



Perun

User and Resource Management System

Michal Procházka

CESNET, Institute of Computer Science Masaryk University



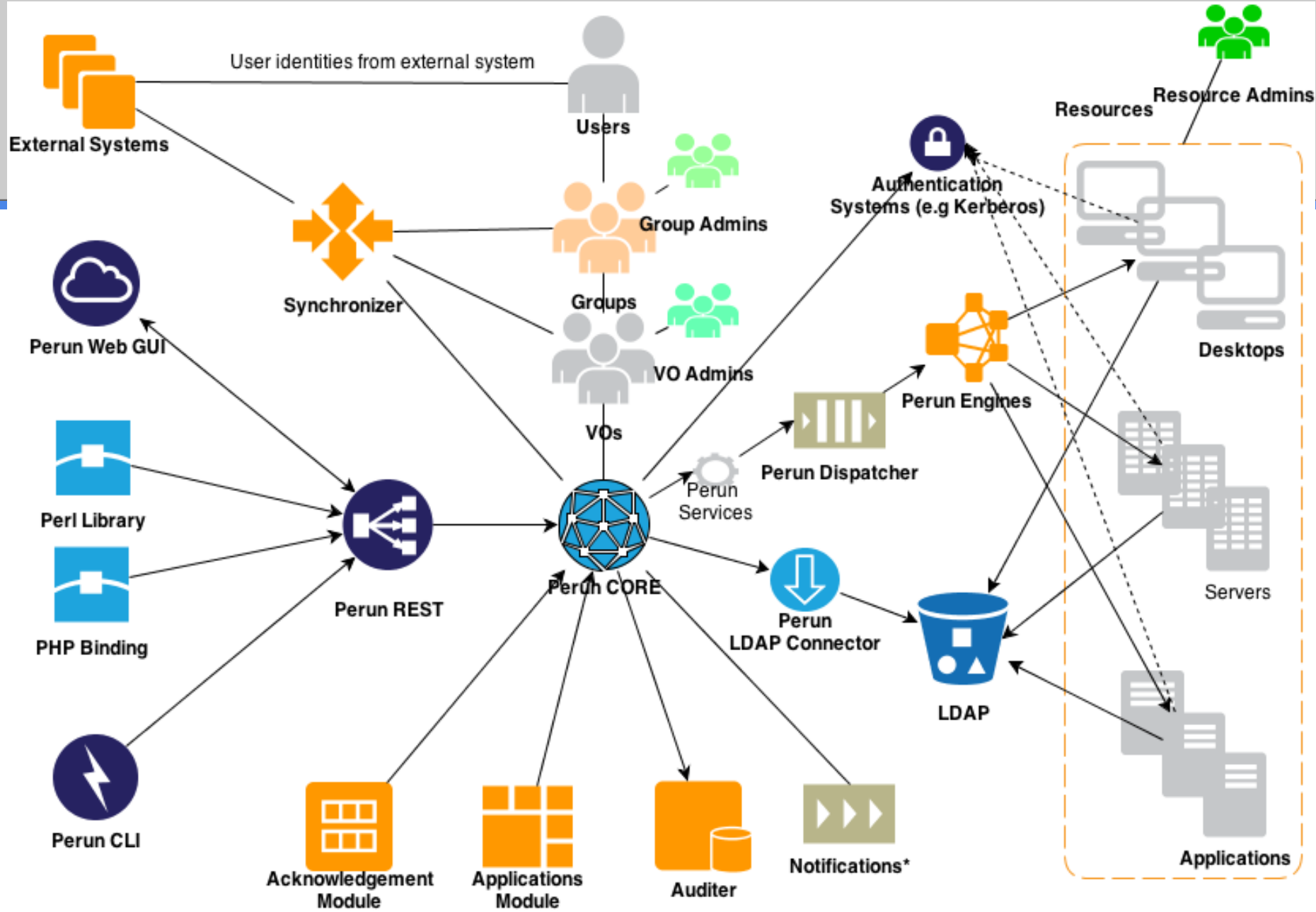
Motivation

- National Grid infrastructure
 - Users from different institutions
 - Different resource providers
- Difficult to manage such different entities
- User registration is needed
- Users already have some digital identity
- Delegation of the right to manage entities
- Configuration of the access rights
- Fill the gap between IF and end services



History

- Perun v 1 (1996-2002)
 - Managed access to the super computers at Masaryk University
- Perun v 2 (2002-2012)
 - Support for Grid resources across whole country
- Perun v 3 (2012-)
 - Support for virtual organizations and rights delegation
 - **Written from scratch**



* Not yet deployed in production



Perun manages

- Virtual organizations
- Users
- Groups
- Resources
- Services
- Application forms



User Management

- User can have assigned several external identities
 - Federated identities, X.509 certificates, social identities, SSH keys, Kerberos principals, ...
 - Identity consolidation
- Application forms
 - Each VO can define its own application form with various requirements on applicant
 - Prefilled information from external authN system



