SEE Identity Federation Training

(Hands-on IdP/SP/Discovery Service)

www.geant.org

OVERVIEW

Important Disclaimer :

This technical documentation should be used only during this training.

If you want to use it or share it with your communality you will need to update it with your own federation environments (ex: metadata, test infrastructure …).

- **Purpose of this documentation**
  - Technical documentation to install and configure identity management tools.
  - At the end of this workshop **you will be able to :**
    - Install and configure openLDAP
    - Install and configure an IdP Shibboleth V4.X
    - connect your IdP with your authentication systems (openLDAP, AD …)
    - Install and configure an SP Shibboleth V3
    - Install and configure a discovery service
    - Join a test federation
- **For whom ?**
  - Federation operators
  - Administrators of IdPs and SPs of research and education organizations
- **Duration :** 3 Days
- **Requirements Hardware:** CPU: 2 Core, RAM: 4 GB, HDD: 20 GB -> 1vm per participant , please contact Anass over slack to have access information.
- **Support and Help if needed during working hours and slots we defined earlier : April 6,8,13 : from 9am to 12pm & 14pm to 17pm (CET time) – Don't hesitate to help each other.**
  Register to slack channel → #technical-help-idp-sp-openldap-ds

OVERVIEW: PART 1

- **In this first part you will:**
  - Install and configure openLDAP
  - Install and configure an IdP Shibboleth V3
  - Connect your IdP with your authentication systems (openLDAP, AD …)
  - Connect your IdP with a SP
  - Connect your IdP with a test federation

- **Minimum basis for the training**
  - Knowledge of the Unix environment;
  - Knowledge of Apache / Jetty environment;

- **About this material**
  - This material can be useful to support self-training, if you have any specific needs, we recommend you to consult the official documentation of Shibboleth:
  - https://wiki.shibboleth.net/confluence/display/IDP4

All materials available:

- **OpenLDAP:**
  - https://github.com/ConsortiumGARR/idem-tutorials/blob/master/idem-fedops/miscellaneous/HOWTO%20Install%20and%20Configure%20OpenLDAP%20for%20federated%20access-CentOS.md
- **Shibboleth IdP**
  - https://github.com/ConsortiumGARR/idem-tutorials/blob/master/idem-fedops/HOWTO-Shibboleth/Identity%20Provider/CentOS/HOWTO%20Install%20and%20Configure%20a%20Shibboleth%20IdP%20v4.x%20on%20CentOS%20with%20Apache2%20%2B%20Jetty9.md
- **Shibboleth DS**
  - https://github.com/ConsortiumGARR/idem-tutorials/blob/master/idem-fedops/HOWTO-Shibboleth/Embedded%20Discovery%20Service/Ubuntu/HOWTO%20Install%20and%20Configure%20a%20Shibboleth%20Embedded%20Discovery%20Service.md

Important :

- **Replace all references to IDEM Federation by your test/production federation.**
- **Suggest to install and configure Apache Directory Studio.**
- **For Shibboleth IdP, the training should stop at chapter 5 included.**
- **Do not try to register your IdP to IDEM federation (ONLY FOR GARR organizations), From chapter 5.XIV please contact the trainers to be registered in a test Federation dedicated to this training.**

Additional information

- VM hostname : vm-0000XX.vm.geant.org
- Use the VM FQDN (vm-0000XX.vm.geant.org) or the institutional domain name as domain name instead of "**example.org**".
- Allow all the "**Strategy A**", the reccomended ones, not 'B'
- Allow http/https' traffic by running the following commands before start:
  - sudo firewall-cmd --permanent --zone=public --add-service=http
  - sudo firewall-cmd --permanent --zone=public --add-service=https
  - sudo firewall-cmd --reload

Useful information

- Useful data information for IdP:

  - IdP Full Qualified Domain Name (FQDN): vm-0000XX.vm.geant.org (where 'XX' is the number assigned to their VM)
  - Attribute Scope/Domain Name: vm-0000xx.vm.geant.org (for tutorial purposes) or institutional domain name instead of "example.org"
  - SSL Certificate path: /etc/pki/tls/certs/vm.geant.org.crt
  - SSL Private Key path: /etc/pki/tls/private/vm.geant.org.key
  - idp.attribute.resolver.LDAP.exportAttributes = cn givenName sn mail eduPersonAffiliation

recommended timeline for hands-on exercises :

- April 6: Follow all the HOWTO and create a working OpenLDAP server
  April 6: End the HOWTO with the step named "**Configure Shibboleth Identity Provider Storage**" included

- April 8: End the HOWTO with the step named "**Connect an SP with the IdP**" included
  April 8: End the HOWTO and **connect the IdP on the Test Federation**

- April 13: Follow all the HOWTO and create a working Service Provider server, connect it with the IdP and test the login

  April 13: Follow all the HOWTO and create a Discovery Service

  April 13: Follow all the HOWTO and create a working Service Provider server, **connect it with a test federation**

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).