# ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ


**ΕΓΚΑΤΑΣΤΑΣΗ, ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΚΑΙ ΠΙΛΟΤΙΚΗ ΔΟΚΙΜΗ**

**ΔΙΑΚΟΜΙΣΤΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ**

Πτυχιακή εργασία


**ΛΙΚΟΛΛΑΡΙ ΑΡΝΤΙΤ**




Αθήνα, 2022

# HAROKOPIO UNIVERSITY

SCHOOL OF DIGITAL TECHNOLOGY

DEPARTMENT INFORMATICS AND TELEMATICS

**EMAIL SERVER INSTALLATION, CONFIGURATION AND PILOT TEST**

Bachelor thesis

**ARNTIT LIKOLLARI**

Athens, 2022

# ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

**Τριμελής Εξεταστική Επιτροπή**


**Καμαλάκης Θωμάς,**

**Αν. Καθηγητής,**

**Τμήμα Πληροφορικής και Τηλεματικής,**

**Χαροκόπειο Πανεπιστήμιο**

**Νικολαΐδη Μάρα**

**Καθηγήτρια,**

**Τμήμα Πληροφορικής και Τηλεματικής,**

**Χαροκόπειο Πανεπιστήμιο**

**Ριζομυλιώτης Παναγιώτης**

**Επικ. Καθηγητής,**

**Τμήμα Πληροφορικής και Τηλεματικής,**

**Χαροκόπειο Πανεπιστήμιο**

Ο Λικολλάρι Αρντίτ,

δηλώνω υπεύθυνα ότι:

1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

2) Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας

3)Όπου υφίστανται δικαιώματα άλλων δημιουργών έχουν διασφαλιστεί όλες οι αναγκαίες άδειες χρήσης ενώ το αντίστοιχο υλικό είναι ευδιάκριτο στην υποβληθείσα εργασία.

# ΕΥΧΑΡΙΣΤΙΕΣ

Ολοκληρώνοντας τη πτυχιακή μου εργασία, θα ήθελα να ευχαριστήσω όλους όσους βοήθησαν σε όλα τα στάδια ανάπτυξής της. Αρχικά, θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου κ. Καμαλάκη Θωμά για την εξαιρετική συνεργασία καθώς και τις εύστοχες υποδείξεις καθ' όλη τη διάρκεια της εκπόνησης της εργασίας. Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου για τη διαρκή υποστήριξη και βοήθεια κατά τη διάρκεια της εργασίας καθώς και την παροχή ερεθισμάτων και συνεργασίας καθ' όλη τη διάρκεια των σπουδών μου.

Πίνακας περιεχομένων

## Περίληψη

Η παρούσα πτυχιακή μελέτη έχει ως στόχο, την εγκατάσταση ενός σύγχρονου διακομιστή ηλεκτρονικού ταχυδρομείου όπου θα μπορεί να ανταπεξέλθει σε αρκετά απαιτητικό περιβάλλον, με αρκετές χιλιάδες χρήστες βασιζόμενο σε τεχνολογίες ανοιχτού λογισμικού. Επιπλέον θα υλοποιήσουμε διασύνδεση με τον υπάρχον κατάλογο χρηστών της σχολής. Ο κατάλληλος διακομιστής για να επιτευχθεί ο σκοπός αυτός είναι ο Zimbra mail client.

Στη συνέχεια θα αναλυθούν τα γενικά χαρακτηριστικά του Zimbra , ο λόγος που το επιλέξαμε , και τα πλεονεκτήματα που τον συνοδεύουν. Στη συνέχεια θα ακολουθήσει μια βάθος επεξήγηση των εργαλείων που χρησιμοποιήθηκαν , το πως επιτυγχάναμε την εγκατάσταση και την επεξήγηση των περιεχομένων του διακομιστή μας. Έπειτα αφού ολοκληρώσουμε την εγκατάσταση θα δημιουργήσουμε high availability στους δύο proxy εξυπηρετητές μας ώστε να αναδειχτεί η αποδοτικότερη λειτουργία του διακομιστή μας, να προσθέσουμε επιπλέον εργαλεία για καλύτερη ασφάλεια του συστήματος μας.

**Λέξεις κλειδιά:** ηλεκτρονικό ταχυδρομείο, λογισμικό, ασφάλεια, βελτιστοποίηση, εξυπηρετητής

## Abstract

The aim of this thesis is to install a modern e-mail server where it can cope with a very demanding environment, with several thousand users based on open source technologies. The right server to achieve this is the Zimbra mail client. Then we will analyze the general features of Zimbra, the reason we chose it, and the advantages that accompany it.

Then we will analyze the general features of Zimbra, the reason we chose it, and the advantages that accompany it. This will be followed by an in-depth explanation of the tools used, how we achieved the installation and the explanation of the contents of our server. Then after completing the installation we will create high availability on our two proxy servers in order to highlight the most efficient operation of our server, to add additional tools for better security of our system.



**Keywords:** email, software, security, optimization, server

# Κατάλογος εικόνων

# Κατάλογος πινάκων

## Κατάλογος εντολών

## Συντομογραφίες

| | |
|---|---|
| LDAP | LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL |
| MTA | MAIL TRANSFER AGENT |
| 2FA | TWO FACTOR AUTHENTICATOR |
| SMTP | SIMPLE MAIL TRANSFER PROTOCOL |
| VIP | VIRTUAL INTERNET PROTOCOL |
| SPF | SENDER POLICY FRAMEWORK |
| DKIM | DOMAIN KEYS IDENTIFIED MAIL |
| DMARC | DOMAIN BASED MESSAGE AUTHENTICATION |
| IP | INTERNET PROTOCOL |
| DNS | DOMAIN NAME SYSTEM |
| IMAP | INTERNET MESSAGE ACCESS PROTOCOL |
| SSH | SECURE SHELL PROTOCOL |
| QR CODE | QUICK RESPONSE CONDE |
| HA | HIGH AVALABILITY |

# Κεφάλαιο 1ο : Εισαγωγή

Ο διακομιστής ηλεκτρονικού ταχυδρομείου επιτυγχάνει την ανταλλαγή μηνυμάτων μέσω του παγκόσμιου ιστού , την αποθήκευση τον μηνυμάτων αυτών και την δυνατότητα σύνδεσης στο ηλεκτρονικό ταχυδρομείο αλλά και χρήση των πλήρους λειτουργειών του από οποιοδήποτε μέσο – διακομιστή. Internet Message Access Protocol ή IMAP είναι ένα πρωτόκολλο Διαδικτύου που συνδυάζει ορισμένες από τις λειτουργίες που παρέχονται από το Post Office Protocol (POP3) και το Webmail, καθώς και την προαιρετική αποθήκευση μηνυμάτων στον υπολογιστή του χρήστη. ("IMAP - Βικιπαίδεια", 2022)

Ταυτόχρονα, ένα αντίγραφο της αλληλογραφίας διατηρείται στον διακομιστή. Η πρόσβαση στον λογαριασμό email γίνεται μέσω ενός ειδικού προγράμματος αλληλογραφίας στην περίπτωσή μας η πρόσβαση θα επιτευχθεί μέσω του δικού μας συστήματος αλλά μπορεί να γίνει και μέσω άλλου διακομιστή. Ωστόσο στο δικό μας σύστημα είμαστε υπεύθυνοι όχι μόνο για την μεταφορά των μηνυμάτων αλλά και για την αποθήκευση τους , την προστασία τους από κακόβουλα λογισμικά αλλά και την επιτυχείς συντήρηση του συστήματος μας.

