

Unil

UNIL | Université de Lausanne



AAA/SWITCH Info-Day 2008

2004-2007 The AAI era at UNIL

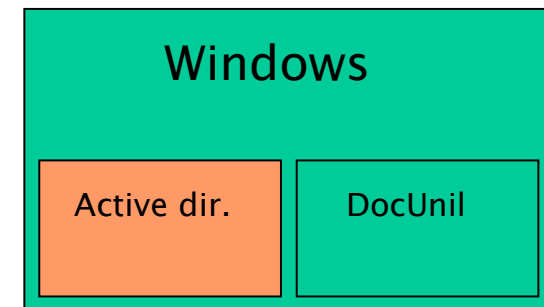
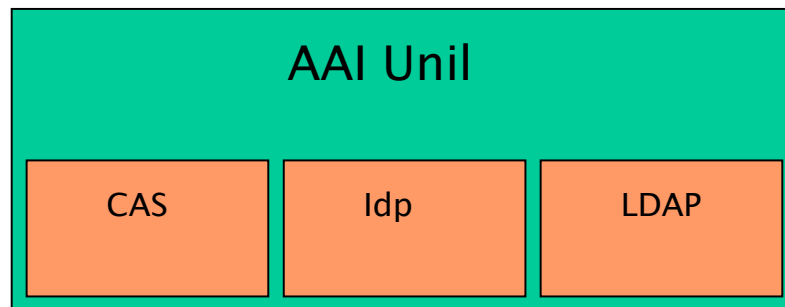
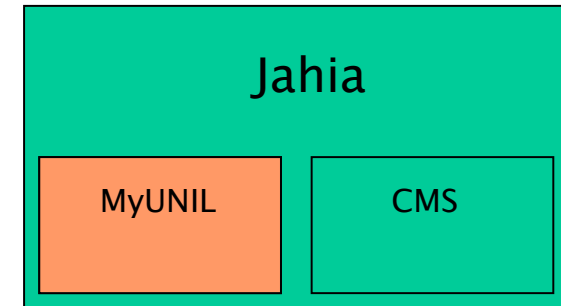
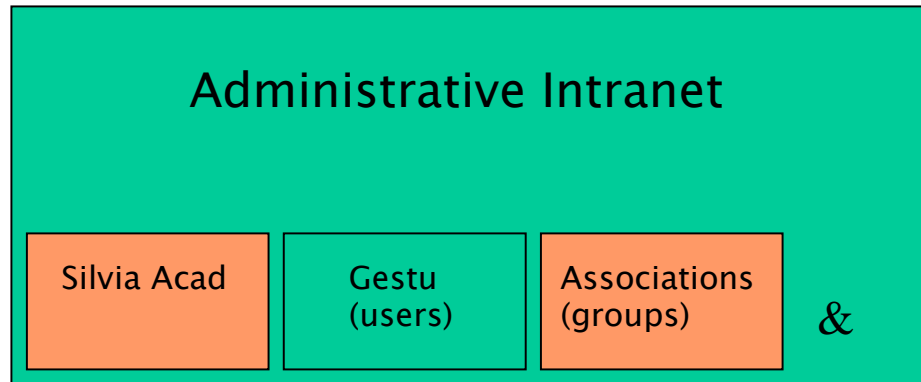
Overview

- Project Summary
- MyUNIL Portal
- Intranet Groups Manager
- Identity Providers
- Conclusions

How the story begins

- External students are registered in faculties and obtain a UNIL identity (UNIL UniqueID) => double identity!
- Goal: Integration of external students into MyUNIL and creation of all necessary components

