LDAP

ΚΟΤΖΑΝΙΚΟΛΑΟΥ ΠΑΝΑΓΙΩΤΗΣ
ΚΟΡΕΑΣ ΠΛΑΤΩΝ

Τι είναι ένας κατάλογος (Directory) ;

Κατάλογος:
Μια συλλογή πληροφοριών που βασικός της σκοπός είναι η **αναζήτηση** και η **ανάγνωση** των δεδομένων και σπανίως η τροποποίηση τους.

Υπηρεσία καταλόγου:
Παρέχει πρόσβαση σε πληροφορίες καταλόγου

Εξυπηρετητής καταλόγου :
Πρόγραμμα το οποίο παρέχει την Υπηρεσία καταλόγου.

Υπηρεσία Καταλόγου

- ✓Οι κατάλογοι τείνουν να περιέχουν περιγραφικές, **βασισμένες σε χαρακτηριστικά πληροφορίες** και δεν υποστηρίζουν τα περίπλοκα σχήματα που συναντώνται στα συστήματα διαχείρισης βάσεων δεδομένων.
- ✓Οι κατάλογοι είναι διαμορφωμένοι έτσι ώστε να παρέχουν γρήγορη απάντηση, ακόμα και όταν γίνονται πολλαπλές αναζητήσεις.
- ✓Έχουν τη δυνατότητα να αντιγράφουν τις πληροφορίες προκειμένου να αυξηθεί η διαθεσιμότητα και η αξιοπιστία, μειώνοντας παράλληλα το χρόνο απόκρισης.

Συστήματα διαχείρισης καταλόγου

Τύποι δεδομένων καταλόγου

- ✓Λογαριασμοί
- ✓Ψευδώνυμα ηλεκτρονικού ταχυδρομείου και λίστες
- ✓Κλειδιά κρυπτογράφησης
- ✓Διευθύνσεις IP
- ✓Hostnames
- ✓Εκτυπωτές

Γνωστές υπηρεσίες καταλόγου

- ✓DNS
- ✓LDAP
- ✓NIS

Κατάλογοι ή Βάσεις δεδομένων

- ✓Οι κατάλογοι έχουν βελτιστοποιηθεί για να είναι άμεση και γρήγορη η ανάγνωση ενώ οι βάσεις δεδομένων για την ισορροπημένη λειτουργία ανάγνωσης και εγγραφής .
- ✓Οι κατάλογοι ακολουθούν **δεντρική δομή** ενώ οι βάσεις δεδομένων έχουν συνήθως σχεσιακή δομή
- ✓Τόσο οι κατάλογοι όσο και οι βάσεις δεδομένων μπορούν να αναπαραχθούν σε πολλά αντίγραφα
- ✓Παρέχουν συστήματα αποθήκευσης δεδομένων που έχουν δυνατότητα επεκτασιμότητας και προηγμένες δυνατότητες αναζήτησης δεδομένων

Πλεονεκτήματα των καταλόγων

Διευκολύνει τη διαχείριση

- ✓ Αλλαγή δεδομένων μόνο μια φορά : π.χ. για άτομα , λογαριασμούς και hosts

Ενοποιημένη πρόσβαση σε πόρους του δικτύου

- ✓ Single Sign On
- ✓ Ενιαίος χώρος αναζήτησης των χρηστών

Βελτίωση της διαχείρισης των δεδομένων

- ✓ Συνοχή στην διαχείριση δεδομένων
- ✓ Ασφάλιση των δεδομένων μέσω ενός μόνο διακομιστή

Τι είναι το LDAP ;

- ✓Το LDAP αποτελεί ένα πρωτόκολλο για την πρόσβαση σε υπηρεσίες καταλόγου και πιο συγκεκριμένα υπηρεσίες καταλόγου που υποστηρίζουν το πρότυπο X.500.
- ✓ Το LDAP τρέχει πάνω από το TCP/IP
- ✓Ανήκει στις υπηρεσίες καταλόγου και όχι στις βάσεις δεδομένων
- ✓Λειτουργεί ως πρωτόκολλο και οι λεπτομέρειες του LDAP καθορίζονται στο RFC2251.

