ΣΤΗΡΙΖΩ | Υποστήριξη Ψηφιακού Σχολείου και νέες υπηρεσίες Πανελλήνιου Σχολικού Δικτύου

Επιχειρησιακό Πρόγραμμα: «ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ» 2007-2013

ΠΡΑΞΗ: «ΣΤΗΡΙΖΩ – Οριζόντιο Έργο Υποστήριξης Σχολείων, Εκπαιδευτικών και Μαθητών στο Δρόμο για το ΨΗΦΙΑΚΟ ΣΧΟΛΕΙΟ, νέες υπηρεσίες Πανελλήνιου Σχολικού Δικτύου και Στήριξη του ΨΗΦΙΑΚΟΥ ΣΧΟΛΕΙΟΥ (ΟΡΙΖΟΝΤΙΑ ΔΡΑΣΗ)»

ΔΡΑΣΗ Α2: Βασικές (κρίσιμες) υπηρεσίες ΠΣΔ

εσίας
έτη

Κατάσταση Έκδοσης	**Υπό έγκριση από ΙΤΥΕ**
Ημερομηνία	**30/7/2012**
Περιγραφή Αρχείου	
Συμπράττων Φορέας	**ΕΠΙΣΕΥ**
Υπεύθυνος Παραδοτέου	**Σακκά Κωνσταντίνα**
Αριθμός Σελίδων	
Ημ/νια παραλαβής από Φορέα	**30/7/2012**
Ημ/νια παραλαβής από ΙΤΥΕ	

Ινστιτούτο Τεχνολογίας Υπολογιστών και Εκδόσεων «Διόφαντος» (ΙΤΥΕ)

ΙΤΥΕ "ΔΙΟΦΑΝΤΟΣ" ινστιτούτο τεχνολογίας υπολογιστών & εκδόσεων

Ευρωπαϊκή Ένωση Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2007-2013 ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Ομαδα Εκπονησης Παραδοτεου

1. Καθ. Ευσταθιος Συκας
2. Δρ. Δημητριος Καλογερας
3. Κωνσταντινα Σακκα
4. Κωνσταντινος Καλευρας

1. ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΥΠΗΡΕΣΙΑΣ

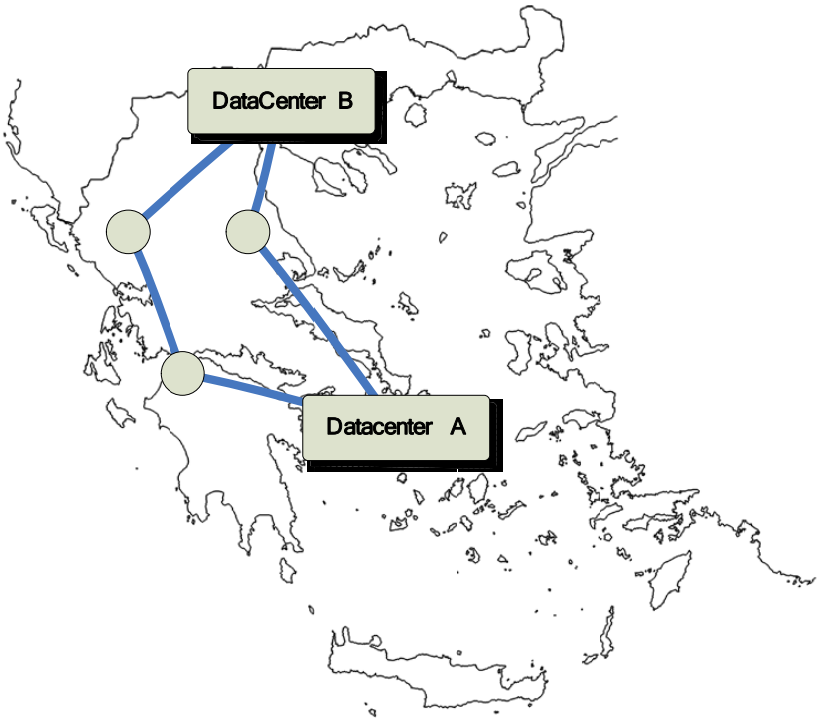
Στόχος της υπηρεσίας καταλόγου είναι η δημιουργία και η λειτουργία ενός αποθετηρίου καταλόγου το οποίο θα συντηρεί τα στοιχεία ταυτοποίησης και παραμετροποίησης του κάθε χρήστη διαφόρων υπηρεσιών του ΠΣΔ (π.χ. e-mail, προσωπικές σελίδες κλπ). Η παραμετροποίηση μπορεί να αφορά και πρόσβαση σε υπηρεσίες από οντότητες (π.χ. πρόσβαση με δρομολογητή ADSL ενός σχολείου) αντί για μεμονωμένα άτομα. Η υπό αυτή την έννοια το ΠΣΔ παρουσιάζει την εικόνα ενός DEN (Directory Enabled Networking) χώρου υπηρεσιών. Η υπηρεσία καταλόγου είναι μια προτυποποιημένη υπηρεσία (κατά ISO και IETF) και έχει ευρεία αποδοχή στο χώρο της δομημένης λειτουργίας υπηρεσιών διαδικτύου.

Εν συντομία σκοπός της παρούσης μελέτης είναι να επικαιροποιήσει την υφιστάμενη υποδομή καταλόγου χρησιμοποιώντας τις υποδομές σύννεφου (cloud) του ΕΑΙΤΥ και λογισμικό καταλόγου ανοικτού κώδικα. Επιπλέον θα μελετήσει και την μετάβαση στην νέα υποδομή ώστε να υπάρχει όσο το δυνατόν μικρότερη επιβάρυνση στις εξαρτώμενες υπηρεσίες.

2. ΠΕΡΙΓΡΑΦΗ ΥΠΗΡΕΣΙΑΣ

2.1 ΓΕΝΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΗΣ ΥΠΗΡΕΣΙΑΣ

Η αρχιτεκτονική της υπηρεσίας καταλόγου βασίζεται στην ιδέα ότι δύο σημεία παρουσίας υλοποιούν εφεδρεία 1+1. Η επιλογή των δύο σημείων παρουσίας επιτρέπει την υλοποίηση ενός σχήματος διαθεσιμότητας 1+1 κατά το οποίο επιτρέπεται πρακτικά ο ένας κόμβος να υποστηρίξει σε οριακές περιπτώσεις το σύνολο των αιτημάτων. Στο σχολικό δίκτυο οι προτεινόμενες θέσεις εγκατάστασης της υποδομής είναι στα κεντρικά data centers τα οποία βρίσκονται στην Αθήνα και στην Θεσσαλονίκη. Τα εν λόγω data centers έχουν την ιδιαιτερότητα ότι συγκεντρώνουν μεγάλο ποσοστό της ευρυζωνικής και λοιπής κίνησης των σχολείων δεδομένου ότι πληθυσμιακά το μεγαλύτερο ποσοστό των σχολείων βρίσκεται στη Αθήνα και στην Θεσσαλονίκη. Αυτό σημαίνει ότι δεν υπάρχει χρόνος μεταγωγής για τις περισσότερες δικτυακές υπηρεσίες μεταξύ των σχολείων και των κεντρικών υποδομών. Επιπλέον τα data centers της Αθήνας και Θεσσαλονίκης έχουν βελτιωμένο εξοπλισμό υποδομής και διασύνδεσης με το βασικό δικτυακό πάροχο, δηλαδή το ΕΔΕΤ. Μεταξύ Αθήνας και Θεσσαλονίκης το ΕΔΕΤ υλοποιεί δύο εναλλακτικές διαδρομές, η πρώτη δρομολογείται μέσω Λάρισας ενώ η δεύτερη μέσω Πάτρας και Ιωαννίνων.



Σχήμα 1 Τοποθέτηση κόμβων και εναλλακτικές διαδρομές για υψηλή διαθεσιμότητα

Με χρήση ορολογίας διαθεσιμότητας, η διασύνδεση των δύο data center για το δίκτυο ευρείας ζώνης (WAN) έχει αντοχή έναντι αστοχίας κόμβου (node failure) και έναντι αστοχίας γραμμής (link failure).

2.1.1 Αρχιτεκτονική κόμβου του Data Center

Κάθε κόμβος - data center αποτελείται από 3 συστήματα υλικού, ένα τύπου A και δύο τύπου B. Τα συστήματα τύπου A υλοποιούν τον κεντρικό εξυπηρετητή εγγραφών (write-master). Αυτός ο εξυπηρετητής υλοποιεί:

1. εγγραφές στον εξυπηρετητή καταλόγου,
2. αναζητήσεις σε αντικείμενα τα οποία δεν είναι δεικτοδοτημένα (indexed),
3. αναζητήσεις οι οποίες επιστρέφουν περισσότερες από μια απαντήσεις (results).

