

Evidence gridových uživatelů ve středoevropské virtuální organizaci

Zora Sebastianová¹ Aleš Křenek^{1,2}

¹Institute of Computer Science, Masaryk University,
Botanická 68a, Brno, Czech Republic

²CESNET, Zikova 4, Praha, Czech Republic

Datakon, 21. 11. 2005

META Centrum – český národní grid

- Grid (mřížka, „výpočtovod“) má za úkol vytvořit stejně snadný a všudypřítomný přístup k výpočetním zdrojům, jako je přístup k elektrické síti.
- V akademickém prostředí ČR bylo od r. 1996 budováno *META Centrum*, včetně následného zapojení do řady gridových projektů EU.
- Projekt je zastřešen sdružením CESNET, aktivně se účastní centra na ZČU, UK a MU.
- *META Centrum* sdružuje a obhospodařuje jak výpočetní zdroje, distribuované po celé republice, tak uživatele, působící v různých organizacích.

Evidence gridových
uživatelů ve
středoevropské
virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí

Perun – správa uživatelských účtů

- Systém Perun je nástroj zaměřený především na správu uživatelských účtů a souvisejících prostředků v *META Centru*. Cílem je udržet **přesný obraz** spravovaných prostředků a usnadnit manipulaci s nimi.
- Spravovanými prostředky jsou především superpočítače, PC clustery, a diskové kapacity.
- Aktuální konfigurace prostředků je udržována v relační databázi, schéma odráží konkrétní požadavky, integritní omezení apod.
- Relativně neobjemná databáze (stovky spravovaných počítačů, stovky aktivních uživatelů), velmi komplikovaná struktura dat a workflow.
- Změny provedené v databázi jsou důsledně propagovány na řízené stroje, které **nemusí být dostupné** v okamžiku provedení změny konfigurace.

Evidence gridových
uživatelů ve
středoevropské
virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí

Perun – služby

- Spravované prostředky jsou členěny do tzv. **služeb**.
Služba – logicky související část konfigurace spravovaných prostředků, kterou má smysl měnit atomicky, včetně zohlednění implementačních omezení.
- Služby jsou vždy směřovány k určitému *cíli* (serveru, clusteru počítačů apod.), na kterém má být provedena úprava, odrážející změnu spravovaných prostředků.

Evidence gridových
uživatelů ve
středoevropské
virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí

Přihláška uživatele *META Centra*

- Nový uživatel *META Centra* vyplní webový formulář přihlášky, jehož součástí je i seznam požadovaných účtů a počáteční heslo. Odesláním se jeho základní osobní údaje uloží v databázi a vygeneruje se přihláška k vytištění
- Podepsanou přihlášku, včetně potvrzení organizace, uživatel pošle poštou nebo doručí osobně na nejbližší kontaktní místo *META Centra*.
- Administrativní pracovník ověří shodu papírové a elektronické přihlášky.
- Správce kontaktního místa elektronickou přihlášku schválí. Uživateli jsou vytvořeny:
 - principál v systému Kerberos
 - diskový prostor na sdíleném systému souborů AFS
 - účty na „hlavních“ počítačích *META Centra*
- Správci dalších zdrojů explicitně schvalují dodatečné položky přihlášky.

Evidence gridových
uživatelů ve
středoevropské
virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí

Projekt EU EGEE a VOCE

- EU EGEE je zřejmě nejrozsáhlejší gridový projekt EU, cílem je vytvoření stabilní infrastruktury pro širokou komunitu uživatelů.
- V rozsáhlém gridovém prostředí přestává být afiliace uživatele k organizaci vypovídající, důležitá je momentální příslušnost uživatele k určitému projektu či oboru výzkumu.
- Uživatelé jsou sdružováni do tzv. **virtuálních organizací** (VO). Virtuální organizace autorizuje své uživatele a naopak správci zdrojů přidělují přístup na základě příslušnosti k VO.
- *Virtual Organization for Central Europe* (VOCE) byla vytvořena jako „catch-all“ VO pro uživatele ze střední Evropy.
- Zapojením do VOCE uživatel získává přístup k prostředkům projektu EGEE, včetně gridového middlewaru a dalšího softwaru a technické podpory.

Evidence gridových
uživatelů ve
středoevropské
virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí

Přihláška uživatele VOCE

- Získání **X.509 certifikátu** u uznávané CA, je použit i pro přístup k [www přihlášce](http://www.voce.org) do VOCE.
- Uživatel vyplní základní osobní údaje
- Standardní kontrola e-mailové adresy odesláním zkušebního e-mailu obsahujícího URL pro pokračování s přihláškou.
- Přihláška je zaregistrována a může být schválena administrátorem (podle příslušnosti k organizaci), nebo je po uplynutí tří dnů schválena automaticky.
- Schválením přihlášky uživatel získává:
 - dedikovaný účet na speciální počítač, tzv. *uživatelský interface*. Na tomto počítači je instalován veškerý software nutný pro spouštění a sledování úloh v gridovém prostředí (tzv. middleware).
 - propagování do autorizačních služeb VOCE

Evidence gridových
uživatelů ve
středoevropské
virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí

Odlišnosti v postupu přihlášení

- Počáteční autentizace X.509 certifikátem (v *META Centru* je zcela přihláška de-facto anonymní).
- Zcela eliminována papírová verze přihlášky (pokryto registrační procedurou CA).
- Aplikována „presumpce neviný“ – bez zásahu administrátora je přihláška automaticky schválena.
- Přihláška neobsahuje požadavky na účty na konkrétní počítače.
- Výrazně širší okruh administrátorů, autentizování X.509 certifikátem.

