DOI: 10.26314/GARR-Conf17-proceedings-21

Accesso ai dati astronomici e radioastronomici: Autenticazione e Autorizzazione in INAF

Franco Tinarelli [1], Sonia Zorba[2], Cristina Knapic[2]

[1] INAF Istituto di Radioastronomia, [2] INAF Osservatorio Astronomico di Trieste

Abstract. L'Istituto Nazionale di Astrofisica gestisce i dati prodotti dalle osservazioni di una serie di telescopi e radiotelescopi, i dati vengono archiviati nei DB gestiti dal servizio IA2. Per l'accesso ai dati è stata sviluppata una suite di applicazioni composta da un modulo di autenticazione chiamato RAP (Remote Authentication Portal) che permette l'autenticazione con eduGAIN, Google, Facebook, LinkedIn, X.509 e con account registrati localmente. La suite è completata da connettori per l'interazione con Grouper, un tool Java EE sviluppato da Internet2 per la gestione dei gruppi e delle identità.

Keywords. Autenticazione, Autorizzazione, Grouper, Account-Linking, eduGAIN

Introduzione

L'Istituto Nazionale di Astrofisica gestisce i dati prodotti dalle osservazioni di una serie di telescopi (Asiago, TNG e LBT) e radiotelescopi (Medicina, Noto e SRT). Essi vengono archiviati nei DB gestiti dal servizio IA2. Per l'accesso ai dati è stata sviluppata una suite di applicazioni, in collaborazione tra IRA (Istituto di Radioastronomia) e IA2 (Archivi astronomici Italiani). La suite è composta da un modulo di autenticazione chiamato RAP (Remote Authentication Portal) che permette l'autenticazione con eduGAIN, Google, Facebook, LinkedIn, X.509 e con account registrati localmente. La suite permette inoltre l'account-linking ed ha un connettore per l'interazione con Grouper, un tool Java EE sviluppato da Internet2 per la gestione dei gruppi e delle identità.

1. RAP

RAP (Remote Authentication Portal) è un'applicazione web scritta in PHP ed è completamente indipendente dalle applicazioni che lo usano come autenticatore. L'applicazione chiamante viene registrata in un file che contiene l'indirizzo di call-back per ritornare i dati dell'utente che si è autenticato.

Le principali funzionalità del programma sono:

- autenticazione con diversi metodi;
- account-linking;
- registrazione in MySQL o LDAP;
- editing dei profili registrati.

Ciascuna delle funzionalità può essere attivata o disattivata a piacimento e se disattivata viene nascosta nell'interfaccia utente. Il meccanismo di autenticazione viene reso più sicu-

Conferenza GARR 2017 - The data way to Science - Selected Papers
Venezia, 15-17 novembre 2017 - ISBN: 978-88-905077-7-9

ro tramite l'associazione della richiesta di autenticazione ad un token, inviato all'applicazione chiamante che lo userà come chiave per richiedere le informazioni di autenticazione, con conseguente eliminazione di dati transienti e token immediatamente dopo l'invio.

Fig. 1
RAP: l'interfaccia utente

La registrazione degli utenti può essere effettuata direttamente da RAP su proprie tabelle associate all'applicazione chiamante o remotamente su DB della stessa applicazione. Analogamente all'indirizzo di call-back anche le informazioni specifiche dei DB, vengono associate all'applicazione chiamante in un file di configurazione dei client.
RAP può utilizzare indifferentemente un DB relazionale o LDAP per la registrazione degli utenti sia in locale che in remoto per la funzionalità di account-linking.
L'utilizzo di LDAP permette, attraverso una procedura di gestione, di accreditare gli utenti al login via SSH su workstation che lo utilizzino come sistema di autenticazione. Successivamente la stessa funzionalità può esser estesa all'utilizzo di Kerberos per quelle applicazioni che ne richiedessero l'utilizzo.

RAP è Open Software e può essere adattato e inserito in una propria applicazione, come realizzato dal team di IA2. Le attuali versioni di RAP sono ospitate su server Apache (httpd). Specifici moduli di Apache sono stati configurati per effettuare la validazione dei certificati X.509 e per realizzare l'autenticazione SAML utilizzando uno Shibboleth Service Provider.

