Apache Syncope OpenSource IdM

Managing Identities in Enterprise Environments

Version 1.3 / 2012-07-26

Table of Contents

List of Figures

1 Executive summary

Identity management (or IdM) represents the joint result of business process and IT to manage user data on systems and applications. IdM involves considering user attributes, roles, resources and entitlements in trying to give a decent answer to the question bumping at every time in IT administrators' mind:

Who has access to *What*, *When*, *How*, and *Why*?

Inside a given organization, an IdM solution will basically

- ✔ provide the right information and tools to the right people, at the right time;
- ✔ enable approval process and delegation of authority;
- ✔ protect IT infrastructure from information theft;
- ✔ help the organization to comply with regulations;
- ✔ ensure the privacy of customer, partner and employee information;
- ✔ facilitate the creation and automate the enforcement of business policies that strengthen security, reduce administration costs and improve productivity.

Conversely, when not implementing an IdM solution, an organization can easily fall into situations in which, for example, new-hired and promoted employees sit idle waiting for granted access to needed tools while former employees can continue to have access for days and weeks after they left the organization. Moreover, compliance process cannot rely upon a verifiable, accurate and timely control over the identities of the people and resources distributed across the organization itself.

This paper introduces a new approach to build and maintain the identity management infrastructure by leveraging the fresh and rising IdM Open Source product named Apache Syncope. In the following, this paper will examine what is required of an identity infrastructure today and introduce Apache Syncope specifications, architecture and technicalities.

2 Requirements for an Identity Infrastructure

Building an identity infrastructure means often taking care of two distinct but tightly related aspects in IT management: identity management and access management; for this reason the preferred term to be used in this context is IAM (Identity and Access Management).

A complete IAM solution provides:

- ✔ identity lifecycle management (with workflow-based provisioning)
- ✔ meta-directory
- ✔ access control
- ✔ role-based management
- ✔ self-service functionalities

A key aspect to outline is that an IAM solution needs to do its job by leveraging – rather than replacing – existing business processes, business rules and technology investments.

Let's consider the situation depicted in Figure 1: a very common scenario in which different groups of users (partners, employees, customers, former employees) have all different ways to access the various systems and applications provided by the organization. Each separate system stores its own username, password, user profile and authorizations. Authorization process is completely independent and delegated to each single application.

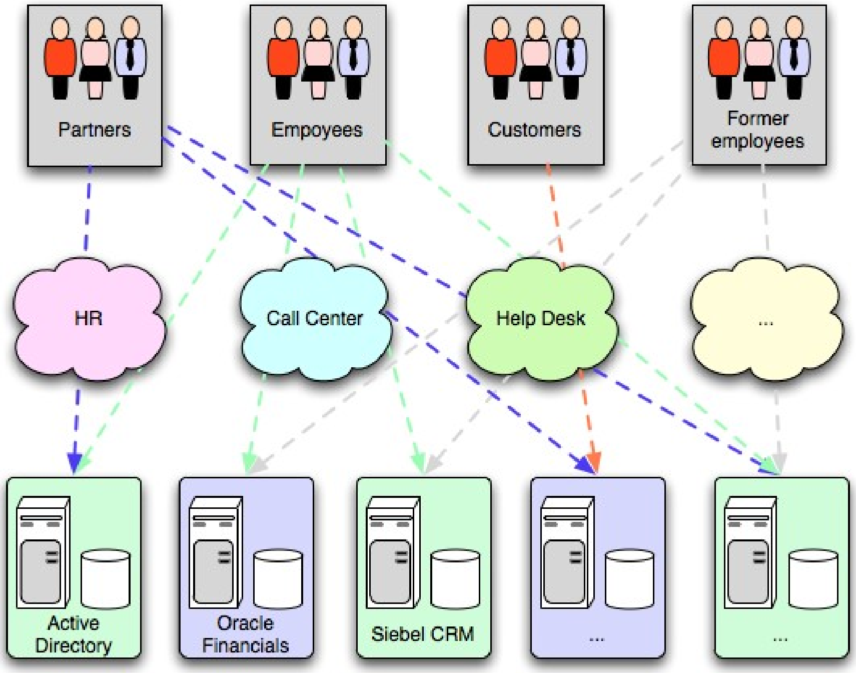

Figure 1: No IAM organization

By introducing a complete IAM solution, the situation becomes similar to what shown in Figure 2:

