Event Driven Identity Management

Tero Hakkarainen, Software Engineer
Lauri Viitanen, Software Engineer
About Helsinki Metropolia University of Applied Sciences

- A multidisciplinary university of applied sciences
- The largest in Finland
- Operating out of Helsinki, Espoo and Vantaa
- Four fields of study:
  - Culture
  - Business
  - Health Care and Social Services
  - Technology
- 16,700 students
- 2,290 Bachelor’s and 210 Master’s graduates in 2012
- Staff 1,250
About Metropolia IT Services

• 17 facilities in Helsinki metropolitan area
• network of over 5000 workstations and servers
• different customer profiles
  o students
  o staff
  o partners
  o guests
• multiple operating systems and platforms
  o workstations
  o web
  o mobile
IAM system architecture in Metropolia

IAM Systems

- CBI Winha Masterdata for Student Identities
- Abusiness HRM Masterdata for Employee Identities
- Amma IAM System
- CAS based single sign on logins
- Shibboleth - SAML2 based logins
- AD sync
- LDAP sync

Identity Target Systems

- Microsoft Active Directory
  - Windows workstation logins
  - IIS based web applications, which uses AD based logins
  - AD schema is used
- Red Hat LDAP Directory Server
  - LDAP based login for applications
  - Linux server logins
  - custom schema is used
- Application X
  - application specific identity data set used while syncing

Password Sync

N
Example: IAM process for employee in Metropolia

IAM Process - Employee

Abusiness HRM

- Input of basic employee data to HRM. Data is based on employment application.
- The employment contract printed from HRM is signed.
- The employment contract becomes valid.

Amme

- Amme reads base dataset from interface.
- Employment contract dates becomes valid in Amme.
- Identity Roles for the employee is activated.
- The employee activates the user account in Amme.

Target Data System

- Base dataset is synced to target systems.
- User identity is synced to target systems. User target system login becomes active.
- User logs into target system.
Amme - IAM system in Metropolia
Identity and Role in Amme

Identity = Aggregate(Roles)
Role = Collection of system specific attributes
Identity and Role in Amme

Identity = Aggregate(Roles)
Role = Collection of system specific attributes

Aggregate =
- Build new attribute from existing attributes
  - e.g. full name = first name + last name
- Build existing attribute from strongest role that contains the attribute
Amme Architecture

UI (MyFaces / JSF) → HTTPS → Amme (Java 6, Spring 3) → JDBC → MySQL → Various → Data Sources & Targets
Amme Data Sources & Targets

- Active Directory
- Winha
- Winha WebService
- HR
- TEM
- Toisu
- Peppi WebService
- UI
- DB
- File I/O
- HTTPS
- Emergency Message
- WinhaMail
- Merex
- Tuubi WebService
Amme Event Triggers

Start
  └── Create
      ├── TaskKeeper
      │    └── Create
      │         ├── winhaStudentTrigger
      │         │    └── Create
      │         │         └── winhaStudentJob
      │         │             └── Execute
      │         │                 └── JdbcEventProducer
      │         │                     └── As
      │         │                             └── Query
      │         │                                 └── <<View>>
      │         │                                     └── Winha
      │         │                                         └── Query
      │         │                                             └── <<View>>
      │         │                                                 └── <<View>>
      │         │                                                     └── AmmeDB
      │         └── hrStaffTrigger
      │             ├── Create
      │             ├── hrStaffJob
      │             │    └── Create
      │             │         ├── JdbcEventProducerHR
      │             │         │    └── Create
      │             │         │         └── Query
      │             │         │             └── <<View>>
      │             │         │                 └── HR
      │             │         └── As
      │             └── Execute
      └── internalPollerTrigger
          └── Create
              ├── internalPollerJob
              │    └── Create
              │         ├── internalPoller
              │         │    └── Create
              │         │         └── Query
              │         │             └── <<View>>
Amme Aggregators

```
... strongestrole_aggregator
copy_aggregator
getcn_aggregator
getmail_aggregator
...
phoneNumberNormalizer_aggregator
password_aggregator
maxValue_aggregator
...
strongestOfOrderedVocabulary_aggregator
...
fullName_aggregator
...
```
Performance of Amme

Environment

• CPU: Intel(R) Xeon(R) CPU @ 2.70GHz
• Memory: 4 GB DIMM @ 1600 Hz

Daily Usage:

• CPU Time: 1 min
• Memory: 100 MB
• Disk: 700 MB
(June 2013)
• Events / Day: 500 ± 10 %
• Target updates / Day: 4000 ± 5 %
Benchmark University's Specs

Environment
- 14500 Students, 3400 Non-students
- CPU: 2 x SUN Ultrasparc-IIIi @ 1500 MHz
- Memory: 2 GB RAM

Quirks
- Passwords & group rights updated in real time
- Everything else updated daily
Benchmark University's Performance

- Run time: 1 hour (0.04x)
- CPU time: 5 minutes (3x)
- RAM usage: N/A (0.1x ?)
- Disk usage: 10-13 GB (14-19x)
Event driven identity management

Conclusions
Event driven identity management from business process point of view

- human interaction with data is minimized: time savings
- changes to identity data is managed as soon as needed, e.g.
  - password change at once to all systems
  - identity end of life is handled properly and automatically
- real life data handling processes for lifespan of identities: master data ownership and data update responsibilities are clear
Event driven identity management from IT point of view

• immediate: changes to data is synced immediately
• trackable: all changes are logged
• accurate: no manual copying of master data
• control: Metropolia is in total control of identity data
Q & A
THANK YOU!
www.metropolia.fi/en/
tero.hakkarainen@metropolia.fi
lauri.l.viitanen@metropolia.fi