Κατάλογοι στο LDAP

Ο κατάλογος στην περίπτωση του LDAP σημαίνει έναν τύπο βάσης δεδομένων που έχει βελτιστοποιηθεί για την αναζήτηση και την ανάκτηση δεδομένων δομής.

Ο κατάλογος χρησιμοποιείται για την αποθήκευση πληροφοριών σχετικά με το προφίλ του χρήστη όπως το όνομα του και τα δικαιώματά του (permissions)

Η δομή του LDAP

Ένας κατάλογος LDAP αποτελείται από **εγγραφές/ entries**

- ✓Οι εγγραφές συνήθως είναι τα στοιχεία των εργαζομένων/χρηστών

Κάθε εγγραφή αποτελείται από **χαρακτηριστικά /attributes**

- ✓Χαρακτηριστικά μπορεί να είναι ονόματα , αριθμοί τηλεφώνου κ.λπ..
- ✓Μια καταχώρηση είναι μια συλλογή χαρακτηριστικών που έχει ένα ***μοναδικό όνομα Distinguished Name (DN)***.
- ✓Το DN χρησιμοποιείται ως αναφορά της κάθε καταχώρησης.
- ✓Κάθε ένα από τα χαρακτηριστικά μιας εγγραφής έχει έναν τύπο μια ή περισσότερες τιμές.

Η δομή του LDAP

- ✓Οι τύποι είναι χαρακτηριστικά που παίζουν το ρόλο μνημονικών ακολουθιών, όπως το “cn” για το κοινό όνομα (common name), ή "mail" για το email.
- ✓Οι καταχωρήσεις τοποθετούνται σε μια ιεραρχική δεντρική δομή.
- ✓Συνήθως αυτή η δομή απεικονίζει τα γεωγραφικά ή/και οργανωτικά όρια.
- ✓Οι καταχωρήσεις που αντιπροσωπεύουν τις χώρες εμφανίζονται στην κορυφή του δέντρου ενώ από κάτω από αυτές αντιπροσωπεύουν τα κράτη και τους εθνικούς οργανισμούς και στο τέλος κάτω κάτω
- ✓Κάτω από αυτούς αντίστοιχα να είναι οι καταχωρήσεις που αντιπροσωπεύουν τις οργανωτικές μονάδες, τους ανθρώπους, τους εκτυπωτές, τα έγγραφα κ.λπ.

Distinguished Names του LDAP

Τα Distinguished Names (DNs)

- ✓Προσδιορίζουν με μοναδικό τρόπο μια εγγραφή LDAP
- ✓Παρέχουν το μονοπάτι προς το γονικό φάκελο LDAP
- ✓dn:cn=John Doe,ou=Sales,dc=plainjoe,dc=org

Τα Αναφορικά (relative) DNs (RDNs) προσδιορίζουν ένα ζεύγος χαρακτηριστικών τα περιεχόμενα ενός καταλόγου

- ✓ex: cn=John Doe ή username=test
- ✓cn=Jane Smith+ou=Sales
- ✓cn=Jane Smith+ou=Engineering

Distinguished Names του LDAP

Τα Distinguished Names (DNs)

- ✓Προσδιορίζουν με μοναδικό τρόπο μια εγγραφή LDAP
- ✓Παρέχουν το μονοπάτι προς το γονικό φάκελο LDAP

π.χ.dn:cn=John Doe,ou=Sales,dc=plainjoe,dc=org

Τα Αναφορικά (relative) DNs (RDNs) προσδιορίζουν ένα ζεύγος χαρακτηριστικών τα περιεχόμενα ενός καταλόγου

