Perun

Thematic Topics

Michal Procházka

Perun Days, CESNET, Prague, 16. 3. 2017

Outline

- Integration with O365 and Google Apps
- Integration with AD/LDAP/389 Directory
- Integration with social identity providers
- Advanced group management
- Import/export from other IdM systems

O365 Integration

- Using AD connector
  - Fast, but only partial management functionality
- Using REST API
  - Slow, more functions than AD connector
- Using PowerShell API
  - Slow, complete management functionality

Google Apps Integration

- Using google apps API
- Manage user within google groups
- Import/export possibilities
- Required business plan with at least one account for management
  - Can utilize personal google accounts for users

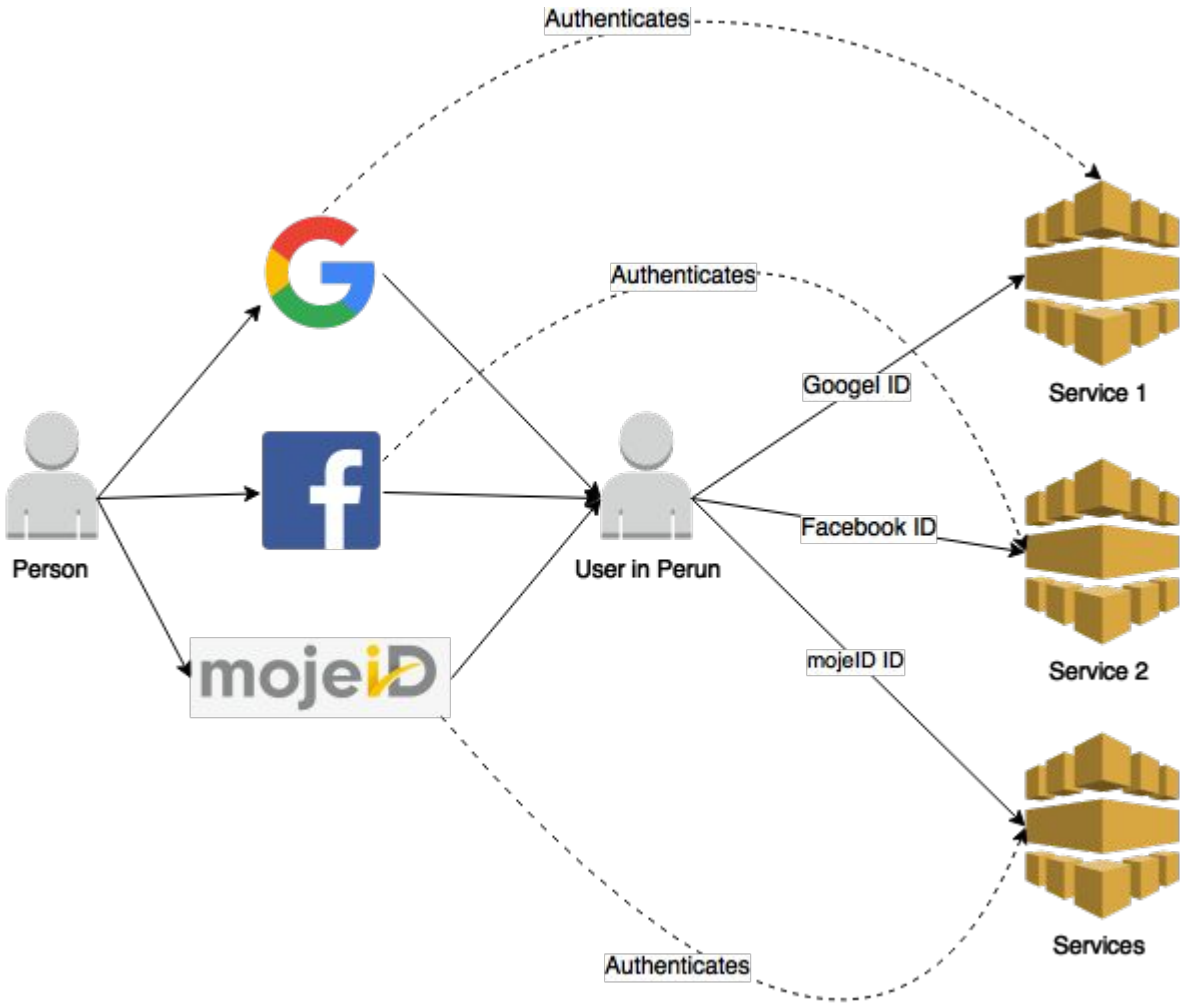
AD/LDAP/389 Integration

- Manageable using LDAP protocol
- Compare data from LDAP with data from Perun →push only difference
- Perun doesn’t manage passwords
- Create user in LDAP during user registration
  - Password will be stored there directly