External Identities

https://perun.metacentrum.cz/perun-gui-krb/#usr/users;usr/detail?id=3354&active=1

Perun Now managing: voms2.grid.cesnet.cz Recently used: KYPO voms1.egee.cesnet.cz No active requests Name: Michal Procházka (change) Roles: SELF, PERUNADMIN Logout

Perun admin

Users x Michal Procházka: Full Details x

Information overview Vos, Groups, Accounts Resources Facilities External identity Publications Certificates, Logins, Passwords Service identities

+ Add - Remove

| <input type="checkbox"/> | UES ID | External source name | ID in external source | Level of as | Count: 19 |
|--------------------------|--------|---|--|-------------|-----------|
| <input type="checkbox"/> | 3414 | PERUNPEOPLE | michalp | 0 | |
| <input type="checkbox"/> | 4976 | PERUNPEOPLE | 6699 | 0 | |
| <input type="checkbox"/> | 5732 | META | michalp@META | 0 | |
| <input type="checkbox"/> | 6247 | LDAPMU | 39700 | 0 | |
| <input type="checkbox"/> | 6551 | https://idp2.ics.muni.cz/idp/shibboleth | 39700@muni.cz | 2 | |
| <input type="checkbox"/> | 7350 | EINFRA | michalp@EINFRA | 0 | |
| <input type="checkbox"/> | 14221 | LDAPCESNET | xprocha7 | 0 | |
| <input type="checkbox"/> | 18102 | /C=NL/O=TERENA/CN=TERENA Personal CA | /C=CZ/O=Masarykova univerzita/CN=Michal Procházka/unstructuredName=39700 | 2 | |
| <input type="checkbox"/> | 18103 | /C=NL/O=TERENA/CN=TERENA eScience Personal CA | /DC=org/DC=terena/DC=tcs/C=CZ/O=Masaryk University/CN=Michal Prochazka 39700 | 2 | |
| <input type="checkbox"/> | 18104 | /C=NL/O=TERENA/CN=TERENA Personal CA | /C=CZ/O=CESNET/CN=Michal Prochazka/unstructuredName=8497 | 2 | |
| <input type="checkbox"/> | 20545 | EGI | michalp@EGI | 0 | |
| <input type="checkbox"/> | 23055 | PERUNEGI | michalp | 0 | |
| <input type="checkbox"/> | 23121 | /C=NL/O=TERENA/CN=TERENA eScience Personal CA | /DC=org/DC=terena/DC=tcs/C=CZ/O=CESNET/CN=Michal Prochazka 8497 | 0 | |
| <input type="checkbox"/> | 23287 | https://login.ics.muni.cz/idp/shibboleth | michalp@meta.cesnet.cz | 0 | |
| <input type="checkbox"/> | 24254 | PERUNSIOLA | tauceti | 0 | |
| <input type="checkbox"/> | 24255 | PERUNPEOPLE | 6444 | 0 | |
| <input type="checkbox"/> | 24256 | SITOLA.FI.MUNI.CZ | tauceti@SITOLA.FI.MUNI.CZ | 0 | |
| <input type="checkbox"/> | 26992 | PERUN | 3354 | 0 | |
| <input type="checkbox"/> | 30054 | https://whoami.cesnet.cz/idp/shibboleth | xprocha7@cesnet.cz | 2 | |



VO and Group Management

- Build-in support for virtual organizations
 - Configurable application form
 - Initial and extension application type
 - VO manager role
 - Delegation of rights to the end users
 - Resource management
- Group management
 - Group manager role
 - Automatic synchronization with external systems
 - Support for VOOT protocol is under development



Resource Management

- Resources are assigned to the VOs
- Configuration of services
 - E.g. unix accounts, access to NFS storage systems, radius ACLs, mailing lists, ACLs for web applications
- Push mechanism
 - omit online queries
 - pushing only on change
- Alternatively publishes data through LDAP



LDAP and Attribute Authority

- Nearly real time synchronization with Perun Core DB
 - Reacts on each change in Perun (new member, change in group membership, ...)
- Attribute Authority can be connected to Perun LDAP



Attributes Management

- Every entity and also each relationship can have assigned attributes
- Different value types: string, number, array
- Attribute modules
 - check proper value of the attribute
 - fill default values



Application Interfaces

- Complete set of functions of each Perun component is available through API
- REST with JSON
- Perl and Java library
- PHP binding



Statistics

- In production since autumn 2012
- >2000 users
- >1800 machines
- 39 virtual organizations
 - national and also international VOs



Conclusion

- System for managing virtual organizations, groups and users
- Consolidate different user's identities
- User registrations
- Do the ACL configurations for services
- Additional value for IF
 - Group management
 - Attribute authority



Thank you for your attention

<http://perun.metacentrum.cz>

CESNET, Institute of Computer Science Masaryk University