π.χ. cn=John Doe ή username=test ,cn=Jane Smith+ou=Sales

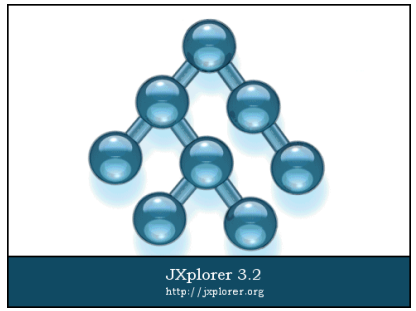
Η λειτουργία του LDAP

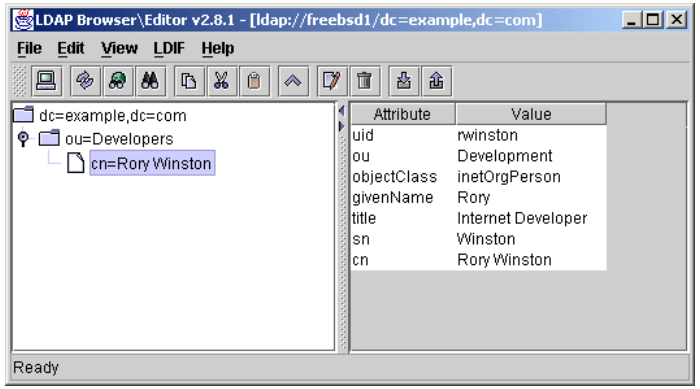
- ✓ Η υπηρεσία καταλόγου LDAP [OpenLDAP] είναι βασισμένη στο μοντέλο επικοινωνίας πελάτη-εξυπηρετητή.
- ✓ Ένας ή περισσότεροι κεντρικοί υπολογιστές LDAP περιέχουν τα δεδομένα που αποτελούν το δέντρο πληροφοριών καταλόγου ***(Directory Information Tree –DIT)***
- ✓ Ο κεντρικός υπολογιστής αποκρίνεται με μια απάντηση ή/και με έναν δείκτη όπου ο πελάτης μπορεί να πάρει τις πρόσθετες πληροφορίες

Browsers για τον LDAP

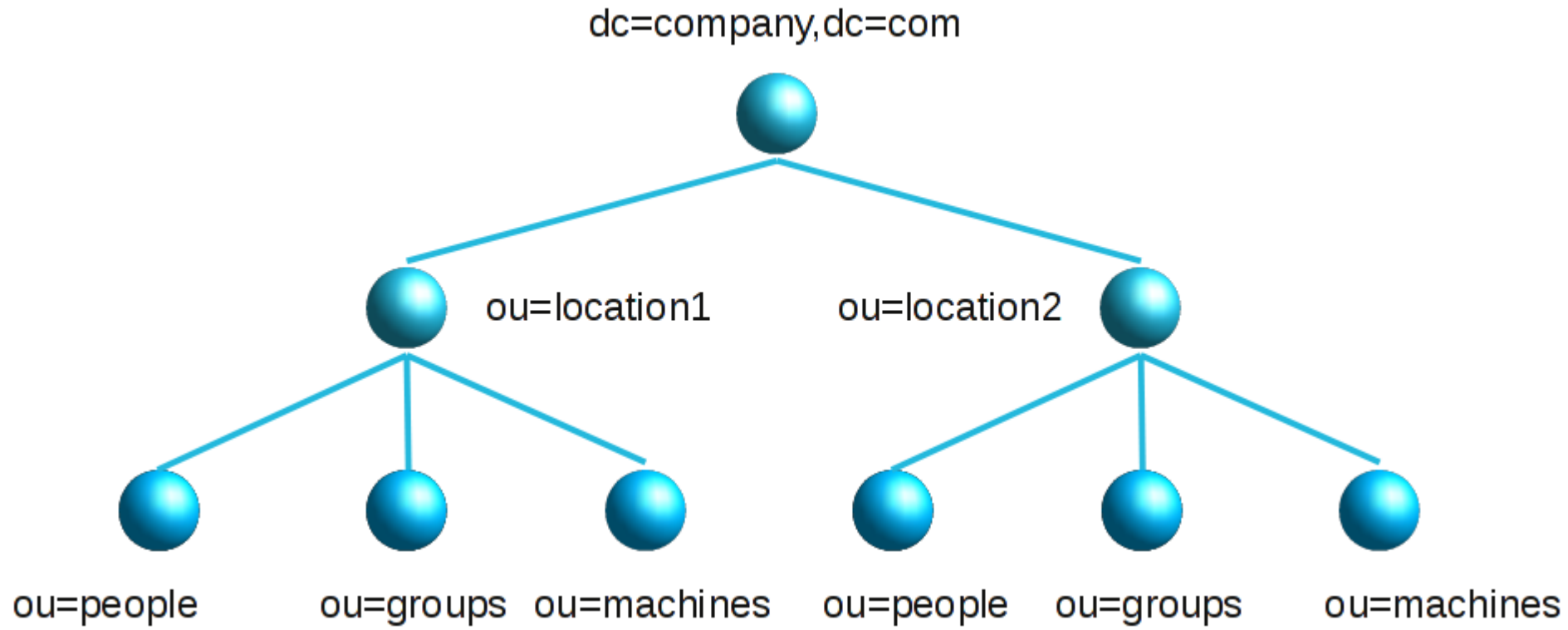
Οι φυλλομετρητές LDAP έχουν την δυνατότητα να συνδεθούν με οποιοδήποτε LDAP εξυπηρετητή και να ανακτήσουν στοιχεία από αυτόν.