Overall components

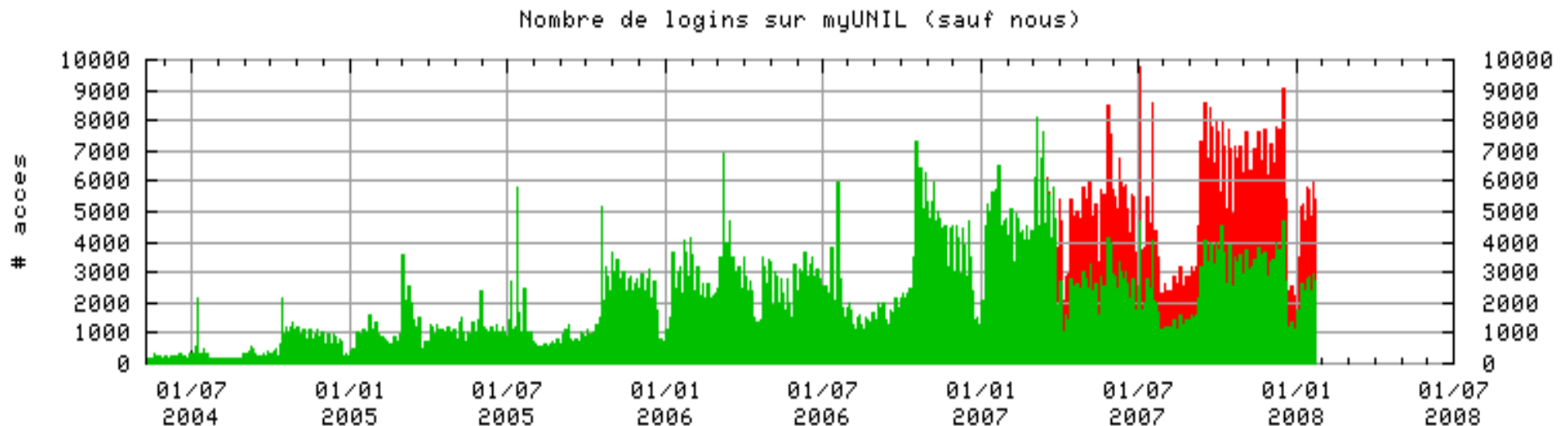


MyUNIL

- Virtual office for UNIL community offering unified access to various sources of information and services
- Contents customized along user's profile:
 - Webmail
 - Docunil (personal disk storage)
 - Courses (docs, course and exams schedules)
 - Academic profile (exams results, attestation)
 - Administrative profile...

MyUNIL (2)

- Software used: Jahia (J2EE)
- Very popular service, ~7000 logins per day



Shibboleth authentication into Jahia

- Actual: DB and LDAP authN
- Login strategy:
 - dedicated Shibboleth login protected by Apache mod_shib
- Need to store Shibboleth attributes into Jahia user
- Need more information about external users qualifying their relationship to UNIL
=> local attributes store

Shibboleth users into Jahia

- Implementation of Shibboleth user into Jahia:
 - Application properties stored in Jahia DB
 - Shibboleth user attributes (into session from request headers)
 - Local user attributes (into session from local store)
- All user's information retrieved via the Shibboleth dedicated login procedure of Jahia

Jahia groups and authorizations

- AuthZ mechanism = **A**ccess **C**ontrol **L**ists relying on groups (DB and LDAP)
- Group members (i.e. Shibboleth users) not known in advance, only at runtime, when they log in.
- Group membership for a Shibboleth user?
=> group filter based upon users' attributes according to RFC 2254/1960.
 - UNIL staff: (&(Shib-SwissEP-HomeOrganization=unil.ch)(Shib-SwissEP-swissEduPersonStaffCategory=>300))

