IdP Migration to Shibboleth 2

SWITCH
Serving Swiss Universities

Patrik Schnellmann
patrik.schnellmann@switch.ch

IdP Migration to Shibboleth 2

- Why update?
- What has changed?
- How to update your IdP

Why update?

Imagine the following situation:

- A very important person wants to hold a video conference
- In 5 minutes, the conference starts
- He cannot log in!
- All he gets is a strange Shibboleth error...
- Because the problem is urgent, he calls you!

- All he knows is that the AAI login did not work.
- Now you have to explain him why ...

Why update (continued)

The facts are:

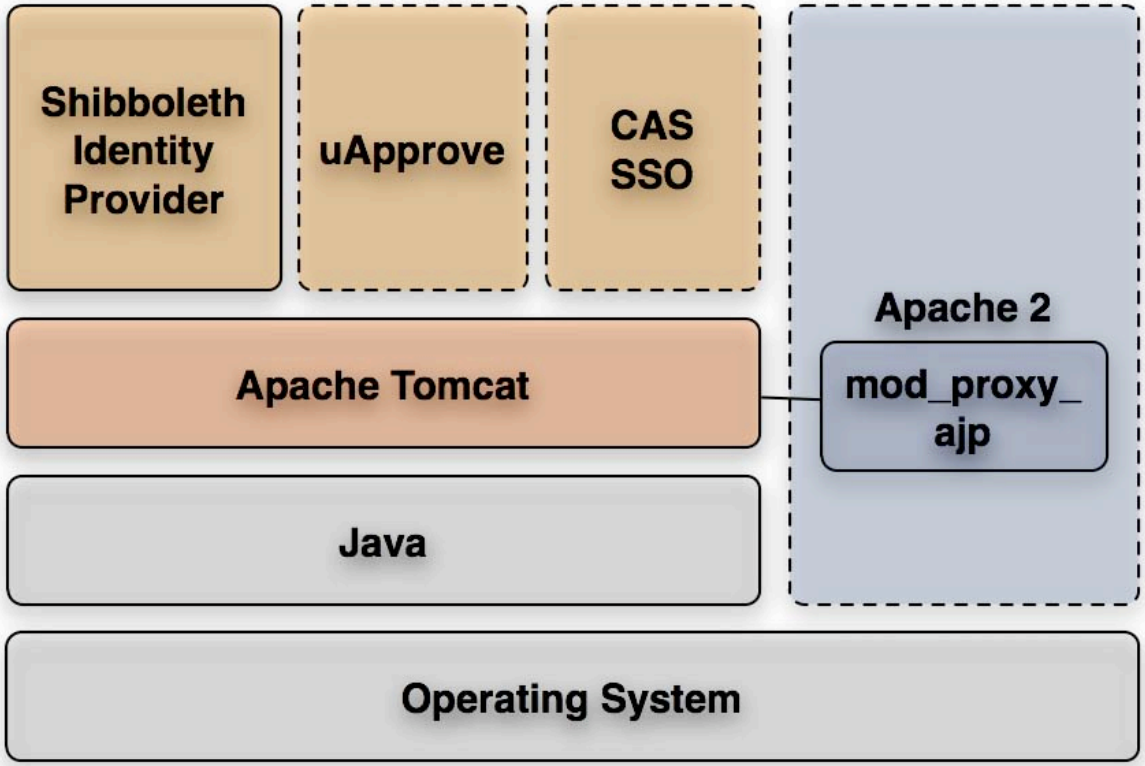
- The story really happened (with different protagonists, though)
- With up-to-date systems that would not have happened

Reasons to update:

- AAI is more reliable with up-to-date IdPs and SPs
- Shibboleth 2 SP's will profit (Attribute Push, no back channel calls)
- Security fixes★

★ http://shibboleth.internet2.edu/security-advisories.html

What has changed?



- IdP has built-in Authentication Handlers (CAS no longer needed)
- CAS is no longer needed for ArpViewer (new: uApprove)
  ⇨ less components to maintain

What has changed (continued)

- IdP automatically downloads metadata and attribute filter (ARP) files
- Database required to support persistent identifiers
- New entity ID (Provider ID) scheme for IdPs:
  “urn:mace:switch.ch:SWITCHaai:example.org” changes to
  “https://example.org/idp/shibboleth”
- IdP installer generates self-signed certificate
- We encourage the use of a self-signed certificate for Shibboleth
- Login site has to be secured with an official certificate

How to update?

- Let the “Best Current Practices” document inspire you
- Install the new IdP in a test environment
- Add IdP in Resource Registry
- Test with Service Providers
- Migrate ArpViewer DB and configuration to new system
- Inform aai-operations@switch.ch about the migration
- Put the new IdP into production

⇨ http://www.switch.ch/aai/howto/

Summary

- Why update?
  - Less components to maintain
  - More reliable AAI
  - Less support calls