IdP Version 3 Upgrade

General observations

SWITCH

SWITCHaai Team
aai@switch.ch

IdP V3, a new milestone

- IdP version 2.0.0 released in March 2008
  - followed by 4 minor releases and 18 patch releases (current is 2.4.4)
- IdP version 3: the first major release after ~7 years
  - 3.0.0: December 2014, only very sparse documentation in the Wiki
  - 3.1.0/3.1.1: March 2015, now being deployed for production use, documentation considerably improved in Q1/Q2 2015
- a good opportunity to start with a fresh environment
  - requires Java 7 or later and Servlet API 3.0 support
  - best run on an platform with an expected lifetime of 5+ years
- *do not* consider an in-place upgrade of your IdP v2 deployment
  - even if the Shibboleth installer claims supporting this to some extent

Operating system recommendations

- rely on an OS with long-term support (5+ years)
- use the same Linux distribution / one from the same family which your organization is already using for other services
- the SWITCH deployment guide has been rewritten to cover
  - Ubuntu Server 14.04 LTS
    released in April 2014, supported through April 2019
  - Red Hat Enterprise Linux 7 / CentOS 7
    released in June 2014, supported through June 2024
- Debian is no longer covered in the SWITCH guide
  - very similar to Ubuntu, though (in case you have strong feelings about staying with Debian)

Java and Webapp environment

- rely on the operating system's default Java version
  - for both Ubuntu 14.04 and RHEL 7, this is OpenJDK 7
  - Java 8 has potential pitfalls with scripted attributes (Rhino/Nashorn engine incompatibilities), so better stay with Java 7 for the time being
- use a Java Servlet container which is provided in the form of a package supported by the OS vendor
  - Tomcat 7 is the primary container for both supported OSes
  - you don't have to bother about manually applying security patches for the Servlet container
- run Apache httpd in front of the Servlet container
  - flexible configuration of the TLS endpoints for the IdP
  - mod_proxy_ajp has proven robust with the IdP v2 in the past

Persistent ID and user consent storage

- the IdP requires a relational database for storing persistent identifiers and user consent data
- for a single-instance IdP, install an SQL database which is packaged by the OS vendor
- starting with the IdP v3 deployment guide, and when installed on the same system as the IdP, SWITCH is favoring PostgreSQL
  - PostgreSQL has a long track record of close SQL standards compliance
  - MariaDB 5.5 (community-developed source fork of MySQL) would also be available as a vendor-supplied package, but for Ubuntu, only in the "universe" component – i.e., without official support for security updates
- your favorite RDBMS can be used as well, of course
  - a JDBC connector is almost all it takes
  - in particular for clusters, other RDBMSes might be better fits

Testing strategy

- **`/etc/hosts`** is your friend
- Set up the IdP v3 on a completely new system
- retain the existing entity ID, SAML endpoints and the SAML certificate
- with SAML 2, most IdP traffic is now front channel
  - straightforward testing possible by simple edits of your **`hosts`** file:
    `192.0.2.3 aai-login.example.org`
- for back-channel testing, a temporary change to an SP's **`hosts`** file can be an option