Perun – Modern Approach for User and Service Management

Michal PROCHÁZKA¹, Slávek LICEHAMMER², Luděk MATYSKA³
CESNET, Zikova 4, Prague, 160 00, Czech Republic
¹Tel: +420 549 496 141, Fax: +420 224 320 269, Email: michalp@ics.muni.cz
²Tel: +420 549 497 591, Fax: +420 224 320 269, Email: slavek@ics.muni.cz
³Tel: +420 549 492 101, Fax: +420 224 320 269, Email: ludek@ics.muni.cz

Abstract: In this paper we are introducing the identity and access management system called Perun. The system provides functionality which covers management of the whole user life cycle in nowadays e-Infrastructures, from user enrolment into the e-Infrastructure to user expiration. The Perun system supports management of virtual organizations, rights delegation, group management and enrolment management for making flexible user management easy to use. In comparison to ordinary identity management systems Perun also provides service and access management. Perun is a complex tool which eases management of research communities or users and services within the organizations. Perun system is used in production on national and international level; selected real deployments are described in this paper too.

Keywords: identity management, identities consolidation, access management, authorization

1. Introduction

An increasing number of services used by researchers require some kind of authentication and authorization. The motivation is quite straightforward, services cost money, represent unique devices or cannot be used indiscriminately, and service providers must know who exactly is accessing the service even if the service is provided free of charge. Therefore proper identification of users must be in place in order to make authentication and authorization doable. Generally user identification is made by Identity Management System (IdM) and is usually done at the user’s home institution or by the third party like social networks. However this is not cure for all situations, because all the service providers would have to believe the users’ identity issuers (e.g. home institutions or social networks) doing identity vetting well. Such trust network is obviously not feasible due to the complexity of peer to peer trust and privacy issues.

In this paper we are introducing an identity and access management system called Perun [1] which addresses problems of identity and access rights management. The system was originally developed for managing users and services in highly distributed environments like computational and storage grids [2]. As IT in general moves towards distributed environments and clouds, Perun started to be useful also for organizations and research groups which facilitate IT services (e-Infrastructures). Perun covers the whole user life cycle in e-Infrastructures from user enrolment, through management of access rights to the expiration of user account. Perun does not work just with users’ identities; it is able to store additional information about the users, organizing them into groups and virtual organizations. Last but not least, groups can be assigned to the services which mean members of the group have a right to use the service. This is the main difference from classical IdM systems, as Perun thus also provides capabilities to manage access control lists at the services. Generally Perun manages users and access rights to services.
Perun is a general tool, but its particular deployment does not require extensive configuration to be done. Perun by default supports several types of deployment with defined set of functionality. It is well suited for organizations or research groups which want to manage access to its services and do not have any identity management system in place or have several heterogeneous identity management systems and they want to consolidate user identities from all of them. Perun can support even more complicated deployments, like sharing a running instance between several institutions, reducing thus the operation costs while providing full functionality.

Up to now we have several successful deployments of the Perun. Current experiences show that Perun helps with managing users and services for small projects within the organization. It is also used for managing virtual organizations in EGI [3] infrastructure and also provides support for real institutions like universities.

This paper is organized as follows. The first chapter describes the whole concept of Perun system. Next two chapters explain how Perun does the identity and groups management. Third chapter is dedicated to the resource and services management. The paper is finished with the chapter describing real deployments of the Perun.

2. System Concept

Initial motivation for developing Perun was to create a system which will be able to manage users and services of the Czech National Grid Infrastructure (MetaCentrum [4]) which has computational and storage resources spread around the country where the users, administrators and user support are from different organizations based in different locations. MetaCentrum provides its services (nearly 10000 CPU cores and 3.5 PB of data storage) to around 700 users from academic area. There are other challenges, for example how to create user accounts on all the machines and services, this obviously cannot be done manually. Also users’ account expiration and suspension must be done automatically in such environment. During the deployment we have discovered that the Perun system can ease user and service management also for other projects and institutions, what has been proved in practise.

In most cases institution or research group has some existing user management and resource management system, but it does not fulfil all the requirements put on modern systems, it does not scale well, it is not robust, it does not provide programmable interfaces and usually it lacks friendly user interfaces. Perun is designed to be placed into the existing infrastructures in order to deliver robust and scalable solution which consolidate existing data about the users and resources and provide management interfaces for users who are formally in responsible for the entities. Data consolidation is done by integrated import plugins which are able to get information from various sources. On the other hand Perun can export all stored information using different export plugins, so the integration can be done step by step. Rights delegation is crucial when we do not want to be dependent on system administrators while doing basic operations with users and resources. Therefore Perun can assign management roles to selected users.