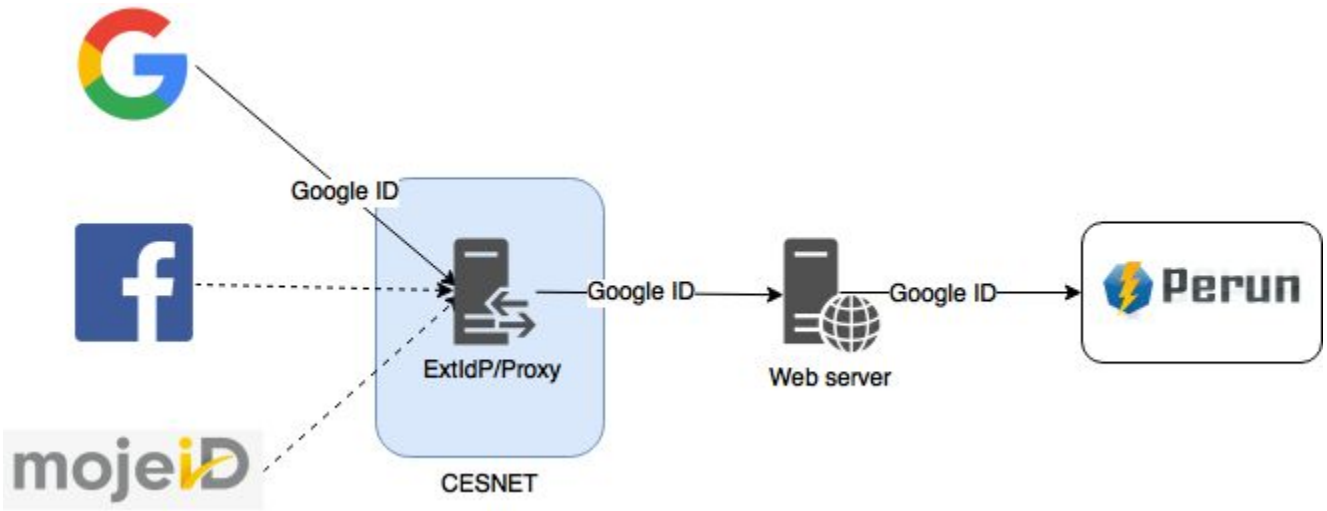
Social Identities Integration

- Perun can manage access to services which uses social logins
- Perun sits behind a web server
  - Web server provides user identity to the Perun
- Users can consolidate their social identity with organizational one
- CESNET’s extIdP/Proxy IdP

