Apache Syncope OpenSource IdM

Gestione delle identità in contesti aziendali

Versione 1.3 / 2012-07-26

Indice

Indice delle figure

1 Sintesi

L'identity Management (o IdM), rappresenta il risultato del lavoro congiunto del business e dell'IT per gestire I dati utenti su sistemi e applicazioni. IdM vuol dire considerare attributi, ruoli, risorse e autorizzazioni nel tentativo di rispondere in modo soddisfacente alle domande che più assillano gli amministratori di sistema:

Chi ha accesso a cosa? Quando? Come? Perché?

All'interno di una organizzazione una soluzione IdM si occupa fondamentalmente di:

- ✔ offrire le risorse e le informazioni giuste, al momento giusto, a chi ne ha i diritti;
- ✔ dare la possibilità di attivare processi di delega e approvazione delle autorizzazioni;
- ✔ proteggere l'infrastruttura IT da possibili furti di informazione;
- ✔ aiutare l'organizzazione a rispettare le norme vigenti;
- ✔ garantire il rispetto della privacy sui dati dei clienti, partner e dipendenti;
- ✔ semplificare la creazione e l'automatizzazione delle politiche di business, in modo tale da rafforzare la sicurezza, ridurre i costi di gestione e aumentare la produttività.

Viceversa, quando una soluzione IdM non viene implementata, un'azienda può facilmente trovarsi in diverse situazioni in cui, per esempio, nuovi assunti o personale promosso si trovino ad aspettare, senza la possibilità di effettuare il proprio lavoro, in attesa dell'autorizzazione all'uso degli strumenti o delle risorse necessari allo svolgimento delle proprie mansioni; oppure ex dipendenti possano continuare ad avere l'accesso, per giorni o addirittura settimane, alle risorse e alle informazioni di cui godevano prima di aver lasciato l'azienda. Inoltre, i processi di conformità a leggi o regolamenti vigenti, non possono essere effettuati attraverso azioni programmate, verificabili e accurate su tutte le identità e risorse gestite all'interno dell'organizzazione stessa.

Questo documento introduce un nuovo approccio per sviluppare e manutenere un'infrastruttura di Identity Management, basando il lavoro sull'uso di un prodotto di nuova concezione, sviluppato con licenza Open Source e denominato Apache Syncope. Nel seguito si esaminerà cosa viene richiesto oggi ad una infrastruttura per la gestione delle identità e si introdurranno le specifiche tecniche e architetturali di Apache Syncope.

2 Requisiti di una infrastruttura di Identity

La costruzione di un'infrastruttura di Identity management spesso significa curare due aspetti distinti, ma strettamente correlati, nell'IT management: la gestione delle identità e la gestione degli accessi; per questa ragione il termine più indicato in questi contesti è IAM (Identity and Access Management).

Una soluzione completa di IAM prevede:

- ✔ gestione del ciclo di vita delle identità (basato su workflow di provisioning)
- ✔ meta-directory
- ✔ controllo degli accessi
- ✔ gestione dei ruoli
- ✔ funzionalità self-service

Un aspetto chiave da sottolineare è che una soluzione IAM effettua il proprio lavoro facendo leva – anziché sostituire – sui processi di business, i ruoli di questi e sugli investimenti tecnologici.

Consideriamo la situazione descritta nella Figura 1: un tipico scenario aziendale in cui differenti gruppi di utenti (partner, impiegati, clienti..) hanno diverse strade per accedere ai vari servizi e applicazioni messe a disposizione dall'azienda. Ognuno di questi "sistemi" ha un proprio store e, di conseguenza, ognuno degli utenti precedentemente visti avrà una propria credenziale di accesso e un proprio profilo su quel sistema. Il processo autorizzativo, in questo caso, è completamente indipendente e delegato ad ogni singola applicazione.

