

Imenički servisi

**KORIŠTENJE OPENLDAP-A ZA LOKALNU
I UDALJENU AUTORIZACIJU NA LINUX-
BASED SERVICE**

**(LOGIRANJE NA KONZOLU, SSH,
APACHE, OSTALO)**



Algebra

visoka škola za
primijenjeno računarstvo

- Uvod, osnove i modeli korištenja OpenLDAP-a
- Osnovne komande i procedure za prijavu na LDAP server
- Terminal/SSH autorizacija
- Apache autorizacija
- Ostalo – postfix, ...

OpenLDAP

Terminal, SSH

Apache web server

Ostalo – postfix, ...



Algebra

visoka škola za
primijenjeno računarstvo

1. Uvod, osnove, modeli



Algebra

visoka škola za
primijenjeno računarstvo

Osnove LDAP-a – 1

- LDAP – imenički servis, nije klasična „baza podataka”
- nema naprednih mogućnosti za roll-back, komplicirane transakcije kao baze – za kompleksne update procedure
- kod direktorija nije bitno ako se prilikom sinhronizacije pojave nekonzistentnosti, ali na kraju se moraju sinhronizirati u konzistentno stanje
- optimizacija za operacije tipa read, browse i search
- LDAP – Lightweight Directory Access Protocol, lightweight protokol za pristup imeničkim servisima po X.500-based direktorijima (RFC 2251,...)
- LDAP koristi TCP/IP i općenito konekcijski orijentirane protokole za komunikaciju
- LDAP model bazira se na zapisima – kolekcija atributa bazirana na unikatnom DN-u (Distinguished Name)
- svaki atribut ima tip i jednu ili više vrijednosti – npr.cn za Common Name, mail za e-mail adrese

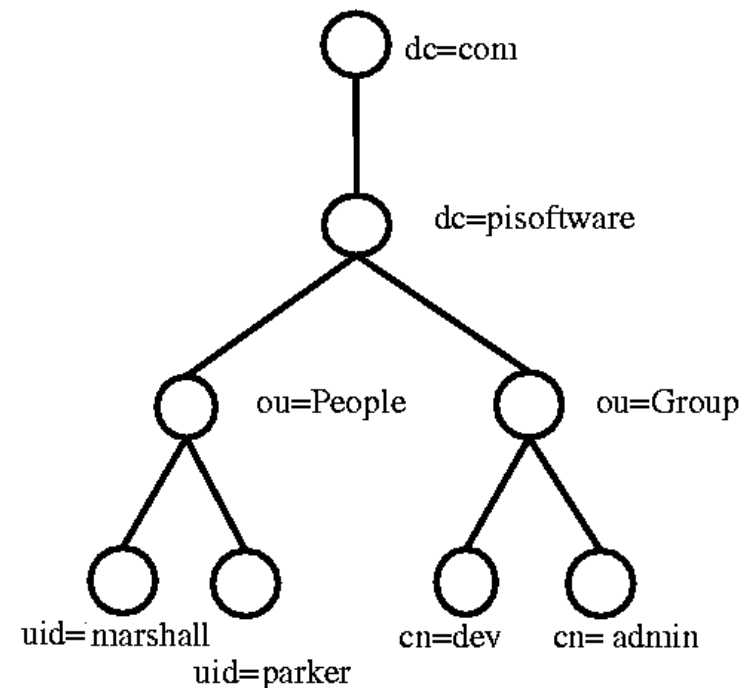


Algebra

visoka škola za
primijenjeno računarstvo

Osnove LDAP-a - 2

- informacije su organizirane u stablastim strukturama
- strukture su obično prilagođene odjelima, lokacijama, ...
- postoje i stand-alone implementacije LDAP-a na Linuxu – slapd (lightweight X.500 directory server)
- različite verzije – LDAPv2 i v3 – v2 obsolete



Algebra

visoka škola za
primijenjeno računarstvo

Za što možemo koristiti OpenLDAP?