In Perun two proven concepts are combined together in order to deliver reliable, robust and scalable solution. First concept known from the grid environment is Virtual Organizations (VO) where they are used for several years with success. VO is simply nothing else than a group of users with defined manager and set of rules which define who can be member of the VO. The benefit of having VO manager can be seen in situations when members of the VO want to use some services. Every user does not need to negotiate an agreement with the service provider; simply VO manager does the job for all the VO members as their representative. Perun can manage unlimited number of VOs of different sizes from few to thousands of members and services. Concept of the VO in Perun is
analogous to the VO in a grid environment, it contains members, groups and resources used by VO members. In Perun we use term resource which describes service used by the users.

The second concept implemented in Perun is the push mechanism used for delivering configurations to the end services. New configuration is sent to the service only if there is some change, also the service stores its configuration locally, so interruption of the Perun service does not affect managed services.

Perun is built from several building blocks which have clearly defined and narrow functionality. The main blocks are core, RPC, registrar and dispatcher with engine. Perun core takes care of data and operations with users, virtual organizations, groups, resources, facilities and services. Perun RPC component is the main programmable interface of the Perun. Other components or external systems can communicate with Perun through the RPC. RPC exports all the functions from the core via HTTPS interface using JSON as a data container. On the top of the Perun RPC there are two user interfaces, command line tools and web based GUI, see Figure 1. Perun registrar is a component dedicated to the user enrolment and registration form management. Dispatcher and engine are responsible for distributing the access control lists and configurations to the managed end services.

For the purpose of this paper we will discuss only those Perun components which are directly dedicated to the identity and resource management.

3. Identity Management

3.1 User life cycle

We have to look at the user account in the identity management system from the wider perspective. The user life cycle is a set of operations with the user’s data. The operations cover all the steps from the user admission into the (virtual) organization till the purge of
the data about the user. User usually goes through the steps mentioned below (some of them are depicted in Figure 2):
1. User fills the application form.
2. User somehow proves that data filled in application form are credible.
3. Identity management system creates an user account.
4. User can be enlisted in the groups.
5. User account expires.
6. User can ask for extension of the membership.
7. User account is deleted.

From the organization’s manager point of view having all the steps mentioned above in one system is crucial, because state of the user account is consistent in every moment. Having group, enrolment and user management systems separated causes problems with synchronization and keeping data consistent.

![Figure 2: Enrolment, VO and propagation management schema](image)

3.2 Enrolment management

In order to get users into a VO, they have to provide information required by the policy of such VO. Usually some contacts and personal information are required. For this purpose Perun is equipped with the Registrar component used to support whole enrolment management. Registrar can be used for creating custom application form to the VO and for
managing the users’ applications. VO manager can define arbitrary fields on the application form. Based on the optional authentication system guarding the application form (e.g. federated login, social networks login, digital certificate) some fields can be filled by values gathered from the authentication system. Applications can be approved/denied automatically or manually by the VO managers. VO manager can also define extension application form which is used for VO members who want to extend theirs membership. Extension registration form usually shows the information about the users stored in Perun and user is required to verify or update the information.

3.3 External systems

In the case where an organization has some existing IdM system Perun can import or periodically synchronize user identities or groups between each other. Perun provides two types of import. We can define external source which is recipe how to get data about the user from existing IdM system. VO manager then can search users in Perun web interface using the external source. The second type is used for group synchronization. VO manager can create group within the VO and set up synchronization of the group with the users from external system. Based on the defined period, Perun synchronizes users with the external source.

4. Group Management

Users are enrolled into the virtual organizations in which they can be additionally organized into the groups and subgroups. Each group can have defined manager who consequently manages memberships in the group. Also it is possible to create an application form, in the same fashion as for the VO, for membership in the group. That allows end users to apply for the group membership by themselves without need of any action from the group manager. In this case the group manager only needs to approve submitted applications or even further he can set the application to be approved automatically. Goal of Perun is not to overstress users in any role. Hence there is always a possibility to delegate part of work, from VO manager to group manager or to end users themselves.

