

Systém pro správu uživatelů a zdrojů



Michal Procházka

Slávek Licehammer, et al.

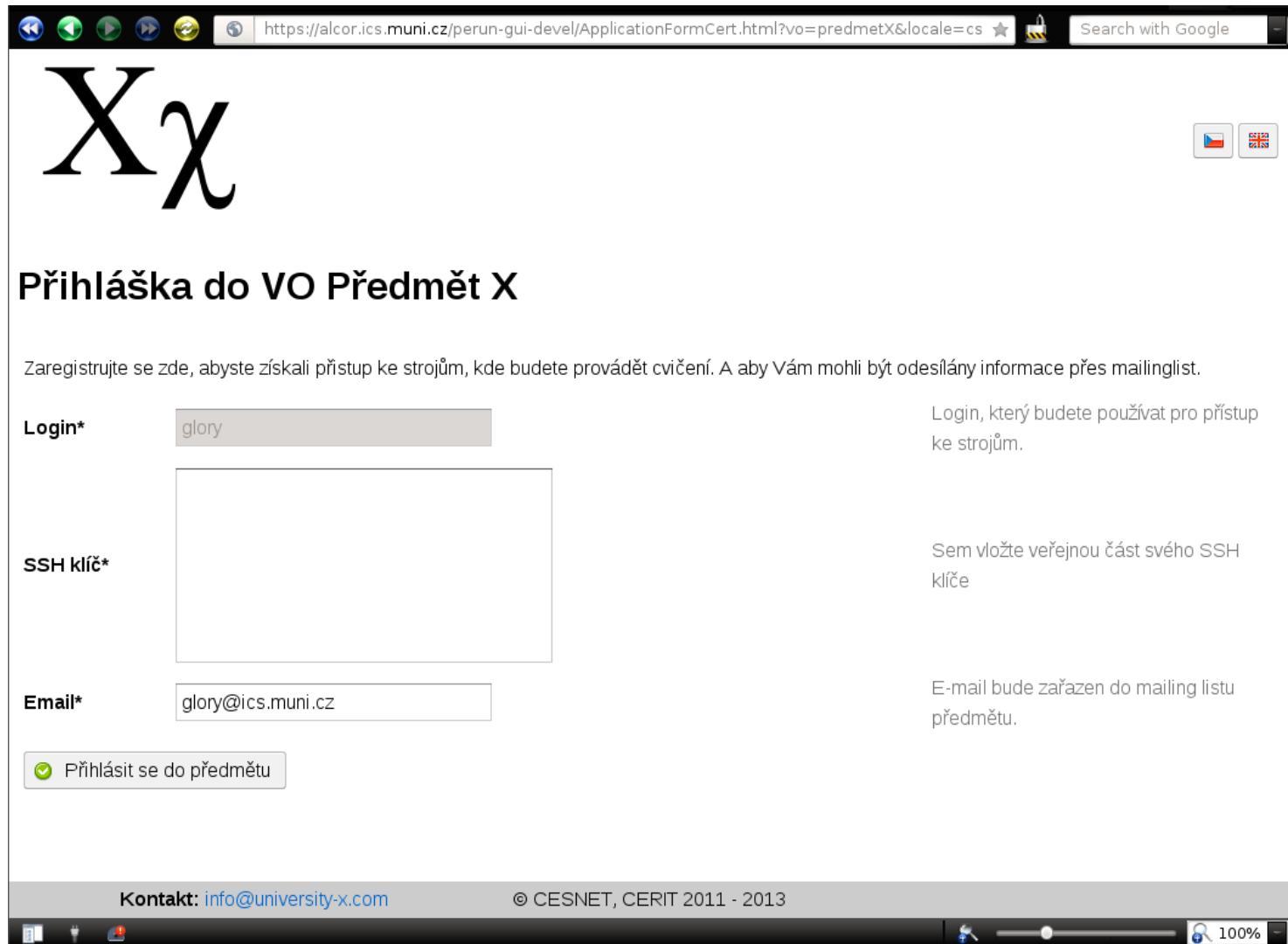
Ukázka využití

- Praktické cvičení pro předmět X
- Účastníci předmětu
 - Studenti
 - Konzultanti z komerční firmy
- Povolit přístup na stroje pomocí SSH klíče
- Zřídit mailing list pro každou skupinu

