

Využití adresářových služeb (LDAP) v projektu MetaCentrum

Jiří Sitera

duben 2001

Tato technická zpráva shrnuje základní informace týkající se problematiky adresářových služeb (protokol LDAP) v rámci projektu MetaCentrum, především údaje o současném stavu a podklady pro další rozvoj.

1 Publikování informací (z MetaDatabáze)

1.1 Data k publikování

- *Informace o lidech*

Informace uchovávané v databázi o lidech, tj. osobní identifikační údaje plus technické informace specifické pro prostředí MetaCentra. Některé z těchto (technických) informací jsou centrálně udržované, některé jsou udržované v režii domovské buňky uživatele.

- *Informace o skupinách uživatelů*

Možnost definice členství jednotlivých uživatelů ve skupinách. Může být využito pro mnoho věcí, primárně je potřeba dotáhnout do funkčního stavu mechanismu centrální údržby přístupových listů k některému aplikačnímu SW.

- *Další informace*

Výhledově by bylo zřejmě účelné uvažovat o prezentaci dat například o existujících SW balících (název, komentář, URL k popisu), která by mohla sloužit např. jako zdroj pro generování částí MetaWebu.

Mezi statické informace publikované přes LDAP pak také určitě patří veškeré konfigurační informace, např. o zdrojích a sběru dat o nich (viz dále – v podstatě konfigurace skriptů pro sběr dat).

1.2 Využití dat

- *Základní „telefonní seznam“ uživatelů*

Kromě běžného přístupu přes LDAP např. pro klienty elektronické pošty také interface na MetaWebu.

- *Podpora infrastruktury MetaCentra*

Dle těchto informací je především možno generovat jednoduchými skripty /etc/passwd a mail aliasy na strojích v MetaCentru (automatické přesměrování na primární zadaný mail uživatele). Souvisí s funkcí MetaDatabáze a mechanismem elektronické přihlášky.

Z informací o příslušnosti lidí ke skupinám je možno generovat příslušné pts skupiny v jednotlivých AFS buňkách.

1.3 Členění dat

Jak již bylo výše zmíněno, základním zdrojem dat je centrální databáze (MetaDatabáze). Jistá část dat však může být udržována samostatně v režii buňky, přičemž centrálně je pouze definován způsob prezentace těchto dat. Základní přehled reprezentace dat poskytuje obrázek 1. Větev People reprezentuje centrálně udržovaná data o lidech a větev Accounts specifická data buňky. Více viz 1.6.