Παρακάτω αναφέρονται μερικές λύσεις διακομιστών ηλεκτρονικού ταχυδρομείου:

| Enteprice | Cloud | Open source |
|---|---|---|
| Gmail | Loop email | Zimbra |
| Microsoft Outlook | Proton mail | Mailcow dockerized |
| Thunderbird | Shift | Iredmail |
| Yahoo! mail | | |

*Πίνακας 1: Λίστα διακομιστών ηλεκτρονικής αλληλογραφίας*

## 1.1 Γενικά χαρακτηριστικά του Zimbra Email Client

Ο σκοπός της πτυχιακής είναι να συμβάλει στο να αλλάξει τον τρόπο με τον οποίο μέχρι στιγμής διαχειριζόμασταν άλλους διακομιστές Ηλεκτρονικού ταχυδρομείου. Ο Zimbra είναι ένας imap /pop3 διακομιστής που παρέχει ένα πλήρες και λειτουργικό σύστημα , εμπεριέχει επίσης εφαρμογή όπου μπορείς να έχεις πρόσβαση. Επιπλέον ο Zimbra παρέχει διαχείσηση antivirus και antispam για αποφυγή κακόβουλων μηνυμάτων, πολύ καλή διαχείριση των πόρων του συστήματος, μείωση κόστους εφόσον μιλάμε για ανοιχτού λογισμικού έκδοση. Στην ανοιχτού λογισμικού έκδοση έχει μεγάλη υποστήριξη από το community όπου μπορείς ευκολά να βρεις κάποια λύση σε ότι χρειαστείς. ("Open Source Email Platform - Zimbra Collaboration Open Source Edition", 2022)

## 1.2 Πλεονεκτήματα Zimbra

Ένα από τα βασικά πλεονέκτηματα του Zimbra είναι ότι πέραν από την πολύ καλή λειτουργικότητα του παρέχει και ανοιχτού λογισμικού έκδοση με την οποία το κόστος συντήρησης και λειτουργίας τέτοιου είδους διακομιστή είναι πολύ μικρό σε σχέση με κάποιον enterprice. Παρέχει πολλές δυνατότητες όπως ο διαχειριστής να μπορεί από οποιοδήποτε browser να έχει πρόσβαση στη διαχείριση του διακομιστή .

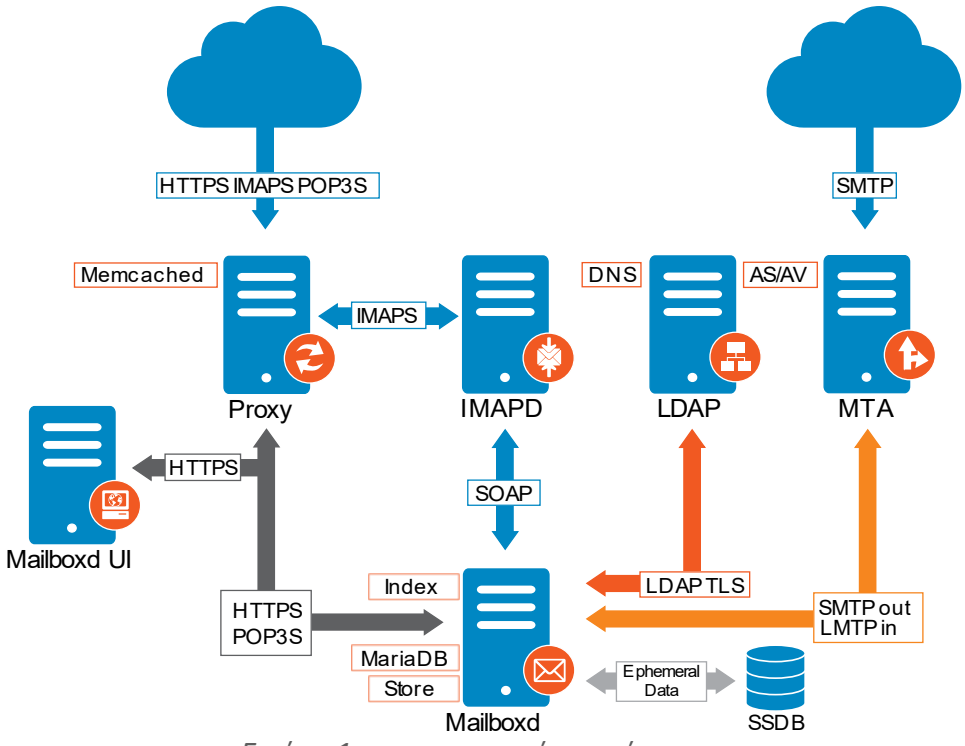
- Είναι ανοιχτού κώδικα / λογισμικού
- Παρέχει επαφές , ημερολόγιο, tasks, και chat
- Έχει μοντέρνο σχεδιασμό
- Έχει μεγάλη κοινότητα- υποστήριξη
- Έχει ήδη antispam και antivirus
- Εύκολη διαχείριση
- Εγκατάσταση σε έναν server ή σε πολλούς
- Μεγάλη υποστήριξη μέσω της κοινότητας
- Είναι ένας ολοκληρωμένος διακομιστής αλληλογραφίας

# Κεφάλαιο 2ο : Εγκατάσταση πολλαπλών server Zimbra

## 2.1 Αρχιτεκτονική Συστήματος

Για να επιτύχουμε τα καλύτερα δυνατά αποτελέσματα την ομαλή λειτουργία και την καλύτερη δυνατή απόδοση του Zimbra email client , συνιστάτε από την ίδια την εταιρία η εγκατάσταση του διακομιστή να υλοποιηθεί σε πολλούς εξυπηρετητές.