Požadavky

- Identifikovat uživatele
- Získat dodatečné informace od uživatele
- Zařadit do odpovídající skupiny
- Konfigurace služeb

Přihláška



The screenshot shows a web browser window with the URL `https://alcor.ics.muni.cz/perun-gui-devel/ApplicationFormCert.html?vo=predmetX&locale=cs`. The page features a large 'X χ ' logo at the top left and two language selection icons (Czech and English) at the top right. The main heading is 'Přihláška do VO Předmět X'. Below this, a paragraph explains the purpose of the registration. The form consists of three input fields: 'Login*' with the value 'glory', 'SSH klíč*' (empty), and 'Email*' with the value 'glory@ics.muni.cz'. To the right of each field is a descriptive text. At the bottom left is a checkbox labeled 'Přihlásit se do předmětu'. The footer contains contact information and copyright details.

X χ

Přihláška do VO Předmět X

Zaregistrujte se zde, abyste získali přístup ke strojům, kde budete provádět cvičení. A aby Vám mohli být odesílány informace přes mailinglist.

Login* Login, který budete používat pro přístup ke strojům.

SSH klíč* Sem vložte veřejnou část svého SSH klíče

Email* E-mail bude zařazen do mailing listu předmětu.

☒ Přihlásit se do předmětu

Kontakt: info@university-x.com © CESNET, CERIT 2011 - 2013

Přístup na přihlášku

- Studenti přistupují na přihlášku pomocí federované identity
- Konzultanti z komerční firmy si vytvoří účet na Hostelu
- Každou přihlášku schvaluje učitel předmětu

Stav přihlášek

https://alcor.ics.muni.cz/perun-gui-devel/PerunWebKrb.html#vo/list;vo/detail?id=60561;vo/appls?ic

Search with Google

Perun Now managing: Recently used: [predmetx.cesnet.cz](#) No active requests

Name: Slávek Licehammer
Roles: SELF, PERUNADMIN

Perun admin

VO manager

Předmět X
Members
Managers
Groups
Resources
SLDs
Facilities states
External sources
Settings
Applications
Application form

Group manager

Facility manager

User

VOs x Předmět X x Předmět X: applications x

Verify Approve Reject Delete State: All Filter Submitted by:

	Created date	Type	State	Submitted by	Loa	Group	Count: 3
<input type="checkbox"/>	2013-03-18	→	REJECTED	Pavel Zlámal	0	...	glory@META
<input type="checkbox"/>	2013-03-18	→	VERIFIED	Michal Štáva	0	...	stava@META
<input type="checkbox"/>	2013-03-17	→	APPROVED	Slávek Licehammer	0	...	glory@META

Perun © CESNET, CERIT 2011 - 2013 license 100%

Nastavení přihlášky

The screenshot shows the Perun web interface. The top navigation bar includes the Perun logo, a 'Now managing' status, and a 'Předmět X' link. The sidebar on the left contains navigation links for 'Perun admin', 'VO manager', 'Předmět X', 'Members', 'Managers', 'Groups', 'Resources', 'SLDs', 'Facilities states', 'External sources', 'Settings', 'Applications', 'Application form', 'Group manager', 'Facility manager', and 'User'. The main content area displays the 'Předmět X: application form' configuration page. It includes a 'Save' button, an 'Add' button, a 'Copy from VO' button, and a 'Preview' button. The 'Approval style' is set to 'Manual' (INITIAL) and 'Manual' (EXTENSION). The 'Module name' is 'Předmět X'. The table below lists the form fields:

Short name	Type	Preview	Edit
	HTML_COMMENT	Registrační formulář pro předmět X.	Edit Delete
username*	USERNAME	<input type="text"/>	Edit Delete
ssh_key*	TEXTAREA	<div></div>	Edit Delete
email*	VALIDATED_EMAIL	<input type="text"/>	Edit Delete
	SUBMIT_BUTTON	Create login	Edit Delete

The footer of the interface shows the Perun logo, the copyright notice '© CESNET, CERIT 2011 - 2013', and a 'license' link.