Τυπικές περιπτώσεις χρήσης του εξυπηρετητή Α είναι από το Περιβάλλον Διαχείρισης Χρηστών (ΠΔΧ) όπου πραγματοποιούνται λειτουργίες αναζήτησης κατά τις οποίες γίνεται τμηματικά ομαδικές αναζητήσεις π.χ. «όλοι οι μαθητές του σχολείου Α». Δεδομένου ότι οι εξυπηρετητές τύπου Α μπορεί να ικανοποιούν οποιοδήποτε τύπου ερωτήσεις (ακόμη και για μη δεικτοδοτημένα αντικείμενα) είναι εφοδιασμένοι με μεγαλύτερη ποσότητα κεντρικής μνήμης (4 GB). Οι εξυπηρετητές έχουν συστοιχίες: α) δίσκων σε τοπολογία RAID 1 (αρχιτεκτονική 1:1) β) τροφοδοτικών και γ) ανεμιστήρων. Εν τούτοις σε περίπτωση αστοχίας χρησιμοποιείται ο εξυπηρετητής τύπου Α στον κατοπτρικό κόμβο (στην Θεσσαλονίκη για την Αθήνα και αντίστροφα).

Άλλη περίπτωση χρήσης του κεντρικού διακομιστή εγγραφών (write-master) είναι μέσω των υπηρεσιών ιστού (Web-Services) τα οποία πραγματοποιούν λειτουργίες εγγραφών (write-operations) για τα συστήματα λογισμικού s-Portal (s-P), γραμματειακό και PKI.

Κάθε κόμβος - data center είναι επιπλέον εφοδιασμένος με δύο εξυπηρετητές τύπου Β. Οι εξυπηρετητές τύπου Β είναι αντίγραφα ανάγνωσης (read-only replicas) των κεντρικών διακομιστών εγγραφών (write-master) και εξυπηρετούν τις εφαρμογές του ΠΣΔ που κάνουν δεικτοδοτημένες αναζητήσεις στον υπηρεσία καταλόγου.

Επιπλέον οι εξυπηρετητές τύπου Β έχουν συστοιχίες: α) δίσκων σε τοπολογία RAID 1 (αρχιτεκτονική 1:1) β) τροφοδοτικών και γ) ανεμιστήρων για την αντιμετώπιση βλαβών εντός του εξυπηρετητή. Σε περίπτωση γενικευμένης αστοχίας θα χρησιμοποιείται ο «δίδυμος» εξυπηρετητής (τύπου Β) στον ίδιο κόμβο. Η μετάβαση (fail-over) πραγματοποιείται μέσω μηχανισμών οι οποίοι είναι διαθέσιμοι στο δικτυακό εξοπλισμό (Layer-4 switches) τόσο σε επίπεδο σύνδεσης εξυπηρετητή όσο και εφαρμογής (server and application failover).

Η εξασφάλιση υψηλής διαθεσιμότητας στην υπηρεσία καταλόγου για την λειτουργία των εγγραφών επιτυγχάνεται με την τεχνική της αντιγραφής (replication, 1+1). Ειδικότερα χρησιμοποιείται η τεχνική multimaster αντιγραφή με δύο κεντρικούς (master) διακομιστές (τους εξυπηρετητές τύπου Α). Οι κεντρικοί διακομιστές εγγραφών (write-masters) επικοινωνούν συχνά μεταξύ τους και ανταλλάσουν πληροφορίες για τις νέες εγγραφές που έχουν πραγματοποιηθεί. Η τεχνική θα μπορούσε να δουλέψει και για περισσότερους από δύο masters επειδή τα υποδέντρα που εγγράφονται από τον καθένα είναι διαφορετικά και έτσι

δεν επέρχεται σύγκρουση. Οι εξυπηρετητές τύπου Α έχουν σχέση master – slave με τους εξυπηρετητές τύπου Β του ίδιου κόμβου.

2.1.2 Λειτουργικότητα υπηρεσίας καταλόγου στο Πανελλήνιο Σχολικό Δίκτυο

Η Υπηρεσία LDAP αποτελεί την βάση για τις περισσότερες υπηρεσίες του σχολικού δικτύου. Αποθηκευμένες στο σχήμα του εξυπηρετητή βρίσκονται όλες οι πληροφορίες για τους εκπαιδευτικούς, τις οργανωτικές μονάδες, τις ρυθμίσεις για διάφορες εφαρμογές. Αυτές τις πληροφορίες χρησιμοποιούν όλες οι εφαρμογές που ταυτοποιούν τους χρήστες, αποθηκεύουν διάφορα δεδομένα που είναι άρρηκτα συνδεδεμένα με αυτούς καθώς και με τις διάφορες οργανωτικές μονάδες. Κατά συνέπεια αποτελεί την βάση δεδομένων για της υπηρεσίες ηλεκτρονικού ταχυδρομείου, ηλεκτρονικών λιστών, φιλοξενίας ιστοσελίδων, συζητήσεων, διαχείρισης τάξης καθώς και διαφόρων ιστοτόπων. Επίσης θα αποτελέσει την βάση για την υπηρεσία μοναδικής ταυτοποίησης χρήστη που αναπτύχθηκε για το παρόν έργο, τόσο για την ταυτοποίηση των χρηστών όσο και για την εξουσιοδότηση τους στις υπηρεσίες

Αναλυτικά οι υπηρεσίες που χρησιμοποιούν αυτή την στιγμή την υπηρεσία LDAP είναι οι παρακάτω.

ΠΕΚ/ΑΑΑ: Η υπηρεσία Πιστοποίησης Εξουσιοδότησης Καταγραφής (ΠΕΚ) /Authentication Authorization Accounting (AAA) με χρήση του πρωτοκόλλου radius για τον έλεγχο πρόσβασης με χρήση τηλεφωνικών γραμμών για την σύνδεσή τους στο Πανελλήνιο Σχολικό Δίκτυο. Τα χαρακτηριστικά γνωρίσματα που χρησιμοποιεί για την εξουσιοδότηση των χρηστών καθώς και τα συνθηματικά για την ταυτοποίηση είναι αποθηκευμένα στην υπηρεσία LDAP.

Ηλεκτρονικό Ταχυδρομείο: Η υπηρεσία ηλεκτρονικού ταχυδρομείου χρησιμοποιεί την υπηρεσία LDAP για την ταυτοποίηση των χρηστών καθώς και κρίσιμες πληροφορίες όπως τα μέγιστα μεγέθη ταχυδρομείου που επιτρέπονται στους χρήστες, τις ηλεκτρονικές τους διευθύνσεις καθώς και τους χώρους αποθήκευσης των μηνυμάτων

Λίστες Ηλεκτρονικού Ταχυδρομείου: Επέκταση της παραπάνω υπηρεσίας χρησιμοποιεί την υπηρεσία LDAP για τις ρυθμίσεις των ηλεκτρονικών λιστών καθώς και για αποθήκευση των μελών που τις αποτελούν.

Φιλοξενία Ιστοτόπων: Η υπηρεσία φιλοξενίας δικτυακών ιστοτόπων χρησιμοποιεί την υπηρεσία LDAP για την ταυτοποίηση των χρηστών καθώς και την αποθήκευση διαφόρων ρυθμίσεων όπως τα όρια αποθήκευσης των χρηστών και οι χώροι τοποθέτησης των ιστοσελίδων τους.

Χώροι Συζητήσεων: Η υπηρεσία συζητήσεων χρησιμοποιεί την υπηρεσία LDAP για ταυτοποίηση των χρηστών.

Ηλεκτρονική Διαχείριση Τάξης: Η εν λόγω υπηρεσία χρησιμοποιεί την υπηρεσία LDAP για ταυτοποίηση των χρηστών.

Περιβάλλον Διαχείρισης Χρηστών: Το Περιβάλλον αυτό προσφέρει ένα κεντρικό σημείο διαχείρισης όλων των εγγραφών στην υπηρεσία καταλόγου. Λειτουργεί σε περιβάλλον web και είναι προσβάσιμο από τους διαχειριστές του Σχολικού Δικτύου. Προσφέρει κατάλληλες φόρμες για όλους τύπους εγγραφών ενώ παράλληλα προσφέρει χρήσιμη επιπλέον λειτουργικότητα (που βρίσκεται σε συνεχή χρήση για την υποστήριξη των δικτυακών υπηρεσιών του Σχολικού Δικτύου) όπως:

- Παροχή εγγύησης μοναδικότητας σε πεδία (attributes) για τα οποία απαιτείται αυτή (πχ όνομα χρήστη, διεύθυνση ηλεκτρονικού ταχυδρομείου).
- Δυνατότητα εκτέλεσης εξωτερικών λειτουργιών με την ολοκλήρωση μίας λειτουργίας (πχ μεταφορά θυρίδας ηλεκτρονικού ταχυδρομείου χρήστη ο οποίος μετακινήθηκε σε άλλη μονάδα).
- Δημιουργία παραγόμενων πεδίων κάτι το οποίο διευκολύνει τη διαχείριση των εγγραφών καθώς ο διαχειριστής απαιτείται να ενημερώνει συγκεκριμένα πεδίων μικρού αριθμού, ενώ όλα τα υπόλοιπα ενημερώνονται αυτόματα από το ίδιο το περιβάλλον.

2.1.3 Λειτουργικότητα υπηρεσίας καταλόγου σε σχέση με υπηρεσίες του E-School

Η Υπηρεσία LDAP είναι ένας από τους θεμελιώδεις λίθους για τις υπηρεσίες του έργου e-school. Παρακάτω παρουσιάζεται επιγραμματικά ο ρόλος της υπηρεσίας LDAP στις επιμέρους υπηρεσίες του e-school.