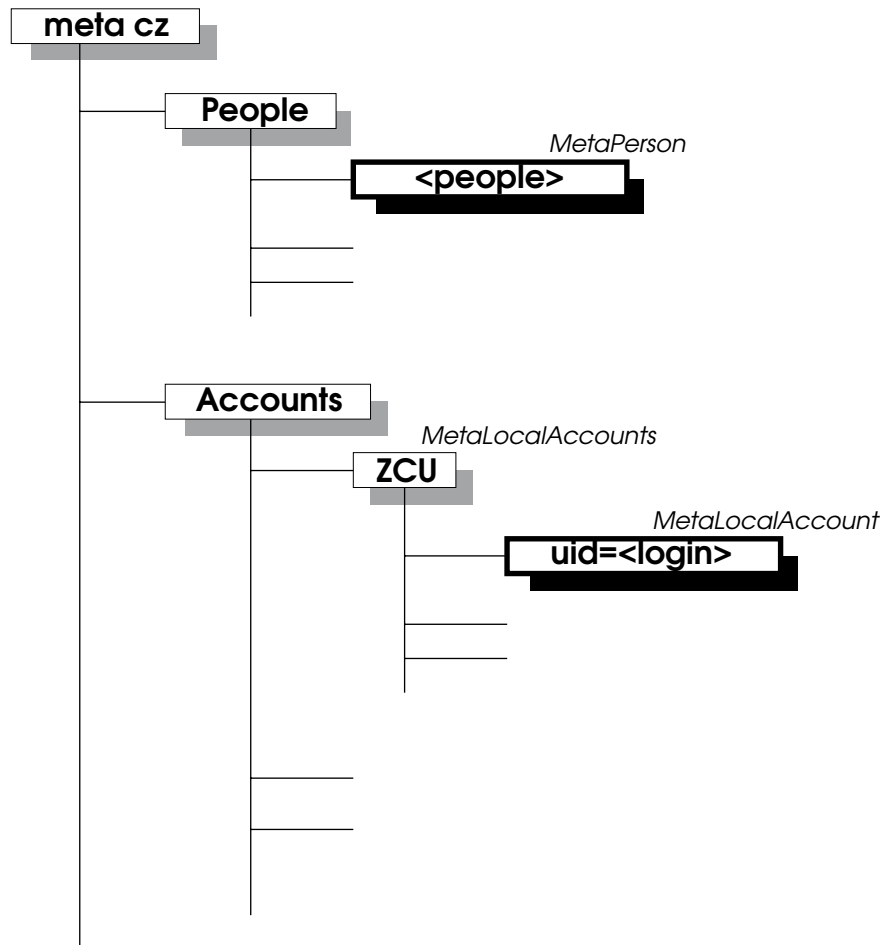
V některých případech je účelné udržovat informace o uživatelských kontech na konkrétních strojích včetně přidělených lokálních prostředků. Tento postup je uplatňován u singulárních uzlů MetaCentra (se speciální přístupovou politikou) jako je např. Origin 2000 v Brně. V případě potřeby mohou být tyto informace udržovány v centrální databázi nebo lokálně v režii buňky. V současné době existuje pouze doporučení pro způsob jejich prezentace v adresářových službách viz 1.9.

1.4 Návrh schématu informací o lidech

Návrh schématu MetaPerson vychází se standardního schéma inetOrgPerson. Rozšiřuje ho o specifické atributy homeCell, homeDirectory a loginShell. Tento postup je vhodný vzhledem ke kompatibilitě se standardními e-mail klienty.

1.4.1 Tvorba dn, rozlišovacího jména položky

Pro jednoznačnou identifikaci a zachování popisnosti se skládá ze dvou atributů. cn – jméno a příjmení a uid – uživatelské jméno.



Obrázek 1: Základní struktura adresářového stromu

Jméno atributu, alias	typ atributu	význam
commonName, cn	cis	jméno a příjmení osoby
surname, sn	cis	příjmení osoby
givenName	cis	jméno osoby
telephoneNumber	tel	telefonní číslo
mail	cis	e-mail adresa
postalAddress	cis	„snail mail“ adresa
organizationName, o	cis	Plné jméno organizace, ke které uživatel přísluší
uid	cis	identifikace člověka jakožto uživatele – uživatelské jméno
homeCell	cis	identifikace domovské buňky v rámci Meta
homeDirectory	cis	cesta k domovskému adresáři v globálním jmenném prostoru
loginShell	cis	implicitní shell uživatele
status	cis	stav uživatele (platný/blokovaný), viz níže
expires	cis	předpokládaná platnost konta v MetaCentru

Tabulka 1: Schéma MetaPerson

1.4.2 Význam atributu status

Sémantika hodnot, jež jsou užívány v položkách propagovaných do LDAPu musí být jasně definována jako (logická) součást schématu. V tuto chvíli je důležitá sémantika hodnot atributu status.

Hodnota atributu status	význam
ACTIVE	aktivní uživatel
DISABLED	pozastavený přístup
EXPIRED	uživatelské konto je již neplatné (záznam slouží pro účtování apod.)

Tabulka 2: Hodnoty atributu status

Sémantika hodnot, jež jsou užívány v položkách propagovaných do LDAPu musí být jasně definována jako (logická) součást schématu.