- ✓LDAP Browser
- ✓phpldapadmin
- ✓Softerra
- ✓LDAP Admin
- ✓JXplorer

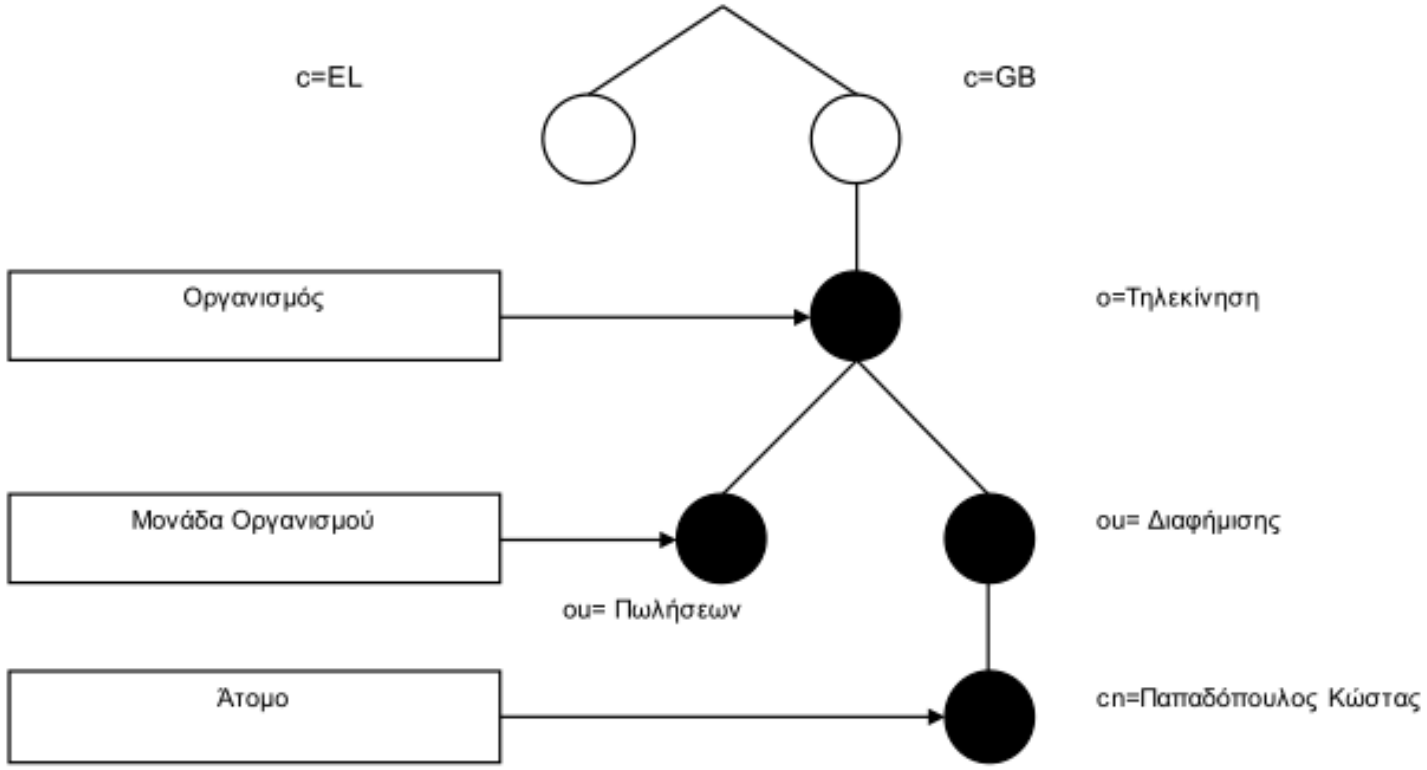




Η δεντρική μορφή του LDAP

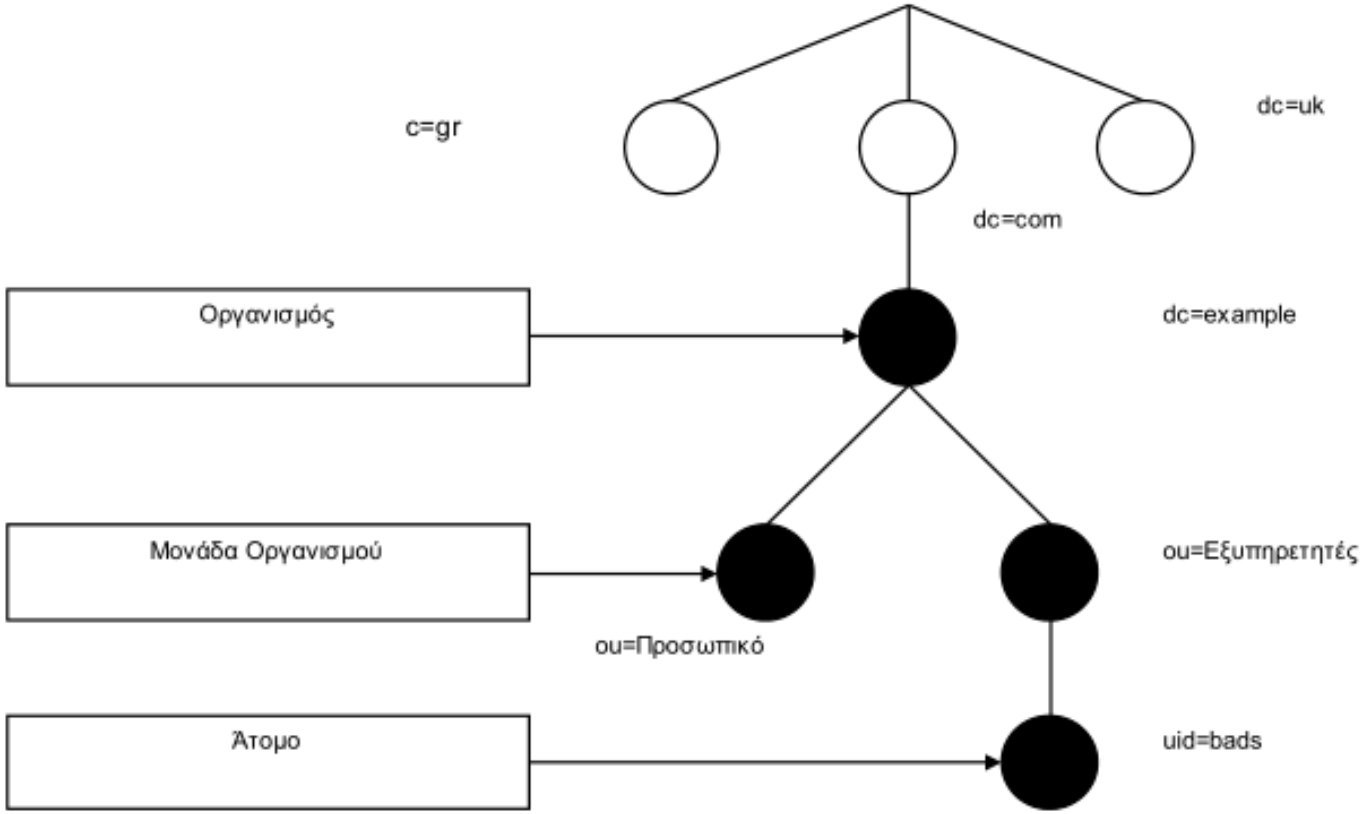


Η δεντρική μορφή του LDAP



Η δεντρική μορφή του LDAP

(χρησιμοποιώντας την DNS ονομασία)



Schema στο LDAP

Με ένα schema μπορούμε να :

- ✓περιγράψουμε τα απαιτούμενα χαρακτηριστικά για την δομή μας
- ✓συγκρίνουμε τα χαρακτηριστικά
- ✓περιορίσουμε το εύρος των τιμών εισαγωγής για τα χαρακτηριστικά
- ✓θέσουμε σύνολο κανόνων που περιγράφει τι είδους δεδομένα αποθηκεύονται
- ✓βελτιστοποιήσουμε την συνοχή και ποιότητα των δεδομένων
- ✓Μειώσουμε τις διπλοεγγραφές των δεδομένων

Οι εντολές για τον LDAP

Εκκίνηση

- ✓Windows : στο command prompt, **C:\openldap>slapd**
- ✓Linux : στο bash shell **/usr/local/etc/libexec/slapd**

