GSR
vim /etc/crunch.conf

Curs 10

Serverul LDAP

Gestiunea Serviciilor de Rețea

22 decembrie 2011

Moto

Simplicity is a great virtue but it requires hard work to achieve it and education to appreciate it. And to make matters worse: complexity sells better.

Edsger Dijkstra

Suport

- "Unix and Linux System Administration"
  - Chapter 19 – Sharing System Files
    - Section 19.3 – LDAP: The Lightweight Directory Access Protocol
- "Professional Linux System Administration"
  - Chapter 16 – Directory Services

Outline

LDAP

- director
- bază de date
- acces citire și scriere, frecvent de citire
- DN, RDN, DC, CN, OU
- LDAP URI
- atribute, filtre

Utilitare LDAP

- `apt-get install ldap-utils`
- `/etc/ldap/ldap.conf`
- `ldapsearch, ldapadd, ldapdelete, ldapmodify, ldappasswd`

Utilitate LDAP

- centralizare informații (autentificare, SSO)
- organizare, flexibilitate
- interfața unică de acces la date organizate/structurate
- acces rapid pentru citire
- funcționare peste rețea
- distributable

Outline

OpenLDAP

- implementare de server LDAP
- rulează pe Linux, BSD, Mac OS X, Solaris, Windows
- instalare
  - `dpkg-reconfigure debconf`
    - dialog, low
    - permite configurarea bazei de date
  - `apt-get install slapd ldap-utils`
  - sau `dpkg-reconfigure -plow slpad` (după `apt-get install`)
- `/etc/init.d/slapd start | stop | restart`

Tool-uri de interacțiune OpenLDAP

- `slap*` – tool-uri offline
  - serverul trebuie să fie oprit
- `ldap*` – tool-uri online
- validare
  - `slaptest`
  - `slapcat`

Configurare de bază OpenLDAP – pre v2.3

- `/etc/ldap/slapd.conf`
- `/etc/default/slapd`
- `man slapd.conf`
- `loglevel 256` sau `loglevel stats`
- `index uid eq`

Configurare de bază OpenLDAP – post v2.3

- `/etc/ldap/slapd.d/`
- `/etc/default/slapd`
- `man slapd-config`
- configurare prin fișiere LDIF

URI-uri OpenLDAP

- `ldap:///` – LDAP simplu (portul 389)
- `ldaps:///` – LDAP securizat (portul 636)
- `ldapi:///` – LDAP local (socketi Unix), folosit pentru autentificare SASL de tip `EXTERNAL`
- `SLAPD_URI` în `/etc/default/slapd`

Ierarhia de configurare OpenLDAP – post v2.3

- directivele documentate în pagina de manual `slapd-config`
- rădăcina în `/etc/ldap/slapd.d/`
- `cn=config` – opțiuni de configurare globale (`GLOBAL CONFIGURATION OPTIONS` în manual)
- `olcDatabase=0config,cn=config` – configurarea bazei de date de configurare
- `olcDatabase=1hdb,cn=config` – configurarea bazei de date LDAP
- `cn=schema,cn=config` – configurarea schemei
- pentru baze de date – `GLOBAL DATABASE OPTIONS` și `GENERAL DATABASE OPTIONS` în manual

Configurare baze de date de configurare

- inițial cu ajutorul formei de autentificare SASL externe (`EXTERNAL`)
  - folosește URI-ul `ldapi:///`
  - `ldapsearch -LLL -Y EXTERNAL -H ldapi:///`
  - `ldapadd -Y EXTERNAL -H ldapi:/// -f test.ldif`
- configurarea parolei pentru rootdn pentru baza de date de configurare (`cn=admin,cn=config`)
  - `ldapadd -Y EXTERNAL -H ldapi:/// -f admin.ldif`

```
1 dn: olcDatabase={0}config,cn=config
2 changetype: modify
3 add: olcRootPW
4 olcRootPW: {SSHA}rARaJcrMxKH+e1INIhGt5Pjqf7+bS8pm
```

Configurare parolă nouă pentru admin bază de date LDAP

```
1 dn: olcDatabase={1}hdb,cn=config
2 changetype: modify
3 replace: olcRootPW
4 olcRootPW: {SSHA}gOoL0jqP2roPeRjDG6ki1BdDqCFxhdWp
```