1.4.3 Přístup k datům

stroj:: ldap-meta.ten.cz

port:: 377

báze:: ou=People, o=meta, c=cz

```
ldapsearch -h ldap-meta.ten.cz -p 377 -b 'ou=People, o=meta, c=cz'  
'sn=sitera'
```

1.4.4 Vzorek LDIF reprezentace uživatele

```
dn: cn=Jiri Sitera + uid=sitera, ou=People, o=meta, c=cz  
objectclass: inetOrgPerson  
objectclass: MetaPerson  
cn: Jiri Sitera  
uid: sitera  
sn: Sitera  
givenName: Jiri  
telephoneNumber: 019 7421 580  
postalAddress: Univerzitni 22, 30614 Plzen  
organizationname: Zapadoceska univerzita  
mail: sitera@civ.zcu.cz  
homeCell: zcu.cz  
homeDirectory: /afs/zcu.cz/users/s/sitera/home  
loginShell: tcsh  
status: ACTIVE
```

1.5 Mechanismus distribuce dat z metadatabáze

Data jsou primárně uložena a spravována prostředky relační databáze. V rámci aplikace Perun je realizována transformace dat do pohledu poskytovaného prostřednictvím adresářových služeb. Zde je také realizován mechanismus update dat v adresářových službách.

Základní funkce:

- Generování LDIF souboru kompletní informace (pro naplnění případně obnovu adresářových služeb).
- Údržba dat při změnách (mění příslušné položky v adresářových službách v reakci na změnu v databázi). Lze dělat několika technologiemi, od generování LDIF souboru a volání řádkové LDAP utility, přes PerLDAP skripty až po procedury uvnitř databáze realizované v jazyce Java¹.
- „Regenerační update“, tj. např. každý den se provede update dat v adresářovém serveru technologií, která je velmi výkonná, spolehlivá a jednoduchá, avšak vyžaduje zastavení serveru. Jako zdroj dat se použije LDIF soubor kompletní informace, update mechanismus je součástí serverových utilit. Tento postup v podstatě odpovídá současné technologii Perunu.

1.6 Umístění a reprezentace lokálních informací

Navržená reprezentace dat slouží pro standardní řešení práce s lokálními daty buňky, které jsou dosud spravovány zcela nezávislými mechanismy. Vlastní realizace údržby těchto dat může být nadále individuálně řešena a skryta za standardizované rozhraní.

Základní lokální informace buňky jsou UNIX uid jednotlivých uživatelů Meta-Centra v dané buňce.

umístění:: podvětev `ou=<buňka>,ou=Accounts,o=meta,c=cz`

reprezentace dat:: návrh schématu položek typu `MetaLocalAccount` a `MetaLocalAccounts` viz tab. 3 a tab. 4; položka typu `MetaLocalAccount` reprezentuje lokální informace o uživateli a položka typu `MetaLocalAccounts` slouží jako kořenová položka příslušného stromu – v případě níže popsané implementace údržby lokálních dat slouží k uložení stavové informace buňky

¹Přesnější diskuze na toto téma viz Petr Holeček a Aleš Křenek. V tuhle chvíli pravděpodobně existuje shoda, že a) současná technologie Perunu není k tomuto vhodná, b) udělat něco podobného není jednoduché a za c) takovou technologii nepotřebujeme.

Jméno atributu, alias	typ atributu	význam
uid	cis	uživatelské jméno – vazba na ostatní informace o uživateli
uidNumber	cis	UNIX uid uživatele pro buňku

Tabulka 3: Objectclass MetaLocalAccount

Jméno atributu, alias	typ atributu	význam
lastUidNumber	cis	poslední použité uid z přiděleného rozsahu – specifická stavová informace mechanismu pro údržbu lokálních informací buňky

Tabulka 4: Objectclass MetaLocalAccounts

1.7 Mechanismus údržby lokálních informací – referenční implementace

Referenční implementace tohoto mechanismu je maximálně jednoduchá. Veškerá data jsou umístěna přímo v adresářových službách.