- Autentifikacija i security – za različite servise
- Standalone ili connected na neki drugi imenički servis
- Access control – po IP-u, imenu domene, ...
- Replikacija (HA, pouzdanost) uz korištenje slurpd-a uz slapd

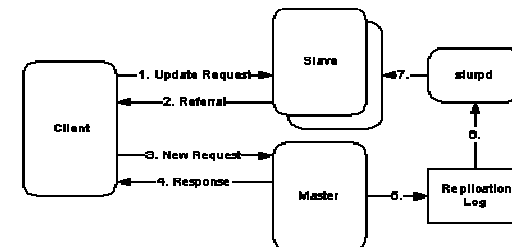
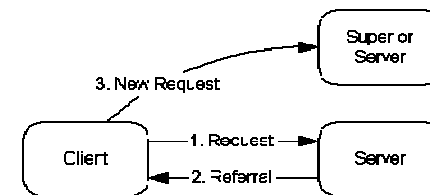
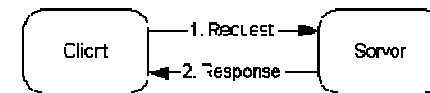


Algebra

visoka škola za
primijenjeno računarstvo

Vrste konfiguracija

- lokalni directory service – bez interakcije sa drugim directory serverima
- lokalni directory service with referrals – lokalni uz referral za sve upite izvan naše domene
- replicirani directory service – koristimo slurpd za propagaciju promjena između master i slave nodeova
- distribuirani – miješani model, više servera, superior/subordinate serveri,



Algebra

visoka škola za
primijenjeno računarstvo

2. OpenLDAP vs NIS



Algebra

visoka škola za
primijenjeno računarstvo

NIS/NIS+

- NIS/NIS+ (Network Information Service)
 - client-server directory protokol koji se koristi u UNIX-oidnim okolinama
- često ga zovu i Yellow Pages ili YP
- može imati master i slave servere
- NIS+ - poboljšana verzija sa podrškom za enkripciju i autentifikaciju preko sigurnog kanala
- da bi NIS+ radio, moraju biti podignuti i podešeni servisi portmap/rpcbind i ntp/time servis
- potrebno poinstalirati yp* pakete
- nakon instalacije, klijenti koriste zajedničke passwd, shadow, i slične datoteke



Algebra

visoka škola za
primijenjeno računarstvo

OpenLDAP vs NIS/NIS+

- LDAP nije samo UNIX-specific, podržan je od više operacijskih sustava
- Active Directory je LDAP-based
- dosta jednostavna implementacija Kerberos autentifikacije kod LDAP-a
- NIS nema skalabilnosti, u osnovnoj verziji nema enkripcije
- integracija – mail, address bookovi, replikacija BIND servera, SAMBA autentifikacija
- NIS/NIS+ su obsolete, samo u rijetkim corporate mrežama
- LDAP se može proširiti dodatnim funkcijama
- LDAP se nakon osnovne konfiguracije lako integrira sa ostalim servisima



