Identity management

Jean-René Rouet <rouet@in2p3.fr>

FJPPL Computing Workshop

11/03/2015

CCIN2P3

cnrs

Outline

- What is an identity management project ?
- Why we need this ?
- How can we do ?
- When ?

What is Identity Management ?

- The ability to store and manage all granted access for your staff in one place
- Granted access are used in many different systems
  - Heterogeneous technologies
  - Systems are not only IT systems
- A good identity management system doesn’t break everything
  - It can be introduced step by step
- It has the ability to answer some questions like
  - What are the credentials of that person in our systems ?
  - Who uses this system today ?
- It has the ability to do some action like
  - Close all the credentials of a person
  - Open an access to computing room for one day for a person

Why we need this ?

- Our systems and accounts (a short list)
  - Computing farm - Unix account
  - Database (mysql-postgresql-oracle) - Database account
  - WebHosting - Sftp account
  - IRods storage - IRods account
  - Collaborative tools
    - Electronic Document System - Application account
    - Wiki - Application account
    - …
  - Code versioning - Account

Why we need this ?

- Each account (except one) is created by the administrator of the system
  - Is it the role of a system expert ?
- We don’t have a global view
  - To do that, we have to aggregate many sources
- No validation workflow (except one)
  - the workflow is the mail exchange or the help desk ticket
- No expiration policy (except one)

Why we need this ?

- Is SSO a solution ?
  - Authentication is not authorization
  - Some systems cannot be connected to SSO
- A identity management system is not a password manager
  - Each system can have a different password policy

How we can do ?

- Find a tool
  - Oracle™ software suite :
    - good tool
    - covers all needs
    - too expensive
    - too complex
  - OpenIDM
    - good tool
    - covers major needs
    - open source
    - more simple
- Implement this tool in our infrastructure

How we can do ?

- OpenIDM
  - it is an orchestrator
  - it starts workflows
  - workflows interact with users by mail or by a web interface
  - workflows interact with systems by connectors
    - some classic connectors already exist
    - you have to develop you connector if needed
  - provides a reconciliation tool between existing systems and its database
    - also uses connectors

How we can do ?

- First step
  - have an openIDM instance ready
  - choose the attributes of an identity in the system
    - ID
    - First Name
    - Last Name
    - Organizational unit
    - (Mail Address)

How can we do ?

- Email Address
  - does not define an identity
  - it can change
- Email address is very important for us
  - it is in the heart of system
  - all users will be contacted by mail, so we need to be sure that it is valid
  - a special workflow is needed for that

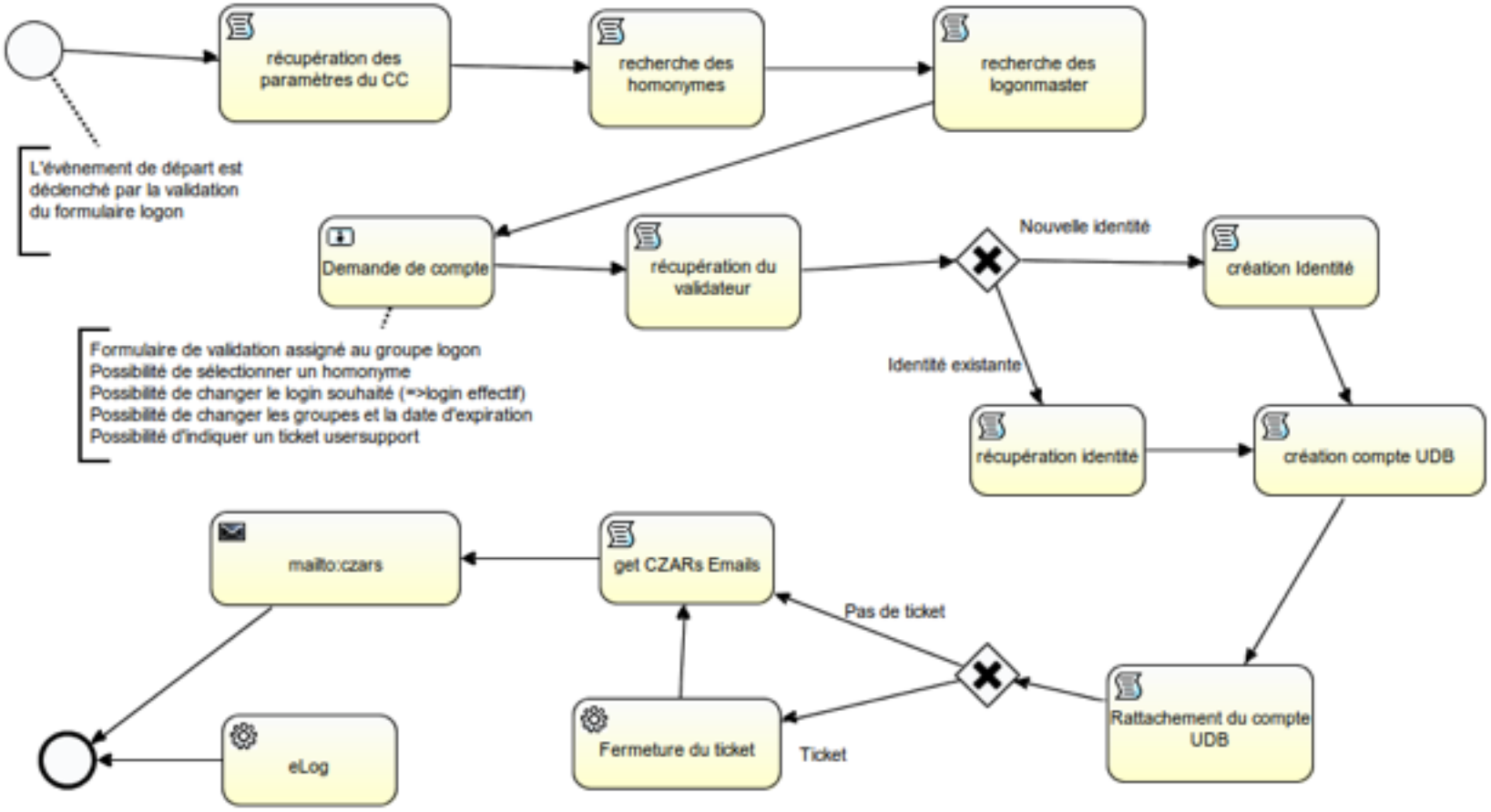
How can we do ?

- Second step
  - First reconciliation if possible
    - ldap server for example, we have that
    - use the provided ldap connector to do that

How can we do ?

- Third step and so on
  - Integrate a system
    - write the connector (java code using OpenICF framework)
    - initial reconciliation
    - describe workflows
      - this task is the most important (see next slide)
    - implement workflows

- Computing account creation workflow
  - BPMN format (Activiti BPM Platform)



How can we do ?

- Special steps
  - Web Interface self-service for users
  - Reporting and accounting

Project status and calendar

- The project is a test phase with
  - initial reconciliation from ldap directory
  - creation workflow for computing accounts
- Before end of 2015
  - production start
  - integration of database account
  - integration of email account <-> Zimbra service
  - tools used today to manage computing accounts will be stopped

People Involved

- Lionel Schwarz
- Dominique Cathala-Martinez
- Philippe Correia
- Jean-René Rouet

- for operation team
  - Frédéric Azevedo
  - Xavier Canehan