Vzorek dat:

```
ldapsearch -h ldap-meta.zcu.cz -p 377 \
-b 'ou=zcu,ou=Accounts,o=meta,c=cz' 'objectclass=*'

dn: ou=zcu, ou=Accounts, o=meta, c=cz
objectclass: top
objectclass: organizationalunit
objectclass: MetaLocalAccounts
ou: zcu
lastuidnumber: 60645

....

dn: uid=sitera, ou=zcu,ou=Accounts,o=meta,c=cz
objectclass: metaLocalAccount
uid: sitera
uidnumber: 60644
```

Mechanismus údržby těchto dat je realizován skriptem v Perlu (s využitím knihovny PerLDAP), který je zodpovědný za přiřazení (lokálního) UNIX uid každému uživateli MetaCentra. K tomu využívá čítač uložený v kořenové po-

ložce příslušného podstromu (uid jsou přidělována sekvenčně z vyhrazeného rozsahu).

1.8 Využití dat – ověřovací implementace

V současnosti jsou k dispozici ověřovací implementace některých základních funkcí. Jsou to zejména:

generátor passwd: Skript pro vytváření `passwd` souborů strojů MetaCentra. Je pravidelně spouštěn pro zajištění aktuálního stavu. Skript používá globální data o lidech a lokální informace buňky (UNIX uid).

Slouží primárně pro řízení přístupu uživatelů MetaCentra – na strojích bez lokálních domovských adresářů udělá vše co je třeba učinit pro „zřízení“ nového uživatele (vzhledem ke stroji).

Implementace: Perl s PerLDAPem

generátor mail aliasů: Podobně jako u `passwd`, slouží k zajištění přeměrování elektronické pošty na strojích MetaCentra na primární adresy jednotlivých uživatelů.

Implementace: Perl s PerLDAPem

telefonní seznam: WEB rozhraní pro přístup k základním informacím – vyhledávání uživatele MetaCentra, jeho telefonu, e-mailu, atd.

Implementace: PHP3 s podporou LDAPu jako modul WEB serveru Apache; testovací implementace je k dispozici na URL:

<http://lupus.zcu.cz/~sitera/metapeople.html>

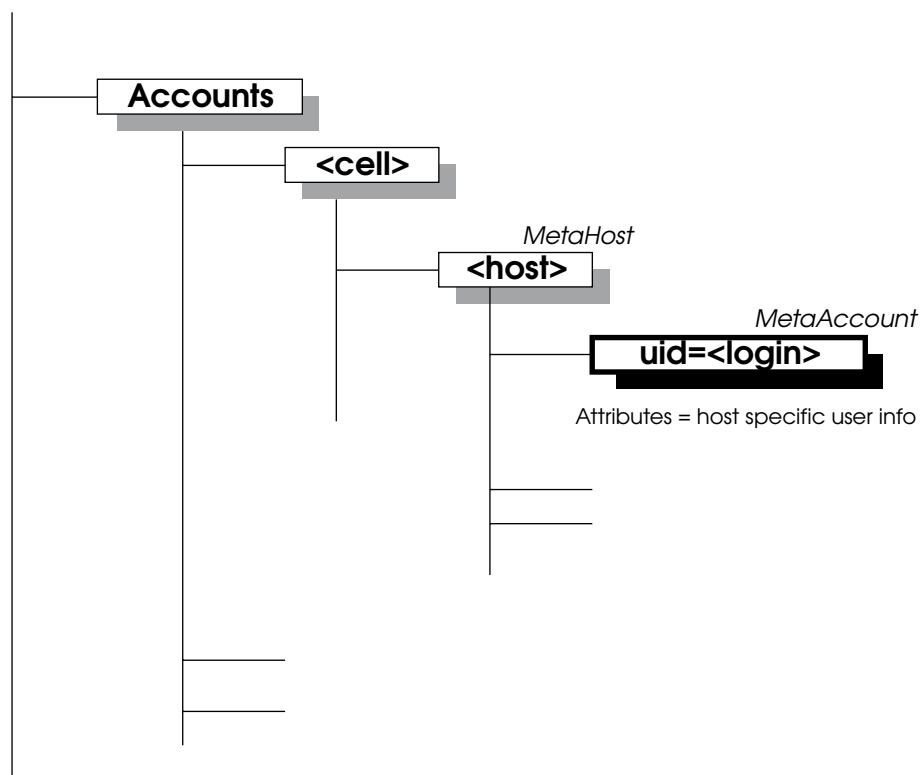
1.9 Návrh reprezentace údajů o uživatelských účtech na jednotlivých strojích