Správa skupin

- Dvě skupiny v rámci předmětu
 - konzultanti
 - studenti
- Každá ze skupin má obraz i jako unixová skupina
 - Definována unikátním jménem a GIDem
- Každá skupina reprezentuje i mailing list

Skupiny v rámci VO

The screenshot shows the Perun web interface. The top navigation bar includes the Perun logo, a search bar, and a status bar indicating 'No active requests'. The sidebar on the left contains navigation links for 'Perun admin', 'VO manager', 'Předmět X', 'Members', 'Managers', 'Groups', 'Resources', 'SLDs', 'Facilities states', 'External sources', 'Settings', 'Applications', and 'Application form'. The main content area displays the 'Předmět X: groups' page, which includes a table of groups.

<input type="checkbox"/>	Name	Description	Count: 4
<input type="checkbox"/>	administrators	Group containing VO administrators	
<input type="checkbox"/>	members	Group containing VO members	
<input type="checkbox"/>	konzultanti	Externí konzultanti předmětu X	
<input type="checkbox"/>	studenti	Studenti předmětu X	

The footer of the interface shows the Perun logo, copyright information '© CESNET, CERIT 2011 - 2013', a license button, and a zoom level of 100%.

Řízení služeb

- Řízení přístupu na unixový stroj
 - Vytvoření unixového účtu na cílovém stroji
 - Vytvoření domovských adresářů
 - Příprava souboru `authorized_keys` pro SSH
- Mailing list
 - Konfigurace mailmana, vytvoření dvou mailinglistů podle skupin

Přiřazené služby

The screenshot displays the Perun web interface in a browser window. The address bar shows the URL: `https://alcor.ics.muni.cz/perun-gui-devel/PerunWebKrb.html#vo/list;vo/detail?id=60561;vo/resource`. The interface includes a top navigation bar with the Perun logo and a sidebar on the left with various management tools. The main content area shows details for a resource with ID 117737, named `predmetx.cesnet.cz`, located at facility `predmetx.cesnet.cz`. The description is "Přístup na stroj predmetx.cesnet.cz". Below this, the "Assigned services" tab is active, showing a table of assigned services. The table has columns for a checkbox, "Name", and "Count". Four services are listed: `fs_home`, `group`, `passwd`, and `sshkeys`, each with a count of 4. The interface also shows a "Now managing" status for "Předmět X" and a "Recently used" status for "predmetx.cesnet.cz". The bottom of the page features a footer with the Perun logo, copyright information "© CESNET, CERIT 2011 - 2013", a license link, and a search bar.

Perun

Now managing: Předmět X Recently used: predmetx.cesnet.cz No active requests

Name: Slávek Lichehammer Roles: SELF, PERUNADMIN

Perun admin

VO manager

Předmět X

Members

Managers

Groups

Resources

SLDs

Facilities states

External sources

Settings

Applications

Application form

Group manager

Facility manager

User

VOs x Předmět X x Předmět X: resources x predmetx.cesnet.cz x

Resource ID: 117737 Resource Name: predmetx.cesnet.cz Facility: predmetx.cesnet.cz Description: Přístup na stroj predmetx.cesnet.cz

Assigned groups Assigned services Service settings

+ Assign - Remove

<input type="checkbox"/>	Name	Count: 4
<input type="checkbox"/>	fs_home	
<input type="checkbox"/>	group	
<input type="checkbox"/>	passwd	
<input type="checkbox"/>	sshkeys	

