

Progetto Cloud Padovana

Integrazione Horizon-INFN AAI

Paolo Andreetto
Eric Frizziero

Bologna 20 Dicembre 2013

Scopi

- Integrare sistemi di single sign on con Openstack Dashboard (Horizon)
- Espandere Openstack Dashboard per supportare la gestione delle registrazioni di utenti
- Minimo intervento nel codice di Openstack (adattamento rapido alle future versioni)

Autenticazione

- Protocollo Shibboleth:
 - INFN AAI
 - Università di Padova
 - Federazione IDEM (da discutere)
- Username & password
- Protocollo OpenID (non a breve)
 - Google, Yahoo, etc.

Autorizzazione

- Completamente basata su Keystone
- Gestione utenti, gruppi, ruoli e policy a carico dell'amministratore della cloud o del progetto
- Nessun utente auto-generato
- Richiesta registrazione e approvazione dell'utente

Dettagli dell'implementazione

➤ Su dashboard

- Autenticazione dell'utente con modulo Apache (mod_shib, mod_auth_openid)
- Estensione della plugin di autenticazione per django (Keystone client)

➤ Su Keystone

- Crea una plugin di autenticazione per Keystone
- Usato token ad-hoc per comunicazioni fra Horizon e Keystone

Registrazione utenti

- Ogni utente, anche se autenticato via AAI, deve richiedere la registrazione dell'utente
- Viene sempre creato un utente locale, utilizzato per accessi con command line tool
- Un utente richiede l'inserimento in uno o piu' project (tenant)
- Un utente puo' richiedere la creazione di un nuovo tenant
- Un utente puo' chiedere di associare piu' Identity Provider al suo account.
- Ogni operazione deve essere gestibile con la dashboard

Stato dei lavori

- Supporto per INFN-AAI completato
- Test con altri IdP basati su shibboleth da fare
- Integrazione di OpenID/OAuth ancora da definire
- Estensione di Horizon stimata al 25%
- Pacchetti RPM disponibili (allineati con Havana su SL6)

Riferimenti

- Sorgenti disponibili su github
<https://github.com/italiangrid/openstack-security-integrations>
- Pacchetti RPM disponibili su repository locale (non accessibile via web)
- Guida installazione su Google Docs (link a richiesta), attualmente non aggiornata