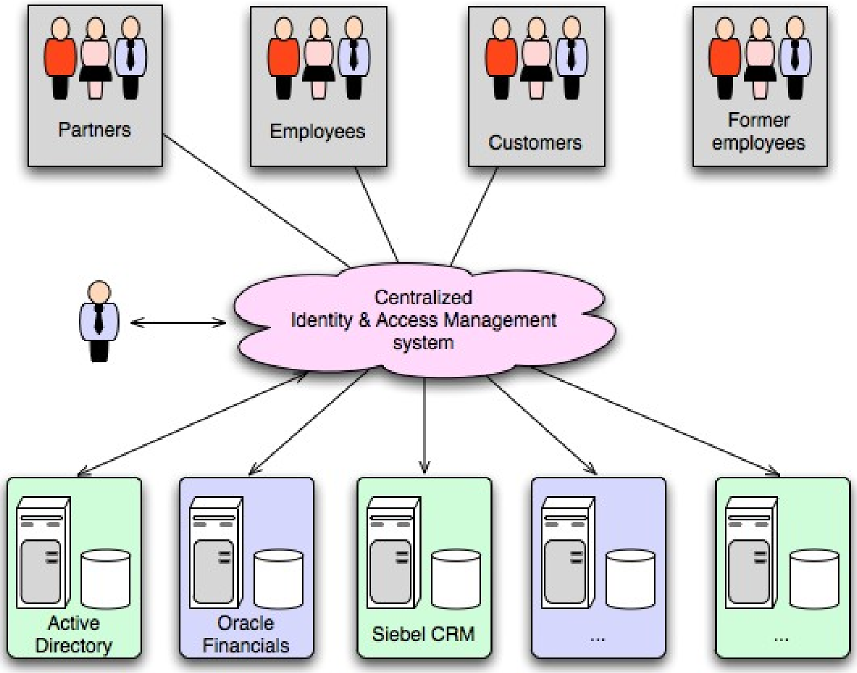

Figure 2: IAM-enabled organization

the centralized IAM system takes care of all security aspects of the communication between users and applications, synchronizes information among different systems, performs auditing and logging of all the processed transactions – if required.

2.1 Identity Lifecycle Management

As suggested by what stated above, one of the most important concepts in a successful IAM solution is the processes and technology used to create and delete accounts, manage account and entitlement changes and track policy compliance, including some or all of the following:

- ✔ Provisioning / de-provisioning
  The automatic creation and expiration of accounts in multiple systems based on data from authoritative data sources, thereby reducing the administrative effort involved in manual account creation and management, and reducing security risk by the automatic application of policies.
- ✔ Workflow
  The automation of steps within the identity lifecycle management process including notification, approval, escalation and creation of audit data.
- ✔ Administration
  The facilitation of the administration of identities, usually through the deployment of a

web-based user administration console. Such interfaces are often used for delegated administration and possibly even user self-service, in conjunction with workflow.

- ✔ Credential management
  Passwords, certificates and smart cards.
- ✔ Role management
  Where Role Based Access Control (RBAC) is in use, facilities for the creation and maintenance of roles, including role definition and role membership.