Τερματισμός

- ✓Linux : στο bash shell **kill -INT cat /usr/local/var/slapd.pid**

Οι εντολές για τον LDAP

Σύνδεση στον LDAP

Χρησιμοποιώντας το LDAP Browser μας συνδεόμαστε στον Ldap Server

π.χ. για τον Softera δημιουργούμε προφίλ δίνοντας τα στοιχεία για τον server:

- ✓Host : localhost Port :389
- ✓Base DN : αυτόν τον κατάλογο που θέλουμε π.χ. c = myldap ή c =gr
- ✓User DN : cn = Manager, c = EL Password: ****

Αποθηκεύουμε το connection

Οι εντολές για τον LDAP

Προσθήκη εγγραφής

ldapadd -f /tmp/entrymods (έστω ότι υπάρχει το αρχείο /tmp/entrymods)

Τροποποίηση εγγραφής

ldapmodify -b -r -f /tmp/entrymods

Διαγραφή εγγραφής

ldapdelete 'cn=Luiz Malere,o=TUDelft,c=NL’

Αναζήτηση εγγραφής

ldapsearch -b 'o=TUDelft,c=NL' 'cn=Rene van Leuken'

URL :LDAP-HOWTO

Παραμετροποίηση του LDAP

Αρχεία παραμετροποίησης του LDAP

- ✓Client: /etc/openldap/ldap.conf
- ✓Server: /etc/openldap/slapd.conf

Τα αρχεία LDIF

- ✓ LDIF σημαίνει ***LDAP Interchange Format***
- ✓ Μορφή ανταλλαγής δεδομένων LDAP
- ✓ Αναπαριστά τις καταχωρήσεις του LDAP σε κείμενο
- ✓ Εύκολη ανάγνωση από άνθρωπο
- ✓ Επιτρέπει την εύκολη τροποποίηση των δεδομένων
- ✓ Εύκολη εισαγωγή και εξαγωγή

Τα αρχεία LDIF

- ✓ Τυποποιημένη μορφή κειμένου για την αποθήκευση των δεδομένων παραμετροποίησης LDAP και των περιεχόμενων του καταλόγου.
- ✓Συλλογή από εγγραφές χωρισμένες με κενές γραμμές
- ✓Χαρτογραφούν τα ονόματα των χαρακτηριστικών με τις τιμές τους

Χρησιμοποιούνται για να :

- ✓ Εισάγουν νέα δεδομένα στον κατάλογο
- ✓ Εξάγουν τους καταλόγους σε LDIF files για αντίγραφα ασφαλείας