Συστήματα Γραμματειακής Υποστήριξης: Η υπηρεσία LDAP υποστηρίζει τα συστήματα Γραμματειακής Υποστήριξης χρησιμοποιούμενη ως κεντρική αποθήκη των πιστοποιητικών των κέντρων πανελληνίων εξετάσεων, των διαπιστευτηρίων και ρόλων των χρηστών του υποσυστήματος διαχείρισης και των αναγνωριστικών και χαρακτηριστικών των σχολικών μονάδων με τοπικές βάσεις δεδομένων που συγχρονίζονται με την Κεντρική Βάση Δεδομένων.

Υπηρεσίες s-Portal: Το σύστημα s-Portal χρησιμοποιεί την υπηρεσία καταλόγου για την αποθήκευση των λογαριασμών των γονέων και κηδεμόνων, ήτοι τα προσωπικά τους στοιχεία καθώς και το μυστικό συνθηματικό τους.

Υπηρεσία Μοναδικής Ταυτοποίησης Χρήστη (Single Sign On): Το σύστημα μοναδικής ταυτοποίησης χρήστη χρησιμοποιεί την υπηρεσία καταλόγου τόσο για την ταυτοποίηση των χρηστών όσο και για την εξουσιοδότηση τους στις υπηρεσίες.

Υποδομή Δημοσίου Κλειδιού (Publik Key Infrastructure): Η υποδομή δημοσίου κλειδιού πρόκειται να χρησιμοποιήσει την υπηρεσία καταλόγου για να αποθηκεύει τα ψηφιακά πιστοποιητικά των χρηστών ως χαρακτηριστικά των εγγραφών τους καθώς και τις λίστες ανάκλησης πιστοποιητικών επιτρέποντας την εύκολη αναζήτηση τους.

2.1.4 Λειτουργικές Εξαρτήσεις

Υπάρχουν ορισμένες εξαρτήσεις από συγκεκριμένες λειτουργικότητες που προσφέρει το λογισμικό:

- Η υπηρεσία mail (τουλάχιστον στην παλαιότερη έκδοση) χρησιμοποιεί τη λειτουργία Class of Service προκειμένου να δημιουργούνται δυναμικά attributes ανά χρήση (κυρίως για την αποθήκευση του mail server).
- Η πρόσβαση εγγραφής στην υπηρεσία περιορίζεται μέσω πολιτικής access list.

2.2 ΕΠΙΛΟΓΗ ΤΗΣ ΠΛΑΤΦΟΡΜΑΣ OPENLDAP

Ο OpenLDAP **Error! Reference source not found.** συνιστά λογισμικό ανοικτού κώδικα Υπηρεσίας Καταλόγου. Η ανάπτυξη του υποστηρίζεται από μία παγκόσμια κοινότητα εθελοντών που επικοινωνούν μεταξύ τους με σκοπό την υλοποίηση του λογισμικού και του συνοδευτικού υλικού. Συνεπώς αποτελεί προϊόν μιας συλλογικής προσπάθειας με στόχο τη δημιουργία ενός πλήρους λειτουργικού προϊόντος λογισμικού. Η χρήση του λογισμικού OpenLDAP είναι ιδιαίτερα διαδεδομένη στα πανεπιστημιακά ιδρύματα και τους ερευνητές, όμως για τις περισσότερες επιχειρήσεις δεν παρουσιάζει μια βιώσιμη off-the-shelf λύση υπηρεσίας καταλόγου.

Το λογισμικό του OpenLDAP περιλαμβάνει τον μοναδικό (stand-alone) διακομιστή LDAP (slapd), LDAP C++ σετ εργαλείων ανάπτυξης λογισμικού (Software Development Kit), βιβλιοθήκες (lldap – LDAP βιβλιοθήκη πελάτη, llber - BER/DER βιβλιοθήκη κωδικοποίησης/αποκωδικοποίησης), συμπληρωματικά εργαλεία (LDIF εργαλεία για μετατροπή δεδομένων, LDAP εργαλεία γραμμής εντολών, SNACC - ASN.1 εργαλεία ανάπτυξης, clients κλπ) και τη σχετική τεκμηρίωση.

Η τελευταία έκδοση, ο OpenLDAP 2.4.31 (21-4-2012) υποστηρίζει τις περισσότερες πλατφόρμες Unix ή UNIX-like (Linux, FreeBSD, NetBSD, OpenBSD, AIX, HP-UX, Solaris κλπ).

Ο διακομιστής LDAP slapd υλοποιεί την έκδοση 3 του πρωτοκόλλου LDAP (RFC 4510) πάνω από IPv4, IPv6 και υποστηρίζει:

- Ισχυρή επαλήθευση ταυτότητας, ταυτοποίηση με τη χρήση πιστοποιητικών και ασφάλεια δεδομένων μέσω της χρήσης Simple Authentication and Security Layer (SASL) και Transport Layer Security (TLS) ή Secure Sockets Layer (SSL). Για τη χρήση SASL χρησιμοποιείται Cyrus SASL λογισμικό το οποίο υποστηρίζει DIGEST-MD5, SASL EXTERNAL, και GSSAPI. Για τη χρήση TLS/SSL χρησιμοποιείται OpenSSL.
- Περιορισμός πρόσβασης σε στρώμα υποδοχής (socket layer) με βάση την πληροφορία τοπολογίας του δικτύου (*TCP wrappers).*

- Στατική/δυναμική πληροφορία ελέγχου πρόσβασης (access control information) στο χαρακτηριστικό *aci* και ενσωματωμένος μηχανισμός ελέγχου πρόσβασης στο δέντρο πληροφοριών του καταλόγου (access control mechanism in-tree).
- Κωδικοσελίδα Unicode και γλωσσικές ετικέτες.
- Επιλογή του περιβάλλοντος διαχείρισης της βάσης δεδομένων (database backend). Περιλαμβάνονται τα περιβάλλοντα διαχείρισης BDB και HDB τα οποία χρησιμοποιούν Sleepycat Berkeley βάση δεδομένων, MDB το οποίο χρησιμοποιεί memory-mapped database, META backend για σύνδεση με ήδη υπάρχοντα LDAP server, CONFIG backend για αποθήκευση του configuration online, MONITOR backend για online παρακολούθηση της καλής λειτουργίας της υπηρεσίας (μέσω LDAP), SHELL διεπαφή σε σενάρια κελύφους (shell scripts) και PASSWD διεπαφή στο αρχείο *passwd*.
- *Περιβάλλον overlays για την προσθήκη επιπλέον λειτουργιών στην υπηρεσία. Παραδείγματα:*
  - *Accesslog: Καταγραφή των αλλαγών σε LDAP βάση.*
  - *Auditlog: Καταγραφή των αλλαγών σε audit text log.*
  - *Constraint: Επιβολή περιορισμών στο συντακτικό συγκεκριμένων attributes (μορφή τιμής, πλήθος τιμών κτλ).*
  - *Dynamic Directory Services: Δυναμικά attributes.*
  - *Dynlist: Δυναμικές λίστες όπου τα μέλη ορίζονται με την μορφή ενός LDAP URL και η λίστα προκύπτει δυναμικά κατά την πρόσβαση στην εγγραφή της για ανάγνωση.*
  - *Pcache: Caching αναζητήσεων σε συνδυασμό με meta backend.*
  - *Refint: Referential integrity.*
  - *Unique: Εφαρμογή attribute uniqueness.*
- Ταυτόχρονη εξυπηρέτηση πολλαπλών βάσεων δεδομένων.
- Δυνατότητα προσαρμογής, μέσω της χρήσης μίας σαφώς ορισμένης C διεπαφής προγραμματισμού εφαρμογών η οποία χρησιμοποιείται για τη επικοινωνία μεταξύ των LDAP υπηρεσιών και του περιβάλλοντος διαχείρισης της βάσης δεδομένων.

- Χρήση πολύ-νηματικών (multi-threaded) διεργασιών για τα εισερχόμενα αιτήματα.
- Αντιγραφή (replication) single master με τη χρήση δυο μεθόδων, *LDAP Sync*-based. Υποστηρίζεται fractional και sparse αντιγραφή.
- Λειτουργία του ως κρυφή LDAP υπηρεσία διαμεσολάβησης.
- Εύκολη διαμόρφωση μέσω της χρήσης ενός και μόνο αρχείου διαμόρφωσης.
- Διατήρηση της διαμόρφωσης online σε δέντρο με ικανότητα αλλαγής της on-the-fly.
- Λειτουργία διαμεσολάβησης με χρήση του meta backend όπου ο εξυπηρετητής συνδέεται άμεσα μέσω LDAP σε άλλο εξυπηρετητή και πραγματοποιεί τις λειτουργίες που ζητούνται από το χρήστη με δυνατότητα ενδιάμεσων μετατροπών (rewrites).