Social Identities Integration



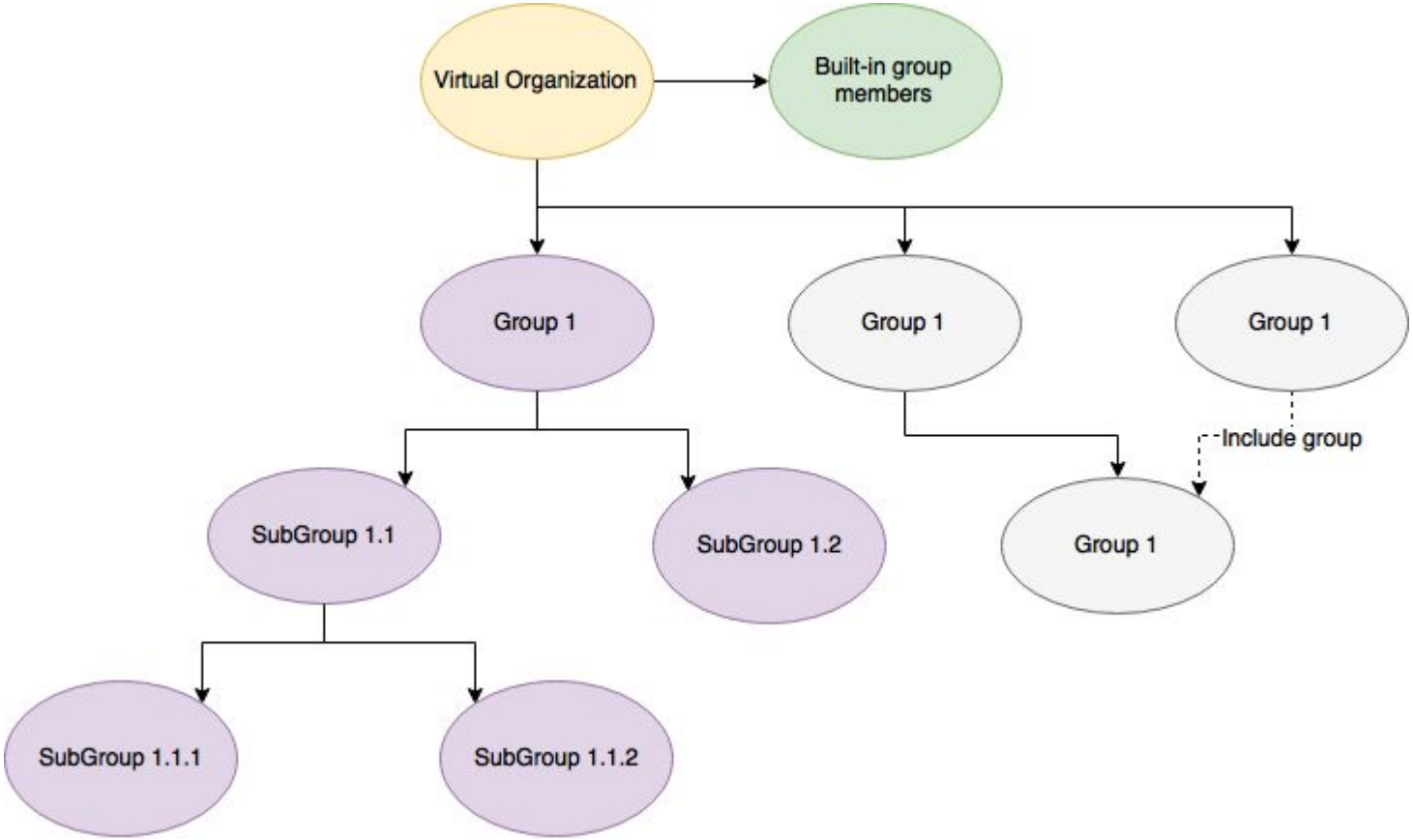
Social Identities Integration



Advanced Group Management

- Groups - unlimited subgroups
  - Tree hierarchy
- Include groups
  - Cross hierarchy dependencies
- Enrollment into the group
  - Same approach as for VO
- Groups can be synced with external sources

Advanced Group Management



Advanced Group Management

- Management of the group can be delegated to the users/service or another group
- Groups can have its own attributes
- Groups can be managed via GUI/CLI/API

Export

- Export is solved via PUSH propagations
  - Export data format is fully customizable
  - Perun must be authoritative source of data
  - Full state is propagated
    - Differences must be done outside Perun
  - Propagation is done on every change
  - Example: pushing data into the AD via LDIF

Import

- Import data about users
  - Customizable mapping between external source and attributes in Perun
  - Import is done to VO or to the Group
  - Import is run as a periodic job
  - Full and lightweight synchronization
  - Currently supported connectors
    - SQL, LDAP/AD, XML, CSV, VOOT, GoogleApps

Example of Import Definition

<attribute name="url">**ldaps://ldap.organization.org**</attribute>
<attribute name="base">**OU=Users,DC=organization,DC=org**</attribute>
<attribute name="query">**(CN=?)**</attribute>
<attribute name="loginQuery">**(CN=?)**</attribute>
<attribute name="user">**CN=perun,OU=System,DC=organization,DC=org**</attribute>
<attribute name="password">**password**</attribute>
<attribute name="referral">**follow**</attribute>
<attribute name="ldapMapping">
firstName={givenName},
lastName={sn},
login={cn},
urn:perun:member:attribute-def:def:mail={mail[0]},
urn:perun:member:attribute-def:def:organization=Masarykova univerzita,
urn:perun:user:attribute-def:def:login-namespace:mu={cn},
titleBefore={title|^(.*):.*},
titleAfter={title|^.*:(.*)},
additionalues_1=https://idp.org.org/idp/shib|cz.metacentrum.perun.core.impl.ExtSourceIdp|{cn}@organization.org|2
</attribute>

Perun

http://perun.cesnet.cz

perun@cesnet.cz