. Usa `https://chat-devel.infn.it/_oauth/iam`.

Abilita: (•) Vero ( ) Falso

URL: https://iam.cnaf.infn.it

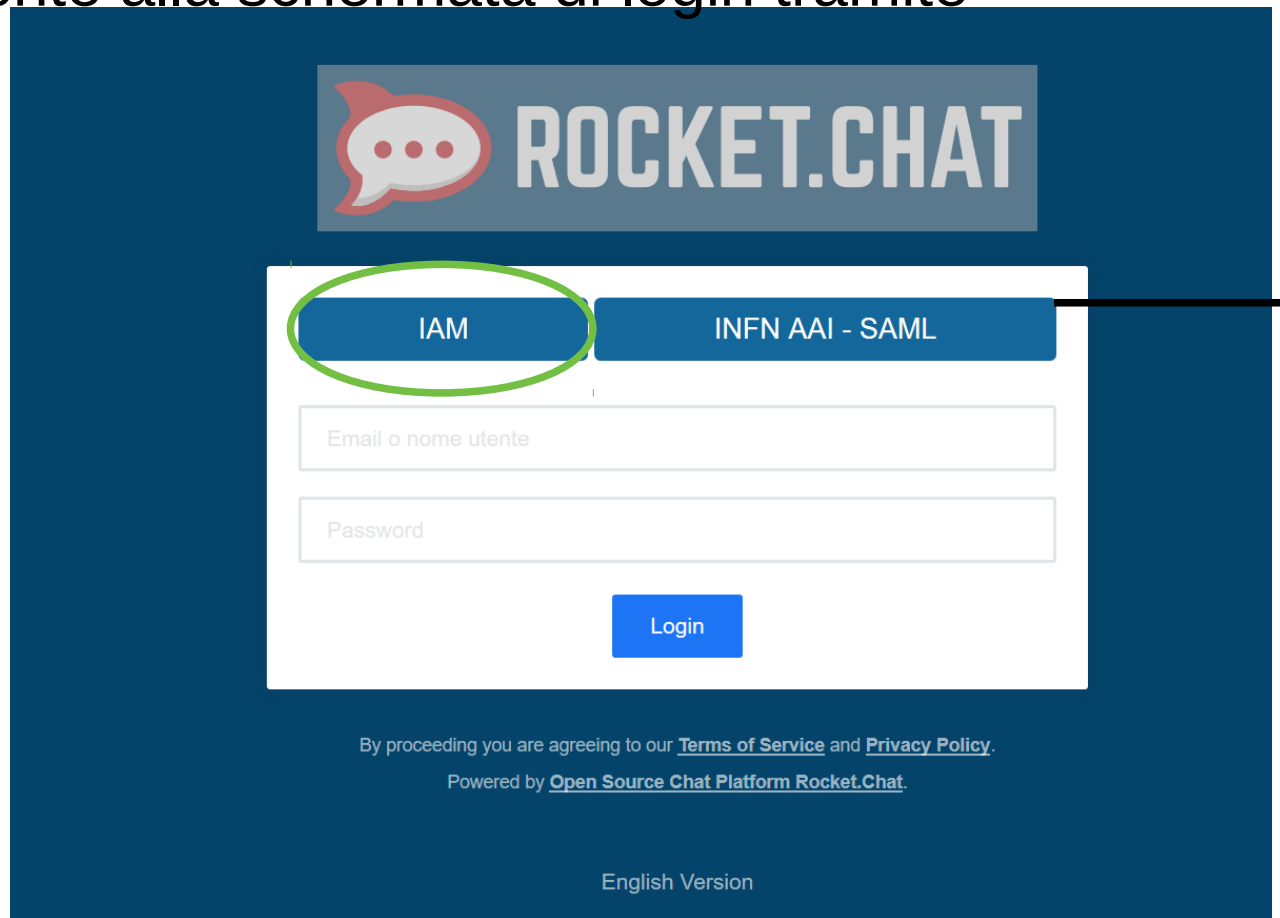
Percorso del token: /token

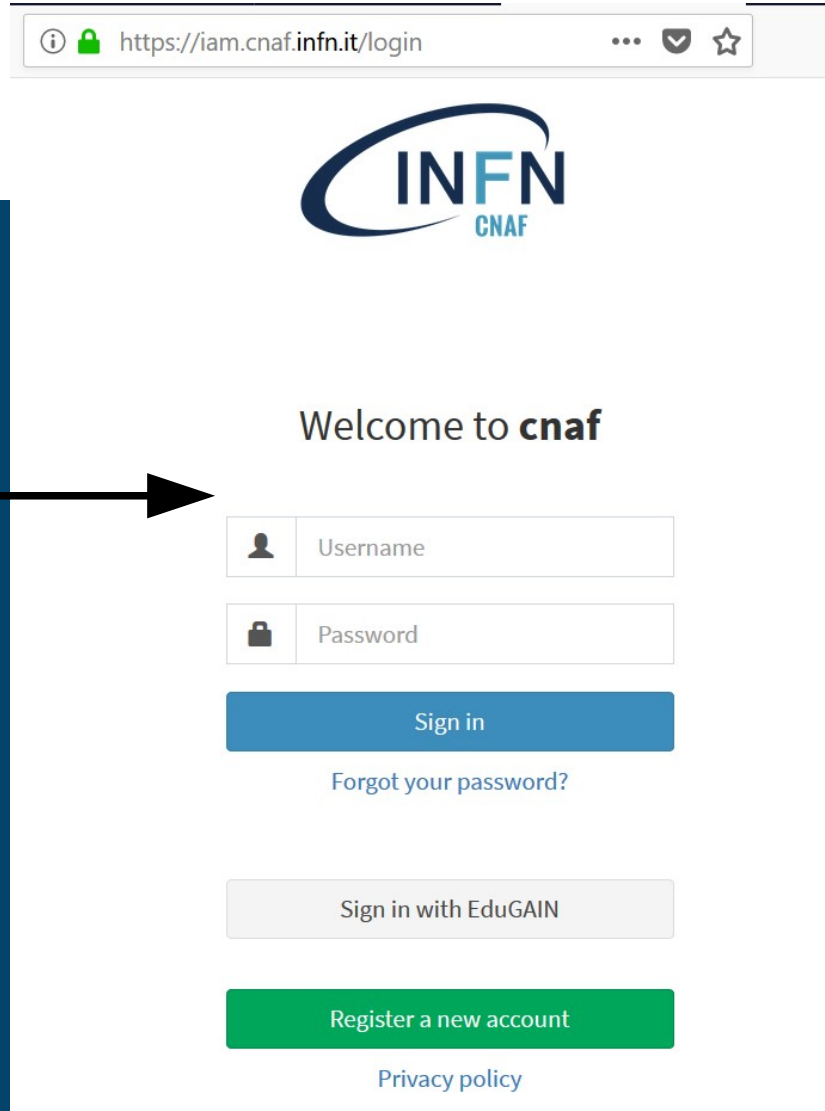
Token inviato tramite: Payload

Test con RocketChat 3/3

Istituto Nazionale di Fisica Nucleare

Nella schermata di login di RochetChat (istanza di test) è presente anche il bottone per il login con IAM, bottone che porta direttamente alla schermata di login tramite iam.cnaf.infn.it





Conclusioni e prossimi passi

Istituto Nazionale di Fisica Nucleare

- Test andato a buon fine subito

  - volevamo testare le funzionalità di RocketChat con un connettore Oauth ed IAM forniva le funzionalità necessarie al testbed

- Valutare se possibile portare RochetChat con questa nuova feature in produzione

- Eventualmente estendere i test ad altri servizi come Pandora o i tool Atlassian (Jira, Confluence etc)

- Valutare assieme al gruppo AAI come integrare le funzionalità testate all’interno dei sistemi INFN

Istituto Nazionale di Fisica Nucleare

Q&A