Perun © CESNET, CERIT 2011 - 2013 license 100%

Distribuce informací

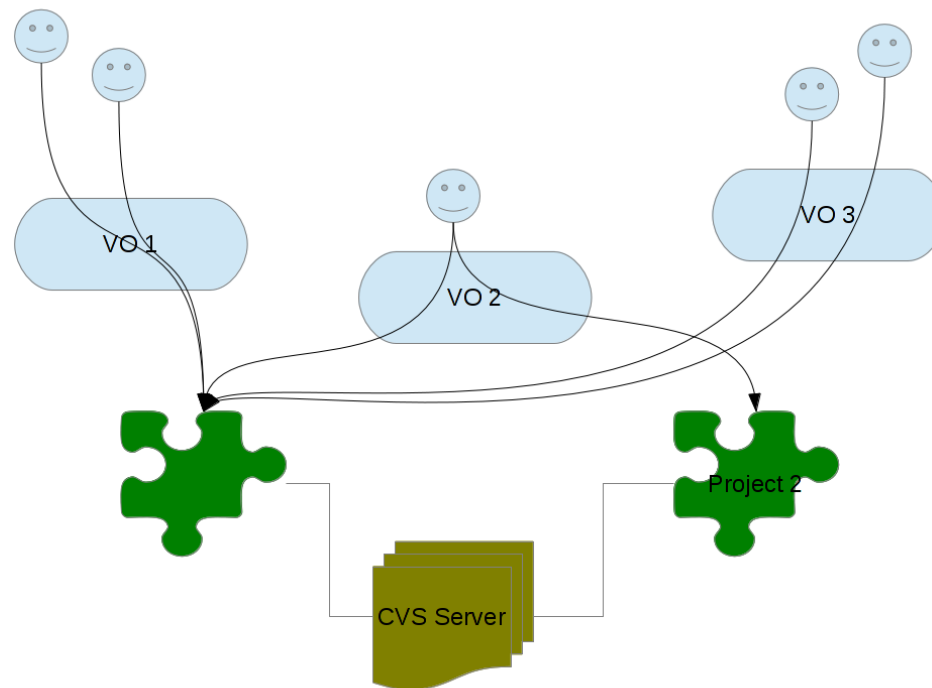
- Propagace
 - Mechanismus pro distribuci konfigurací
 - Minimalizace single point of failure
 - Propagace pouze při změně
 - Konfigurovatelný transportní mechanismus
 - SSH, FTP, e-mail, Jabber, ...
- LDAP
 - Pro aplikace vyžadující "vidět" změny okamžitě

Závěr

- Z pohledu uživatele
 - Přístup na přihlášku a vyplnění informací
 - Obdrží notifikaci o úspěšném schválení přihlášky
- Z pohledu učitele předmětu
 - Vytvoření přihlášky
 - Vytvoření skupin
 - Schvalování přihlášek
 - Přiřazování do skupin (lze automaticky)
- Z pohledu administrátora stroje a mailmana
 - Definování parametrů služeb passwd, group, fs_home a mailman
 - Instalace klienta perun-slave na stroje

Přístup na stejnou službu z více VO

- Příkladem je CVS server
- Lidé z různých VO pracují na společných projektech



Rozhraní Peruna

- Uživatelské
 - Webové GUI
 - CLI
- Programátorské
 - REST + json
 - Perl knihovna
 - Java knihovna
- Podporované autentizace
 - Federace, X.509, Kerberos, anonymní přístup

