COmanage

Understanding its role

Gerben Venekamp
SURFsara

September 29, 2017

DTLPrpgrammersmeeting@SURFnet – Utrecht

SURF SARA

What are Federations

Dictionary definition

federation

fɛdəˈreɪʃ(ə)n/

noun

plural noun: federations

1. a group of states with a central government but independence in internal affairs.
   “the Russian Federation”
2. the action of forming states or organizations into a single group with centralized control.
   “a first step in the federation of Europe”

Introduction of federations

https://aarc-project.eu/documents/training-modules/federations-101/

Why do you want federated login

- Increase reliability
  - As an SP you know you have a validated identity
  - When a person leave the organisation, access to resources is blocked
- Scalability
  - As an SP you have less work in account creation
- Increase security
  - Users use strong organisational passwords
  - Users provide their credentials on trusted pages only

AAI issues

What are we all trying to solve

1. Using identities from “external” IdPs
2. Giving people without an IdP access to services, eg. social IDs (Google, Facebook)
3. Federated access to non-web applications

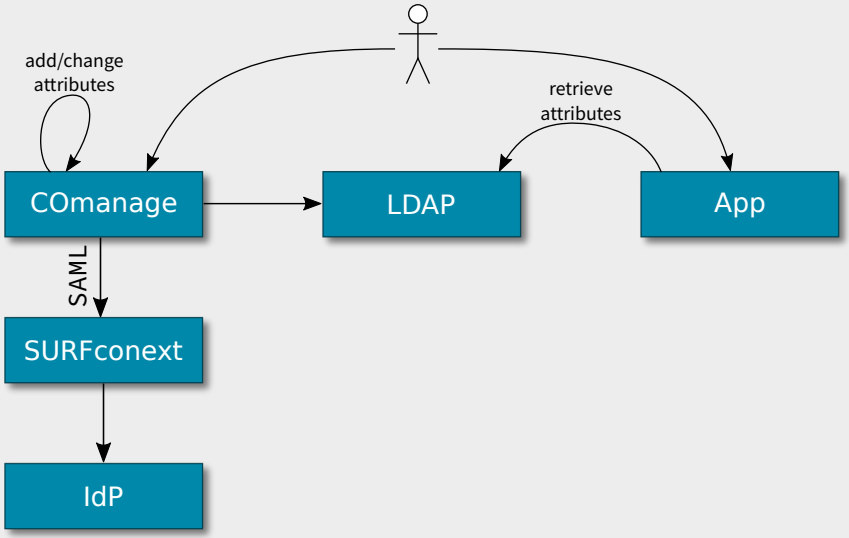
What is COmanage

- Tool for managing identities and attributes across multiple domains, such as a VOs and groups.
- Developed by Internet2: `http://www.internet2.edu/products-services/trust-identity/comanage/`
- COmanage wiki: `https://spaces.internet2.edu/display/COmanage/Home/`
- Built on top of CakePHP
- Needs `REMOTE_USER`
- Apache 2.0 license

COmanage Strengths

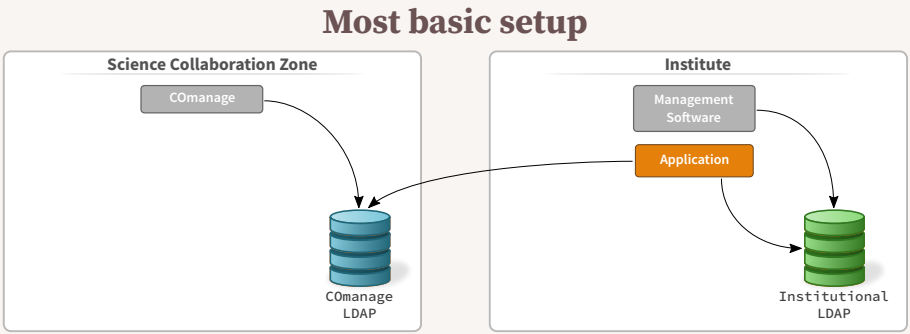
- Uses plugins to extend functionality
  - Enrollment flow
  - Provisioning
- Support for different roles: admin, CO-admin, member.
- Attribute aggregation: attributes from an IdP and attribute authorities act as a single source of information.
- Authenticated user is able to manage some of her own attributes, like her public SSH key.
- Attributes can be used for authorization decisions, i.e. based on more then just the attributes coming from an IdP.
- COmanage is an effective solution for non-web domain, i.e provision authorization data to LDAP.
- Auditing.

Flow


add/change
attributes
retrieve
attributes
COmanage
LDAP
App
SAML
SURFconext
IdP

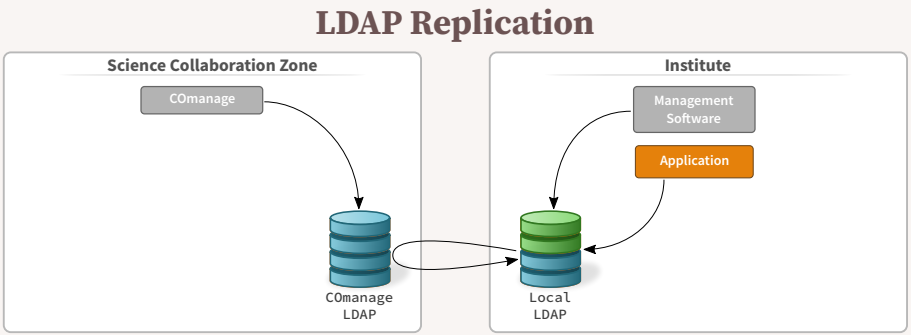
LDAP deployment

Basic LDAP depoyment model



LDAP deployment

LDAP replication depoyment model



What is SAML

tl;dr

- Use an identity that you already have, instead of getting yet another one.
- For web based services, i.e. works well with browsers
- Also for non-web based service, its called SAML ECP, but does not work so well.

What is SAML

What you always wanted to know, but never dared to ask

Of course you know what SAML is. Just in case you want some information, or are not sure of all the terminology used, below are a number of sources you can use:

- `https://blog.surf.nl/en/saml-for-dummies/`
- `https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language`

Science Collaboration Zone

A SURF project