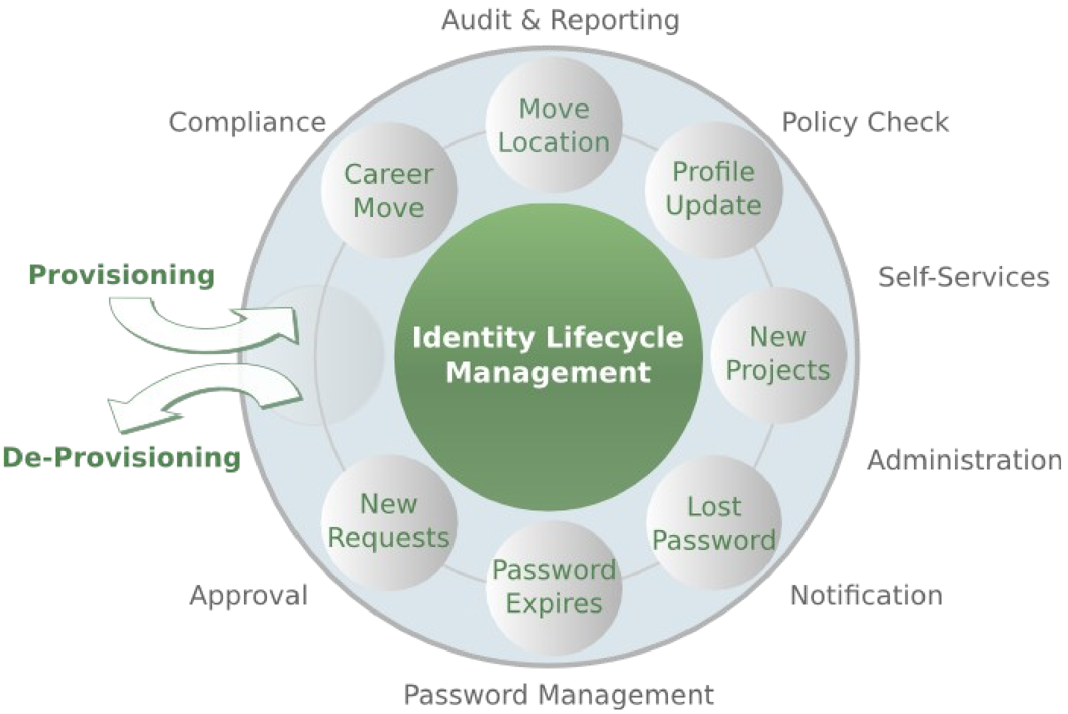

Figure 3: Identity Lifecycle

3 Apache Syncope, Open Source IdM

Apache Syncope[1] is an IdM solution, implemented in JEE technology and released under Apache 2.0 license[2].

Apache Syncope features most of what expressed above in terms of pure identity management. For deployment scenarios in which access management features are requested as well, Apache Syncope perfectly fits together with some Open Source access management solutions, like as Apache Shiro[3], OpenAM[4], CAS[5] or 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 Why Open Source

Identity Management is a middleware area in which only proprietary vendors (like as Sun Microsystems, Oracle, Novell, IBM and others) used to be able to provide organizations with adequate tools. Such proprietary tools were also very often built to deal with widespread adopted FOSS enterprise systems like as LDAP servers (OpenLDAP, OpenDS), DBMS (MySQL, PostgreSQL) and webservices.

Moreover, the considerably high license cost of these products acted as a barrier for small or no-profit organizations that would instead benefit from applying identity management in their infrastructure.

3.2 High-level Architecture

From an high-level point of view, the component architecture of Apache Syncope can be summarized by Figure 4. Apache Syncope is composed by two main subsystems:

1. the core
   The web application that implements IdM features; it offers a RESTful interface for caller applications, implements the provisioning core by mean of its workflow engine and its propagation layer, manages data persistence.

[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. the administration console
   The web management interface for configuring and administering Apache Syncope. Like as other external applications, the console communicates with the core by REST calls.

