Shibboleth/Federation Operator Tutorial

TIIME Workshop 2018

Speaker: David Hübner,
DAASI International

Date: 6 Feb 2018

Agenda

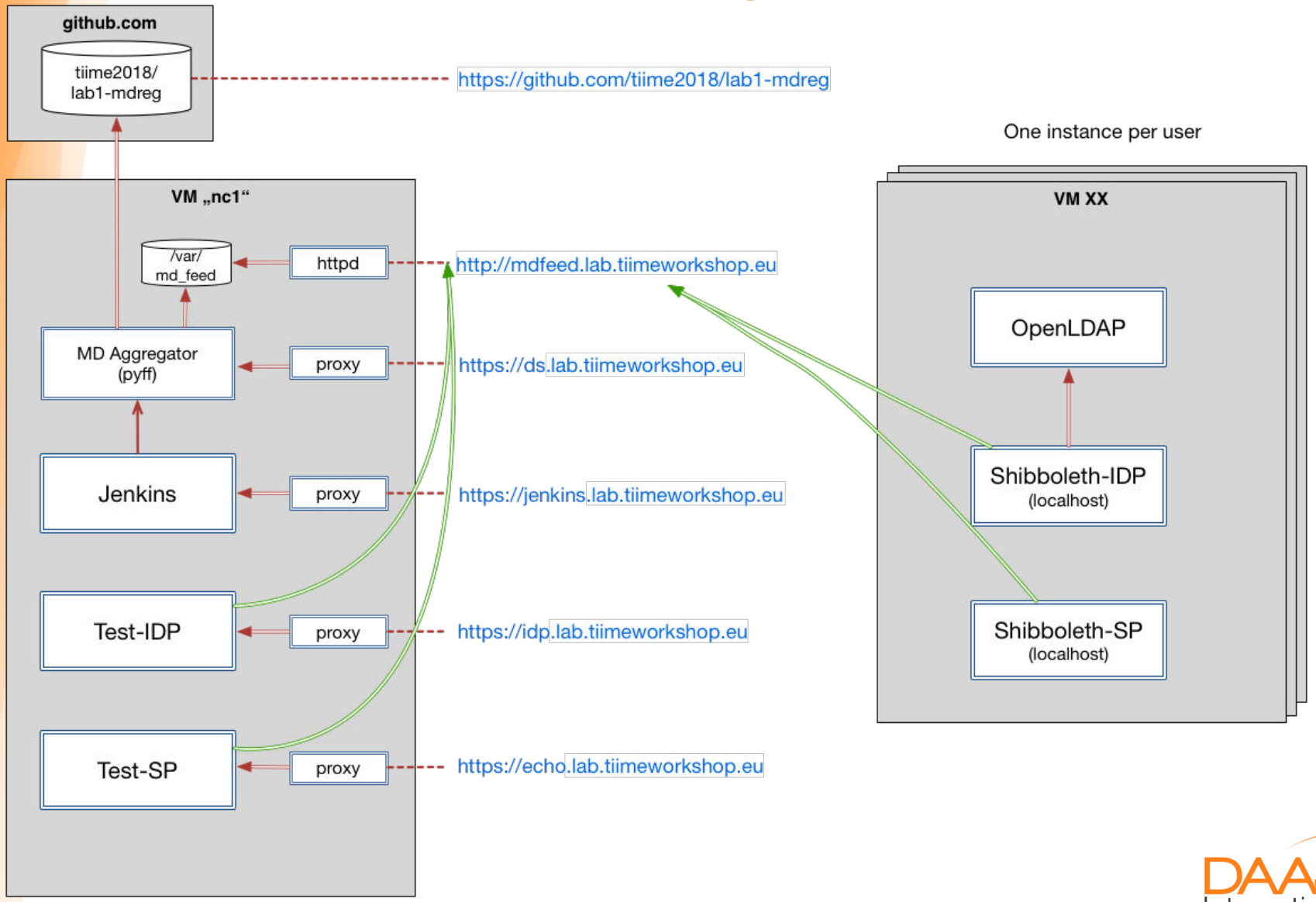
1. Welcome and Introduction to the Workshop
2. Introduction to Shibboleth
3. Federation Tools from Shibboleth
4. PyFF as an Alternative
5. Shibboleth IdP Hosting
6. Plugin Interfaces of Shibboleth IdP V3
7. Hands-On Session