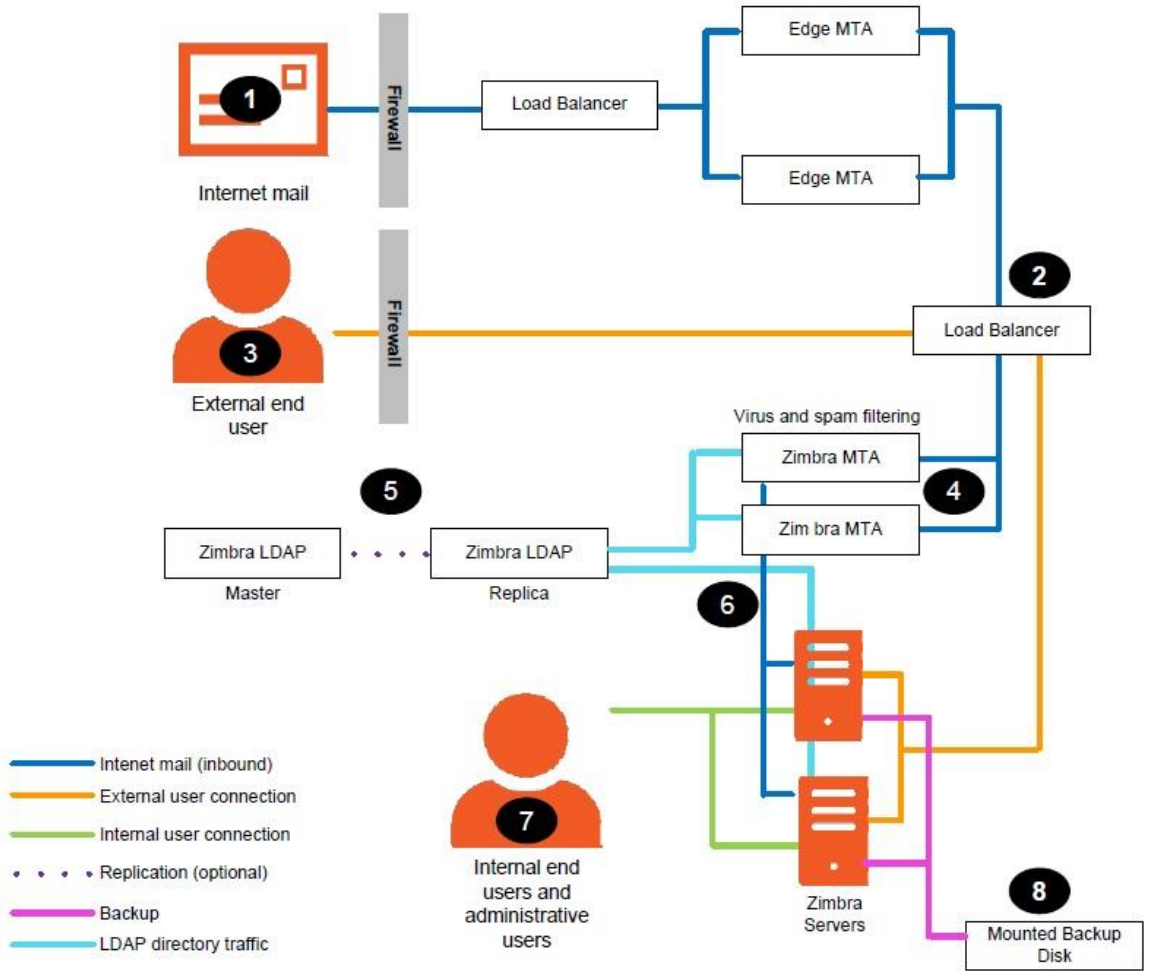
Το κατάλληλο λειτουργικό σύστημα για τους εξυπηρετητές μας είναι το centos 7 η minimal έκδοση το οποίο βασίζεται πάνω σε linux. Η εγκατάσταση του Zimbra μπορεί να υλοποιηθεί και σε άλλα λειτουργικά συστήματα βασιζόμενα σε linux εκδόσεις . Όμως centos 7 minimal απαιτεί ελάχιστους πόρους συστήματος και αυτό σε συνδυασμό με τους πόρους που απαιτεί, ο διακομιστής Zimbra το κάνει έναν ωραίο συνδυασμό ως προς την διαχείριση των πόρων του συστήματος. ("Zimbra Collaboration Multi-Server Installation Guide", 2019)




*Εικόνα 1: αρχιτεκτονική συστήματος*

Στη δική μας περίπτωση η εγκατάσταση θα γίνει σε 8 servers οι οποίοι θα είναι σε centos 7 minimal έκδοση. Ο σκοπός της εγκατάστασης σε πολλαπλούς εξυπηρετητές και όχι σε έναν είναι για να επιτύχουμε καλύτερη διαχείριση των πόρων του συστήματος, στην περίπτωση υλοποίησης της εγκατάστασης σε έναν διακομιστή απαιτεί επιπλέον πόρους, μειώνει την ασφάλεια συστήματος και το κάνει πιο ευάλωτο σε διάφορες επιθέσεις.

Οπότε η εγκατάσταση θα υλοποιηθεί με την εξής μορφή, δυο server ldap01 και ldap02 όπου ο δεύτερος θα είναι πιστό αντίγραφο του πρώτου συμβάλλοντας στην καλύτερη αποθήκευση/ των χρηστών , δυο server mta01 και mta02 οι οποίοι είναι υπεύθυνοι για την αποστολή και να λάβουν φιλτράροντας το εισερχόμενο μήνυμα, δυο εξυπηρετητές mailbox01 και mailbox02 όπου είναι οι διακομιστές αλληλογραφίας , και τέλος δύο εξυπηρετητές proxy και proxy01 οι οποίοι συμβάλλουν στο επιτύχουμε μεγάλη διαθεσιμότητα αλλά και να προστατεύσουν τους διακομιστές αλληλογραφίας . ("Zimbra Collaboration Multi-Server Installation Guide", 2019)




*Εικόνα 2: ροή μηνύματος στο σύστημα*

Στην προηγούμενη φωτογραφία φαίνεται η ροή ενός email που θα έρθει στον διακομιστή μας. Εμείς όμως τον proxy δεν θα τον εγκαταστήσουμε μέσα στον mta server αλλά ξεχωριστά . Το Zimbra όμως σου παρέχει να μπορείς να βάλλεις τον mta-proxy σε έναν server.

## 2.2 Προετοιμασία Συστήματος

Για να μπορέσουμε να υλοποιήσουμε την εγκατάσταση αγοράστηκε το domain huadit.eu. Ωστόσο η σχόλη έχει ήδη δικό της domain όνομα οπότε οι παρακάτω ρυθμίσεις θα γίνουν για το υπάρχον domain της σχολής. Επίσης πρέπει σε κάθε server να ορίσω hostname και στη συνέχεια να ρυθμίσω το /etc/hosts ωστέ να δείχνει την ip και το hostname. Στην περίπτωση μας θα έχουμε:

| DNS NAME | IP | ROLE |
|---|---|---|
| ldap01.huadit.eu | 185.190.142.65 | Master ldap |
| ldap02.huadit.eu | 194.163.145.237 | Replica ldap |
| mta01.huadit.eu | 5.182.33.217 | Mail transfer agent |
| mta02.huadit.eu | 5.182.33.219 | Mail transfer agent |
| mailbox01.huadit.eu | 185.241.151.39 | Logger / mailbox |
| mailbox02.huadit.eu | 185.230.138.207 | Mailbox server |
| proxy.huadit.eu | 173.212.253.146 | Proxy server |
| proxy1.huadit.eu | 173.249.51.17 | Proxy server |