Ο Πίνακας 1 περιλαμβάνει τις επεκτάσεις LDAPv3 οι οποίες υποστηρίζονται από την έκδοση 2.3.X

LDAPv3 RFCs	**Λειτουργίες**
RFC 2247 & RFC 3088	DNS-based service location
RFC 2696	Simple Paged Result Control
RFC 2849	LDIFv1
RFC 3062	LDAP Password Modify Extended Operation
RFC 3296	Named Referrals / ManageDSAit control
RFC 3673	All Operational Attributes + attribute list feature
RFC 3687	Component Matching Rules
RFC 3866	Language Tag and Range options

LDAPv3 RFCs	**Λειτουργίες**
RFC 3876	Matched Values control
RFC 4370	Proxy Authorization control
RFC 4522	The Binary Encoding Option
RFC 4523	X.509 Certificate Schema
RFC 4524	COSINE Schema
RFC 4525	Modify/Increment extension
RFC 4526	Absolute True (&) and False (|) Filter extension
RFC 4527	Pre/Post Read controls
RFC 4528	Assertion control
RFC 4529	Requesting Attributes by Object Class feature
RFC 4530	entryUUID operational attribute
RFC 4532	WhoAmI? Operation
RFC 4533	Content Synchronization operation
	No-Op control
	Schema updates over LDAP via cn=config
	Password Policy (ppolicy overlay)
	Permissive Modify control

Πίνακας 1 – *LDAPv3 επεκτάσεις του OpenLDAP 2.3.X*

2.2.1 Απαιτήσεις

Στην τρέχουσα υλοποίηση η υπηρεσία καταλόγου απευθύνεται στις εξής κατηγορίες χρηστών:

- Σχολικές μονάδες
- Εκπαιδευτικοί
- Μαθητές

Για τις σχολικές μονάδες προβλέπονται οι ακόλουθοι λογαριασμοί:

- Επίσημος λογαριασμός μονάδας ο οποίος παρέχει email και dialup πρόσβαση
- Λογαριασμός σύνδεσης μέσω κατάλληλου δρομολογητή και γραμμής ADSL ή ISDN στο Σχολικό Δίκτυο.
- Λογαριασμός dial out για απομακρυσμένη πρόσβαση στο δρομολογητή του σχολείου (εφόσον το σχολείο δε συνδέεται με γραμμή ADSL)
- Συμμετοχή της μονάδας στην ιεραρχία του Σχολικού Δικτύου κάτω από το δέντρο ou=units

Για τις υπόλοιπες κατηγορίες χρηστών οι λογαριασμοί είναι προσωποποιημένοι. Με βάση τα διαθέσιμα στοιχεία οι υπηρεσίες του Σχολικού Δικτύου απευθύνονται σε:

- 16.000 σχολικές και διοικητικές μονάδες
- 130.000 εκπαιδευτικούς
- 600.000 μαθητές (δευτεροβάθμια εκπαίδευση).

Με βάση τα στοιχεία αυτά λοιπόν προκύπτουν συγκεκριμένες απαιτήσεις σε αποθηκευτικό χώρο για τα δεδομένα της υπηρεσίας καταλόγου αλλά και για τη διαστασιολόγηση της απαιτούμενης μνήμης των εξυπηρετητών για την καλή λειτουργία της υπηρεσίας. Για κάθε εγγραφή η υπηρεσία καταλόγου απαιτείται να διατηρεί πέραν της ίδιας της εγγραφής ένα

αριθμό από αρχεία δεικτών (index files) για την επιτάχυνση των λειτουργιών αναζήτησης. Με βάση την εμπειρία λειτουργίας της υπηρεσίας προβλέπεται μέγιστος απαιτούμενος χώρος περίπου 10KB ανά εγγραφή. Κατά συνέπεια προκύπτουν οι ακόλουθες απαιτήσεις σε χώρο ανά κατηγορία εγγραφών:

- 1300MB (1,3GB) για τους εκπαιδευτικούς
- 6000MB (6GB) για τους μαθητές
- 500MB (0,5GB) για τις μονάδες (16.000 x 3 =~ 50.000)

Πέραν των παραπάνω προβλέπονται επιπλέον τύποι εγγραφών όπως mailing lists ανά σχολική μονάδα. Ρεαλιστική μακροπρόθεσμη πρόβλεψη είναι για επιπλέον 500MB για τις εγγραφές αυτές (50.000 εγγραφές).

Οι συνολικές μέγιστες απαιτήσεις που προκύπτουν από την παραπάνω ανάλυση είναι για περίπου:

830.000 εγγραφές και 8300MB (8,3GB) αποθηκευτικού χώρου.

2.3 Υψηλη διαθεσιμοτητα υποδομης Καταλογου

Με δεδομένη την ύπαρξη εναλλακτικών διαδρομών και κόμβων για τις υποδομές των Datacenter την κρίσιμη εξάρτησης άλλων υπηρεσιών από την υπηρεσία καταλόγου έχει αποφασιστεί να δομηθεί η υπηρεσία καταλόγου με χαρακτηριστικά υψηλής διαθεσιμότητας. Η υψηλή διαθεσιμότητα της υπηρεσίας θα επιτευχθεί μέσω των χαρακτηριστικών της επιλεγόμενης πλατφόρμας λογισμικού η οποία επιτρέπει τη λειτουργία πολλαπλών εξυπηρετητών ως master servers (οπότε θα είναι δυνατή η πραγματοποίηση αλλαγών σε κύριο και εφεδρικό εξυπηρετητή) και τη χρήση εναλλακτικών εξυπηρετητών σε επίπεδο υπηρεσίας πελάτη. Αναλόγως με τη διαθεσιμότητα υλικού, η λειτουργία fail-over μεταξύ των εξυπηρετητών μπορεί να γίνει είτε στο επίπεδο της υπηρεσίας πελάτη, είτε ακόμα και μέσω έξυπνων δικτυακών συσκευών (Layer-4/7 switches). Καθώς η υπηρεσία LDAP χρησιμοποιεί το πρωτόκολλο TCP (αντί για το UDP όπως η υπηρεσία RADIUS), η παρακολούθηση της υγείας των ανοικτών συνδέσεων (sessions) και η μετακίνηση τους σε fail-over εξυπηρετητή

είναι δυνατή άμεσα με οποιαδήποτε Layer-4 συσκευή, χωρίς να απαιτείται η τελευταία να φτάσει στο Layer-7 επίπεδο (επίπεδο εφαρμογής). Κατά συνέπεια δεν απαιτείται η χρήση ιδιαίτερα εξελιγμένων συσκευών δρομολόγησης (οι οποίες να έχουν τη δυνατότητα επεξεργασίας απευθείας των LDAP sessions) αλλά μόνο η διαχείριση (tracking) συνδέσεων (sessions) σε επίπεδο TCP, κάτι που μειώνει τα κόστη και διευκολύνει την οργάνωση των datacenters που θα φιλοξενήσουν την υποδομή.

2.4 ΑΠΑΙΤΗΣΕΙΣ ΛΕΙΤΟΥΡΓΙΑΣ -ΠΕΡΙΒΑΛΛΟΝ ΛΕΙΤΟΥΡΓΙΑΣ ΣΥΝΝΕΦΟΥ

Οι γενικές απαιτήσεις υποδομής που έχουν γνωστοποιηθεί από τον κύριο του έργου (Ε.Α.ΙΤΥ) είναι για ένα ιδεατό περιβάλλον σύννεφου (cloud). Χρειάζεται να επιβεβαιωθεί και να ελεχθεί η λειτουργία μετάπτωσης από κύριο σε εφεδρικό κόμβο με χρήση των ενδογενών μηχανισμών μετάπτωσης του σύνεφου π.χ. vmotion για περιβάλλον vmware, xenmotion για περιβάλλον Xen, live migration για kvm.

Οι γενικές απαιτήσεις ανά ιδεατό εξυπηρετητή αφορούν:

- Το αντίστοιχο δύο πυρήνων (2 core) επεξεργασίας.
- Ελεύθερο χώρο δίσκου τουλάχιστον 60 GB (ώστε να είναι δυνατή η άνετη επέκταση της υπηρεσίας και το online backup). Το σύστημα I/O είναι από τα πλέον σημαντικά στοιχεία της υπηρεσίας και απαιτείται να είναι όσο το δυνατόν ταχύτερο (με μικρή διαφοροποίηση στους μέσους χρόνους αναζήτησης/εγγραφής).
- Τουλάχιστον 4GB μνήμης με 8GB ως προτεινόμενο μέγεθος.

2.5 ΛΕΙΤΟΥΡΓΙΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΜΕ ΕΝΑ DATA CENTER

Η λειτουργία της υπηρεσίας σε περιβάλλον data center επιτρέπει την ύπαρξη κύριου και εφεδρικού εξυπηρετητή της υπηρεσίας. Ο κύριος και ο εφεδρικός εξυπηρετητής είναι απολύτως ίδιοι και λειτουργούν ως master. Απλώς οι υπηρεσίες πραγματοποιούν εγγραφές μόνο σε ένα (με το δεύτερο να λειτουργεί ως εφεδρικός) ενώ η ανάγνωση μπορεί να γίνεται από οποιονδήποτε εξυπηρετητή.

Η ενεργοποίηση του πρωτοκόλλου VRPP/CARP επιτρέπει την χρήση μιας δυναμικής διεύθυνσης (για master LDAP server) μεταξύ των δύο σταθμών. Ορίζεται ένα σταθμός σαν master ο οποίος έχει στην κατοχή του την δυναμική διεύθυνση και ο εφεδρικός ο οποίος την

ανακτά σε περίπτωση βλάβης. (Το υποδίκτυο της δυναμικής διεύθυνσης είναι το ίδιο με το δίκτυο της συνάρθροισης (δηλ. το δίκτυο που παράγεται από το LACP)). Με αυτό τον τρόπο για τον εξωτερικό κόσμο δλδ. τους ldap clients υπάρχει μια δ/ση εξυπηρετητή. Εάν είναι επιθυμητή υψηλότερη διαθεσιμότητα (node-protection) αναφορικά με τις διπλές φυσικές οδεύσεις των εξυπηρετητών προτείνεται η χρήση Multi-chassis-LACP) εφ΄όσον υποστηρίζεται από τους μεταγωγείς Ethernet του acenter.