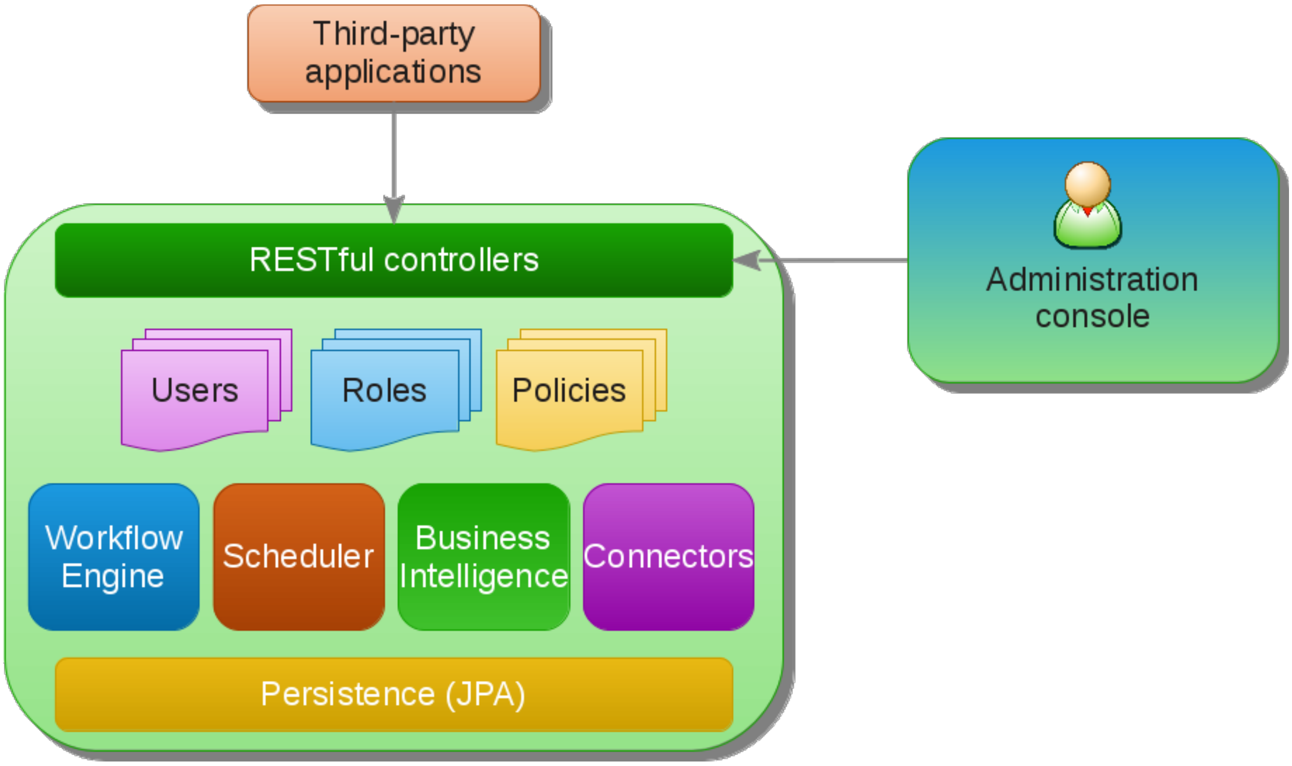

Figure 4: High-level Apache Syncope architecture

3.2.1 Business Intelligence

This central component orchestrates the whole data flow throughout the system. Gets involved upon RESTful calls, processes data alongside the defined workflow, propagates to and synchronize from configured external resources, if needed.

3.2.2 RESTful controllers

RESTful controllers take care of the communication with outside world. Implemented by leveraging Spring's REST and MVC features, these controllers exchange data in both XML and JSON formats.

3.2.3 Workflow engine

Workflow engine is a pluggable aspect of Apache Syncope: this lets every deployment choose among one of provided engine implementations or define new, custom ones.

Default implementation is based on Activiti BPM, reference Open Source implementation that supports the definition of an XML descriptor in which user lifecycle is defined. This aspect makes the whole system very flexible to adapt to different situations.

Default implementation also provides notification, approval and end-user request management.

3.2.4 Scheduler

A whole set of operations is performed by Apache Syncope without being triggered from an external RESTful call; in this case Quartz, the reference Open Source implementation in this respect, takes care of running the required tasks.

3.2.5 Persistence (JPA)

All the data used by Syncope (users, roles, attributes, resources, ...) is managed at an high level with a standard JPA 2.0 approach and persisted to underlying database.

This approach makes Apache Syncope successfully deployable on most DBMS without any modification on the source code. Currently, Apache Syncope supports MySQL, PostgreSQL, H2, MS SQL Server and Oracle DB.

3.2.6 Connectors

Connector layer is implemented by leveranging ConnId.