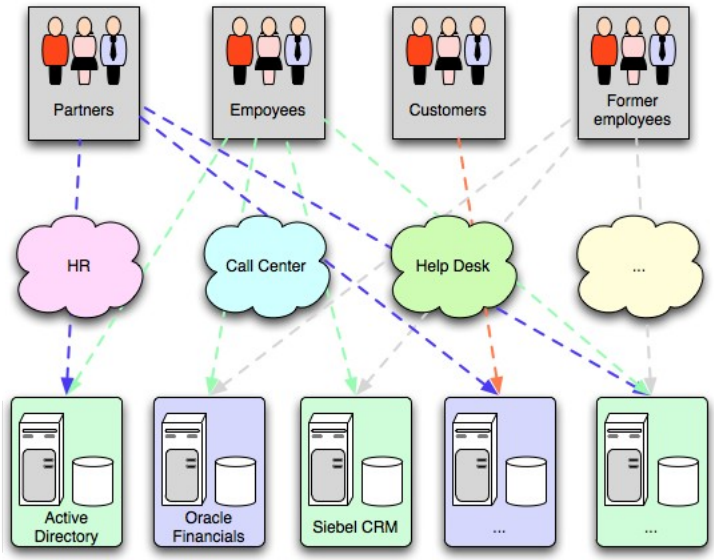

Figura 1: Organizzazione senza IAM

Attraverso l'introduzione di una soluzione completa di Identity and Access Management, la situazione vista precedentemente si trasforma completamente; come visibile in Figura 2:

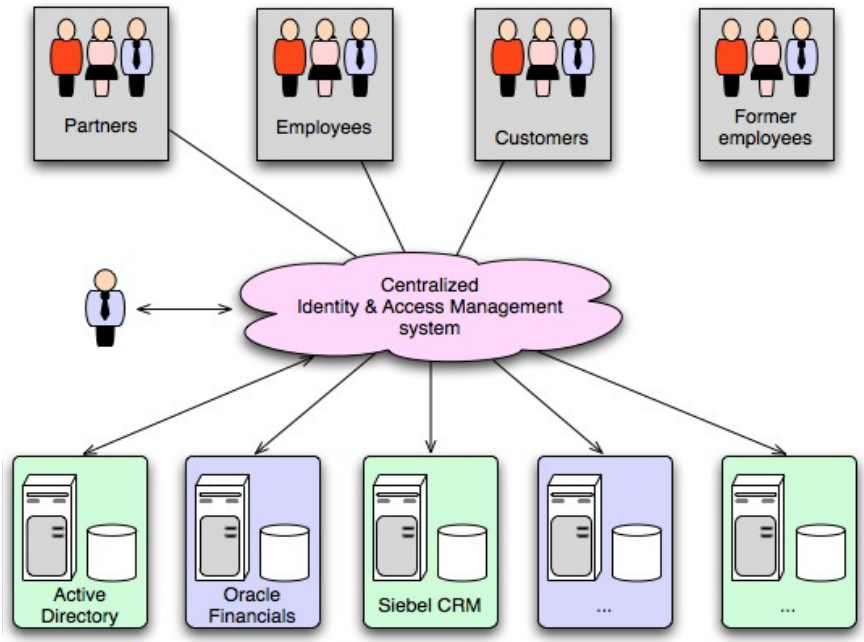

Figura 2: Organizzazione con IAM

il sistema centralizzato di IAM si prende in carico tutti gli aspetti legati alla sicurezza delle comunicazioni tra gli utenti e le applicazioni, sincronizza le informazioni tra i diversi sistemi, si occupa dell'auditing e del logging di tutti le transazioni richieste con diversi livelli di configurazione.

2.1 Gestione del ciclo di vita delle identità

Come suggerito da quanto descritto precedentemente, i concetti fondamentali alla base di una soluzione IAM di successo sono i processi e le tecnologie usate per la cancellazione, la creazione e la gestione degli account, la modifica dei diritti d'accesso alle risorse e il tracciamento della conformità delle policy, il tutto attraverso una o più delle seguenti operazioni:

- ✔ Provisioning/de-provisioning
  L'automatizzazione della creazione e della scadenza di account, su sistemi diversi, basate sui dati provenienti da fonti autoritative; lo scopo di queste operazioni è minimizzare l'onere amministrativo dovuto all'esecuzione manuale delle predette operazioni, diminuendo i rischi di sicurezza grazie all'applicazione di policy in modo automatico.
- ✔ Workflow
  L'automatizzazione dei passi all'interno del processo di gestione del ciclo di vita dell'identità, compresi notifica, approvazione, escalation e creazione di dati di audit.

