



Perun

WP3 meeting, Vienna

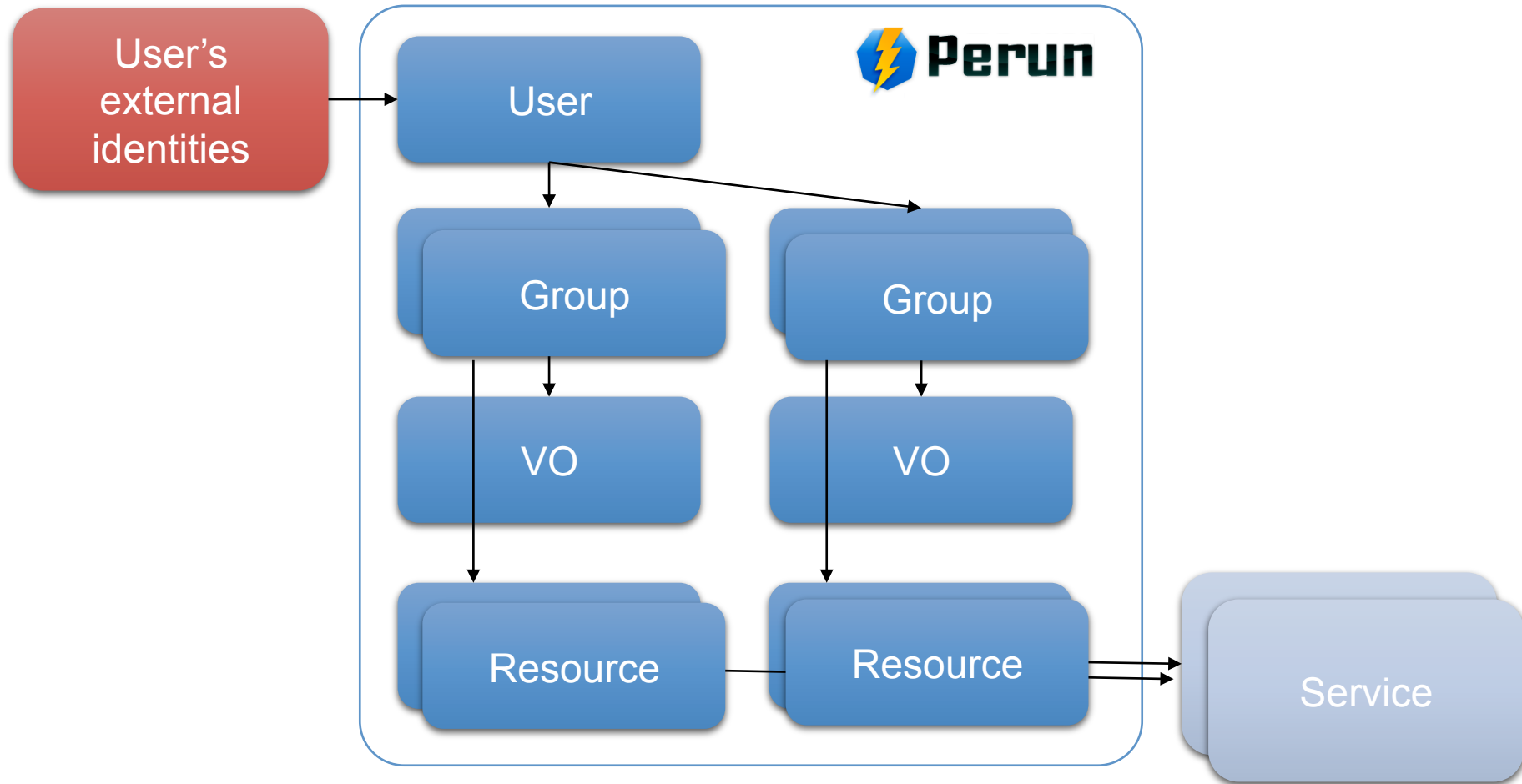
Michal Procházka | CESNET | 10. 3. 2016 | WP3

Brief overview



- Identity and Access Management system (IAM)
- Relies on existing users' identities
- Strong emphasis on delegation support
- Supports push and pull mechanisms to distribute ACLs
- Application integration via number of APIs
- Doesn't store any user's credentials
- Rich attribute management