Algebra

visoka škola za
primijenjeno računarstvo

3. OpenLDAP autentifikacija za SSH



Algebra

visoka škola za
primijenjeno računarstvo

SSH i LDAP

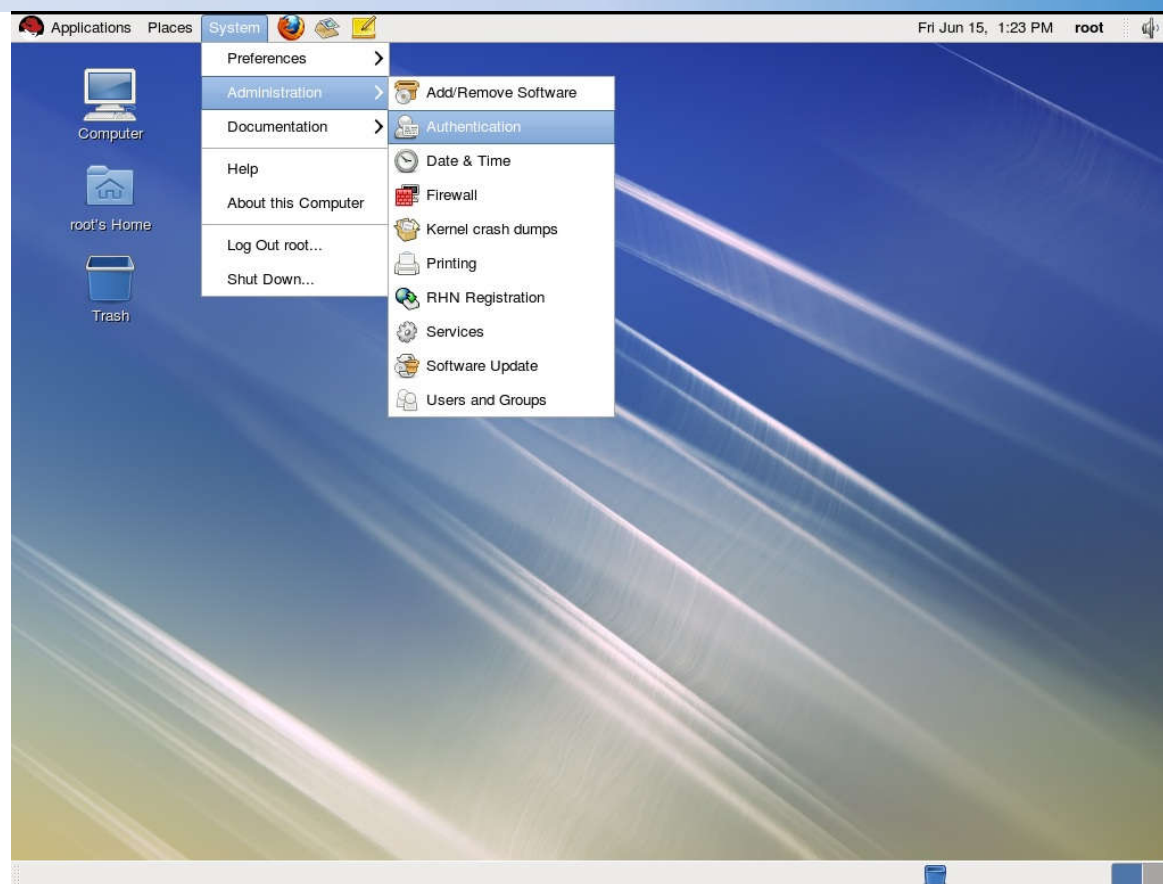
- SSH je kao secure protokol za terminalnu komunikaciju (i FTP) idealan kandidat za LDAP autentifikaciju
- koristimo LDAP kao centralni imenički servis kroz koji dijelimo korisnička imena i lozinke (kao AD)
- ukoliko imamo podešen LDAP server i na njemu sve potrebne podatke – korisnička imena, lozinke i sl., konfiguracija LDAP klijenata je trivijalan zadatak
- requirementi – poinstaliran SSH server, authconfig* paketi (ako želimo automatski mountati korisničke home direktorije, i autofs)
- uobičajeno se koristi sa autofs-om , servisom koji može automatski mountati korisničke home direktorije preko NFS-a (UNIXoidni file/folder sharing protokol)