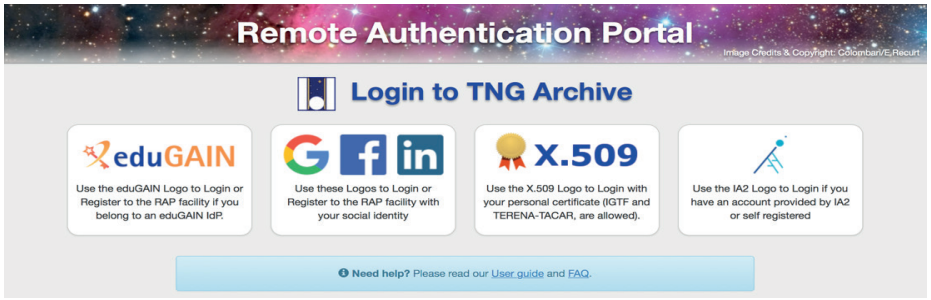

Fig. 2
IA2: Accesso al Data Base del telescopio TNG

2. Account-Linking

L'account-linking è stato realizzato con due possibili implementazioni alternative. La prima prevede, all'atto della registrazione, l'invio via e-mail di un codice univoco che identifica l'utente. Se l'utente desidera unire due suoi account può quindi inserire questi codici all'interno dell'interfaccia di RAP. La seconda implementazione prevede che l'utente effettui un login su una pagina di gestione del suo account e ricerchi altri utenti registrati ai quali inviare una "richiesta di join". L'utente target della richiesta riceverà un messaggio e-mail con un link di conferma, contenente un token univoco che identifica la richiesta di join. L'account-linking avviene solo se l'utente apre il link e clicca su un pulsante di conferma.

3. Grouper

Grouper è stato scelto da IA2 per organizzare le autorizzazioni d'accesso alle risorse fornite tramite i propri servizi in quanto strumento maturo e già utilizzato con successo da altre organizzazioni che operano nell'ambito della ricerca. Esso inoltre ha il vantaggio di fornire un'interfaccia web che consente di delegare agli utenti alcune delle operazioni di amministrazione dei gruppi. Grouper non è nativamente in grado di gestire l'account linking, e la relativa autorizzazione per questo è stato necessario personalizzarne alcune componenti, in modo da renderlo compatibile con il modello dati utilizzato da RAP per rappresentare gli utenti.

Grouper memorizza le informazioni relative a gruppi e permessi all'interno di un suo database, detto registry. L'installazione di Grouper utilizzata da IA2 si appoggia attualmente su un database MySQL, tuttavia, poiché Grouper è basato sulla tecnologia ORM Hibernate, si potrebbero utilizzare indistintamente molte altre tipologie di RDBMS.
Grouper è stato installato su server Tomcat.

4. Il Connettore

La suite è completata dal connettore tra RAP e Grouper, sviluppato dal team IA2, che permette l'autenticazione su Grouper tramite l'utilizzo di un sistema multi protocollo che non era nativamente supportato da Grouper.

Grouper con la modifica apportata alla sua nativa basic authentication, importa da RAP le diverse identità possedute dall'utente che si è autenticato come un'unica, per gestire i gruppi di cui è amministratore. RAP espone queste informazioni attraverso un servizio REST protetto da password.

Due moduli di Grouper sono stati personalizzati per poter dialogare con questo web service: il Source Adapter e l'Authentication Filter. La creazione di questi componenti custom avviene estendendo delle classi Java, modificando i file XML della configurazione di Grouper e infine ricompilando Grouper.

Nel gergo di Grouper un Source Adapter è un componente che può essere interrogato per ricavare informazioni riguardo un insieme di utenti. Ogni installazione di Grouper può avere uno o più Source Adapter. I Source Adapter messi a disposizione da Grouper permettono di interrogare LDAP o database relazionali. Il Source Adapter scritto da IA2 interroga invece il servizio REST di RAP, che restituisce le informazioni in formato JSON.