Groups Manager: Goals

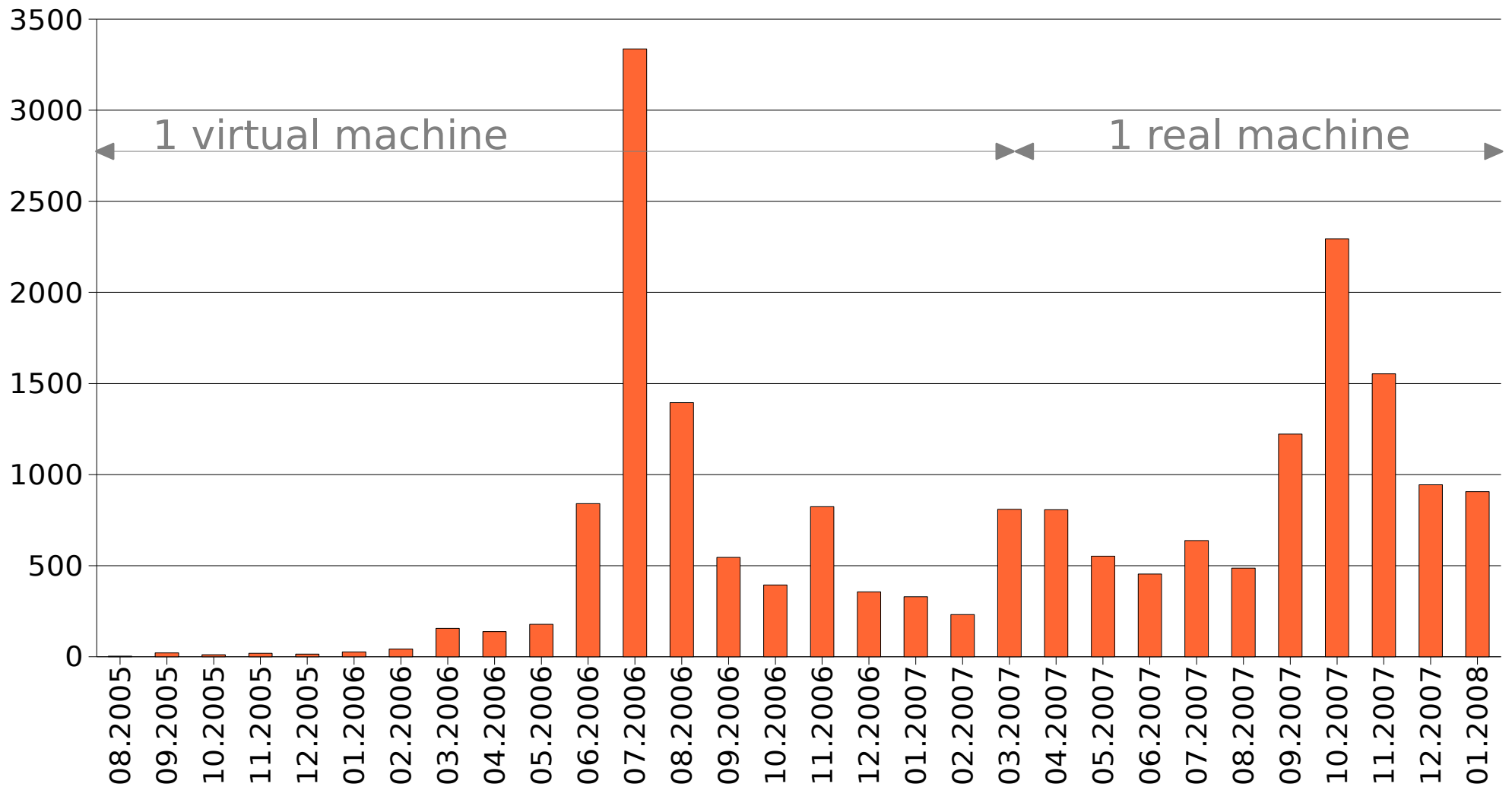
- Integrate AAI users into the big administrative database
- Manage groups containing internal (UNIL) or external AAI users
- New version of an old application
- Proof of concept Web Service interface

Groups Manager: Features

- Implemented in PHP5, MVC-style
- Customized to UNIL needs
 - Mostly an Intranet-only application
 - Ability to immediately push changes to other services (LDAP, AD, Sympa)
- Web Service use:
 - Add/remove group members
 - Allows user-initiated group membership through MyUNIL

Identity Provider History

Average logins/day during one month



Identity Providers

- Already in production
 - Load-balanced (DNS round-robin) LDAP directories (people and authentication)
 - 2 Identity Providers (1 active, 1 backup)
- Will enter production
 - Cluster the IdPs for failover
 - Hardware load-balancing

Conclusions

- Re-factoring of LDAP structure used as store for Shibboleth groups and users' local attributes
- Third-party applications login from MyUNIL (Webmail, Docunil, Admin DB)
 - For UNIL users: custom solution with encrypted password as a Shibboleth attribute
 - For external users: generic login (access only to documents courses)

Conclusions (2)

- Status: production for Q1/08
- Still no AAI integration in external students' registration :-(
 - UniqueID can't be easily given (hard to remember)
 - We lack a technical mean to capture it during registration
 - Changing some administrative processes takes quite a long time...
 - External students end up with two accounts

References

- MyUNIL portal: <http://my.unil.ch/>
- Jahia web site: <http://www.jahia.org/>
- RFC “The String Representation of LDAP Search Filters”:
 - <http://www.ietf.org/rfc/rfc1960.txt>
 - <http://www.ietf.org/rfc/rfc2254.txt>
- “Redundant Identity Provider at UNIL”
 - <http://www.switch.ch/proxy/aai/support/presentations/opcom-2007/AAI-OpCom-40-Redundant-IdP.pdf>

Questions