DAASI International

Hands-On Session

DAASI International

Lab components



VM Software Stack

- *CentOS7*
- *Apache Webserver*
- *Tomcat 7*
- *OpenLDAP with some example users*
- Shibboleth IdP V3.3.2
- Minimal pre-configuration

DAASI International

Lab Exercise Step 1

- Download VM image [add link]
- Import in VirtualBox
- Boot into headless mode
- Connect via `ssh root@localhost -p 2222`
- Access https://localhost:1443 in your browser
  - IdP Status page should already work
  - SP quicklinks do not work (no SP installed yet)
- Install Shibboleth SP: `yum install shibboleth`
- Start shibd: `systemctl enable shibd --now`
- Restart Apache: `systemctl restart httpd`
- Now all the quicklinks should work

DAASI International

Lab Exercise Step 2

- Every entity (IdPs and SPs) in SAML is identified by a unique Entity ID
- In order for this lab exercice to work, every participant needs a unique Entity ID
- Configuration of SP in [/etc/shibboleth/shibboleth2.xml]
  - Change entityID in line 23 to something unique
  - e.g. https://localhost/shibboleth/[XX]
- Configuration of IdP in [/opt/shibboleth-idp/conf/idp.properties]
  - Change entityID in line 5 to something unique
  - e.g. https://localhost/idp/shibboleth/[XX]
  - Do the same for the IdP metadata in [/opt/shibboleth-idp/metadata/idp-metadata.xml]

DAASI International

Lab Exercise Step 3

- Restart shibd and tomcat
- Generate metadata and save it to some local folder
  - Rename the file to something meaningful
  - e.g user[XX]_sp.xml and user[xx]_idp.xml
  - Verify at https://mdval.test.portalverbund.at/
  - Upload to git at https://github.com/tiime2018/lab1-mdreg/tree/master/metadata/upload

Lab Exercise Step 4

- Generate new SP certificates
  - ./etc/shibboleth/keygen.sh -f
  - chown shibd:shibd *etc*shibboleth/sp-*
- Systemctl restart shibd

Lab Exercise Step 5

- Let‘s create the aggregated metedata!

DAASI International

Lab Exercise Step 6

- The SP and IdP on your VM need to load the aggregated metadata
- Aggregated metadata is available here: http://mdfeed.lab.tiimeworkshop.eu/metadata.xml
- MD signing certificate: http://mdfeed.lab.tiimeworkshop.eu/metadata_crt.pem
- Discovery service (DS): https://ds.lab.tiimeworkshop.eu/role/idp.html
- Configure SP
  - Download certificate
  - Adapt [/etc/shibboleth/shibboleth2.xml]:
    - Load metadata with above URLs
    - Change <SSO> Handler to DS
- Configure IdP
  - Adapt [/etc/shibboleth-idp/conf/metadata-providers.xml]

DAASI International

Lab Exercise Step 7

- Restart shibd and tomcat
- Access protected resource on localhost
- Whoops.
- Hint: [/var/log/shibboleth/shibd.log]

DAASI International

Lab Exercise Step 8

- Generate new SP metadata
- Edit IdP metadata and add some info in the <Extensions> element
  - ```
    <mdui:UIInfo>
      <mdui:DisplayName xml:lang="en"></mdui:DisplayName>
      <mdui:Description xml:lang="en"></mdui:Description>
    </mdui:UIInfo>
    ```
- Save IdP and SP metadata
- Check validity
- Upload to git

DAASI International
    ```

Lab Exercise Step 9

- Let‘s generate updated aggregated metadata :)

DAASI International

Lab Exercise Step 10

- Make your SP and IdP reload the metadata
  - Quick and dirty: just restart shibd and tomcat
- Once again access the protected resource on localhost
-

DAASI International

Lab Exercise Step 11

- Recall: configuration of attributes needs to happen on IdP and SP
- IdP in [/opt/shibboleth-idp/conf/attribute-filter.xml]
  - e.g. just to your SP‘s entityID
- SP in [/etc/shibboleth/attribute-map.xml]
  - Uncomment the relevant attributes
  - Change REMOTE_USER in [/etc/shibboleth/shibboleth2.xml]
- Restart shibd and tomcat

DAASI International

Lab Exercise Step 12

- Once again access the protected resource

DAASI International

Thanks!

https://www.daasi.de

DAASI International