Groups play crucial role in resource management. By assigning group to resource all the members from the group gain rights to utilize the resource. Because of that it is strongly recommend having a group for each purpose or role in the VO. Usually users tend to create group for each resource or for set or resources with very close purpose, e.g. "group of users with administrator privilege on machine X". Solution suggested and supported by the Perun is to create groups based on real roles, e.g. "group of administrators" and then assign these groups to appropriate resources, for example to resource representing administrator access on the machine X. Using such approach users management becomes easier because when the new user comes into VO, she is put into group according to her role in the VO and she immediately gets an access to all the resources which she needs for work. Moreover if she needs some more resources then with high probability all members within the same group (with the same role) need these resources too. In such situation VO manager simply assigns additional resources to this group.

This workflow has strong requirements for establishing purposeful roles within the VO, which can be unaccustomed for VO managers at first. It usually requires paradigm shift in way how users are managed so far, but it will definitely pay up at the end. Therefore Perun is trying to support this workflow as much as possible and not only in Perun itself but also in documentation and tutorials.

On the other hand the described workflow is not enforced by any component in Perun. Anyone can pick any suitable solution for her use-case or customize Perun in any possible
way. To sum it up, Perun is not only provided as a tool, but also as well-established workflow for managing users and resources.

5. Resources Management

To make resource management efficient, requirements of both involved parties, the services providers and the managers of virtual organizations have to be considered. Services providers need to have an easy way to make their services (resource) available to the VO. Moreover they want to do none or only minimal changes to theirs service in order to support users from the VO and full control of the whole configuration process. On the other hand VO managers only need to enable their users to utilize the resources.

We used so called facility as a basic unit for resource management in Perun. The facility is configurationally homogeneous entity which provides the services. The facility can represent host, cluster, storage element, wiki page and so on. The only condition for the facility is that the setting is the same for whole facility.

When the facility configuration is finished the services provider can make an agreement with any VO, particularly with the VO managers. The agreement should cover conditions under which VO members can use the service. The service provider than can create a resource for these VOs. Resource defines technical conditions and restrictions on usage of the facility by the VO. Consequently the VO manager can decide which users from the VO can use the resource or delegate this right to any group manager.

Described behaviour is the key feature of resource management in Perun because service providers do not want to take care of each individual user. The whole resource management is reduced only to the initial settings which really make overall configuration process as easy as possible.

5.1 Services

In the context of Perun we need to distinguish between the Perun service and the service which is consumed by the users. The Perun service is used for preparing and delivering the configuration for the consumed services.

Each Perun service has a set of required attributes which are necessary for the Perun service to run properly. Each attribute has its concrete name and well defined purpose, e.g. attribute represents name of the user or an email of the user. Attributes can be assigned to each individual entity and also to the relationship of the entities. Data stored in attributes are strictly validated in accordance to service requirements. Therefore Perun never propagate faulty or incomplete configuration to the service. The services which receive configuration from the Perun do not need to do any validation and integration checks of the data.

5.2 Propagations

We can assume that Perun holds desired state of all services configurations. Goal is to project this state to target services. To achieve that Perun provides two modes of configuration transport: pull and push model, see Figure 2 bottom grey box.

The pull mode is represented by an integrated LDAP server. Perun exports data useful for service configurations to the LDAP server hence the services can pull them from it.

In this case Perun prepares data for each service in a suitable format and then sends the data via selected communication channel. Configurations can be sent using simple file copy or email, jabber or any other standard system for exchanging data. The most common way is to send the configuration over the SSH which provides reliable authentication of each party. When the configuration end up at the target service, optionally so called slave script is executed and additional configuration tweaks are done. Using slave script the service
administrator can merge local configurations with the ones from the Perun or can instrument the service to reload the new configuration.

Slave scripts are managed completely by the administrator of the service. Therefore the administrator can control very precisely how the data from Perun affects configuration of the service.

Push mechanism is the preferred one, because when unpredictable outage of the Perun occurs, the services are not affected, because they do not do any online queries to Perun. The only disadvantage is that the service runs the last known configuration before the outage. At the end of the outage Perun will immediately send the up-to-date configuration (if changed).

6. Rights delegation

Perun was designed to support more than one group/VO/research community; therefore there was a strong emphasis on rights delegation. The operator of the Perun system is not needed for the management of VOs and users or resources. Perun has three basic roles and several derived roles. Main roles represent VO manager, group manager and facility manager. Managers have full rights to operate with theirs entities. The VO manager can introduce new members into the VO, define the registration form and assign VO groups to the resources. Obviously she can create groups and assign VO members as group managers. The group manager can only add or remove users from the groups where she is a manager. The facility manager is responsible for the services which are provided to the VO. The facility manager has full privileges over her services. The role of the administrator of the Perun is just creating the VO and then passing the rights to the VO managers, the rest of the work is done by the users. Therefore Perun can be deployed also on national or even on higher level.

