Authentication e authorization federate nelle cloud

Estensioni a Shibboleth per l'applicazione in conesti di cloud computing

Andrea Biancini[1], Luca Prete[2] e Simon Vocella[2]
[1]*INFN – Sezione di Milano Bicocca*
[2]*Consortium GARR*
andrea.biancini@mib.infn.it, {luca.prete, simon.vocella}@garr.it

1 CONTESTO CLOUD E FEDERAZIONI DI IDENTITÀ

Con il termine cloud computing si fa riferimento all'accesso a risorse informatiche (capacità computazionale, storage, applicazioni, ecc.) on demand. Il paradigma cloud prevede la definizione di interfacce di controllo delle risorse e protocolli di accesso solitamente tramite Internet. Nei modelli architetturali tradizionali i dati il software e la potenza di elaborazione sono tutti mantenute localmente sul computer dell'utente. Nel modello cloud la piattaforma dell'utente ha un ruolo di terminale semplificato per il controllo e l'accesso ai dati, laddove la potenza di elaborazione e lo storage reale dei dati sono delegati al provider di servizio. Grazie alla virtualizzazione, i sistemi cloud fanno della trasparenza la loro caratteristica fondamentale. Per trasparenza s'intende la capacità di astrarre dallo strato fisico, mascherando i dettagli tecnici non rilevanti per l'utente. Attraverso questi meccanismi è possibile disaccoppiare la gestione delle risorse fisiche dal loro utilizzo. Questo permette di concentrare le risorse fisiche, creare economie di scala e liberare gli utenti dalle complessità tecnologiche non necessarie. In questo senso il concetto di cloud si sposa molto bene con quello degli schemi di federazione di risorse, tipici del mondo della ricerca.

GARR promuove un approccio federato alla gestione delle identità degli utenti in collaborazione con le istituzioni che afferiscono alla Federazione IDEM (Federazione IDEM, 2012). In particolare la Federazione IDEM definisce il formalismo per creare una federazione d'identità comune in grado di autenticare e autorizzare l'accesso alle risorse e ai servizi esposti sul web. Una soluzione cloud per l'università e la ricerca dovrebbe porsi l'obiettivo di proseguire ed estendere i modelli di federazione esistenti, sfruttando al meglio i benefici offerti dalle federazioni d'identità. Nell'ambito storage cloud, GARR ha avviato un'attività sperimentale per la realizzazione di un servizio, al momento disponibile solo per uso interno, chiamato GARRbox (Valli et al., 2012). GARRbox fornisce agli utenti spazio di storage on-demand utilizzando un approccio federato sia tra le risorse fisiche sia tra gli utenti. Il sistema offre all'utente diverse interfacce, tra le quali un'interfaccia web, l'accesso ai dati tramite il protocollo S3 di Amazon e, a breve, un'interfaccia WebDAV e un client simile a quello sviluppato da Dropbox per la sincronizzazione dei dati.

2 LIMITAZIONI ATTUALI

Dall'esperienza maturata realizzando un servizio di storage cloud è emersa la constatazione di alcune limitazioni delle tecnologie su cui IDEM si poggia nel caso specifico del supporto alle soluzioni cloud. In particolare IDEM si poggia sull'implementazine di SAML 2 offerta da Shibboleth (Morgan et al., 2004), una delle soluzioni d'identità federata maggiormente utilizzate.

Per poter sfruttare al meglio i meccanismi di autorizzazione esistenti applicandoli alle cloud è necessario risolvere due aspetti:

1. Cloud per definizione è multiprotocollo, quindi non accessibile unicamente da web browser. In questo caso l'approccio standard offerto da Shibboleth può essere limitante e poco flessibile per applicazioni mobile e client.
2. In ambito cloud sono emersi nuovi protocolli che sono diventati standard de facto. Alcuni di essi descrivono e disciplinano gli aspetti di autenticazione e autorizzazione. I meccanismi federati di Shibboleth devono offrire interfacce compatibili con questi nuovi standard.

Questi aspetti verrano discussi dettagliatamente durante la presentazione, in quanto problemi aperti. Sino a oggi la comunità ha cercato di realizzare autenticazione e autorizzazione Shibboleth per applicazioni non web. Tuttavia le soluzioni disponibili, come Moonshot (Howlett and Hartman, 2005), sono complesse e difficilmente integrabili con quanto esistente. Queste piattaforme non sono idonee a risolvere il secondo problema: non supportano i protocolli di autenticazione proposti dalle cloud. In aggiunta, non sembrano offrire un modello di interoperabilità semplice rispetto alle federazioni che usano Shibboleth, il quale basa l'autorizzazione su coppie username-password o sull'uso di certificati.

3 SOLUZIONI PROPOSTE

L'intervento discuterà come siano state realizzate tre estensioni a Shibboleth che risolvono i problemi tra AAI e cloud federate. Le estensioni realizzate sono le seguenti:

1. **Autenticazione e autorizzazione per applicazioni non web-based** (Java e Python).
   Permette di sfruttare i meccanismi di autenticazione tipici delle realtà federate anche in applicazioni che non richiedono l'uso di un browser internet. I meccanismi di autenticazione di Shibboleth sono stati implementati in una libreria che comunica con l'SP e l'IdP, utilizzando HTTPS e Basic-Authentication.

La libreria è stata sviluppata sia per Java, come modulo JAAS (Java, 2002, sia per Python: a oggi i linguaggi principali per realizzare applicazioni utente di alto livello. Attraverso questa estensione è possibile autenticare gli utenti utilizzando gli schemi federati SP/IdP di Shibboleth da applicazioni desktop tradizionali. Inoltre la soluzione garantisce la Single-Sign-On accedendo a risorse web dalle applicazioni che integrano la API.