- ✔ Amministrazione
  La facilitazione della gestione delle identità, di solito attraverso l'uso di una console di amministrazione. L'uso di questa interfcaccia grafica è efficace per la delega delle attività amministrative e la possibilità di creare, in congiunzione con i workflow, interfacce self-service utilizzabili dagli utenti stessi.
- ✔ Credential management
  Password, certificati e smart card.
- ✔ Role management
  Facilitare, negli ambienti in cui è usato anche un sistema di controllo degli accessi basato su ruoli, la gestione di questi ultimi attraverso la loro creazione e manutenzione, comprendendo la definizione di nuovi ruoli o loro interazioni.

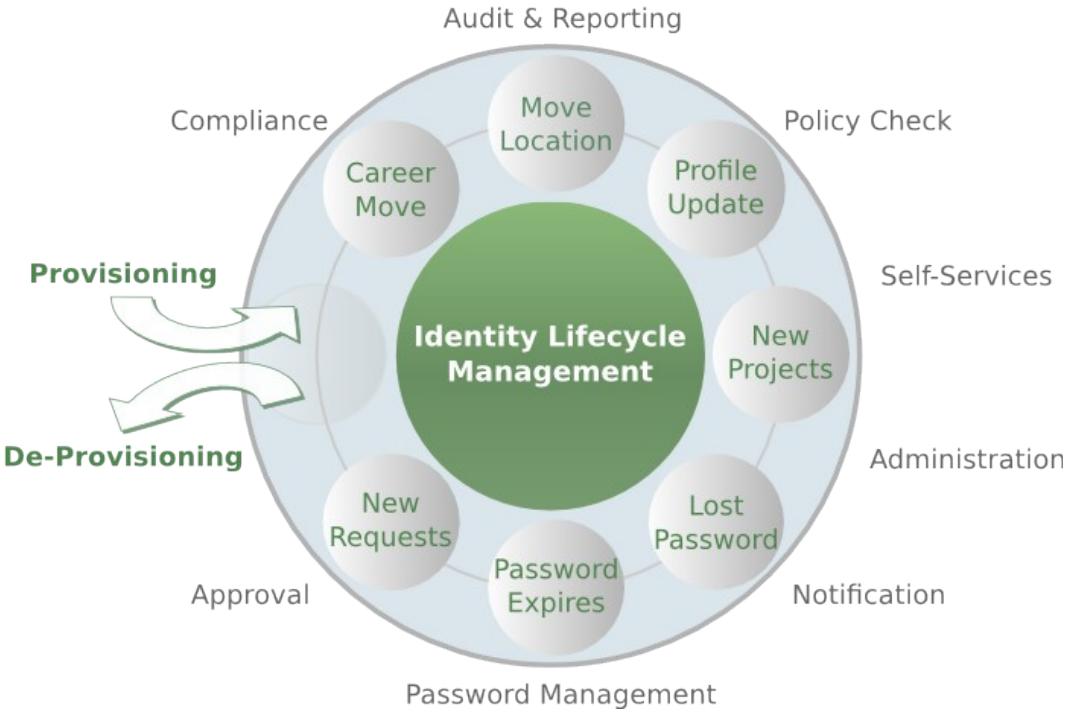

Figura 3: Ciclo di vita delle identità

3 Apache Syncope, Open Source IdM

Apache Syncope[1] è una soluzione IdM, implementata con tecnologia J2EE e rilasciata sotto licenza Apache 2.0[2].

Apache Syncope implementa molto di quanto sopra espresso in termini di pura gestione delle identità. Per i casi in cui sia necessario mettere in campo anche funzionalità di gestione degli accessi, Apache Syncope si adatta perfettamente all'ambiente configurandosi con diverse soluzioni di access management Open Source, come Apache Shiro[3], OpenAM[4], CAS[5] o JOSSO[6].

Disclaimer: Apache Syncope is an effort undergoing incubation at The Apache Software Foundation (ASF), sponsored by the Apache Incubator PMC. Incubation is required of all newly accepted projects until a further review indicates that the infrastructure, communications, and decision making process have stabilized in a manner consistent with other successful ASF projects. While incubation status is not necessarily a reflection of the completeness or stability of the code, it does indicate that the project has yet to be fully endorsed by the ASF.