Εναλλακτικά εάν η υποδομή του Datacenter υποστηρίζει μεταγωγείς επιπέδου 7 είναι εφικτή η ενσωμάτωση της λειτουργίας SLB (service load balancing) είτε στο foundry - brocade (http://www.brocade.com/support/Product_Manuals/ServerIron_SLBGuide/health.pdf) switch είτε στο Cisco switch

(http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxf7.html#wp2435940) για την παροχή υψηλής διαθεσιμότητας στην υπηρεσία.

Οι γενικές οδηγίες για service load balancing και για τους δύο κατασκευαστές είναι οτι συγκροτείται μια ομάδα από real servers οι οποίοι αποτελούν την φάρμα. Στην συνέχεια συγκροτείται ένας virtual server ο οποίος (ο οποίος λειτουργεί εντός του Layer 7 switch) προωθεί τις κλήσεις/αιτήσεις στην φάρμα με βάση κάποια πολιτική (τυχαία, round-robin, με βάρη κλπ) προώθηση. Ο τρόπος με τον οποίο καθορίζονται η διαθεσιμότητα των πραγματικών εξυπηρετητών μέσω του ιδεατού είναι με την συγκρότηση health-checks ή probes ανάλογα με τον κατασκευαστή. Στην περίπτωση της cisco τα probes τα οποία ελέγχουν την διαθεσιμότητα της υπηρεσίας με χρήση udp ή icmp packet. Στην περίπτωση του server-iron ορίζεται μια κλήση ldap για έλεγχο της διαθεσιμότητας της υπηρεσίας. Σε περίπτωση απάντησης συμπεραίνειται η λειτουργία του πρωτοκόλλου του πραγματικού εξυπηρετητή. Σε περίπτωση απάντησης με icmp port unreachable προκύπτει οτι δεν εξυπηρετείται το εν λόγο πρωτόκολλο.

2.5.1 Λειτουργία σε περιβάλλον με εφεδρικό data center

Το ΠΣΔ έχει προδιαγράψει την λειτουργία δύο data center ένα εκ των οποίων θα βρίσκεται στην Κωλλέτη και το δεύτερο στο υπολογιστικό κέντρο του ΕΑΙΤΥ στην Πάτρα ή στο Υπ. Παιδείας. Ανεξάρτητα της φυσικής τοποθεσία θα παρουσιάσουμε ένα υποθετικό σενάριο λειτουργίας το οποίο μένει να επιβεβαιωθεί όταν λειτουργήσουν τα δύο data center.

Η βασική υπόθεση είναι οτι οι ldap clients έχουν ρυθμισμένους δύο ldap servers για την αποστολή αιτήσεων/κλήσεων και θα ήταν επιθυμητό αυτή η ρύθμιση να κρατηθεί σε αυτό το επίπεδο. Στο νέο σενάριο κάθε μία διεύθυνση θα παραπέμπει σε ένα virtual server σε ξεχωριστό data center. Σε αυτή την περίπτωση θα χρειαστεί να μειωθεί ο χρόνος μετάπτωσης των clients από τον κύριο στον εφεδρικό σε τιμή που να καθορίζεται από το χρόνο μετάπτωσης της δρομολόγησης από το κεντρικό στο εφεδρικό εξυπηρετητή.

3. ΠΑΡΟΥΣΑ ΚΑΤΑΣΤΑΣΗ ΛΕΙΤΟΥΡΓΙΑΣ ΤΗΣ ΥΠΟΔΟΜΗΣ ΠΕΚ/ΑΑΑ ΤΟΥ ΠΣΔ (ΠΑΝΕΛΛΗΝΙΟΥ ΣΧΟΛΙΚΟΥ ΔΙΚΤΥΟΥ)

Η υπηρεσία καταλόγου (LDAP) του Πανελλήνιου Σχολικού Δικτύου βασίζεται στην πλατφόρμα λογισμικού Oracle (former Sun) Directory Server και προσφέρει λειτουργίες πιστοποίησης/εξουσιοδότησης και αναζήτησης μέσω πρωτοκόλλου LDAP σε υπηρεσίες οι οποίες χρησιμοποιούν το πρωτόκολλο αυτό. Η υπηρεσία λειτουργεί σε έξι (6) εξυπηρετητές Sun Solaris (αποκλειστική χρήση της υπηρεσίας) ενταγμένους στα datacenter του ΠΣΔ σε Αθήνα και Θεσσαλονική. Σε κάθε datacenter βρίσκονται 3 εξυπηρετητές, ένας write master και δύο read-only slaves. Στους write masters παράλληλα παρέχονται web services interfaces για χρήση απο τις υπηρεσίες του ΠΣΔ οι οποίες τα απαιτούν (κυρίως η υπηρεσία e-School).

Η τρέχουσα υλοποίηση της υπηρεσίας βασίζεται σε εμπορικό λογισμικό, το οποίο, παρότι είναι ακόμα ελεύθερα διαθέσιμο, απαιτεί συμβόλαιο υποστήριξης. Παράλληλα, η υποστήριξη του λειτουργικού Solaris δεν είναι πλέον διαθέσιμη στα πλαίσια του ΠΣΔ, με συνέπεια συνολικά η υποστήριξη της υπηρεσίας να μην είναι δυνατή, ιδιαίτερα σε περίπτωση bug.

3.1 ΕΞΑΡΤΗΣΕΙΣ ΝΕΑΣ ΥΠΗΡΕΣΙΑΣ

Βασική εξάρτηση της νέας υπηρεσίας είναι η παροχή κατάλληλου υλικού (νέοι εξυπηρετητές) για την εγκατάσταση και διαμόρφωση της. Οι νέοι εξυπηρετητές πρέπει να επιτρέπουν την εύκολη διαχείριση τόσο του λειτουργικού, όσο και του λογισμικού που θα χρησιμοποιηθεί στη νέα υπηρεσία. Τα προτεινόμενα λειτουργικά είναι FreeBSD ή Linux.

Σε περίπτωση κατά την οποία η διαθεσιμότητα νέων εξυπηρετητών αργήσει, προτείνεται να γίνει δοκιμαστική εγκατάσταση της υπηρεσίας σε εξυπηρετητή της ομάδας ανάπτυξης του ΕΜΠ, στην οποία θα ενσωματωθούν όλες οι νέες λειτουργίες που προβλέπονται από τη φάση ανάπτυξης. Όταν οι νέοι εξυπηρετητές γίνουν διαθέσιμοι, θα υπάρξει άμεση εγκατάσταση (με χρήση του ήδη αναπτυγμένου configuration και εργαλείων λογισμικού) και ενεργοποίηση της.

4. ΠΕΡΙΓΡΑΦΗ ΑΝΑΠΤΥΞΗΣ

Βασικό συστατικό στοιχείο της φάσης ανάπτυξης της υπηρεσίας θα είναι η μετάβαση της υπηρεσίας απο την κλειστή εμπορική πλατφόρμα της Oracle (πρώην Sun) στο ελεύθερο λογισμικό OpenLDAP. Στα πλαίσια της μετάβασης ιδιαίτερη προσοχή θα δωθεί:

- Στην μετάβαση του σχήματος πληροφορίας σε OpenLDAP ώστε να είναι δυνατή η μεταφορά των δεδομένων της υπηρεσίας χωρίς αλλαγές.
- Της μετάβασης της πολιτικής ασφάλειας (access lists) στο σχήμα του νέου λογισμικού.
- Στην υποστήριξη και ενσωμάτωση λειτουργικότητας που θεωρείται χρήσιμη όπως:
    - Δυναμικά attributes.
    - Referential Integrity
    - MemberOf entry attribute, dynamic groups.
    - Audit logging.
    - Attribute Uniqueness.
    - Δυναμικό, LDAP based configuration.
    - On the fly indexing, schema changes.
- Στη χρήση επιπλέον λειτουργικότητας που παρέχει ο OpenLDAP όπως:
    - Attribute constraints/allowed values.
    - Dynamic Directory Services (προσωρινές εγγραφές οι οποίες πιθανώς να φανούν χρήσιμες στη διαδικασία εγγραφής νέων χρηστών).
    - Password policy.
    - Χρήση meta backends και rewrite overlays για την υλοποίηση LDAP Proxy.

Παράλληλα θα εξεταστεί σε πραγματικές συνθήκες σε συνεργασία με τους υπεύθυνους των υπόλοιπων υπηρεσιών η σκοπιμότητα δημιουργίας ενός εξυπηρετητή κλασματικού συγχρονισμού ο οποίος θα περιέχει περιορισμένο σύνολο attributes ανά εγγραφή προς χρήση απο υπηρεσίες υψηλού φόρτου και επαναλαμβανόμενων αναζητήσεων (υπηρεσία email και mailing lists).