LDIF και BackUp

Δημιουργία αντιγράφων ασφαλείας για ένα κατάλογο LDAP

- slapcat > backup.ldif
- Ή για καθημερινό backup slapcat > backup-`date +%F`.ldif

Αποκατάσταση ενός LDAP καταλόγου service ldap stop

- rm -rf /var/lib/ldap/*
- slapadd < backup.ldif
- service ldap start

Στην περίπτωση του Softera επιλέγουμε File -> LDIF export -> EL.ldif

OpenLDAP

- ✓ LDAP server: slapd
- ✓ Client εντολές: ldapadd, ldapsearch
- ✓ Backend αποθήκευση: Berkeley DB
- ✓ Backend εντολές : slapadd, slapcat
- ✓ Σχήμα: /etc/openldap/schema
- ✓ Δεδομένα: /var/lib/ldap

API και LDAP

Java

- ✓Tomcat 7 - Realm
- ✓Apache Directory Client API
- ✓jLDAP
- ✓JNDI
- ✓OpenDJ LDAP SDK
- ✓UnboundID

Python

python-ldap.org

PHP

ldap.php

Παράδειγμα σύνδεσης PHP και LDAP

```
<?php $ldap_dn = "cn=admin,dc=myldap,dc=org"; $ldap_password ="*****";
$ldaptree = "OU=Managers,DC=myldap,DC=org";
$ldapconn = ldap_connect("192.168.63.101");
ldap_set_option($ldapconn, LDAP_OPT_PROTOCOL_VERSION, 3);
$result=ldap_bind($ldapconn, $ldap_dn, $ldap_password);
if($result) { $search = ldap_search($ldapconn,$ldaptree, "(cn=*)") or die
("Error"); $data = ldap_get_entries($ldapconn, $search);
print_r($data);
} else {echo "Invalid user/pass or other errors!";} }
```

Παράδειγμα σύνδεσης Tomcat και LDAP

Δείτε περισσότερα στα ακόλουθα urls

http://docs.oracle.com/javase/7/docs/technotes/guides/jndi/index.html

http://tomcat.apache.org/tomcat-7.0-doc/realm-howto.html

```
<Realm className="org.apache.catalina.realm.JNDIRealm"
connectionURL="ldap://localhost:389"
userPattern="uid={0},ou=people,dc=mycompany,dc=com"
roleBase="ou=groups,dc=mycompany,dc=com"
roleName="cn"
roleSearch="(uniqueMember={0})"
/>
```

Ασφάλεια στον LDAP

LDAP Injection

- ✓LDAP Injection attacks είναι απειλές αντίστοιχες με τις SQL injection
- ✓Στόχος είναι η εκμετάλλευση τρωτών σημείων του LDAP και η «εκτέλεση» μη εξουσιοδοτημένων LDAP queries

Αποτροπή:

- ✓Θα πρέπει να υπάρχουν οι κατάλληλοι μηχανισμοί (filters) ώστε να γίνεται validation όλες οι παράμετροι που περνάνε από τον χρήστη πριν εκτελεστούν από τον server

Βιβλιογραφία

Έντυπη

- Understanding and deploying LDAP directory services, 2nd edition, Addison-Wesley
- Practical Spring LDAP, Apress

Ηλεκτρονική

- https://tomcat.apache.org/tomcat-7.0-doc/realm-howto.html
- http://idiotechie.com/secure-web-application-in-java-ee6-using-ldap/
- https://www.digitalocean.com/community/tutorials/understanding-the-ldap-protocol-data-hierarchy-and-entry-components
- https://www.digitalocean.com/community/tutorials/how-to-manage-and-use-ldap-servers-with-openldap-utilities
- https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-a-basic-ldap-server-on-an-ubuntu-12-04-vps
- https://www.digitalocean.com/community/tutorials/how-to-use-ldif-files-to-make-changes-to-an-openldap-system
- https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-openldap-and-phpldapadmin-on-ubuntu-16-04
- https://www.digitalocean.com/community/tutorials/how-to-configure-openldap-and-perform-administrative-ldap-tasks
- https://directory.apache.org/api/java-api.html