Tento návrh se týká reprezentace údajů o účtech na jednotlivých strojích resp. přístupu k nim. Jedná se pouze o doporučení reprezentace tohoto typu informací v adresářových službách. Takové informace jsou udržovány pouze pro singulární případy, kdy je nutné pro nějaký stroj používat jinou než globální politiku přidělování uživatelských účtů (obvykle se jedná o jistou formu speciální globální politiky např. z licenčních důvodů).

Základní struktura návrhu je patrná z obr.². Návrh příslušného typu položky je v tab.³. dn položky je tvořeno uživatelským jménem uživatele a strukturálně patří do větve identifikované jménem stroje vůči němuž specifická data položka reprezentuje.

²obr:struktura2

³tab:MetaAccount



Obrázek 2: Návrh umístění informací specifických vzhledem ke stroji

Jméno atributu, alias	typ atributu	význam
uid	cis	uživatelské jméno – vazba na ostatní informace o uživateli
homeQuota	cis	specifická informace pro daný stroj – kvóta lokálního domovského adresáře
scratchQuota	cis	kvóta lokálního scratch prostoru

Tabulka 5: Návrh typu položky (objectclass) MetaAccount

Jméno atributu, alias	typ atributu	význam
hn	cis	jméno stroje – položky v tomto podstromu reprezentují data specifická vůči jmenovanému stroji

Tabulka 6: Návrh typu položky (objectclass) MetaHost

2 Sběr informací o stavu zdrojů

Cílem tohoto systému je poskytnutí jednotného rozhraní pro přístup k informacím o aktuálním stavu distribuovaného výpočetního prostředí. Tento systém slouží zejména pro účely plánování a optimalizace přidělování zdrojů.

Ukázalo se, že infrastruktura postavená nad dostupnými adresářovými servery při zachování jistých pravidel je schopná akceptovat množství změn za jednotku času dostatečné pro realizaci tohoto systému.

2.1 Sběr dat

Po zkušenostech s démonem pro sběr dat realizovaným v Perlu a prostřednictvím knihovny PerLDAP (problémy s managementem paměti) se současný návrh skládá ze dvou komponent:

- Jednoduchý program v jazyce C běžící jako démon a realizující funkci popsateľnou (v terminologii projektu Globus) jako heartbeat. Program periodicky zapisuje do adresářových služeb informaci o funkci monitorovaného zdroje (vlastní heartbeat, tj. v principu pouze timestamp a některé základní údaje, např. load).
- Skript vycházející z testovacího skriptu `statinfo`, tj. jistá inteligence a flexibilita realizovaná v jazyce Perl. Chování modifikovatelné dle konfigurace uložené ve větvi `ou=Resources`, `o=meta`, `c=cz`. Jde především o definici dat, které se mají pro daný prostředek sbírat a frekvenci sběru. Základní interval sběru výrazně delší než u výše uvedeného démona. Skript spouštěn pravidelně z `crona`.

2.2 Prezentace dat

Existují dvě větve informací o zdrojích:

- `ou=Resources`, `o=meta`, `c=cz`
„Statické“ informace o existujících zdrojích, tj. především jejich konfigurace a vlastnosti (pro vyhledávání vhodných zdrojů).
- `ou=Stat`, `o=meta`, `c=cz`
Sbíraná, rychle se měnící data. Aktuální stav zdrojů. Jasná vazba na entity v předcházející skupině.