*Πίνακας 2: Λίστα με τους εξυπηρετητές , και η ip τους*

Σε κάθε server θα ξεχωριστά τρέξουμε την εντολή

```
1. sudo hostnamectl set-hostname <hostname>
2. sudo vim /etc/hosts
```

*Απόσπασμα εντολών 1: hostname και hosts παραμετροποιήσεις.*

Για παράδειγμα :

hostnamectl set-hostname ldap01.huadit.eu για τον ldap01
και στο αρχείο /etc/hosts
<server ip> <hostname>
192.168.1.21 ldap01.huadit.eu για τον ldap01

Αφού δημιουργήσουμε σε κάθε ένα server ξεχωριστά τα hostname και προσθέσουμε στο αρχείο /etc/hosts το hostname δίπλα από την ip του κάθε ένα server θα πρέπει να δημιουργήσουμε τα dns records τους .Για να λειτουργήσει και να μπορέσει να λάβει μηνύματα ένας ηλεκτρονικός διακομιστής θα πρέπει να έχει mx records στο dns του domain του ώστε να μπορέσει να λάβει τα μηνύματα.Ο Zimbra χρειάζεται mx records μόνο για τους mta01.huadit.eu και mta02.huadit.eu και A records για όλους τους Server . Επίσης θα πρέπει να έχουμε και reverce dns records. ("List of DNS record types - Wikipedia", n.d.)

**A records :**

| | | | | |
|---|---|---|---|---|
| ldap01.huadit.eu | 14400 | A | 0 | 185.190.142.65 |
| ldap02.huadit.eu | 14400 | A | 0 | 194.163.145.237 |
| mailbox01.huadit.eu | 14400 | A | 0 | 185.241.151.39 |
| mailbox02.huadit.eu | 14400 | A | 0 | 185.230.138.207 |
| mta01.huadit.eu | 14400 | A | 0 | 5.182.33.217 |
| mta02.huadit.eu | 86400 | A | 5 | 5.182.33.219 |
| proxy.huadit.eu | 14400 | A | 0 | 173.212.253.146 |
| proxy1.huadit.eu | 14400 | A | 0 | 173.249.51.17 |

*Εικόνα 3: A εγγραφές για όλους τους εξυπηρετητές*

**Mx Records:**

| | | | | |
|---|---|---|---|---|
| huadit.eu | 14400 | MX | 0 | mta01.huadit.eu |
| huadit.eu | 86400 | MX | 5 | mta02.huadit.eu |

*Εικόνα 4: MX εγγραφές*

**Reverce dns records:**

| IP Address | PTR Record |
|---|---|
| 185.241.151.39 | mailbox01.huadit.eu |
| 173.212.253.146 | proxy.huadit.eu |
| 185.230.138.207 | mailbox02.huadit.eu |
| 194.163.145.237 | ldap02.huadit.eu |
| 5.182.33.217 | mta01.huadit.eu |
| 173.249.51.17 | proxy1.huadit.eu |
| 144.91.126.9 | ip-9-126-91-144.static.contabo.net |
| 185.190.142.65 | ldap01.huadit.eu |
| 5.182.33.219 | mta02.huadit.eu |
| 2a02:c206:2072:5285:0000:0000:0000:0001 | mailbox02.huadit.eu |
| 2a02:c206:2073:7625:0000:0000:0000:0001 | mailbox01.huadit.eu |
| 2a02:c206:2073:9748:0000:0000:0000:0001 | ldap02.huadit.eu |
| 2a02:c206:2074:3539:0000:0000:0000:0001 | mta01.huadit.eu |
| 2a02:c206:2074:3540:0000:0000:0000:0001 | mta02.huadit.eu |
| 2a02:c207:2071:5728:0000:0000:0000:0001 | ldap01.huadit.eu |
| 2a02:c207:2077:1272:0000:0000:0000:0001 | proxy.huadit.eu |
| 2a02:c207:2077:1273:0000:0000:0000:0001 | proxy1.huadit.eu |

*Εικόνα 5: Reverse dns εγγραφές*

Η 144.91.126.9 ip διεύθυνση είναι μια επιπλέον προσθήκη στατικής ip η οποία θα χρειαστεί αργότερα ώστε να επιτύχουμε το high availability.Τέλος θα πρέπει σε κάθε server ξεχωριστά να σταματήσουμε και να απενεργοποιήσουμε το postfix ώστε αργότερα να αποφύγουμε port conflicts και να εγκαταστήσουμε τα προ απαιτούμενα πακέτα που χρειάζεται ο Zimbra για να ολοκληρωθεί η εγκατάσταση. ("Zimbra Collaboration Multi-Server Installation Guide", 2019)

**Οι εντολές είναι :**

```
1. systemctl stop postfix && systemctl disable postfix
2. yum install unzip net-tools sysstat openssh-clients perl-core libaio nmap-ncat libstdc++
   wget -y
3. mkdir zimbra && cd zimbra   #
4.  wget https://files.zimbra.com/downloads/8.8.15_GA/zcs-
   8.8.15_GA_3869.RHEL7_64.20190918004220.tgz
5. tar -zxvf zcs-8.8.15_GA_3869.RHEL7_64.20190918004220.tgz
6. cd  zcs-8.8.15_GA_3869.RHEL7_64.20190918004220
7.  ./install.sh
```

*Απόσπασμα εντολών 2: Προαπαιτούμενα εγκατάστασης*

**Επεξήγηση εντολών:**

Αρχικά θα χρειαστεί να απενεργοποιήσουμε την υπηρεσία postfix σε κάθε εξυπηρετητή για να αποφύγουμε τυχόν port conflicts , πχ το Zimbra mta και το postfix χρησιμοποιούν την θύρα 25, όταν θα κάνουμε εγκατάσταση τους mta servers δεν θα μπορέσει να εκκινηθεί το Zimbra mta διότι η θύρα 25 θα χρησιμοποιείται ήδη. Το Zimbra για την εγκατάσταση του απαιτεί κάποια πακέτα να υπάρχουν στο σύστημα πριν την εκκίνηση της εγκατάστασης τους.

Εφόσον έχουμε εγκαταστήσει τα προ απαιτούμενα πακέτα του zimbra , θα δημιουργήσουμε έναν κατάλογο με όνομα Zimbra, και μέσα σε αυτόν θα κάνουμε λήψη το Zimba αρχείο συμβατό με centos 7 που στην περίπτωση μας είναι η έκδοση 8.8.15 . Θα το αποσυμπιέσουμε και στη συνέχεια μέσα στο φάκελο zimbra που δημιουργήσαμε , θα μεταβούμε στο αποσυμπιεσμένο αρχείο και θα εκτελέσουμε την εντολή εκκίνησης της εγκατάστασης. ("Try Zimbra Collaboration Open Source Edition", n.d.)

