Shibboleth IdP 3.x

Hinweise zu Installation und Konfiguration

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

DFN-AAI Workshop
5./6. September 2017, FH Westküste

Installation

- Shibboleth Wiki:
  https://wiki.shibboleth.net/confluence/display/IDP30/Installation
- DFN-AAI Wiki mit Schritt-für-Schritt Doku:
  https://wiki.aai.dfn.de/de:shibidp3
- Zum Ausprobieren: Virtuelle Maschine mit Installationsfahrplan vom Shibboleth IdP 3.x Workshop 2016 an der TU Kaiserslautern:
  https://www.aai.dfn.de/aktuelles/archiv/idp-3x-workshop-2016-tu-kaiserslautern/
- Weitere Materialien: Shibboleth IdP 3.x Workshop 2016 an der FU Berlin:
  https://www.aai.dfn.de/aktuelles/archiv/idp-3x-workshop-2016-fu-berlin/
- Trainingsunterlagen von SWITCH:
  https://www.switch.ch/aai/support/presentations/shibboleth-training-2015/

Überblick Konfigurationsdateien (1)

- … liegen unter **./conf**
- .xml und .properties Dateien
- Zentral: **idp.properties**
  wird bei Installation teilweise mit Werten belegt
- (Föderations-)Metadaten: **metadata-providers.xml**
- LDAP-Parameter für Login und Attribute Resolver: **ldap.properties**
- Attribute: **attribute-resolver.xml** und **attribute-filter.xml**
- SQL-DB für Storage (Session Storage, SAML2 persistent NameID, User Consent): **global.xml**
- SAML Profile: **relying-party.xml**

Überblick Konfigurationsdateien (2)

- Login / Authentifizierungsmodule unter **./conf/authn** (LDAP, Username+Passwort, x509, Kerberos etc.)
- Logging: **logback.xml**
- SAML2 Name IDs: **saml-nameid.properties** und **saml-nameid.xml**
- Intervalle, in denen Konfigurationsänderungen diverser IdP-interner Dienste geprüft werden: **services.properties**
- Subject Canonicalization: unter **./conf/c14n**, insbesondere **simple-subject-c14n-config.xml** (Groß-/Kleinschreibung)
- Zugriff (IP-Bereiche) auf bestimmte Verwaltungsseiten: **access-control.xml**, Zuordnung unter **./conf/admin/general-admin.xml**

Weitere Anpassungsmöglichkeiten

- Velocity Templates für HTML-Seiten (Login, Logout, User Consent etc.) im Verzeichnis **./views**
- Sprachspezifische Properties, Beschriftungen unter **./messages**
- CSS Stylesheets, Grafiken, zusätzliche JARs, angepasste web.xml unter **./edit-webapp**
  → Änderungen erfordern Neu-Generierung des IdP-Servlets: **./bin/build.sh**
- **Zur IdP-Installation und -Konfiguration siehe unter https://wiki.aai.dfn.de/de:shibidp3**
- **[Beispiele, Demo]**

Wartung und Pflege (1)

- Abfrage **Status-Seite** unter
  `https://idp.uni-musterstadt.de/idp/status`
  IP-basierter Zugriff wird über `./conf/access-control.xml`
- **Certificate / Key Rollover:**
  https://www.aai.dfn.de/dokumentation/zertifikate/zertifikat-erneuern/
- **Update** (https://wiki.shibboleth.net/confluence/x/JoIgAQ):
  - Zuvor unbedingt die **Release Notes** lesen!!!
    https://wiki.shibboleth.net/confluence/display/IDP30/ReleaseNotes
  - Download der aktuelle Version unter
    https://shibboleth.net/downloads/identity-provider/latest/
  - Entpacken und `./bin/install.sh` ausführen
  - Als Zielverzeichnis die bestehende Installation auswählen (zuvor Backup erstellen!)
  - Dateien unter `./conf`, `./views`, `./messages` und `./edit-webapp` werden nicht überschrieben
  - Siehe auch https://wiki.aai.dfn.de/de:shibidp3upgrade

Wartung und Pflege (2)

- Monitoring und Statistiken
  - Cacti:
    https://wiki.aai.dfn.de/de:shibidp3monitoring
  - F-TICKS (anonymisiert, in erster Linie für eduroam)
    https://wiki.shibboleth.net/confluence/x/MYJKAQ
- Abwehr Brute Force mit fail2ban:
  https://wiki.aai.dfn.de/de:shibidp3fail2ban
- Secret Key Management (Cookies, Session Info)
  https://wiki.aai.dfn.de/de:shibidp3sealer
  Anleitung basiert auf Doku von SWITCH:
  https://www.switch.ch/aai/guides/idp/installation/#encryptionrotation
- Troubleshooting:
  https://wiki.aai.dfn.de/de:shibidp3troubleshoot
- User Deprovisionierung via Attribute Query
  https://wiki.aai.dfn.de/de:shibidp3userdepro

Vielen Dank für Ihre Aufmerksamkeit!

Ideen? Fragen? Anmerkungen?

Kontakt

Portal: https://www.aai.dfn.de

E-Mail: aai@dfn.de

Tel.: +49 30 884299-9124