3.1 Perché Open Source

L'Identity Management è un area middleware in cui solo vendor commerciali (quali Sun Microsystems, Oracle, Novell, IBM e altri) sono stati finora in grado di fornire strumenti adeguati alle organizzazioni. Tali strumenti proprietari sono stati spesso realizzati tramite l'adozione di sistemi FOSS quali server LDAP (OpenLDAP, OpenDS), DBMS (MySQL, PostgreSQL) e webservice.

Inoltre, i costi di licenza considerevolmente alti di questi prodotti sono stati finora una barriera per le organizzazioni di piccola/media dimensione o no-profit che avrebbero altrimenti beneficiato dall'utilizzo di sistemi di identity management all'interno della loro infrastruttura.

3.2 Architettura di alto livello

Ad alto livello, i componenti dell'architettura di Apache Syncope possono essere riassunti dalla Figura 4. Apache Syncope è composto da due principali sottosistemi:

1. core
   L'applicazione web che implementa le principali caratteristiche di IdM; essa offre un'interfaccia RESTful per le chiamate applicative, implementa il provisioning attraverso il suo motore di workflow e lo strato di propagazione, infine gestisce la persistenza dei dati.

1 http://incubator.apache.org/syncope/
2 http://www.apache.org/licenses/LICENSE-2.0.html
3 http://shiro.apache.org/
4 http://forgerock.com/openam.html
5 http://www.jasig.org/cas/
6 http://www.josso.org/

2. Console di amministrazione
   L'interfaccia web di gestione per configurare e amministrare il core di Syncope. Come ogni altra applicazione esterna, la console comunica con il core attraverso chiamate REST.