## 2.3 Εγκατάσταση Zimbra Ldap Servers

Το ldap είναι ένα πρωτόκολλο ανοιχτού τύπου το όποιο είναι υπεύθυνο για την παροχή πρόσβασης υπηρεσιών καταλόγου και αποθήκευσης . Η ανάγκη για καλύτερη διαχείριση του πρωτοκόλλου αυτού , για τη δημιουργία αντιγράφων ασφαλείας απαιτεί την εγκατάσταση δύο ldap εξυπηρετητών και ο δεύτερος θα είναι πιστό αντίγραφο του κυρίου ώστε να αποφύγουμε πιθανόν απώλειες χρηστών από επιθέσεις ή από κάποιο άλλο σφάλμα.

Αφού λοιπόν έχουμε υλοποιήσει τα προ απαιτούμενα θα μεταβούμε στο αποσυμπιεσμένο αρχείο zcs-8.8.15_GA_3869.RHEL7_64.20190918004220. Και θα ξεκινήσαμε την εγκατάσταση με την εντολή { **./install.sh }** που βρίσκεται μέσα στο αρχείο αυτό.

Όταν εκτελέσουμε την εντολή ./install.sh Θα δούμε ένα μενού επιλογών το οποίο θα μας ρωτήσει τι θέλουμε να εγκαταστήσουμε στον συγκεκριμένο server για τους δυο ldap servers

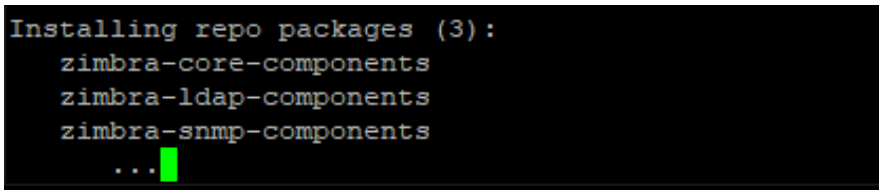
θα διαλέξουμε μονο :

| |
|---|
| Install zimbra-ldap [Y] y |
| Install zimbra-snmp [Y] y |

*Πίνακας 3: zimbra ldap πακέτα*

Ο snmp είναι λογισμικό για να κάνει καταγραφή τους server, την κατάσταση τους και είναι προαιρετικός, όμως θεωρώ ότι είναι ένα χρήσιμο εργαλείο το οποίο θα μας βοηθήσει και είναι καλό να το έχουμε στο σύστημα μας. ("Zimbra Collaboration Multi-Server Installation Guide", 2019)

**Στη συνέχεια θα δούμε αυτή την εικόνα** :




*Εικόνα 6: zimbra ldap πακέτα*

**Για τον ldap01.huadit.eu θα έχουμε τις εξής ρυθμίσεις**:

```
Main menu

   1) Common Configuration:
        +Hostname:                              ldap01.huadit.eu
        +Ldap master host:                      ldap01.huadit.eu
        +Ldap port:                             389
        +Ldap Admin password:                   set
        +Store ephemeral attributes outside Ldap: no
        +Secure interprocess communications:    yes
        +TimeZone:                              Europe/Athens
        +IP Mode:                               ipv4
        +Default SSL digest:                    sha256

   2) zimbra-ldap:                              Enabled
        +Create Domain:                         yes
        +Domain to create:                      huadit.eu
        +Ldap root password:                    set
        +Ldap replication password:             set
        +Ldap postfix password:                 set
        +Ldap amavis password:                  set
        +Ldap nginx password:                   set
        +Ldap Bes Searcher password:            set

   3) zimbra-snmp:                              Enabled
        +Enable SNMP notifications:             yes
        +SNMP Trap hostname:                    ldap01.huadit.eu
        +Enable SMTP notifications:             yes
        +SMTP Source email address:             admin@huadit.eu
        +SMTP Destination email address:        admin@huadit.eu

   c) Collapse menu
   s) Save config to file
   q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help)
```

*Εικόνα 7: Zimbra ldap01 μενού ρυθμίσεων εγκατάστασης*

Τέλος θα οριστικοποιήσουμε τις αλλαγες μας.

Εφόσον εγκαταστήσουμε τον ldap01 θα πρέπει να ενεργοποιήσουμε το Multi-Master Replication ώστε ο ldap02 να είναι πιστή αντιγραφή του ldap01 σε περίπτωση που ο ldap01 δεν είναι διαθέσιμός , είτε δεχτεί επίθεση είτε για κάποιό άλλο λόγο.

```
[root@ldap01 ~]# su - zimbra
Last login: Tue Jan 11 05:21:19 EST 2022 on pts/0
[zimbra@ldap01 ~]$ ./libexec/zmldapenable-mmr -s 1 -m ldap://ldap02.huadit.eu:389/
[zimbra@ldap01 ~]$  ./libexec/zmldapenable-mmr -r 101 -m ldap://ldap02.huadit.eu:389/
[zimbra@ldap01 ~]$ /opt/zimbra/libexec/zmldapmmrtool -q
Master Server ID: 1
Master replication agreement: 1
rid: 100 URI: ldap://ldap02.huadit.eu:389/ TLS: critical
Master replication agreement: 2
rid: 101 URI: ldap://ldap02.huadit.eu:389/ TLS: critical
[zimbra@ldap01 ~]$
```

*Εικόνα 8: Ενεργοποίηση λειτουργίας mmr*

Στη συνέχεια θα συνεχίσουμε την εγκατάσταση του ldap02.huadit.eu και θα πραγματοποιήσουμε τις παρακάτω ρυθμίσεις.

```
Main menu

   1) Common Configuration:
        +Hostname:                              ldap02.huadit.eu
        +Ldap master host:                      ldap01.huadit.eu
        +Ldap port:                             389
        +Ldap Admin password:                   set
        +Store ephemeral attributes outside Ldap: yes
        +Value for zimbraEphemeralBackendURL:  ldap://default
        +Secure interprocess communications:   yes
        +TimeZone:                              Europe/Athens
        +IP Mode:                               ipv4
        +Default SSL digest:                    sha256

   2) zimbra-ldap:                              Enabled
        +Create Domain:                         yes
        +Domain to create:                      huadit.eu
        +Ldap replication type:                 mmr
        +Ldap Server ID:                        2
        +Ldap root password:                    set
        +Ldap replication password:             set
        +Ldap postfix password:                 set
        +Ldap amavis password:                  set
        +Ldap nginx password:                   set
        +Ldap Bes Searcher password:            set

   3) zimbra-snmp:                              Enabled
        +Enable SNMP notifications:             yes
        +SNMP Trap hostname:                    ldap02.huadit.eu
        +Enable SMTP notifications:             yes
        +SMTP Source email address:             admin@ldap02.huadit.eu
        +SMTP Destination email address:        admin@ldap02.huadit.eu

   c) Collapse menu
   s) Save config to file
   q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
```