Στα πλαίσια της επέκτασης και βελτίωσης της υπηρεσίας συγχρονισμού με εξωτερικές υπηρεσίες μέσω web services (e-School, e-Datacenter) θα αναπτυχθεί (σε συνεργασία με τους υπεύθυνους των υπηρεσιών) διαδικασία συγχρονισμού χωρίς την παρέμβαση ανθρώπινου παράγοντα. Στην τρέχουσα κατάσταση ο συγχρονισμός γίνεται με χρήση ουρών καταγραφής αλλαγών με συνέπεια τυχόν απώλεια συγχρονισμού να δημιουργεί σοβαρό πρόβλημα καθώς δεν είναι εύκολη η επιδιόρθωση τυχόν προβλημάτων χωρίς παρέμβαση των διαχειριστών. Η επέκταση θα αναπτύξει επιπλέον διαδικασία αρχικού συγχρονισμού μέσω της οποίας θα είναι δυνατός ο επανα-συγχρονισμός (μέσω μίας λειτουργίας ανταλλαγής στοιχείων για τα υπάρχοντα δεδομένα μεταξύ των βάσεων) και άμεσης αυτοματοποιημένης επαναφοράς του συγχρονισμού.

4.1 ΔΥΝΑΜΙΚΑ ATTRIBUTES

Στην τρέχουσα υλοποίηση χρησιμοποιείται η λειτουργία class-of-service του εξυπηρετητή της Sun ώστε να δημιουργούνται δυναμικά attributes στις εγγραφές των χρηστών με βάση τα attributes εγγραφών που θεωρούνται 'παραγωγοί'. Η επιλογή των εγγραφών στις οποίες προστίθενται τα attributes αυτά γίνεται με χρήση κατάλληλων LDAP URLs (τα οποία περιέχουν LDAP φίλτρα). Είναι απαραίτητο να βρεθεί ένα ισοδύναμος μηχανισμός για την υλοποίηση στο νέο περιβάλλον.

Στην περίπτωση του OpenLDAP θα γίνει χρήση δύο overlays για την προσθήκη δυναμικών attributes:

- Overlay collect το οποίο επιτρέπει τον ορισμό ενός παραγωγού entry τα attributes του οποίου θα κληρονομούνται από όλες τις εγγραφές οι οποίες βρίσκονται κάτω από το δέντρο του παραγωγού. Η χρήση της μεθόδου αυτής μπορεί να ακολουθηθεί για attributes τα οποία ισχύουν για όλες τις εγγραφές σε ένα δέντρο.
- Overlay dynlist το οποίο επιτρέπει τη δημιουργία δυναμικών λιστών attributes σε entries σύμφωνα με την περιγραφή του ακόλουθου συνδέσμου. Τα DN των λιστών θα πρέπει να προστίθενται σε κάθε εγγραφή η οποία θα περιέχει παραγόμενα attributes, κάτι το οποίο παρότι δεν επιτρέπει 'double reference' (δημιουργία εγγραφής η οποία ορίζει το LDAP φίλτρο των εγγραφών στις οποίες θα προστίθονται τα δυναμικά της

attributes), κάνει το σχήμα διαχείρισης πιο σαφές και διαχωρισμένο: Διαχείριση των παραγόμενων attributes στην εγγραφή παραγωγού και ξεκάθαρη προσθήκη των εγγραφών στις οποίες θα ισχύουν.

4.2 ΚΛΑΣΜΑΤΙΚΟΣ ΣΥΓΧΡΟΝΙΣΜΟΣ

Καθώς το συνολικό μέγεθος της βάσης της υπηρεσίας είναι αρκετά μεγάλο, αυτό θέτει περιορισμούς στη δυνατότητα ευέλικτου και αποδοτικού caching των δεδομένων, λόγων των ετερογενών αναζητήσεων στην υπηρεσία και πιθανών περιορισμών στο διαθέσιμο υλικό. Σε αυτά τα πλαίσια είναι σκόπιμο, αναλόγως με τις ειδικότερες ανάγκες άλλων υπηρεσιών να δωθεί εξυπηρετητής αποκλειστικά για τις ανάγκες υπηρεσίας υψηλών αναγκών (πχ υπηρεσία email) στον οποίο θα συγχρονίζονται μόνο οι εγγραφές και τα attributes τα οποία είναι απαραίτητα για την καλή λειτουργία της (πχ μόνο εγγραφές χρηστών και attributes που έχουν σχέση με την πιστοποίηση/εξουσιοδότηση και λειτουργία της υπηρεσίας πελάτη).

Κατ' αυτόν τον τρόπο το μέγεθος της βάσης θα μειωθεί σε εξαιρετικά μεγάλο βαθμό και θα περιέχει μόνο εγγραφές (και attributes) οι οποίες απαιτούνται από την υπηρεσία πελάτη. Το caching θα είναι ευκολότερο, μικρότερου μεγέθους και στοχευμένο με συνέπεια καλύτερη λειτουργία του συνδυασμού. Οι υπόλοιποι 'κανονικοί' εξυπηρετητές της υπηρεσίας καταλόγου θα μπορούν να συνεχίσουν να χρησιμοποιούνται από όλες τις υπόλοιπες υπηρεσίες του ΠΣΔ ενώ παράλληλα θα λειτουργούν ως 'backup' για την υπηρεσία πελάτη του κλασματικού εξυπηρετητή.

Ένα άλλο θετικό στοιχείο είναι ότι, καθώς οι απαιτήσεις σε υλικό για ένα τέτοιο εξυπηρετητή είναι μικρές, θα μπορεί να αξιοποιηθεί καλύτερα υποδομή cloud του ΠΣΔ με εύκολη επέκταση της υπηρεσίας με βάση τις πραγματικές και εξελισσόμενες ανάγκες του ΠΣΔ.

Σε επίπεδο υλοποίησης θα χρησιμοποιηθεί η δυνατότητα για ορισμό παραμέτρων όπως φίλτρο, attributes, scope και Base DN στη διαμόρφωση της λειτουργίας συγχρονισμού του OpenLDAP, όπως περιγράφεται στον ακόλουθο σύνδεσμο.

4.3 REPLICATION WEB SERVICES

Η χρήση web services για την επικοινωνία με την υπηρεσία καταλόγου στην περίπτωση της πραγματοποίησης αλλαγών παρουσιάζει τα πλεονεκτήματα που έχουν περιγραφεί στα παραδοτέα του έργου e-School.

Πλεονεκτήματα χρήσης υπηρεσιών ιστού (web services) για την πραγματοποίηση αλλαγών στην υπηρεσίας Καταλόγου

- Διατηρείται η ήδη υπάρχουσα λογική ανάπτυξης εφαρμογών που προβλέπει τη δημιουργία συγκεκριμένου και αυστηρά ορισμένου πλαισίου συναρτήσεων – λειτουργιών οι οποίες καλούνται για την υλοποίηση εργασιών (με συγκεκριμένες παραμέτρους) και οι οποίες αναλαμβάνουν την εκτέλεση τους και την επιστροφή των αποτελεσμάτων (functional API).
- Χρησιμοποιείται μία τεχνολογία (web service) που είναι ανεξάρτητη της προγραμματιστικής πλατφόρμας με συνέπεια να παρέχει τη δυνατότητα συνεργασίας μεταξύ ετερογενών συστημάτων (πχ .Net με Java), ενώ τα πρωτόκολλα επικοινωνίας (HTTP, XML, WSDL, SOAP) είναι ιδιαίτερα διαδεδομένα και πολύ καλά ορισμένα με συνέπεια να αποφεύγονται τυχόν περιπτώσεις ασυμβατότητας.
- Όλες οι αλλαγές στα δεδομένα της υπηρεσίας καταλόγου πραγματοποιούνται κεντρικά διαμέσου των web services και όχι με απευθείας πρόσβαση από τις εξωτερικές υπηρεσίες. Αυτό έχει ως συνέπεια να μπορεί να οριστεί πολύ καλύτερα η πολιτική ασφάλειας επί των δεδομένων και να υπάρχει πλήρης έλεγχος επί των λειτουργιών που πραγματοποιούνται. Αντί οι εξωτερικές υπηρεσίες να έχουν αυξημένα δικαιώματα αλλαγών στα δεδομένα, απλά καλούν συγκεκριμένες συναρτήσεις. Έτσι, οι αλλαγές που μπορεί να πραγματοποιηθούν είναι πολύ συγκεκριμένες, γίνονται όλες από το ίδιο σημείο και μπορούν εύκολα να παρακολουθηθούν και να αποσφαλματοποιηθούν.
- Η κεντρική πραγματοποίηση των λειτουργιών επιτρέπει τη διατήρηση κεντρικού ιστορικού αλλαγών. Παράλληλα, ο συγγραφέας/διαχειριστής των web services έχει τη δυνατότητα να επιλέξει το επίπεδο λεπτομέρειας εργασιών που θα διατηρούνται στο ιστορικό. κάτι που δεν είναι δυνατό με την υπηρεσία καταλόγου όπου απλά διατηρούνται γενικές πληροφορίες για τις ενέργειες που εκτελούνται (αναλυτικό ιστορικό δεν είναι δυνατό να διατηρείται λόγω του πολύ μεγάλου πλήθους λειτουργιών, ιδιαίτερα αναζητήσεων, που πραγματοποιούνται σε μία υπηρεσία καταλόγου).
- Είναι δυνατόν να οριστούν εξωτερικές λειτουργίες που εκτελούνται πριν ή μετά την κλήση/ολοκλήρωση των web services. Έτσι για παράδειγμα η μετακίνηση ενός χρήστη στο δέντρο πληροφοριών, μπορεί να οδηγεί στην εκτέλεση εξωτερικής λειτουργίας που μετακινεί το mailbox του σε άλλο εξυπηρετητή email.
- Δεν απαιτείται η παροχή όλων των τυχόν attributes που μπορεί να περιέχει μία εγγραφή αλλά μόνο

των απολύτως απαραίτητων για την πραγματοποίηση της λειτουργίας. Τα υπόλοιπα attributes μπορούν να είναι παραγόμενα με βάση κατάλληλους κανόνες και συναρτήσεις. Έτσι για παράδειγμα μπορεί από το username του χρήστη να προκύπτει το email του (με βάση τον τύπο email=<username>@<domain>) ενώ τα όρια χρήσης της απομακρυσμένης σύνδεσης του (ημερήσιο και εβδομαδιαίο όριο) να είναι στατικά ορισμένα και να λαμβάνουν συγκεκριμένες και προκαθορισμένες τιμές τις οποίες δεν μπορεί να επηρεάσει ούτε ο χρήστης, ούτε η εξωτερική υπηρεσία που καλεί το web service.