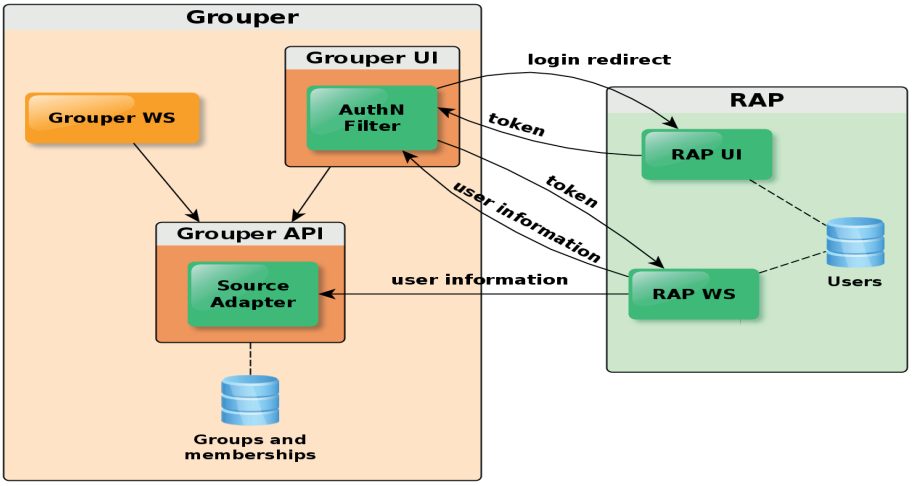

Fig. 3
RAP + Grouper: schema funzionale

In questo modo un insieme di identità sulle quali è stata effettuata una procedura di account-linking viene interpretato da Grouper come un'entità atomica. Nella Grouper UI, a fianco del nome di ogni utente vengono elencate le sue diverse identità.

L'Authentication Filter è un servlet filter che va configurato nel deployment descriptor della Grouper UI. Verifica la presenza di un utente associato al cookie di sessione, in caso contrario effettua un redirect su RAP e si autentica allo stesso modo degli altri client.

5. Conclusioni

L'implementazione di un meccanismo di autenticazione multi protocollo (SAML2.0, OAuth2, X.509), la registrazione automatica su RDBMS, LDAP e Kerberos, l'account-linking delle identità e la gestione di gruppi di utenti permette oggi l'accesso ai dati prodotti dagli strumenti osservativi di INAF e permetterà in futuro l'accesso alla impressionante mole di dati prodotta dal radiotelescopio SKA.

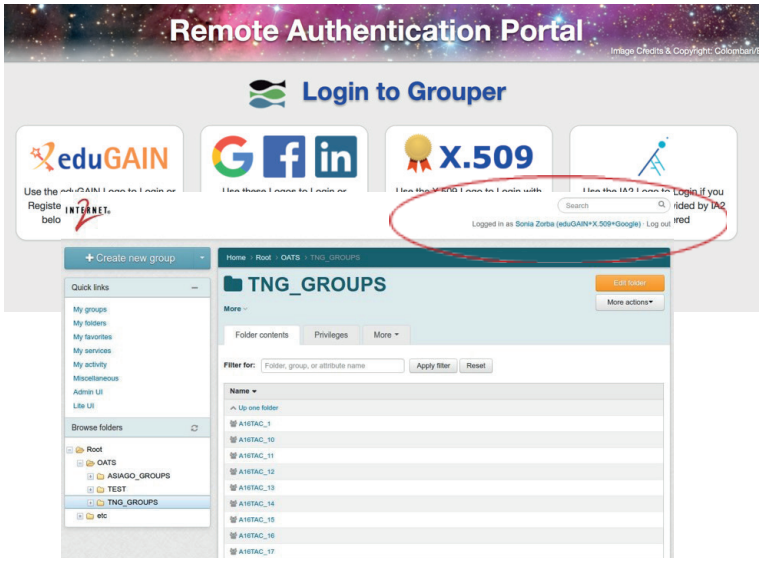

Fig. 4
Login in Grouper utilizzando RAP

Riferimenti bibliografici

F. Pasian, S. Bertocco, A. Bignamini, A. Costa, G. Jerse, C. Knapic, M. Molinaro, E. Sciacca, G. Taffoni, F. Tinarelli, F. Vitello, S. Zorba (2017), "Authentication & Authorization Technology Benchmarking Report", Asterics Project

Autori

Franco Tinarelli f.tinarelli@ira.inaf.it

System e Network Manager dell'Istituto di Radioastronomia dal 1988. Ha sviluppato software per la schedula delle osservazioni VLBI. Partecipa al work package SKA TM per il quale ha sviluppato il primo prototipo di A&A e il software RAP.

Sonia Zorba zorba@oats.inaf.it

Dal 2015 lavora come full-stack web developer presso il Centro Italiano Archivi Astronomici (IA2). Sviluppa interfacce per l'accesso ai dati e tool di supporto, sia ad uso interno che nell'ambito del Virtual Observatory.

Cristina Knapic knapic@oats.inaf.it

Tecnologo presso INAF-OATs, si occupa degli archivi astronomici italiani (IA2) dal 2008. Ha sviluppato sistemi di archiviazione distribuita, interfacce e servizi web compatibili con il Virtual Observatory. Attualmente si occupa di vari work packages sia di SKA che dei SKA Regional Centers partecipando al progetto AENEAS.