*Εικόνα 9: zimbra ldap02 μένου ρυθμίσεων εγκατάστασης*

Πρέπει αναφέρω ότι για να συγχρονιστούν οι δυο ldap χρειάζεται οι κωδικοί που δημιουργήσαμε κατά την εγκατάσταση του ldap01 να χρησιμοποιηθούν και στους υπολοίπους server οπότε κατά την εγκατάσταση του ldap02 χρειαζόμαστε αρχικά το ldap admin password και ldap replication password αλλά και τους υπολοίπους που δημιουργήσαμε. ("Zimbra Collaboration Multi-Server Installation Guide", 2019)

## 2.4 Εγκατάσταση Zimbra mta servers

Το mta ή αλλιώς mail transfer agent όπως αναφέρει και το όνομα του είναι ο “πράκτορας” που είναι υπεύθυνος για την μεταφορά του ηλεκτρονικού μηνύματος. Ο Zimbra mta διαφέρει με τους κοινούς mta διότι μας προσφέρει επιπλέον δικό του antispam, antivirus, και το πακέτο amavisd που περιέχει τον spammassasin και το clamAV. ("Zimbra Collaboration Multi-Server Installation Guide", 2019)

Είναι ένας ολοκληρωμένος μεταφορέας μηνυμάτων που με τις κατάλληλες παραμετροποιήσεις μπορεί να γίνει ένας πολύ δυνατός “πράκτορας” . Επίσης μας παρέχει τη δυνατότητα να ενεργοποιήσουμε το cbpolicyd που θα το αναλύσουμε παρακάτω και θα δείξουμε τα βήματα εγκατάστασης του.

Για την εγκατάσταση των Zimbra mta θα χρειαστούμε τα παρακάτω πακέτα τα οποία θα τα εγκαταστήσουμε και τους δύο εξυπηρετητές mta που θα έχουμε στο συστημά μας.

| |
|---|
| Install zimbra-mta [Y] y |
| Install zimbra-dnscache [Y] y |
| Install zimbra-snmp [Y] y |

*Πίνακας 4: zimbra mta πακέτα*

**Έτσι για τον mta01.huadit.eu έχουμε :**

```
1) Common Configuration
   Hostname:                                 mta01.huadit.eu
   Ldap master host:                         ldap01.huadit.eu
   Ldap port:                                389
   Ldap Admin password:                      set
   LDAP Base DN:                             cn=zimbra
   Store ephemeral attributes outside Ldap: yes
   Value for zimbraEphemeralBackendURL:     ldap://default
   Secure interprocess communications:      yes
   TimeZone:                                 Europe/Athens
   IP Mode:                                  ipv4
   Default SSL digest:                       sha256

 2) zimbra-mta
    Status:                                   Enabled
    Enable Spamassassin:                      yes
    Enable Clam AV:                           yes
    Enable OpenDKIM:                          yes
    Notification address for AV alerts:      admin@huadit.eu
    Bind password for postfix ldap user:     set
    Bind password for amavis ldap user:      set

 3)zimbra-dnscache
    Status:                                   Enabled
    Master DNS IP address(es):                8.8.4.4 1.1.1.1  8.8.8.8
    Enable DNS lookups over TCP:              yes
    Enable DNS lookups over UDP:              yes
    Only allow TCP to communicate with Master DNS: no
```

*Εικόνα 10: zimbra mta μενού ρυθμίσεων εγκατάστασης*

**Ρυθμίσεις:**

1) Common configuration
    - Hostname & ldap master host
    - Ldap admin password

2) Zimbra-mta
   Πρέπει να βάλουμε το
    - Bind password for postfix ldap user:
    - Bind password for amavis ldap user:

Τους κωδικούς που δημιουργήσαμε όταν κάναμε εγκατάσταση τον ldap01.
Και τέλος

3) DNS Cache configuration

Στο Master DNS IP address(es): βάζουμε 8.8.4.4 1.1.1.1  8.8.8.8.

Την ίδια διαδικασία θα επαναλάβουμε και για τον mta02.huadit.eu με την μόνη διαφορά ότι στο common configuration το hostname θα είναι :
mta02.huadit.eu . Όλες οι άλλες ρυθμίσεις θα είναι όπως οι ρυθμίσεις που κάναμε κατά την εγκατάσταση του mta01. ("Zimbra Collaboration Multi-Server Installation Guide", 2019)

## 2.5 Εγκατάσταση Zimbra mailbox servers

Οι Zimbra mailbox θα είναι οι εξυπηρετητές που είναι υπεύθυνοι για την είσοδο των χρηστών στην αλληλογραφία τους. Η εγκατάσταση των δύο mailbox είναι προαιρετική ωστόσο σε μεγάλα συστήματα με χιλιάδες αλληλογραφίες είναι χρήσιμη ώστε να μοιραστούν οι χιλιάδες λογαριασμοί χρηστών. Μπορούμε να εγκαταστήσουμε και επιπλέον από δύο mailbox εξυπηρετητές , οσούς δηλαδή κρίνουμε ότι είναι απαραίτητο για κάθε σύστημα. ("Zimbra Collaboration Multi-Server Installation Guide", 2019)

Ωστόσο το πακέτο logger θα πρεπει να εγκατασταθεί μόνο στον έναν από τους δυο εξυπηρετητές και στην δίκη μας περίπτωση θα τον κάνουμε εγκατάσταση στον mailbox01.huadit.eu .

**Τα πακέτα που θα κάνουμε εγκατάσταση στον mailbox01.huadit.eu ειναι:**

| Install zimbra-logger [Y] y |
|---|
| Install zimbra-snmp [Y] y |
| Install zimbra-store [Y] y |
| Install zimbra-apache [Y] y |
| Install zimbra-spell [Y] y |

*Πίνακας 5: mailbox01 πακέτα*

**Ενώ στον mailbox02 θα κάνουμε εγκατάσταση** :

| Install zimbra-snmp [Y] y |
|---|
| Install zimbra-store [Y] y |
| Install zimbra-apache [Y] y |
| Install zimbra-spell [Y] y |

*Πίνακας 6: mailbox02 πακέτα*

**Ρυθμίσεις κατά την εγκατάσταση των mailbox:**

```
Main menu

   Common Configuration:


   1) Hostname:                                mailbox01.huadit.eu
   2) Ldap master host:                        ldap01.huadit.eu
   3) Ldap port:                               389
   4) Ldap Admin password:                     set
   5) LDAP Base DN:                            cn=zimbra
   6) Store ephemeral attributes outside Ldap: yes
   7) Value for zimbraEphemeralBackendURL:     ldap://default
   8) Secure interprocess communications:      yes
   9) TimeZone:                                Europe/Athens
  10) IP Mode:                                 ipv4
  11) Default SSL digest:                      sha256
```