2.3 Současný experimentální návrh struktury dat pro sběr aktuálních informací o stavu zdrojů

Návrh schématu vychází ze schémat projektu Globus. Naše rozšíření MetaStatInfo bude obsahovat specifické údaje potřebné pro naše účely, v tuto chvíli obsahuje pouze atribut uptime.

2.3.1 Příklad LDIF reprezentace stroje

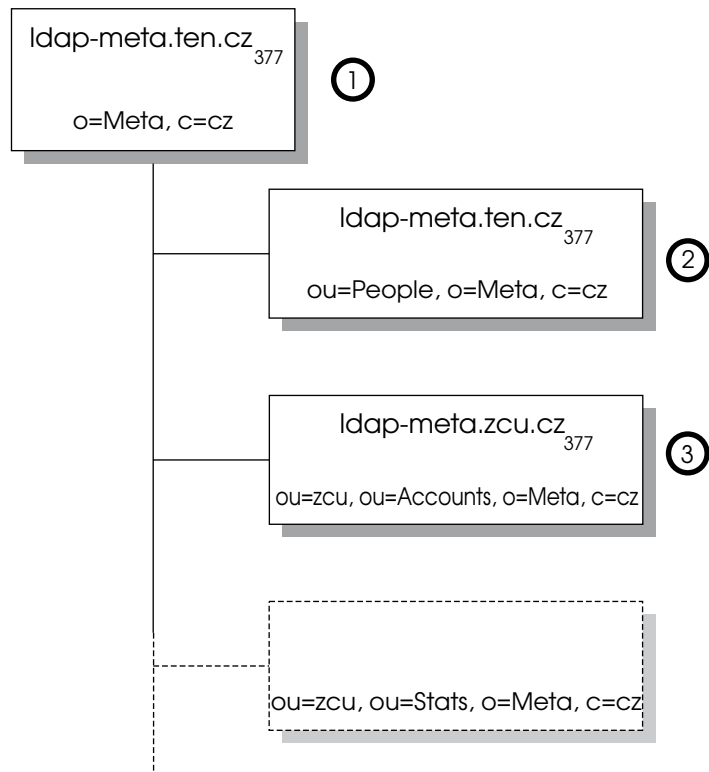
```
dn: hn=pasifae.zcu.cz, ou=zcu,ou=stat,o=meta,c=cz
rn: Host pasifae.zcu.cz
hn: pasifae.zcu.cz
imageobject: undefined
objectclass: GlobusTop
objectclass: GlobusPhysicalResource
objectclass: GlobusComputeResource
objectclass: GlobusOperatingSystemInformation
objectclass: GlobusCpuInformation
objectclass: GlobusSystemDynamicInformation
objectclass: MetaStatInfo
heartbeat: 930586330
cpuload1: 0.41
uptime: 14 days
cpuload5: 0.14
cpuload15: 0.19
lastupdate: Mon Jun 28 18:12:10 1999
```

Testovací skript metastats periodicky získává informace o všech monitorovaných strojích a vypisuje je. Posuzuje hodnotu heartbeat podle aktuálního systémového času (na základě definované mezní difference) a dle výsledku určuje platnost ostatních dat.

3 Fyzická infrastruktura LDAP serverů

Základní ideou je rozdělení LDAP stromu dle typu dat a jejich zdroje. Část dat replikovaná (kořen stromu, „statická“ data), část dat rozdělena (rychle se měnící data) – v každé buňce lokálně zápis a přístup zvenčí vzdáleně na čtení.

Aktuální struktura LDAP stromu z hlediska fyzického umístění pro poskytování přístupu k informacím o lidech je znázorněna na obr. 3 (s následujícím členěním z hlediska údržby: 1) replikace, 2) generování z relační databáze prostřednictvím Perunu s možností redundance, 3) dle lokálních potřeb).