Architecture



Users Management



- Users are organized into Virtual Organizations (VO)
 - VO has managers
 - VO has membership rules
 - VO has assigned resources
- Users can be organized into the groups within the VO
 - Subgroups are supported
 - Groups can have managers
- VOs and Groups can have its own enrolment schema
- Users can be imported into VOs and Groups

Enrolment Management



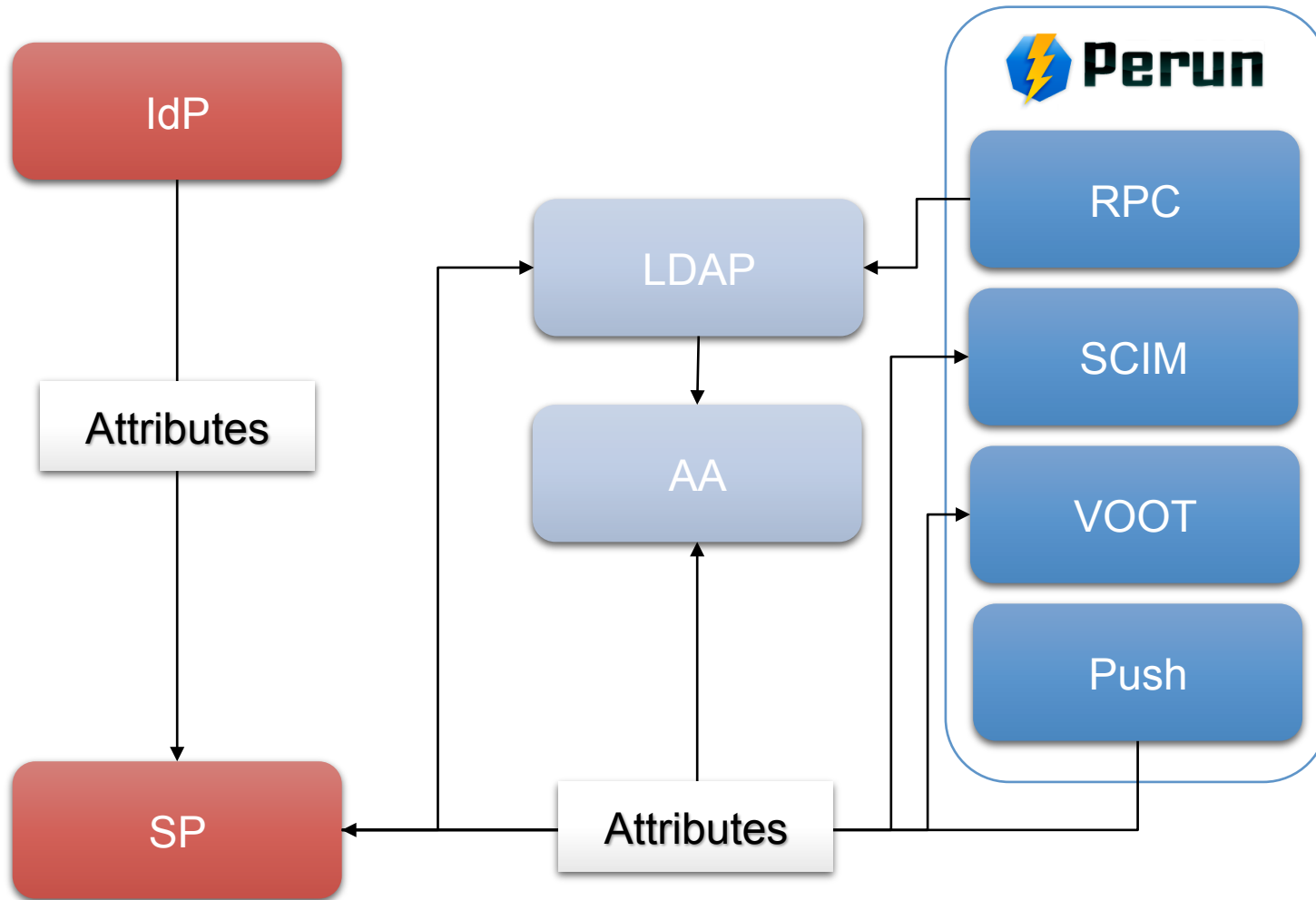
- Enrolment schemas
 - Application form
 - Invitation
 - Synchronization from external system
- Fully customizable VO/Group application form
 - Application form data can be filled with data from authN mechanism
- Invitation via e-mail
 - Fully customizable e-mail notification
- Synchronization from external system
 - Direct connection to LDAP/SQL/XML/VOMS/CSV/VOOT sources