Connid is the continuation of Identity connectors, a project that used to be part of the market leader Sun IdM and have been released by Sun as an Open Source project. This makes the connectors layer particularly reliable since most connectors are already implemented in the framework and widely tested. Lately, the original project has been forked into the new ConnId project, whose main purpose is to provide all that is required nowadays for a modern Open Source project: Apache Maven driven build, artifacts and mailing lists. Additional connectors – like as SOAP, CSV and Active Directory – are also provided.

Apache Syncope supports either

- ✔ *propagation* towards external resources (when user data is copied from Syncope to external resources)
- ✔ *synchronization* from external resources (when user data is pulled from external resources into Syncope)

Propagation and synchronization operations – a.k.a tasks – are saved for reporting and later re-execution.

3.3 History

3.3.1 The Origin

Syncope was conceived by a bunch of Italian, Open Source addicted, IdM professionals. The main idea was to create a thin, versatile and incisive product and to develop an Open Source Identity Manager able to satisfy the requirements of enterprise environments.

Syncope IdM was released under terms of Apache License 2.0 since its beginning and was hosted at Google Code.

A brand new company, Tirasa, aiming to speed up the development and the adoption of Syncope IdM, was founded.

3.3.2 At the Apache Software Foundation

On Februay 12th 2012, Syncope IdM was officially accepted at the Apache Incubator.

The Apache Incubator project is the entry path into The Apache Software Foundation (ASF) for projects and codebases wishing to become part of the Foundation's efforts. All code donations from external organisations and existing external projects wishing to join Apache enter through the Incubator. Syncope IdM staff started such entry path by formulating an incubating proposal and opening a discussion at the general Incubator mailing list: this proposal was voted and accepted.

By joining the Apache Software Foundation, Syncope IdM team expected to get more visibility and attract more people to rising Syncope community, thus making Syncope IdM more stable, reliable and supported.

Goodbye Syncope IdM, welcome Apache Syncope!

3.3.3 Today

Apache Syncope is live and kicking: check the official ASF website for more information!

4 Success Stories

A few examples of sucessful projects based on Apache Syncope are reported here.

4.1 SURFnet

SURFnet is a non-profit ‘task organisation’ forming part of SURF, the Dutch higher education and research partnership for ICT-driven innovation.

SURFnet’s mission is to improve higher education and research by promoting, developing, and operating a trusted, connecting ICT infrastructure that facilitates optimum use of the possibilities offered by ICT.

SURFnet is currently studying Syncope to include it in its identity management and collaboration middleware for provisioning / deprovisioning needs and will be doing the actual service development in 2012.

4.2 Bibliotheek.nl

Stichting Bibliotheek.nl is the Dutch foundation that aims to expand and manage the Digital National Library. The foundations work is commissioned by the individual local libraries in the Netherlands. Its activities include:

- ✔ creating a central portal to boost the visibility of the national library on the internet;
- ✔ developing a common information infrastructure that local libraries can connect to;
- ✔ implementing digital services;
- ✔ collaborate and build relationships with libraries and other organizations within the cultural sector.

One of the projects was implementing a centralized identity and access management infrastructure. The IAM infrastructure aims to hold all users of the national library in the Netherlands, fed by a continuous feed from the local libraries. This way, all Dutch library members can authenticate and use digital services connected to the IAM infrastructure.

In accordance with the guidelines set out by the government for (semi-) governmental institutions, Stichting Bibliotheek.nl gave high preference for Open Source products to implement the IAM infrastructure. The part of the project responsible for implementing the identity management layer was won by Everett that offered a solution based on Apache Syncope. Everett is systems integrator specialized in Identity and Access Management.

The product offers functionality that can compete with commercial products. It is lightweight, scalable and very flexible. Stichting Bibliotheek.nl is very content with Apache Syncope as a product and intends to extend its services based on it.

5 Enterprise Support

One of most criticised aspects of Open Source software adoption in enterprise environments is about the lack of enterprise-class operational support.

Tirasa[7], an Open Source company active part of the ASF community, provides value add support, professional services and tranining around Apache Syncope.

A dedicated enterprise support site is available, featuring demos, project samples, additional documentation and support plans ranging from the product evaluation to the production roll-out and afterwards: http://syncope.tirasa.net/

[7] http://www.tirasa.net/