Demo vytvoření nové služby

- Správa přístupu uživatelů na webovou aplikaci na základě federované identity

3

 Add

<input type="checkbox"/>	defaultHomeMountPoint	resource	def	String	Default mount point for members
<input type="checkbox"/>	defaultShell	resource	def	String	Default shell for members
<input type="checkbox"/>	defaultUnixGID	user_facility	def	Integer	null
<input type="checkbox"/>	desc	facility	def	LinkedHashMap	short description
<input type="checkbox"/>	description	group	core	String	null
<input type="checkbox"/>	description	resource	core	String	null
<input type="checkbox"/>	disk	facility	def	LinkedHashMap	Description of installed disks
<input type="checkbox"/>	displayName	user	core	String	User's display name
<input type="checkbox"/>	eduPersonAffiliation	member	opt	String	User's affiliation
<input type="checkbox"/>	eduroamIdentities	user	def	ArrayList	List of eduroam identities
<input checked="" type="checkbox"/>	eppn	user	def	String	null
<input type="checkbox"/>	filesLimit	member_resource	def	Integer	Hard quota for number of files
<input type="checkbox"/>	filesQuota	member_resource	def	Integer	Soft quota for number of files


```

#!/usr/bin/perl
use strict;
use warnings;
use perunServicesInit;
use perunServicesUtils;
use File::Basename;

our $SERVICE_NAME = basename($0);
local $::PROTOCOL_VERSION = "3.0.0";
my $SCRIPT_VERSION = "3.0.0";

perunServicesInit::init;
my $DIRECTORY = perunServicesInit::getDirectory;
my $data = perunServicesInit::getHierarchicalData;

my $dir = "$DIRECTORY/$::SERVICE_NAME";
mkdir $dir or die "Can't create dir $dir: $!";

our $A_U_EPPN;      *A_U_EPPN = \urn:perun:user:attribute-def:def:eppn';
our $A_F_APACHE_AUTHZ_FILE; *A_F_APACHE_AUTHZ_FILE = \urn:perun:facility:attribute-def:def:apacheAuthzFileFed';

my %facilityAttributes = attributesToHash $data->getAttributes;

my $file = "$dir/$SERVICE_NAME";
open FILE, ">$file" or die "Cannot open $file: $!";

my $pathFile = "$dir/path";
open PATHFILE, ">$pathFile" or die "Cannot open $pathFile: $!";
print PATHFILE %facilityAttributes{$A_F_APACHE_AUTHZ_FILE};
close PATHFILE or die "Cannot close $pathFile: $!";

foreach my $rData ($data->getChildElements) {
    foreach my $memberAttributes (dataToAttributesHashes $rData->getChildElements) {
        print FILE "require user ", $memberAttributes->{$A_U_EPPN}, "\n";
    }
}

close(FILE) or die "Cannot close $file: $!";

perunServicesInit::finalize;

```

```
#!/bin/bash
```

```
PROTOCOL_VERSION='3.0.0'
```

```
function process {
```

```
    ### Status codes
```

```
    I_CHANGED=(0 '${DST_FILE} updated')
```

```
    I_NOT_CHANGED=(0 '${DST_FILE} has not changed')
```

```
    E_DEST_PATH=(50 'Problem with getting destination file path from $FROM_PERUN_DIR/$DIR/path')
```

```
    create_lock
```

```
    DST_FILE=`cat "$WORK_DIR/path"`
```

```
    [ $? -eq 0 ] || log_msg E_DEST_PATH
```

```
    CHANGED=0
```

```
    # Create diff between old.perun and .new
```

```
    diff_mv "$WORK_DIR/apache-fed" "${DST_FILE}" \
```

```
        && log_msg I_CHANGED && CHANGED=1 || log_msg I_NOT_CHANGED
```

```
    if [ $CHANGED -eq 1 ] ; then
```

```
        /etc/init.d/apache2 force-reload
```

```
    fi
```

```
}
```

Perun

Now managing: fe.du1.cesnet.cz

No active requests

Name: [Slávek Licehammer \(change\)](#)

Roles: SELF, PERUNADMIN

Perun admin

VO manager

Group manager

Facility manager

[All facilities states](#)

[fe.du1.cesnet.cz](#)

[Hosts](#)

[Resources](#)

[Managers](#)

[Services propagation](#)

[Propagation status](#)

[Services destinations](#)

[Services settings](#)

User

Facilities

fe.du1.cesnet.cz (storage)