7. Examples of real deployments

Perun is an open source project, so source codes can be downloaded from GitHub [5]. CESNET provides Perun also in two modes. Perun as a Software as a Services (SaaS) and a virtual appliance. SaaS is suitable only for deployments with very reliable network connection to the CESNET servers. Virtual appliance is well suited for cloud deployments and also for local installation. Thus Perun instance can run directly on a hardware owned by the institution and serves “nearby” users. This also solves potential privacy problems, when the personal data of the users cannot move outside a perimeter of the institution or the country (common legal requirements).

The Perun instance which runs at CESNET currently manages 89 national and international virtual organizations with 720 groups, over 2800 users and 1700 services. It is provided as SaaS. The main benefit for the users is that they have only one user account registered at Perun and they can request membership in any VO or group managed by this Perun instance. Users who participate in national and international projects appreciate such approach, they do not need to create user account per project. Moreover they can update personal information or settings (like e-mail address) in one place and this change will be consequently automatically propagated to end services.

In the next subsections selected real deployments are briefly described. We have selected one big project MetaCentrum, one small research project and one project associated with EGI cloud infrastructure.

7.1 MetaCentrum

MetaCentrum is the Czech National Grid Infrastructure providing thousands CPUs and petabytes of storage capacity to the users coming from academic environment all around
the country. MetaCentrum also utilizes resources from other national e-Infrastructure project called CERIT-SC [6], which provides comparable computational and storage capacity. Both MetaCentrum and CERIT-SC solves similar challenges.

As far as user management is concerned, Perun manages around 1400 users’ accounts on all machines in MetaCentrum and CERIT-SC infrastructure. Managing user accounts means that Perun has to prepare configuration for Linux machines and instrument them to create the UNIX accounts, configure storages, prepare user’s home directories with proper quotas set. Users are also put into several mailing lists, have an access to the wiki pages and request tracker system. From the VO manager point of view, Perun takes care of users’ enrolments into the MetaCentrum virtual organization. Also it can switch users’ accounts to expired state and notify user in advance before it happens.

MetaCentrum provides various software which requires user to accept the license. With the Perun this process is fully automated using automatically approved application forms for groups which represent individual software. The text of the licence is part of the group application form and the form cannot be submitted without an agreement of the licence.

### 7.2 C4E

C4E is a research project running at Masaryk University. It is a typical project with a two year lifetime. Members of the project are not only from Masaryk University but also from other academic institutions and private companies. Perun provides basic identity management, so all the members of the C4E project are listed in one place. For all the members basic services are provided like access to the restricted wiki pages, project management system and membership in mailing lists. For selected users a UNIX accounts on computers located in cloud are created.

### 7.3 Fedcloud

Fedcloud is an EGI initiative which provides an abstract layer on top of the various cloud providers. User can utilize cloud resources in the same way as grid resources. Perun is responsible for managing the user accounts at different cloud infrastructures, e.g. OpenStack or OpenNebula. Therefore it can be easily deployed on each Fedcloud site regardless of backend they use.

Different types of cloud infrastructures use different authentication mechanisms. Perun assures that each backend gets information about users' credentials which the particular backend requires. Moreover if the backend can provide several authentication mechanisms then Perun can provide required data for each of them, therefore the user can decide which authentication mechanism she wants to use to access the service.

To sum it up Perun is useful for Fedcloud mainly for its flexibility and ability to adjust itself to be compatible with existing widely heterogeneous infrastructures.

### 8. Possible deployments in developing countries

In the previous section we have described existing real Perun deployments. This section will introduce possible deployments advisable in developing countries which are limitations in relation to well-trained IT staff, IT resources and last but not least problems with power supply and network outages. Perun has been designed to overcome such limitations. Power or network outage affecting Perun system does not interrupt services which are configured using push mechanism. The Perun system is available as a pre-installed virtual appliance therefore installation is reduced only to configuration options specific for the particular deployment. Most of the administration in Perun is spread among defined roles resulting in low demands on persons who are interacting with Perun.
The next subsections briefly describe two services which play a major role in delivering valuable services and strengthen collaboration among researchers.