- Ο διαχειριστής των web services μπορεί να ορίσει συγκεκριμένες και αρκετά περίπλοκες πολιτικές επί των τιμών των παρερχομένων attributes, κάτι που δεν είναι δυνατό από την υπηρεσία καταλόγου. Έτσι για παράδειγμα μπορεί να ορίσει συγκεκριμένη πολιτική επί του επιλεγόμενου username/password ή να ορίσει απαγορευμένες τιμές για άλλα attributes.
- Οι εξωτερικές υπηρεσίες δεν απαιτείται να γνωρίζουν απολύτως τίποτα για το σχήμα δεδομένων που χρησιμοποιείται από την υπηρεσία καταλόγου. Απλά παρέχουν τιμές σε συγκεκριμένα και αυστηρά ορισμένα ορίσματα των λειτουργιών που έχουν συμφωνηθεί χωρίς να έχουν γνώση πώς αυτά αντιστοιχίζονται σε attributes στις εγγραφές της υπηρεσίας καταλόγου. Ο διαχειριστής των δεδομένων, μπορεί να κάνει οποιαδήποτε μετατροπή, προσθήκη, αφαίρεση στο σχήμα δεδομένων χωρίς να απαιτείται να ενημερώσει τις εξωτερικές υπηρεσίες παρά μόνο να κάνει τις κατάλληλες αλλαγές στον κώδικα των web services (αν απαιτείται).
- Η λειτουργία διαγραφής χρήστη μπορεί να υλοποιηθεί με την μορφή λήξης εγγραφής και όχι διαγραφής της. Έτσι για παράδειγμα κάποιος χρήστης του οποίου η εγγραφή έχει λήξει μπορεί να ενημερωθεί μέσω email (χρησιμοποιώντας εξωτερικό port-operation όπως περιγράφηκε προηγουμένως) ώστε να μπορέσει να αλλάξει email διεύθυνση σε εύλογο χρονικό διάστημα. Κατ' αυτόν τον τρόπο δίνεται η δυνατότητα για ορισμό συγκεκριμένης πολιτικής λήξης και διαγραφής εγγραφών αντί για την απλή διαγραφή τους όταν αυτό ζητείται από εξωτερική υπηρεσία. Παράλληλα, η εγγραφή ενός χρήστη στην υπηρεσία καταλόγου μπορεί να αντιστοιχεί σε πολλαπλές εγγραφές σε εξωτερικές υπηρεσίες στην οποία περίπτωση η λειτουργίας διαγραφής θα πρέπει απλά να διαγράφει τα attributes που αντιστοιχούν στην κάθε εξωτερική υπηρεσία κάτι που μπορεί να υλοποιηθεί πολύ εύκολα μέσω των web services.

Ο τρόπος χρήσης τους όμως παρουσιάζει μία συγκεκριμένη διάκριση ανάλογα με τον πελάτη των web services:

- Η πρώτη κατηγορία είναι οι web based εφαρμογές οι οποίες χρησιμοποιούν τα web services για να εκτελέσουν λειτουργία αλλαγής η οποία έχει ζητηθεί απο χρήστη της κάθε εφαμοργής. Ο χρήστης εκτελεί εκείνη τη στιγμή την εφαρμογή και μπορεί να ανταποκριθεί άμεσα σε κάθε σφάλμα που θα παρουσιαστεί κατά την εκτέλεση της λειτουργίας που αιτήθηκε. Παράλληλα, η εκτέλεση των λειτουργιών απο τη φύση της είναι σειριακή με μεσολάβηση ανθρώπινου παράγοντα με συνέπεια να μπορεί να ακολουθηθεί η αντίστροφη διαδικασία σε οποιαδήποτε περίπτωση λάθους. Παράδειγμα αυτής της κατηγορίας είναι η εφαρμογή sPortal.

1.

- Η δεύτερη κατηγορία είναι η λειτουργία συγχρονισμού μεταξύ ετερογενών βάσεων δεδομένων και υπηρεσίας καταλόγου. Παραδείγματα είναι η υπηρεσία Γραμματειακής Υποστήριξης και οι εφαρμογές του e-Datacenter. Στην περίπτωση αυτή είναι απαραίτητο:

2.

  - Ο πάροχος και ο καταναλωτής δεδομένων (βάση δεδομένων και υπηρεσία καταλόγου) να είναι εξαρχής συγχρονισμένες ώστε οι αλλαγές να πραγματοποιούνται πάνω στις ίδιες εγγραφές.
  - Οι αλλαγές να γίνονται πάντα σειριακά και με χρονολογική σειρά καθώς σε αντίθετη περίπτωση υπάρχει το ενδεχόμενο μία αλλαγή που βασίζεται για την πραγματοποίηση της σε άλλη προγενέστερη να αποτύχει και τα δύο μέρη να αποσυγχρονιστούν.

Από τα παραπάνω φαίνεται ότι στη δεύτερη κατηγορία είναι εύκολο να υπάρξει αποσυγχρονισμός (ενώ υπάρχει εξαρχής απαίτηση τα δύο μέρη να εκκινούν τη διαδικασία συγχρονισμένα). Κατά συνέπεια δεν είναι επαρκές να υπάρχει διαδικασία για αποστολή αλλαγών (changelog) αλλά απαιτείται να οριστεί πλήρης διαδικασία αρχικοποίησης και επανασυγχρονισμού.

Η διαδικασία που θα οριστεί βασίζεται στη λογική του Syncronization Protocol που χρησιμοποιείται στην πλατφόρμα εξυπηρετητή LDAP OpenLDAP για το συγχρονισμό των replicas. Η διαδικασία μπορεί να εφαρμοστεί πάντα ακόμα και αν δεν υπάρχει ιστορικό αλλαγών (αν και σε αυτή την περίπτωση η λειτουργία συγχρονισμού είναι πιο απλή και γρήγορη). Βασίζεται στη λειτουργία PresentEntry(). Ουσιαστικά για κάθε εγγραφή στην πάροχο βάση δεδομένων γίνεται μία παρουσιαση της στην υπηρεσία καταλόγου. Η υπηρεσία καταλόγου κάνει οποιαδήποτε αλλαγή στην εγγραφή απαιτείται, ενώ θέτει τιμή σε κατάλληλο attribute με το timestamp της αλλαγής (ουσιαστικά το timestamp της έναρξης της διαδικασίας ώστε αυτό να είναι το ίδιο για όλες τις εγγραφές). Παράλληλα, όσο χρόνο διαρκεί η διαδικασία συγχρονισμού δεν επιτρέπεται να ξεκινήσει δεύτερη διαδικασία. Με το τέλος της διαδικασίας όσες εγγραφές δεν έχουν ανανεωθεί μπορούν να διαγραφούν και τα δύο μέρη είναι πλέον συγχρονισμένα.

Σε περίπτωση που υπάρχει ιστορικό αλλαγών (changelog) αποστέλλονται μόνο οι αλλαγές και αν βρεθεί ότι τα δύο μέρη (για οποιοδήποτε λόγο) έχουν αποσυγχρονιστεί ή το ιστορικό αλλαγών δεν περιέχει όλες τις αλλαγές που απαιτούνται μπορεί να εκτελεστεί πάλι η διαδικασία πλήρους συγχρονισμού.

Για το σκοπό αυτό θα απαιτηθεί να:

- διατηρούνται ορισμένα επιπλέον στοιχεία στον πάροχο και στον καταναλωτή δεδομένων (data version, update timestamp κτλ).
- οριστούν επιπλέον web services για τη διαδικασία αρχικοποίησης/συγχρονισμού (Present Phase).

4.3.1 Βάση Δεδομένων e-School (Πάροχος)

Οι απαιτήσεις από την βάση δεδομένων (πάροχο δεδομένων) είναι οι εξής:

1. Διατήρηση Global Data Version για ολόκληρη τη βάση: Απλώς ένας αριθμός ο οποίος αυξάνει κατά ένα σε κάθε write (add/delete/modify) operation.
2. Changelog: Αν διατηρούμε changelog για τα operations τότε ανά operation διατηρούμε και το αντίστοιχο dataversion.