*Εικόνα 11: zimbra mailbox01 κοινές ρυθμίσεις εγκατάστασης*

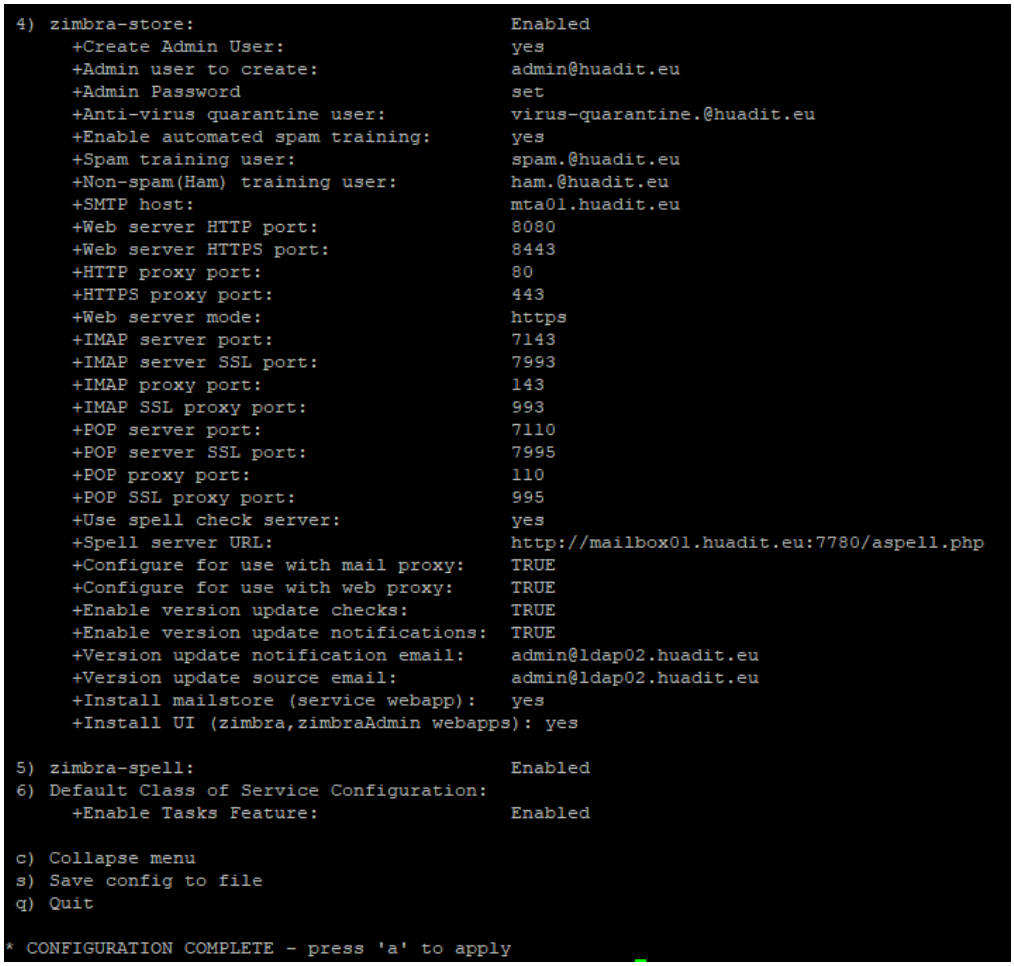
**Στο common configuration αλλάζουμε**:

- Hostname βάζουμε mailbox01.huadit.eu
- Ldap master host ldap01.huadit.eu
- Ldap admin password

**Το ίδιο θα κάνουμε και για τον mailbox02.huadit.eu όμως το hostname θα είναι mailbox02.huadit.eu**

Στη συνέχεια στο Zimbra store θα κάνουμε τις παρακάτω αλλαγές

- Θα δημιουργήσουμε το admin password
- Θα βάλουμε το smtp host : mta01.huadit.eu για mailbox01
- Θα βάλουμε το smtp host : mta02.huadit.eu για mailbox02 όταν κάνουμε την εγκατάσταση του mailbox02
- Configure for use with mail proxy: **TRUE**
- Configure for use with web proxy: **TRUE**
- Install UI (zimbra,zimbraAdmin webapps): **yes**
- Install mailstore (service webapp): **yes**




*Εικόνα 12: zimbra store ρυθμίσεις*

Έτσι για την εγκατάσταση του δευτέρου mailbox θα ακολουθήσουμε τα ιδιά βήματα χωρίς να κάνουμε εγκατάσταση το Zimbra logger.

## 2.6 Εγκατάσταση Zimbra proxy servers

Θα εγκαταστήσουμε τους proxy και proxy1 servers ώστε οι χρήστες να έχουν πρόσβαση στο ηλεκτρονικό τους ταχυδρομείο μέσω αυτών των δύο server , αυτό το κάνουμε ώστε να «κρύψουμε» ή για την ακρίβεια να προστατεύσουμε τους mailbox01 και mailbox02. Επιπλέον στους δύο αυτούς εξυπηρετητές θα υλοποιήσουμε το high availability για καλύτερη διαθεσιμότητα. ("Zimbra Collaboration Multi-Server Installation Guide", 2019)

**Τα πακέτα που θα εγκαταστήσουμε στον poxy.huadit.eu και proxy1.huadit.eu είναι τα εξής:**

| |
|---|
| Install zimbra-snmp [Y] y |
| Install zimbra-memcached [Y] y |
| Install zimbra-proxy [Y] y |

*Πίνακας 7: zimbra proxy πακέτα*

**Στην συνέχεια για την εγκατάσταση του proxy θα έχουμε τις εξής ρυθμίσεις:**

```
Main menu

   1) Common Configuration:
        +Hostname:                              proxy.huadit.eu
        +Ldap master host:                      ldap01.huadit.eu
        +Ldap port:                             389
        +Ldap Admin password:                   set
        +LDAP Base DN:                          cn=zimbra
        +Store ephemeral attributes outside Ldap: yes
        +Value for zimbraEphemeralBackendURL:  ldap://default
        +Secure interprocess communications:   yes
        +TimeZone:                              Europe/Athens
        +IP Mode:                               ipv4
        +Default SSL digest:                    sha256

   2) zimbra-snmp:                              Enabled
        +Enable SNMP notifications:             yes
        +SNMP Trap hostname:                    proxy.huadit.eu
        +Enable SMTP notifications:             yes
        +SMTP Source email address:             admin@huadit.eu
        +SMTP Destination email address:        admin@huadit.eu

   3) zimbra-proxy:                             Enabled
        +Enable POP/IMAP Proxy:                 TRUE
        +Enable strict server name enforcement? TRUE
        +IMAP server port:                      7143
        +IMAP server SSL port:                  7993
        +IMAP proxy port:                       143
        +IMAP SSL proxy port:                   993
        +POP server port:                       7110
        +POP server SSL port:                   7995
        +POP proxy port:                        110
        +POP SSL proxy port:                    995
        +Bind password for nginx ldap user:     set
        +Enable HTTP[S] Proxy:                  TRUE
        +Web server HTTP port:                  8080
        +Web server HTTPS port:                 8443
        +HTTP proxy port:                       80
        +HTTPS proxy port:                      443
        +Proxy server mode:                     redirect

   c) Collapse menu
   s) Save config to file
   q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
```