2. **Autenticazione e autorizzazione di sistemi Linux** (tramite PAM e NSS).
   Questa estensione sfrutta un meccanismo simile a quello descritto nel punto precedente. Anch'esso è bastato su HTTPS e Basic authentication e permette l'autenticazione di utenti in sistemi Linux. Per realizzare questa estensione sono stati implementati dei moduli specifici per PAM (Morgan and Kukuk, 1996) e NSS (The Free Software Foundation, 1987), i meccanismi standard di user authentication e di naming service di Linux. Grazie ai moduli sviluppati un sistema Linux permette l'accesso a utenti definiti su Shibboleth. Al login, l'SP e l'IdP sono contattati per autenticare l'utente e per ottenere i dati necessari alle logiche di autorizzazione.
   Tramite questa estensione anche diversi applicativi Linux, come SSH, NFS o Apache, ereditano la possibilità di autenticare gli utenti attraverso Shibboleth. Molte applicazioni native realizzate su Linux, infatti, delegano i compiti di autenticazione al sistema operativo attraverso i moduli PAM. Grazie all'estensione, il sistema e le applicazioni riconoscono gli utenti della federazione in modo trasparente e senza nessuna ulteriore modifica.

3. **Autenticazione e autorizzazione tramite lo schema di sicurezza del protocollo S3**.
   Questa estensione permette di effettuare l'autenticazione Shibboleth di utenti che utilizzino il protocollo S3 (Amazon S3, 2012) per la gestione dei dati. Il protocollo S3 è stato sviluppato da Amazon per il proprio servizio di storage cloud ed è diventato lo standard de facto più utilizzato nelle cloud, commerciali e Open Source.
   L'autenticazione di S3 non avviene tramite l'uso di username e password ma attraverso la condivisione di un segreto tra l'utente e l'applicazione server. A ogni richiesta il client cripta una stringa con una chiave segreta condivisa con il server che non viene mai trasmessa o distribuita. Il server, eseguendo la stessa operazione, confronta i risultati della cifratura autenticando l'utente in caso di corrispondenza delle informazioni. Per integrare tale modello di autenticazione in Shibboleth è stato necessario sviluppare un nuovo LoginHandler per l'IdP. Il modulo perme di verificare le credenziali utente utilizzando il segreto condiviso nel modo normato dal protocollo.

4 CONCLUSIONI E SVILUPPI FUTURI

L'intervento mostrerà come i risultati ottenuti tramite le estensioni arricchiscano le funzionalità di GARRbox, garantendo l'accesso alle risorse cloud sia tramite il web sia attraverso protocolli di l'accesso ai dati (quali ad esempio CIFS e WebDAV, attualmente in sperimentazione). Si discuteranno inoltre le difficoltà incontrate nell'implementazione degli schemi autorizzativi per Shibboleth del protocollo S3.
Il servizio di storage, come primo esempio di soluzione cloud, sfrutta ed estende tutti i meccanismi e le prescrizioni di IDEM. Il lavoro svolto per le estensioni rappresenta un primo passo verso meccanismi più complesso di estensione delle federazioni di identità verso i modelli e le tecnologie cloud.

Sebbene il lavoro descritto risolva le esigenze specifiche del progetto GARRbox, che ha dato lo spunto all'attività, sono necessarie ulteriori indagini per raggiungere un livello di servizio migliore, in particolare:

- **Supporto a WAYF**. Le estensioni proposte non supportano il protocollo WAYF, per contattare l'IdP dell'ente di affiliazione dell'utente a seguito della verifica della sua identità. Occorre una nuova estensione per effettuare il discovery dei provider di identità utilizzando i profili descritti da SAML 2.
- **Gestione multi-dominio per l'autenticazione in sistemi Linux**. Qualora l'estensione per l'autenticazione utente su macchine Linux dovesse essere utilizzata in contesti federati di grandi dimensioni, sarebbe necessario risolvere un problema di mappatura degli utenti. I sistemi Linux associano a ogni utente uno user-id numerico univoco. Gli id utente utilizzati dagli IdP dovrebbero essere associabili bi-univocamente agli user-id dei sistemi.
- **Accounting**. L'attrattività di accesso delle risorse tramite il modello cloud è legata in gran parte a modelli di accounting semplici e chiari. Occorre capire come coniugare gli strumenti di monitoring dei singoli servizi cloud con quanto offerto dalle federazioni di identità, ad esempio come gestire in modo federato l'uso di risorse virtuali fino all'esaurimento delle disponibilità assegnate ad un utente.

RIFERIMENTI

Amazon S3 (2012). *Simple storage service protocol*. http://aws.amazon.com/s3.

Federazione IDEM (2012). *Infrastruttura di Autenticazione e Autorizzazione della rete GARR*. https://www.idem.garr.it/.

The Free Software Foundation (1987). *Name Service Switch*. http://www.gnu.org/.

Howlett, J. and Hartman, S. (2005). *Project Moonshot*. Tech. rep. 07

Java (2002). *Java Authentication and Authorization Service*. http://java.sun.com/products/jaas/.

Morgan, A. G. and Kukuk, T. (1996). The linux-pam system administrators'guide. http://kernel.org/.

Morgan, R. L., Cantor, S., Carmody, S., Hoehn, W., and Klingenstein, K. (2004). Federated security: The shibboleth approach. *EDUCAUSE Quarterly*, 27(4):12–17.

Valli, C., Biancini, A., Reale, M., Farina, F., Vocella, S., Galeazzi, F. (2012). GARR Cloud Storage GARRBox. *Proceedings of TICAL 2012*.