Evidence gridových
uživatelů ve
středoevropské
virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí

Implementace v systému Perun

- **Jádro systému beze změny.**
- Přidány statické datové záznamy v konfiguračních tabulkách.
- Přidána tabulka pro autorizaci „externích“ administrátorů.
- Nové služby pro ovládání autorizačních mechanismů VOCE.
- Specializovaná www aplikace pro uživatele VOCE (přihláška) a administrátory (odmítnutí přihlášky, správa seznamu uživatelů, ...).

Evidence gridových
uživatelů ve
středoevropské
virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí

Statické datové záznamy

- Cluster *voce* – virtuální cluster pro účely VOCE. Účty na tomto clusteru indikují příslušnost uživatelů k této VO. Jediným strojem, který je v rámci Peruna zahrnut v tomto clusteru, je uživatelský interface.
- Realm *VOCE* – primárním autentizačním prostředkem *META Centra* je Kerberos, nutno oddělit standardní jmenný prostor uživatelských jmen od jmen užívaných pro VOCE. To umožňuje uživatelům používat v rámci VOCE specifické logname a heslo.
- Tabulka pro autorizaci externích administrátorů – přiřazuje určitou skupinu externích uživatelů k množině administrátorů, odpovědných za manipulaci s jejich daty. Uživatelé a jejich administrátoři jsou seskupováni podle svých certifikátů, resp. prefixů *subject name* těchto certifikátů.

Evidence gridových
uživatelů ve
středoevropské
virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí

Účty na výpočetních uzlech

- Účty na výpočetních uzlech gridu (v rámci VOCE i mimo něj) nespádají pod správu systému Perun přímo.
- Zpravidla na těchto počítačích ani nejsou vytvářeny dedikované účty pro každého uživatele; gridoví uživatelé zde spouští úlohy na několika málo speciálních účtech, které jsou používány opakovaně.
- V projektu EGEE fungují dva primární autorizační mechanismy
 - *grid-mapfile* – lokální autorizační informace, tj. mapování X.509 identit na lokální účty – generovaný z LDAPu
 - VOMS – služba poskytující speciální krátkodobé certifikáty obsahující i příslušnost k VO.
- Oba typy autorizačních dat jsou pro VOCE generovány systémem Perun při každé změně.

Evidence gridových
uživatelů ve
středoevropské
virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí

Služby a notifikace

● Služby

- *passwd* – původní služba, v rámci VOCE se uplatňuje na user-interface stroji pro aktualizaci souborů /etc/passwd a /etc/group
- *fs* – původní služba, v rámci VOCE se uplatňuje na user-interface stroji pro aktualizaci filesystemu.
- *voceldif* – služba určená k vytvoření a distribuci souboru ve formátu LDIF pro autorizační LDAP servery
- *voms* – služba aktualizuje databázi využívanou autorizačním gridovým systémem VOMS.

● Notifikace

- notifikace administrátorovi o vložení přihlášky – upozorňuje na možnost přihlášku rychle schválit nebo zamítnout
- notifikace uživateli o zamítnutí přihlášky
- notifikace uživateli o vytvoření účtu
- notifikace uživateli o blížící se expiraci účtů
- notifikace uživateli o zrušení účtu resp. pozastavení členství administrátorem

Evidence gridových
uživatelů ve
středoevropské
virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí

Shrnutí a nejdůležitější výsledky

- Evidence uživatelů VOCE představuje výrazné změny proti původním předpokladům:
 - uživatelé jsou autentizováni jiným mechanismem
 - nepočítá se se zcela jednoznačným mapováním identity uživatele na účet na výpočetním uzlu
 - množina uživatelů je přidělována ke svým administrátorům zcela novým mechanismem
- Řešení bez agresivních zásahů do systému Perun:
 - přidání jedné pomocné tabulky, umožňující nový mechanismus členění administrátorské odpovědnosti za jim příslušející uživatele
 - přímočaré rozšíření systému autorizace
 - přidání několika nových modulů služeb a notifikací
- Vypovídá o flexibilitě koncepce celého systému.
- Celkový přístup je potenciálně aplikovatelný i v jiném prostředí.

Evidence gridových uživatelů ve středoevropské virtuální organizaci

Z. Sebastianová,
A. Křenek

METACentrum

EU EGEE a VOCE

Implementace

Shrnutí