Resource Management



- Service can be assigned to the VOs
 - E.g. storage service can be split among several VOs with different configuration
 - VO managers decide who can have access to the services
 - Access control is done by GBAC
- Perun delivers ACLs to services via various mechanisms
 - Push – directly push the ACL on every change
 - Pull – services can ask Perun via LDAP/VOOT/SAML2/...
- Owner of the service has full control over her service
- Support for Security Teams

Getting user's information



Interfaces



- Perun RPC
 - REST like interface
 - JSON
- Web GUI
 - JavaScript based application communicating with Perun RPC
- Perl/Java libraries
- PHP binding

Some Statistics



- 3 production instances
- CESNET's instance manages
 - > 200 virtual organizations
 - > 2000 services
 - > 15 000 users
- Masaryk University instance manages
 - > 60 000 users
- ELIXIR instance is integrated with IDP/SP proxy

Distribution and Development



- Open source (Apache licence) available on GitHub
 - <https://github.com/CESNET/perun>
- Services connectors available on GitHub
 - <https://github.com/CESNET/perun-services>
- Java based application
- Development tools: Maven, GIT and Jenkins
- Development supported by CESNET and Masaryk University

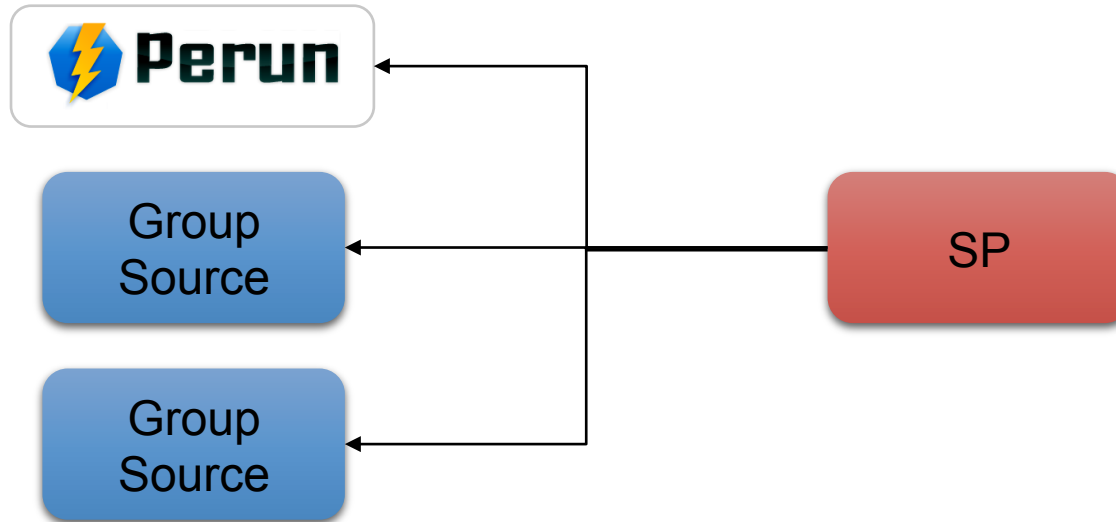
Relation to the GMF

Perun as a Proxy



Relation to the GMF

Perun as a Group Source



Status of the Pilot with DokuWiki



- ✓ <https://docuwiki-magic.cesnet.cz>
- ✓ Perun
- ✓ VO
- ✓ SP
- ✓ AA
- ✓ Authz rules

- Only new version of the DokuWiki is missing
 - Therefore no changes have been done to the DokuWiki



<https://perun.cesnet.cz>

perun@cesnet.cz

Michal Procházka | CESNET | 10. 3. 2016 | WP3