8.1 eduroam

eduroam [7] is currently the largest production federated service in academia. It allows academic users to connect to the network using credentials issued by their home organization. Researchers can easily roam among institutions not only within one country but also around the world and stay connected to the network. Currently eduroam is available in 67 countries.

eduroam infrastructure requires an authentication server located at the organization and connected to the identity management system of the organization. If an organization wants to participate in the eduroam project, it must deploy a database of the users, prepare a user registration process for identity vetting, provide user authentication service and run a radius server. All of these components except radius server are built-in in Perun, however radius can be easily connected to the Perun database. Deploying Perun is well suited for organizations with missing identity management system, built-in enrolment, group, user and resource management components provide all necessary functionality needed to setup and feed radius server for eduroam. Moreover the organization can use other Perun components which help with controlling access to the other IT services within the organization.

8.2 Identity federation

The concept of identity federations is quite old and nowadays it is used by all big players on the Internet, for example Google and Facebook provide their authentication system to be used by third party. Users can simply use their Google or Facebook login to access other services. In academia users federated identity is connected with a student or researcher account at their home organization in order to allow them to consume services available only for academic users. During the past years nearly 30 national academic identity federations have been established [9].

There is a similarity in concept with eduroam, users can use services located in other countries or institutions using their home organization’s credentials. Basic building blocks of the identity federation are identity provider (IdP) and service provider (SP). IdP acts as a component which authenticates users and is located at the user’s home institution. SP is the component providing services for the authenticated users.

The number of services and resources available using identity federations is still growing. Latest statistics show more than 5000 service providers are available within academic identity federations. Most of the digital content providers support federated login, also services proposed by the CHAIN-REDS [8] project are available using federated identity. Therefore it is advisable to provide federated identity for all the researchers and students by their home organization (university, academies of sciences, research communities). The requirements are similar as for eduroam infrastructure. Every user has to have an account at the identity management operated by her home institution. Identity federation does not provide only authentication of the user, but also transferring additional information about the user in order to provide data for authorization decision.

User's identity in Perun can have assigned various attributes therefore Perun can act as a backend for the IdP. Deployment is done just by installing Perun instance and identity provider software, all the required processes are ready to use in Perun. IdP can be then connected to the Grid Identity Poll (GrIDP) federation and users will have immediately access to the Science Gateways [10]. Services which have been available only within the organization and have potential to be useful also for users from other organizations can be
integrated into the federation, what is much easier to achieve than configure access for every user separately.

9. Economic benefits

Collaboration is essential for the research especially for researches from a developing country who want to share theirs results and ideas with researches from developed countries. IT services are well suited for enabling such collaboration across the world even in a real time. In order to personalize collaboration tools or to restrict access to the content within the collaboration platform proper identification of the users must be in place. Identification process heavily depends on proper identity management of the users and also selection of the particular technology used for user authentication with the services used for collaboration. All of this puts non trivial requirements on management of users and their credentials. Perun is delivering a whole ecosystem around the user and resource management, therefore when the organization or research community deploy Perun they can manage theirs users, group, users’ enrolments and resources without need to buy or maintain several separated pieces of software. Based on our experiences from national grid infrastructure we do not need to use any other software except Perun for managing whole ecosystem for shared resources provided for the researches. All examples of real deployments mentioned in section 7 run on a single instance of Perun which significantly reduces costs on the maintenance and management.

10. Conclusion

In this paper we have described Perun, a user and resource management system which is able to do the access management. The Perun system targets mainly distributed environments and also geographically spread user communities. Easy deployment and wide range of functions covering users’ enrolment, identity consolidation, group management and services configurations predestine Perun as a tool which eases adoption of technologies like eduroam, PKI, identity federations and shared resources. Using Perun research communities from within the organization or even from different parts of the world can access shared resources in an easy and secure way. Perun lowers the bar which is needed for managing access to the IT services, especially in developing countries where there is lack of IT specialists and resources. Research communities can focus on theirs research and they do not need to spend time setting up and configuring access to the services like wikis, mailing lists, network, etc. Even more the Perun deployment at a NREN level can act as Software as a Service for all connected institutions and therefore significantly reduce demands on human and IT resources.

Acknowledgment

Perun development has been supported by CESNET under "Projects of Large Infrastructure for Research, Development, and Innovations" (LM2010005) and programme Center CERIT Scientific Cloud, part of the Operational Program Research and Development for Innovations, reg. no. CZ. 1.05/3.2.00/08.0144. Promotion of the Perun in the developing countries is made under the CHAIN-REDS project umbrella.

References