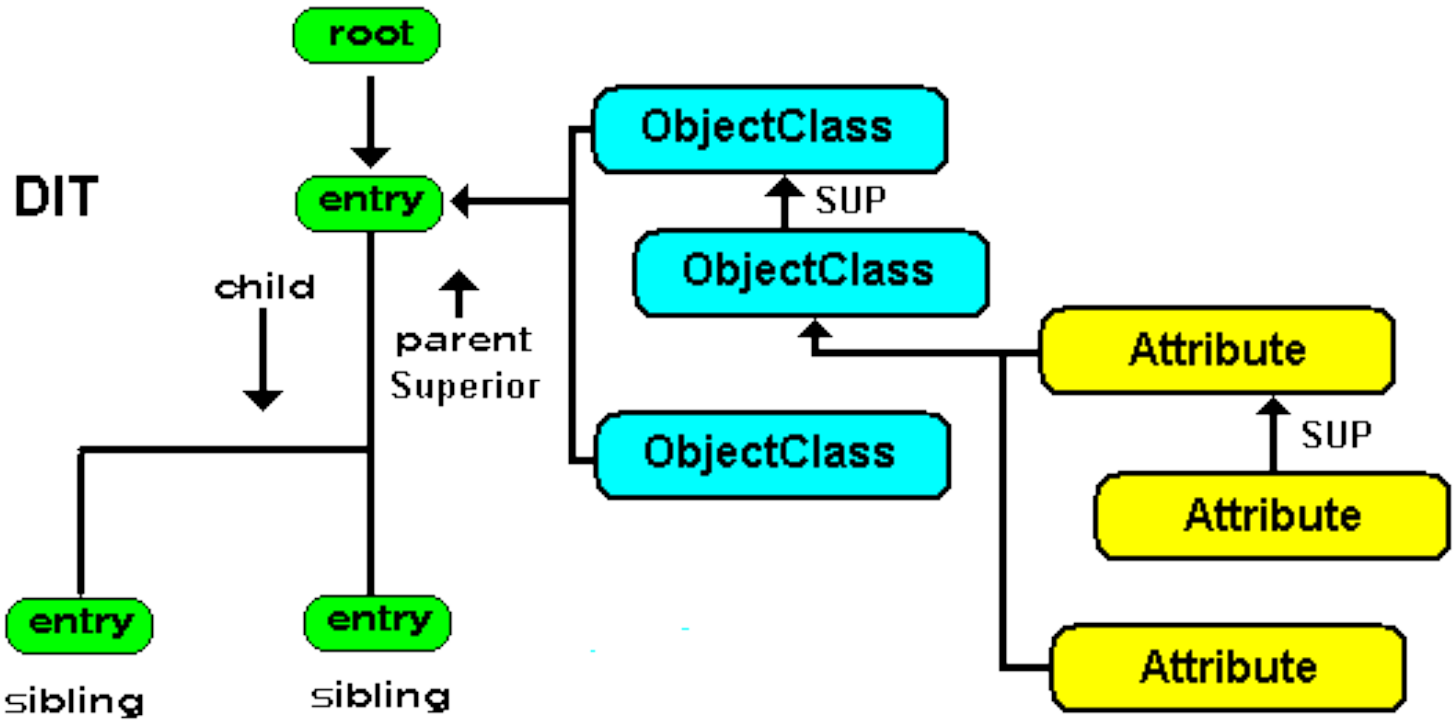
- `ldapadd -x -D cn=admin,cn=config -w password -f rootdn-passwd.ldif`

Configurare niveluri de logging

```
1 dn: cn=config
2 changetype: modify
3 replace: olcLogLevel
4 olcLogLevel: stats
```

- se configurează o listă de evenimente ce se doresc jurnalizate
- `ldapadd -x -D cn=admin,cn=config -w password -f change-logging.ldif`

Schemas


root
DIT
entry
child
parent
Superior
ObjectClass
SUP
ObjectClass
ObjectClass
Attribute
SUP
Attribute
Attribute
entry
entry
sibling
sibling

Outline

Securizare OpenLDAP

- "selective listening": `/etc/default/slapd`
- autentificare la server (bind): simple, SASL
- controlul accesului (ACL)
- suport TLS
- SSF (Security Strength Factors)