Algebra

visoka škola za
primijenjeno računarstvo

SSH i LDAP – procedura - 1



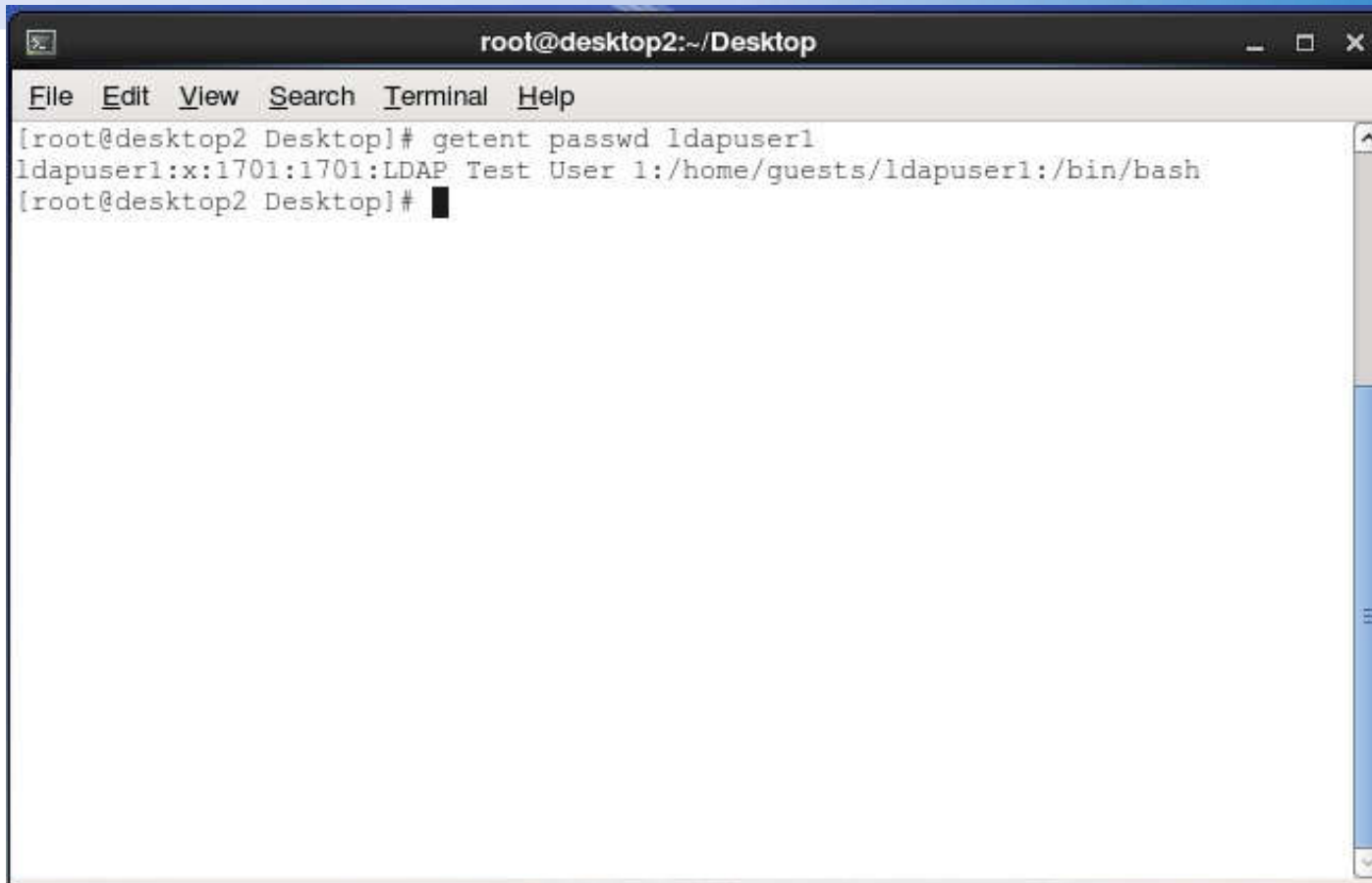
Algebra

visoka škola za
primijenjeno računarstvo

SSH i LDAP – procedura - 2



SSH i LDAP – procedura - 3



```
root@desktop2:~/Desktop
File Edit View Search Terminal Help
[root@desktop2 Desktop]# getent passwd ldapuser1
ldapuser1:x:1701:1701:LDAP Test User 1:/home/guests/ldapuser1:/bin/bash
[root@desktop2 Desktop]#
```



Algebra

visoka škola za
primijenjeno računarstvo

SSH i LDAP – procedura - 4

- da bismo imali potpuni osjećaj „flexible office” – da bismo imali svoje datoteke i direktorije mountane nakon logiranja, najbolje je koristiti servis autofs
- primjer:
 - u /etc/auto.master dodamo liniju:
/home/guests /etc/auto.ldapusers
 - u datoteku /etc/auto.ldapusers dodamo:
* 192.168.0.254:/home/guests
- zaustavimo i pokrenemo servis autofs:
service autofs stop; service autofs start
- kada se nakon toga pokušamo ulogirati kao LDAP user, po upisivanju ispravnog korisničkog imena i lozinke mounta nam se korisnički direktorij sa nekog unaprijed dodijeljenog mrežnog sharea – isto kao Group Policy redirekcija My Documents foldera za usere na mrežni share na NAS-u ili nekom drugom serveru