Obrázek 3: Struktura LDAP stromu z hlediska rozdělení dat na části technicky poskytované samostatně

3.1 Implementace

Základní používaný SW (server a LDAP knihovny) je v současnosti mix Netscape a OpenLDAP. S nástupem OpenLDAPu verze 2.0.x přechod na OpenLDAP. Současná infrastruktura serverů pro přístup k datům o lidech je založena na OpenLDAPu. Jako hlavní vývojový nástroj je používána knihovna PerLDAP. Více viz odkazy a literatura.

4 Témata k diskuzi a společné poznámky

- *Zabezpečení přístupu k adresářovým službám*
Z WEBu, ze systémových skriptů, pro replikaci i obecně. Především KRB5 SASL autentizace a SSL zabezpečení komunikace.
- *Adresářové služby a česká diakritika*
„cestina“ nebo LDAPv3 UTF8 kódování versus LDAPv2 klienti (mail klienti).
- *Schéma pro reprezentaci lidí*
Zde je mnoho jednotlivostí o kterých lze diskutovat: tvorba dn (složené rdn?), cn (umísťovat sem titul?), ... K diskuzi je i řada referencí (RFC2307, gridforum, ...).
- *Realizace redundance na úrovni klienta adresářových služeb*
Je třeba vybrat jednu z metod práce klienta s více servery pro zajištění transparentního chování při výpadcích serverů či komunikace.
- *Koncepce sběru informací o stavu zdrojů a služeb*
V oblasti sběru a prezentace dat o stavu distribuovaného výpočetního prostředí je třeba se zabývat řadou věcí. Zejména je nutné získat a utřídit informace o požadavcích plánování, kde je problémem především údržba a prezentace historie stavu. S tím souvisí zkoumání technologií pro přístup k datům z jiných systémů nebo aplikací (např. dávkový systém) přes jednotné rozhraní (LDAP).
Nápad pro ilustraci⁴: Možnost integrace/využití SW NetSaint pro základní (Meta nespecifické) parametry strojů. NetSaint je obecně užívanou platformou pro sběr těchto informací a možná by bylo výhodné uvažovat o jakési bráně k těmto informacím (zřejmě výhodnější než dříve diskutovaná možnost brány ke klasickému SNMP monitoru typu HP OpenView). Podobně

⁴Ve skutečnosti je zřejmě nutno hledat jiné, méně známé, avšak pro účely metacomputingu vhodnější monitorovací systémy.

je tomu i v oblasti problematiky historie naměřených údajů. Zde se lze zmínit o nápadu týkajícího se možnosti využití existujících mechanismů, např. RRD_TOOL (MRGT) (vazba na adresářové služby pro získávání dat i konfigurace a brána pro přístup k sumarizovaným datům zvenčí).

Reference

- [LDAPuvod] Jiří Sitera, *Adresářové služby – úvod do problematiky*, jako technická zpráva TEN 4/2000
<http://www.ten.cz/doc/techzpravy/2000-4>
- [EurOpen] Jiří Sitera, *Adresářové služby jako informační infrastruktura distribuovaného výpočetního prostředí*, sborník konference EurOpen.CZ, listopad 1999, ISBN 80-902715-0-2.
- [Pleiades] Projekt Pleiades – domovská stránka,
<http://home.zcu.cz/projekty/lps/ldap>
- [skriptLDAP] Jiří Sitera, *Skriptovací jazyky a jejich využití pro přístup k adresářovým službám protokolem LDAP*,
<http://home.zcu.cz/projekty/lps/ldap/projekt/www/papers/skriptLDAP.ps>
- [Globus] Projekt Globus
<http://www.globus.org>
- [openldap] The OpenLDAP Project, *Open source suite of LDAP applications and development tools*, <http://www.openldap.org>
- [perldap] Netscape Communications, *PerLDAP Central*,
http://developer.netscape.com/tech/directory/perldap_central.html