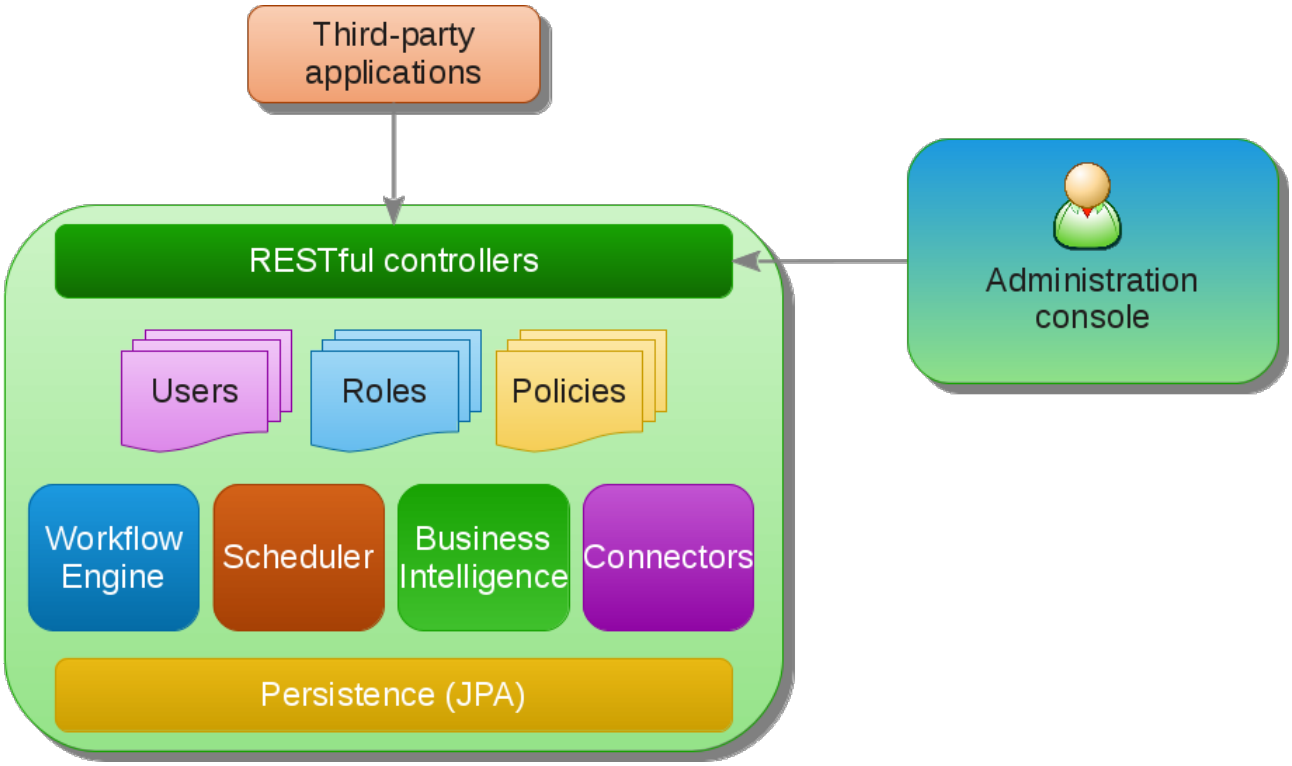

Figura 4: Architettura di alto livello

3.2.1 Business Intelligence

Questo componente centrale nell'architettura di apache Syncope si occupa dell'orchestrazione dell'intero flusso di dati in tutto il sistema. Viene attivato dalle chiamate RESTful, processa i dati insieme del workflow definito, si occupa della persistenza e della propagazione e della sincronizzazione delle risorse configurate dove necessario.

3.2.2 RESTful controllers

I controller RESTful si occupano della comunicazione con il mondo esterno. Implementati attraverso l'uso di Spring REST e MVC, il controller scambia dati sia in formato JSON sia XML.

3.2.3 Workflow engine

Il motore di workflow è un aspetto totalmente personalizzabile di Apache Syncope: questo permette di scegliere di volta in volta se utilizzare una delle implementazioni fornite o se costruirne una nuova personalizzata.

L'implementazione di default è basata su Activiti BPM, implementazione Open Source di riferimento che supporta la il formato XML per un descrittore del ciclo di vita degli utenti. Questo aspetto rende l'intero sistema estremamente flessibile ed in grado di adattarsi a situazioni diverse.

L'implementazione di default fornisce inoltre notifiche, approvazioni e gestione delle richieste utente.

3.2.4 Scheduler

Diverse operazioni sono eseguite da Apache Syncope senza essere direttamente invocate da chiamate RESTful; in questo caso Quartz, implementazione Open Source di riferimento, si occupa di lanciare e gestire i task richiesti.

3.2.5 Persistence (JPA)

Tutti i dati usati da Syncope (utenti, ruoli, attributi, risorse, ...) sono gestiti con l'approccio standard JPA 2.0 e mantenuti nel database sottostante.

Questo approccio fa sì che Apache Syncope sia utilizzabile con successo su molti DBMS senza alcuna modifica al codice sorgente. Al momento Apache Syncope supporta MySQL, PostgreSQL, H2, MS SQL Server e Oracle DB.

3.2.6 Connectors

Il livello dei connettori è implementato tramite ConnId; ConnId è stato ideato per separare l'implementazione di un'applicazione dalla dipendenza al sistema con il quale queste devono connettersi.

ConnId è la continuazione degli Identity connectors, un progetto che è stato parte integrante dell'IdM di Sun, leader del mercato fino all'acquisizione da parte di Oracle, anche se sono stati rilasciati come progetto indipendente ed Open Source. Questa scelta ha reso il livello dei connettori particolarmente affidabile in quanto molti i connettori forniti dal framework sono ormai largamente testati. Successivamente, dal progetto originale è stato derivato il nuovo progetto ConnId, con l'obiettivo principale di fornire tutto ciò che è necessario ad un progetto Open Source moderno: build basato su Apache Maven, artifacts e mailing lists. Sono inoltre forniti connettori aggiuntivi, come SOAP, CSV e Active Directory.

Apache Syncope supporta

- ✔ la *propagazione verso* risorse esterne (quando i dati degli utenti vengono copiati da Syncope verso le risorse esterne)
- ✔ la *sincronizzazione* da risorse esterne (quando i dati degli utenti sono presi dalle risorse esterne verso Syncope)

Le operazioni di propagazione e sincronizzazione, chiamati task, sono salvate per fini di reportistica o essere, nel caso, rieseguite successivamente.

3.3 Storia

3.3.1 Le Origini

Syncope è stato concepito da alcuni professionisti IdM appassionati di Open Source. L'idea era quella di creare un prodotto agile, leggero ed incisivo e di sviluppare un Identity Manager Open Source in grado di soddisfare i requisiti degli ambienti enterprise.

Syncope IdM è stato rilasciato sotto licenza Apache 2.0 sin dall'inizio ed era ospitato su Google Code.