Facility ID: 762

Facility Name: fe.du1.cesnet.cz

Facility Type: storage

Hosts

Services propagation

Propagation status

Services destinations

Services settings

Allowed VOs

Managers

Owners

Reload

	Service	Type	Status	Scheduled	Started	Ende	Count: 12
<input type="checkbox"/>	fs_home	GENERATE	DONE	2012-12-12 16:48:08	2012-12-12 16:50:02	2012-12-12 16:50:05	
<input type="checkbox"/>	fs_home	SEND	PROCESSING	2012-12-12 16:52:12	2012-12-12 16:54:01	Never	
<input type="checkbox"/>	group	GENERATE	NONE	2012-12-12 16:48:08	2012-12-12 16:50:02	2012-12-12 16:50:04	
<input type="checkbox"/>	group_nfs4	GENERATE	NONE	2012-12-12 16:48:00	2012-12-12 16:50:02	2012-12-12 16:50:04	
<input type="checkbox"/>	group_nfs4	SEND	DONE	2012-12-12 16:52:00	2012-12-12 16:54:01	2012-12-12 16:56:53	
<input type="checkbox"/>	group	SEND	ERROR	2012-12-12 16:52:12	2012-12-12 16:54:01	2012-12-12 16:56:53	
<input type="checkbox"/>	passwd	GENERATE	NONE	2012-12-12 16:48:03	2012-12-12 16:50:02	2012-12-12 16:50:04	
<input type="checkbox"/>	passwd_nfs4	GENERATE	DONE	2012-12-12 16:48:00	2012-12-12 16:50:02	2012-12-12 16:50:03	
<input type="checkbox"/>	passwd_nfs4	SEND	PLANNED	2012-12-12 16:52:00	Never	Never	

Perun

© CESNET, CERIT 2011 - 2013

license

Zoom (100%) 100%

Now
managing:

fe.du1.cesnet.cz

Recently used:

aaieye.cesnet.cz

predmetx.cesnet.cz

✔ No active requests

Name: Slávek Licehammer

Roles:

Perun admin

VO manager

Group manager

Facility manager

→ All facilities states

fe.du1.cesnet.cz

 Hosts

Resources

 Managers

➡ Services propagation

 Propagation status

Services destinations

Services settings

User

Facilities

fe.du1.cesnet.cz (storage)

Tasks results: group SEND

Destination	Type	Service	Status	Time	Return code	Standard Message	Error Message
fe1.du1.cesnet.cz	host	group	DONE	2012-12-12 16:54:02	0	See debug log.	Slave script ends with return code: 0
fe2.du1.cesnet.cz	host	group	ERROR	2012-12-12 16:54:02	0	See debug log.	Group GIDs in group file are not uniq: 1001 1010
fe3.du1.cesnet.cz	host	group	DONE	2012-12-12 16:54:02	0	See debug log.	Slave script ends with return code: 0
fe4.du1.cesnet.cz	host	group	DONE	2012-12-12 16:54:02	0	See debug log.	Slave script ends with return code: 0
fe5.du1.cesnet.cz	host	group	DONE	2012-12-12 16:54:02	0	See debug log.	Slave script ends with return code: 0
fe6.du1.cesnet.cz	host	group	DONE	2012-12-12 16:54:02	0	See debug log.	Slave script ends with return code: 0

Statistiky

27 VO

ČEZtest, fedcloud.egi.eu, linkYX, ...

231 facilities

1800 strojů

1937 unikátních uživatelů

Dokumentace

- Uživatelská
 - <https://wiki.metacentrum.cz/wiki/Perun>
- Programátorská
 - JavaDoc

Aktuálně spravované služby

AFS	zakládání pts záznamů a uživatelských adresářů
fs_home, fs_scratch	zakládání uživatelských adresářů
fedcloud_export	správa uživatelských účtů pro FedCloud
group, group_nfs4, passwd, passwd_nfs4, passwd_scp, mailaliases	správa linuxového účtu
k5login, sshkeys	řízení přístupu k uživatelským účtům
k5login_root, sshkeys_root	řízení přístupu k účtu root
mailman	správa mailing listů
pbs_phys_cluster, pbs_pre	správa PBS serveru
apache_ssl	správa přístupu uživatelů na web na základě osobních certifikátů
flexlm_iptables	řízení přístupu k licenčnímu serveru flexlm pomocí iptables
users_export	export uživatelů pro potřeby accountingu na CESNETu
voms	správa uživatelů pro voms server
radius	řízení přístupu k WiFi

Kontakt

perun@cesnet.cz