Algebra

visoka škola za
primijenjeno računarstvo

SSH i LDAP - zaključak

- potrebno je podesiti sistemsku autentifikaciju kroz LDAP (korištenjem prethodno spomenutog authconfig alata)
- SSH nakon toga automatski radi kao sistemski servis koji koristi LDAP autentifikaciju
- NIS/NIS+ su obsolete, samo u nekim corporate mrežama
- LDAP se može proširiti dodatnim funkcijama
- LDAP se nakon osnovne konfiguracije lako integrira sa ostalim servisima



Algebra

visoka škola za
primijenjeno računarstvo

Apache i LDAP autentifikacija - 1

- Apache web server, kao sistemski servis, može nakon konfiguracije koristiti LDAP za autentifikaciju korisničkog pristupa web stranicama ili – češće – određenim dijelovima/direktorijima na web stranicama
- potrebno je imati instaliran pakete od Apache web servera (httpd)



Algebra

visoka škola za
primijenjeno računarstvo

Apache i LDAP autentifikacija - 2

- htpasswd autentifikacija – flat-file autentifikacija bazirana na datoteci sa korisničkim imenima i lozinkama

Primjer:

Htpasswd –cm /etc/httpd/conf/.htpasswd korisnik

(dva puta upisati password)

, nakon čega treba u konfiguracijsku datoteku od Apache web servera (/etc/httpd/conf/httpd.conf) dodati:

```
<Directory /var/www/html/secret>
```

```
    AuthType Basic
```

```
    AuthName "Restricted htpasswd Files"
```

```
    AuthUserFile /etc/httpd/conf/.htpasswd
```

```
    Require valid-user
```

```
</Directory>
```

- nakon promjene konfiguracije potrebno je restartati servis httpd (apache):

service httpd restart

- U browseru napisati url:

[http://IP ili ime servera na kojem smo editirali konfiguracijsku datoteku/secret/index.html](http://IP_ili_ime_servera_na_kojem_smo_editirali_konfiguracijsku_datoteku/secret/index.html)

- za provjeru je potrebno napraviti direktorij /var/www/html/secret i u njemu npr.index.html datoteku za prikazivanje

- Primjer:

```
<html>
```

```
<title>Testna htpasswd  
stranica</title>
```

```
<body>
```

```
<h2> Ovo je testna .htpasswd  
stranica!</h2>
```

```
</body>
```

```
</html>
```



Algebra

visoka škola za
primijenjeno računarstvo

Apache i LDAP autentifikacija - 3

- LDAP autentifikacija – potrebno je izmjeniti konfiguracijsku datoteku od Apache web servera i dodati:LDAPTrustedGlobalCert CA_BASE64 /etc/pki/tls/example-ca.crt

<Directory /var/www/html/ldapsecret>

AuthName "Restricted LDAP Files"

AuthType Basic

AuthBasicProvider ldap

AuthLDAPURL

"ldap://instructor.example.com/dc=example,dc=com" TLS

Require valid-user

</Directory>

- nakon promjene konfiguracije potrebno je restartati servis httpd (apache):

service httpd restart

- U browseru napisati url:

[http://IP ili ime servera na kojem smo editirali kofiguracijsku datoteku/ldapsecret/index.html](http://IP_ili_ime_servera_na_kojem_smo_editirali_kofiguracijsku_datoteku/ldapsecret/index.html)

- za provjeru je potrebno napraviti direktorij /var/www/html/ldapsecret i u njemu npr.index.html datoteku za prikazivanje

- Primjer:

<html>

<title>Testna stranica za LDAP autorizaciju</title>

<body>

<h2> Ovo je testna stranica sa LDAP autorizacijom!</h2>

</body>

</html>



Algebra

visoka škola za
primijenjeno računarstvo

4. Ostale primjene OpenLDAP-a



Algebra

visoka škola za
primijenjeno računarstvo

Dodatne primjene OpenLDAP-a

- autorizacija za druge servise:
 - postfix i sendmail (mail serveri), webmin, ...
 - NFS (UNIXoidni file sharing servis)
 - SAMBA (MS-compatible file sharing servis)
 - Active Directory integracija



Algebra

visoka škola za
primijenjeno računarstvo

Pitanja?



Algebra

visoka škola za
primijenjeno računarstvo