4.3.2 Υπηρεσία Καταλόγου (Καταναλωτής)

Στην περίπτωση της υπηρεσίας καταλόγου απαιτούνται οι ακόλουθες προσθήκες στο σχήμα, στην κεντρική εγγραφή της υπηρεσίας (ρίζα δέντρου) και σε κάθε εγγραφή:

Στη ρίζα του δέντρου (dc=sch,dc=gr) προστίθενται τα παρακάτω πεδία:

- umddataversion;x-grammateiako=<DataVersion>
- umdupdatetimestamp;x-grammateiako=<timestamp>
- umdongoingupdatetimestamp;x-grammateiako=<timestamp>

3.

Σε κάθε Directory Entry το οποίο συγχρονίζεται με τον πάροχο δεδομένων προστίθενται τα παρακάτω πεδία:

- umddatasource=grammateiako
- umdupdatetimestamp;x-grammateiako=<timestamp>

4.

Προετοιμασία Δεδομένων

Πριν την έναρξη της διαδικασία συγχρονισμού με μαζικό τρόπο (bulk) απαιτείται να τεθεί το umddatasource σε όλους τους τύπους εγγραφών οι οποίες έχουν ώς πηγή το e-School (για τον αρχικό συγχρονισμό των δύο βάσεων).

Διαδικασία

Περιγράφονται οι νέες συναρτήσεις λειτουργιών οι οποίες θα γίνουν διαθέσιμες αλλά και η σειρά εκτέλεσης τους:

- GetDataVersion(). Επιστρέφει το Data Version για όλη το δέντρο.
  - Αν δεν υπάρχει changelog ή έχει χαθεί το synchronization ή το changelog δεν περιέχει επαρκή πληροφορία τότε εκτελείται η ακόλουθη συνάρτηση:

- StartTotalUpdate(DataVersion, UpdateTimestamp): To UpdateTimestamp είναι απλά το timestamp της έναρξης του update. Ενημερώνει το umdongoingupdatetimestamp on dc=sch,dc=gr. Επιστρέφει:
  - DataCurrent: No action needed
  - UpdateStarted
  - UpdateInProgress: Another update is running
  - Error
- PresentEntry(EntryQualifier, EntryType, [...Attributes...]): Ενημερώνει την εγγραφή αν απαιτείται καθώς και το umdupdatetimestamp,umddatasource. Εκτελείται σειριακά για όλες τις εγγραφές στη βάση του e-School.
- EndTotalUpdate(DataVersion, UpdateTimestamp): Ενημέρωση umdupdatetimestamp, umddataversion on dc=sch,dc=gr. Για όλες τις εγγραφές με (umddatasource=grammateiako) && (umdupdatetimestamp < <UpdateTimestamp>): Set to delete. Delete umdongoingupdatetimestamp

5.

- Αν υπάρχει το changelog
  - StartUpdate(DataVersion, UpdateTimestamp): Updates umdongoingupdatetimestamp. Επιστρέφει:
    - DataCurrent: No action needed
    - UpdateStarted
    - UpdateInProgress: Another update is running
    - Error
  - Normal Operations: Εκτέλεση των ήδη υπάρχουσων λειτουργιών με προσθήκη του UpdateTimestamp ώς argument.
- EndUpdate(DataVersion, UpdateTimestamp): Update umdupdatetimestamp, umddataversion, delete umdongoingupdatetimestamp on dc=sch,dc=gr.

5. ΜΕΤΑΒΑΣΗ ΣΕ ΝΕΑ ΥΠΗΡΕΣΙΑ

Για την μετάβαση στο νέο λογισμικό OpenLDAP θα αξιοποιηθεί η υπάρχουσα εμπειρία της ομάδας ανάπτυξης σε αντίστοιχη μετάβαση στο ΕΜΠ και η λειτουργικότητα που προσφέρει το meta backend του OpenLDAP. Η βασική ιδέα για την μετάβαση της υπηρεσίας είναι η προετοιμασία των δεδομένων με την απαραίτητη μετατροπή ορισμένων πεδίων και στην συνέχεια η εισαγωγή τους στην νέα βάση. Στην συνέχεια περιγράφονται η προετοιμασία των δεδομένων (βήμα 1-3) και κατόπιν η μετάβαση στους νέους εξυπηρετητές. Ειδικότερα:

1. Προσθήκη του υπάρχοντος σχήματος δεδομένων που χρησιμοποιείται στο υπάρχον περιβάλλον (i.e. Sun Ldap) στο διαθέσιμο σχήμα του OpenLDAP. Παράλληλα θα καθοριστούν τυχόν αναγκαίες αλλαγές για επικαιροποίηση του σχήματος (πχ αντί για τη χρήση του attribute 'l' για την επισήμανση του DN της τελικής μονάδας στην οποία ανήκει ο χρήστης θα χρησιμοποιηθεί το νεότερο attribute edupersonprimaryorgunitdn της κλάσης eduperson).
2. Εγκατάσταση βοηθητικού εξυπηρετητή (ή στον εξυπηρετητή ανάπτυξης) στο οποίο θα ενεργοποιηθεί η λειτουργικότητα meta backend το οποίο θα συνδέεται με την υπάρχουσα υπηρεσία στο βασικό εξυπηρετητή (dsw.att.sch.gr) και θα εμφανίζεται για τις εφαρμογές πελάτες ως ιδεατό backend. Ο εξυπηρετητής θα λειτουργεί ως 'proxy', και θα χρησιμοποιεί την λειτουργία των rewrites ώστε το ιδεατό backend να εμφανίζει το σχήμα δεδομένων όπως θα χρησιμοποιηθεί από την τελική υπηρεσία.
3. Η εξαγωγή-τροποποίηση των δεδομένων διαφόρων πεδίων του παλαιού καταλόγου στη νέα μορφή δεδομένων με την εκτέλεση κατάλληλου ldap search για όλο το δέντρο και την πληροφορία που περιέχει δια μέσω του βοηθητικού εξυπηρετητή με χρήση της λειτουργίας proxy. Το αποτέλεσμα της εξαντλητικής αναζήτησης θα είναι ένα ldif αρχείο το οποίο θα χρησιμοποιηθεί για την αρχικοποίηση της νέας υπηρεσίας με τα νέα τροποποιημένα δεδομένα του πλήρους δέντρου. Θα γίνουν δοκιμές εισαγωγής των δεδομένων στους νέους εξυπηρετητές και ταυτόχρονα θα πραγματοποιηθούν δοκιμές καλής λειτουργίας του σχήματος μετάβασης.

4. Πριν την μετάβαση θα μειωθεί ο χρόνος caching των DNS εγγραφών των παλαιών εξυπηρετητών σε ελάχιστο χρόνο μερικών δευτερολέπτων ώστε να είναι δυνατή η άμεση μετάβαση της υπηρεσίας στη νέα χωρίς ιδιαίτερο downtime.
5. Για την μετάβαση αρχικά η παλαιά υπηρεσία θα τεθεί σε read-only mode ώστε να επιτρέπονται μόνο αναζητήσεις. Με χρήση του ιδεατού backend θα γίνει εξαγωγή των δεδομένων και αρχικοποίηση της νέας υπηρεσίας.
6. Μετά την ολοκλήρωση δοκιμών καλής λειτουργίας η υπηρεσία καταλόγου θα μεταβεί στους νέους εξυπηρετητές με αλλαγή των DNS εγγραφών.

6. ΕΡΓΑΣΙΕΣ ΑΝΑΠΤΥΞΗΣ

- Εγκατάσταση νέου λογισμικού σε δοκιμαστικό εξυπηρετητή, μετάβαση υπάρχοντος σχήματος δεδομένων στη νέα έκδοση.
- Δοκιμές ικανότητας ανταπόκρισης της υπηρεσίας σε αυξημένο αριθμό αιτήσεων.
- Διαστασιολόγηση της υπηρεσίας, τόσο σε ότι αφορά τον αριθμό των εξυπηρετητών, όσο και στο μέγεθος τους (ανάγκες σε διαθέσιμη μνήμη, χώρο σε σκληρό δίσκο κτλ).
- Ανάπτυξη λειτουργίας συγχρονισμού με ετερογενείς βάσεις δεδομένων χωρίς παρέμβαση ανθρώπινου παράγοντα.
- Υλοποίηση εξυπηρετητή κλασματικού συγχρονισμού για χρήση απο συγκεκριμένες υπηρεσίες υψηλού φόρτου ερωτήσεων (πχ email). Η τελική ενσωμάτωση του εξυπηρετητή στην υπηρεσία θα εξαρτηθεί και απο τα αποτελέσματα της διαστασιολόγησης και ικανότητας ανταπόκρισης της υπηρεσίας.
- Υλοποίηση εξυπηρετητή Proxy LDAP με χρήση meta-backend και rewrites. Η χρήση του θα είναι στην παροχή LDAP backend για χρήση απο τελικούς χρήστες ενώ η βασική υπηρεσία καταλόγου θα παραμείνει κλειστή σε ένα DMZ προς χρήση μόνο απο υπηρεσίες του ΠΣΔ.
- Δοκιμή της υπηρεσίας σε συνεργασία με άλλες ομάδες του ΠΣΔ.

7. ΠΑΡΑΔΟΤΕΑ

- Λειτουργική υπηρεσία (η τελική φάση θα εξαρτηθεί από τη διαθεσιμότητα εξυπηρετητών).
- Τεκμηρίωση.

8. ΑΝΑΦΟΡΕΣ

OpenLDAP server: http://www.openldap.org