AAI OpCom Meeting

University of Zurich

IdP migration from Shibboleth 1.3 to 2.1

Luzian Scherrer, IT-Services, University of Zurich
luzian.scherrer@id.uzh.ch

Four phases

- Planning
- Installation & Testing
- Migration
- Troubleshooting

Timeframe Planning

Mid February 2009

Kick off meeting with all involved people from UZH

End of February 2009

Start of testphase (= new IdP ist ready for testing)

End of May 2009

End of testphase, last option to cancel

End of June 2009

Production

➡ *5 Months in total, it was more than enough*

Infrastructure Planning

Redundancy ☺ Complexity ☹

- 2 Hosts / Loadbalancer
  Database for PersistentID not shared ➡ third host
  Memory not shared (Terracotta) ➡ active/standby
  ➡ Redundancy, not balancing the load

  IdP Hosts: VMs, 1 CPU, 4GB RAM, 15GB HDD, SLES10
  Loadbalancer: Alteon 3408 (will be Cisco ACE soon)

Installation

- Installation according to https://www.switch.ch/aai/support/documents/

- Completely separate installation from running IdP
➡ different EntityID

- Required software installed from SLES supplied RPMs
Exceptions: Java, Tomcat and Shibboleth
manually under /usr/local
➡ used the same versions as SWITCH recommends

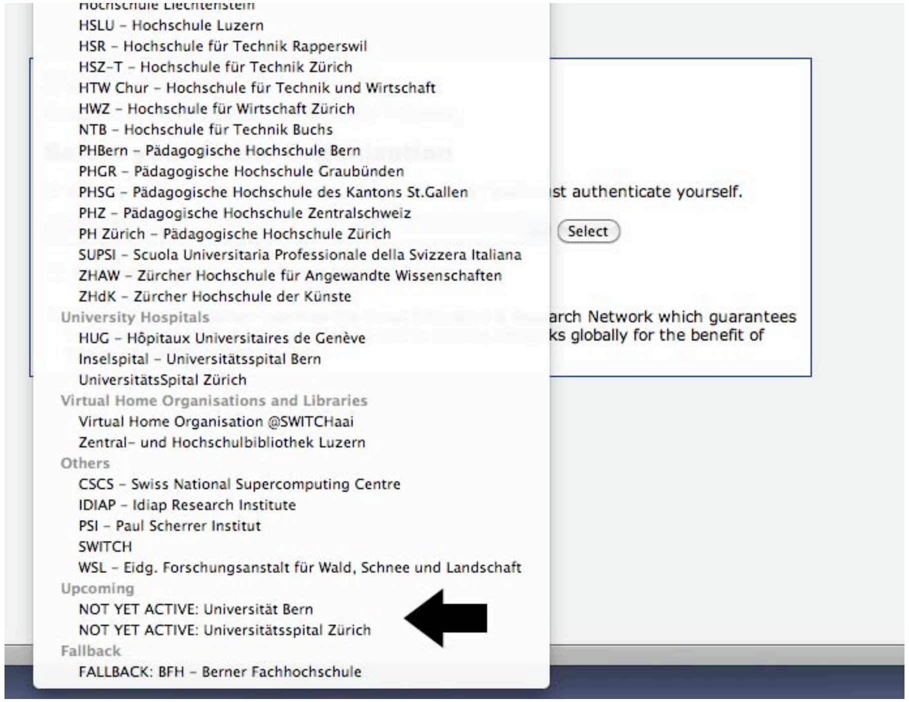
Installation

Additional steps

- Updated attribute-resolver.xml with our own attributes
- Updated “Specific Attribute Release Policy Rules” in the AAI-RR with our own policies for our custom attributes

Testing

1. SWITCH added metadata for new IdP as special include to metadata.switchaai.xml
2. SWITCH added new IdP to DS under “upcoming”



Hochschule Liechtenstein
HSLU – Hochschule Luzern
HSR – Hochschule für Technik Rapperswil
HSZ-T – Hochschule für Technik Zürich
HTW Chur – Hochschule für Technik und Wirtschaft
HWZ – Hochschule für Wirtschaft Zürich
NTB – Hochschule für Technik Buchs
PHBern – Pädagogische Hochschule Bern
PHGR – Pädagogische Hochschule Graubünden
PHSG – Pädagogische Hochschule des Kantons St.Gallen
PHZ – Pädagogische Hochschule Zentralschweiz
PH Zürich – Pädagogische Hochschule Zürich
SUPSI – Scuola Universitaria Professionale della Svizzera Italiana
ZHAW – Zürcher Hochschule für Angewandte Wissenschaften
ZHdK – Zürcher Hochschule der Künste

University Hospitals
HUG – Hôpitaux Universitaires de Genève
Inselspital – Universitätsspital Bern
UniversitätsSpital Zürich

Virtual Home Organisations and Libraries
Virtual Home Organisation @SWITCHaai
Zentral- und Hochschulbibliothek Luzern

Others
CSCS – Swiss National Supercomputing Centre
IDIAP – Idiap Research Institute
PSI – Paul Scherrer Institut
SWITCH
WSL – Eidg. Forschungsanstalt für Wald, Schnee und Landschaft

Upcoming
NOT YET ACTIVE: Universität Bern
NOT YET ACTIVE: Universitätsspital Zürich

Fallback
FALLBACK: BFH – Berner Fachhochschule

st authenticate yourself.

arch Network which guarantees
ks globally for the benefit of

Testing

Information for SP admins

- Update metadata
- SP Login Link Composer
  http://www.switch.ch/aai/support/serviceproviders/sp-compose-login-url.html
- EntityID of the new IdP

Troubles Before Migration

- **EZproxy not Shib 1.3 compatible**
  Solution: Upgrade to 5.1c or higher; new configuration needed, see https://wiki.aai.switch.ch/twiki/bin/view/AAIMisc/UpgradeEZProxy
- **Custom attributes not delivered**
  Reason: we had the permit rules in updateARP.pl’s config.txt but not in AAI-RR
  Solution: update the “Specific Attribute Release Policy Rules” in AAI-RR
- **OLAT (SP) uses its own DS**
  Solution: they had to update their DS at the same time as SWITCH updated the central DS

Migration

SWITCH updates the DS, nothing more…

Troubles After Migration

- **Some SPs did not update the metadata automatically**
  Solution: update metadata (and do it automatically)
- **Some SPs did use direct login-links to the old IdP**
  Solution: adjust links
- **CASUS (e-learning)**
  “wir vermuten, dass es sich um eine inkompatibilität mit dem nicht mehr supported JavaSP 1.3 handelt”
- **Troubles under high load (online semester enrollment)**
  Solution: had to increase maxThreads in Tomcat’s server.xml (defaults implicitly to 200). Don’t forget to adjust Apache threads too.
- **External users behind firewalls that did not allow access to the new IdP**
  Solution: identify and inform them so they can update FW rules

Summary

- Planning & installation was straight forward
- Easy to test and easy to go back in case of problems because old and new IdP are running in parallel
- A few minor problems but solvable with great support from SWITCH

Summary

- Planning & installation was straight forward
- Easy to test and easy to go back in case of problems because old and new IdP are running in parallel
- A few minor problems but solvable with great support from SWITCH

Getting the SAML 2 ✓ was not too hard!