Controlul accesului în LDAP

- `man slapd.access`
- `access to * by * read`
  - toți utilizatorii pot citi (chiar și cei anonimi)
- `access to *`
  ```
        by self write
        by anonymous auth
        by * read
  ```
  - utilizatorul curent își poate actualiza informația
  - utilizatorul anonim se poate autentifica peste intrările existente
  - utilizatorii obișnuiți care au făcut bind pot citi conținutul
  - util pentru gestiunea parolelor
  - prima intrare găsită este cea selectată (vezi `anonymous`)

Controlul accesului în LDAP (2)

- ```
  access to attrs=userPassword,shadowLastChange
          by dn="cn=admin,dc=swarm,dc=cs,dc=pub,dc=ro" write
          by anonymous auth
          by self write
          by * none
  ```
  - gestiunea parolelor
  - utilizatorul privilegiat are drepturi complete
  - utilizatorul anonim se poate autentifica
  - utilizatorul curent poate să își schimbe parola
  - utilizatorii obișnuiți care au făcut bind nu au acces
- forma generică: `access to <what> by <who> <access>`
  ```

Controlul accesului în LDAP – LDIF

```
1 dn: olcDatabase={1}hdb,cn=config
2 changetype: modify
3 replace: olcAccess
4 olcAccess: {0}to attrs=userPassword,shadowLastChange by
anonymous auth by dn="cn=admin,dc=test,dc=ro" write by * none
5 olcAccess: {1}to * by self read by
dn="cn=admin,dc=garm,dc=cs,dc=pub,dc=ro" write by * none
```

Suport SSL/TLS în OpenLDAP

- TLS(v1)/SSL(v3)
- în doua moduri
  - automat: pe portul 636 (LDAPS), URI de forma `ldaps://`
  - prin definiție: pe portul standard 389 (LDAP), clientul pornește TLS (`StartTLS`)

Directive TLS

- `TLSCACertificateFile` – certificatele CA-urilor de încredere
- `TLSCertificateFile` – certificatul serverului
- `TLSCertificateKeyFile` – cheia privată a serverului
- serverul trebuie să aibă acces la cheia privată
  - din cauza permisiunilor pe `/etc/ssl/private/`, utilizatorul `openldap` trebuie adăugat la grupul `ssl-cert`

Configurare TLS în OpenLDAP

```
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile:
/etc/ssl/certs/ssl-cert-snakeoil.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ssl-cert-snakeoil.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile:
/etc/ssl/private/ssl-cert-snakeoil.key
-
add: olcTLSVerifyClient
olcTLSVerifyClient: never
```

Configurare client pentru folosire TLS

- `/etc/ldap/ldap.conf` sau `/.ldaprc`
- `TLS_REQCERT none` în cazul în care nu se știe care este CA-ul
- `TLS_CACERT /path/to/cert` pentru a indica CA-ul
- `TLS_CACERTDIR /path/to/cert/dir/` pentru a indica directorul cu certificate de CA
- `ldapsearch -x -LLL -Z ...`

Configurare TLS-only

- `/etc/default/slapd`
  - `SLAPD_SERVICES="ldapi:/// ldaps:///"`
- în `/etc/ldap/ldap.conf` – `BASE ldaps://...`
- sau `ldapsearch -x -LLL -H ldaps://...`

Replicare LDAP

- toleranță la defecte și fiabilitate
- inițial slurpd: push mode
- syncrepl
- delta syncrepl

Outline

Cuvinte cheie

- OpenLDAP
- slapd
- `/etc/ldap/slapd.d/`
- `/etc/default/slapd`
- `man slapd-config`
- `ldapi:///`
- `cn=config`
- `cn=admin,cn=config`
- `-Y EXTERNAL`
- root DN
- schema
- SASL
- SSF
- ACL
- `oclAccess`
- TLS/SSL
- `TLS_REQCERT`
- `TLS_CACERT`
- replicare
- `syncrepl`

Resurse utile

- http://www.debian-administration.org/article/OpenLDAP_installation_on_Debian
- http://en.wikipedia.org/wiki/LDAP
- http://www.openldap.org/doc/admin24/index.html
- http://www.openldap.org/doc/admin24/sasl.html
- http://www.openldap.org/doc/admin24/access-control.html
- http://www.openldap.org/doc/admin24/tls.html
- http://www.openldap.org/pub/ksoper/OpenLDAP_TLS.html
- http://www.zytrax.com/books/ldap/
- http://www.zytrax.com/books/ldap/ch5/step2.html#step2
- http://www.zytrax.com/books/ldap/ch15/

Outline