Una nuova azienda, Tirasa, è stata fondata con l'obiettivo di acceleare lo sviluppo e la diffusione di Syncope IdM.

3.3.2 L'Apache Software Foundation

Il 12 febbraio 2012 Syncope IdM è stato ufficialmente accettato nell'Apache Incubator.

Il progetto Apache Incubator è il punto di ingresso nella Apache Software Foundation (ASF) per i progetti ed i sorgenti che desiderino diventare parte della Foundation stessa. Tutte le donazioni di codice da organizzazioni e progetti esterni che vogliano entrare in Apache passano tramite l'Incubator. Lo staff di Syncope IdM ha iniziato questo percorso formulando una incubating proposal ed avviando una discussione nella mailing list apposita: la proposta è stata votata e accettata.

L'ingresso nella Apache Software Foundation significava, per il team di Syncope IdM, maggiore visibilità e attrattiva di più sviluppatori all'interno della community in modo da rendere Syncope IdM più stabile, affidabile e supportato.

Addio Syncope IdM, benvenuto Apache Syncope!

3.3.3 Oggi

Apache Syncope è un progetto attivo e vivace: ecco il sito ufficiale ASF per maggiori informazioni!

4 Storie di successo

In questo paragrafo vengono riportate alcune esperienze di progetti basati su Apache Syncope.

4.1 SURFnet

SURFnet è una organizzazione no-profit facente parte di SURF, la partnership Olandese per l'innovazione ICT in ambito universitario e di ricerca.

La missione di SURFnet è di migliorare l'università e la ricerca per mezzo della promozione, sviluppo e messa in opera di infrastrutture ICT sicure che facilitino l'utilizzo ottimale delle possibilità offerte dall'ICT stessa.

SURFnet sta valutando l'impiego di Syncope all'interno del proprio software di gestione delle identità e collaborazione. Lo sviluppo vero e proprio avverrà nel 2012.

4.2 Bibliotheek.nl

Stichting Bibliotheek.nl è la fondazione olandese che si occupa di espandere e gestire la biblioteca digitale nazionale. Il lavoro della fondazione è commissionato dalle biblioteche periferiche. Alcune tra le attività svolte:

- ✔ creare un portale centrale che aumenti la visibilità della biblioteca nazionale su internet;
- ✔ sviluppare una infrastruttura informativa comune alla quale le biblioteche locali possano connettersi;
- ✔ implementare servizi digitali;
- ✔ collaborare e costruire relazione con biblioteche ed altre organizzazioni culturali.

Uno dei progetti aveva il compito di implementare una infrastruttura centralizzata per la gestione degli accessi e delle identità. L'obiettivo della infrastruttura IAM è quello di gestire tutti gli utenti della biblioteca nazionale olandese, sulla base delle utenze inserite continuativamente dalle biblioteche locali. In questo modo tutti i membri della biblioteca olandese possono autenticarsi ed utilizzare i servizi digitali connessi con l'infrastruttura IAM.

In accordo con le linee guida predisposte dal governo per le istituzioni (semi-) governative, Stichting Bibliotheek.nl ha dato preferenza a prodotti Open Source per implementare l'infrastruttura IAM. La sezione del progetto relativa all'implementazione del livello di gestione delle identità è stata vinta da Everett, che ha offerto una soluzione basata su Apache Syncope. Everett è un systems integrator specializzato in gestione degli accessi e delle identità.

Il prodotto offre funzionalità che possono competere con le controparti commerciali. È leggero, scalabile e molto flessibile. Stichting Bibliotheek.nl è molto soddisfatta di Apache Syncope come prodotto ed intende estendere i propri servizi in questo ambito grazie ad esso.

5 Supporto Enterprise

Uno degli aspetti maggiormente criticati circa l'adozione di software Open Source in ambiente enterprise riguarda la mancanza di supporto operativo di livello enterprise.

Tirasa[7], azienda Open Source attiva nella community ASF, fornisce supporto, servizi professionali e formazione per Apache Syncope.

Tirasa gestisce un sito di supporto enterprise dedicato, con demo, progetti di esempio, documentazione aggiuntiva e piani di supporto dalla valutazione del prodotto fino alla messa in produzione e oltre: http://syncope.tirasa.net/

7 http://www.tirasa.net/