*Εικόνα 13: zimbra proxy μενού εγκατάστασης*

**Κι εδώ είναι οι ρυθμίσεις για τον proxy1 θα είναι οι εξής:**

```
Main menu

   1) Common Configuration:
        +Hostname:                              proxy1.huadit.eu
        +Ldap master host:                      ldap01.huadit.eu
        +Ldap port:                             389
        +Ldap Admin password:                   set
        +LDAP Base DN:                          cn=zimbra
        +Store ephemeral attributes outside Ldap: yes
        +Value for zimbraEphemeralBackendURL:   ldap://default
        +Secure interprocess communications:    yes
        +TimeZone:                              Europe/Athens
        +IP Mode:                               ipv4
        +Default SSL digest:                    sha256

   2) zimbra-snmp:                              Enabled
        +Enable SNMP notifications:             yes
        +SNMP Trap hostname:                    proxy1.huadit.eu
        +Enable SMTP notifications:             yes
        +SMTP Source email address:             admin@huadit.eu
        +SMTP Destination email address:        admin@huadit.eu

   3) zimbra-proxy:                             Enabled
        +Enable POP/IMAP Proxy:                 TRUE
        +Enable strict server name enforcement? TRUE
        +IMAP server port:                      7143
        +IMAP server SSL port:                  7993
        +IMAP proxy port:                       143
        +IMAP SSL proxy port:                   993
        +POP server port:                       7110
        +POP server SSL port:                   7995
        +POP proxy port:                        110
        +POP SSL proxy port:                    995
        +Bind password for nginx ldap user:     set
        +Enable HTTP[S] Proxy:                  TRUE
        +Web server HTTP port:                  8080
        +Web server HTTPS port:                 8443
        +HTTP proxy port:                       80
        +HTTPS proxy port:                      443
        +Proxy server mode:                     redirect

   c) Collapse menu
   s) Save config to file
   q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help)
```

*Εικόνα 14: zimbra proxy1 μενού εγκατάστασης*

Και στις δύο εγκαταστάσεις που κάναμε βάλαμε στο **common configuration**

- Ldap master host : ldap01.huadit.eu
- Ldap admin pass

Και στο **Zimbra-proxy** προσθέσαμε:

- Bind password for nginx ldap user
- Proxy server mode σε redirect

Τελος αφού ολοκληρώσουμε με επιτυχία και τις δυο εγκαταστάσεις χρειάζεται να ενεργοποιήσουμε το admin console proxy στο port 9071 οπότε θα εκτελέσουμε τις παρακάτω εντολές σε proxy και proxy1.

```
1. sudo su zimbra                                    #σύνδεση σαν zimbra χρήστης πλέον
2. /opt/zimbra/libexec/zmproxyconfig -e -w -C -H `zmhostname`   #ενεργοποιέι το admin
   console στη θύρα 9071
3. zmproxyctl restart                                #επαννεκίνηση proxy
4. ss -tunelp | grep 9071          #έλεγχος ένα η θύρα 9071 είναι listen
```

*Απόσπασμα εντολών 3: zimbra proxy admin console*

Ως συνέπεια πλέον να μπορούμε να συνδεθούμε στο admin control με το url:

https://proxy.huadit.eu:9071
https://proxy1.huadit.eu:9071

και στο webui μέσω του url:

https://proxy.huadit.eu
https://proxy1.huadit.eu

## 2.7 Ρύθμιση Zimbra logger υπηρεσίας και τελικές ρυθμίσεις για την λειτουργία του διακομιστή

### 2.7.1 Zimbra logger service

Ο Zimbra-logger περιέχει εργαλεία για την καταγραφή του συστήματος μας, και την αναφορά τους. Η εγκατάσταση του είναι προαιρετική εφόσον όμως πραγματοποιηθεί θα πρέπει να γίνει εγκατάσταση μόνο σε έναν mailbox server , έτσι κι αλλιώς σε πολλαπλούς Zimbra server το logger μπορεί να ενεργοποιηθεί μόνο σε έναν διακομιστή. (Koranga, 2014)

Θα πρέπει στο mailbox01 server να αλλάξουμε τα αρχεία */etc/rsyslog.conf* , /etc/sysconfig/rsyslog file *και θα εκτελέσουμε τις παρακάτω εντολές.*

```
1. sudo nano /etc/rsyslog.conf
```

*Απόσπασμα εντολών 4: mailbox01 rsyslog.conf*

*και να έχουμε ένα αρχείο όπως το παρακάτω :* (Koranga, 2014)

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

```
1. sudo nano /etc/sysconfig/rsyslog
```

*Απόσπασμα εντολών 5: rsyslog αρχείο*

και θα προσθέσουμε το εξής μέσα στο αρχείο αυτό: (Koranga, 2014)
**SYSLOGD_options=”-r -m 0”**

Εφόσον ρυθμίσουμε το rsyslog στον mailbox01 θα πρέπει να φορτωσουμε τις αλλαγές που κάναμε.

```
1. /opt/zimbra/libexec/zmfixperms -e -v
2. /opt/zimbra/libexec/zmsyslogsetup
3. sudo systemctl restart rsyslog.service
4. sudo su - zimbra
5. /opt/zimbra/libexec/zmloggerinit
6. /opt/zimbra/bin/zmupdateauthkeys
```

*Απόσπασμα εντολών 6: mailbox01 updates*

Στη συνέχεια για να δούμε εάν ο mailbox01 είναι ο logger για τους υπόλοιπους Zimbra server θα πρέπει να πάμε σε κάθε ένα server ξεχωριστά να συνδεθούμε σαν χρήστες Zimbra και να εκτελέσουμε την εντολή όπως στην παρακάτω εικόνα.

```
[zimbra@proxy1 ~]$ zmprov gacf | grep zimbraLogHostname
zimbraLogHostname: mailbox01.huadit.eu
```

*Εικόνα 15: εντολή εύρεσης zimbra logger*

Εφόσον διασταυρώσουμε ότι ο mailbox01 είναι όντως ο logger για όλους τους server μας, τότε μπορούμε να συνεχίσουμε παρακάτω αλλιώς θα χρειαστεί να διορθώσουμε τον logger οπού έχουμε πρόβλημα με την παρακάτω εντολή σαν Zimbra χρήστης .

- **zmprov mcf zimbraLogHostname <mailbox01.huadit.eu>**

Τέλος για να λειτουργήσει σωστά το σύστημά μας πρέπει να ρυθμίσουμε τον κάθε ένα Zimbra server ξεχωριστά ώστε να συνδέεται με τον logger server αλλα και να συχρονιστούν μεταξύ τους με τις παρακάτω εντολές.

```
1. sudo /opt/zimbra/libexec/zmfixperms -e -v
2. sudo su - zimbra
3. /opt/zimbra/bin/zmupdateauthkeys ; exit
4. /opt/zimbra/libexec/zmsyslogsetup
5. sudo systemctl restart rsyslog
6. sudo su - zimbra -c "zmcontrol restart"
```

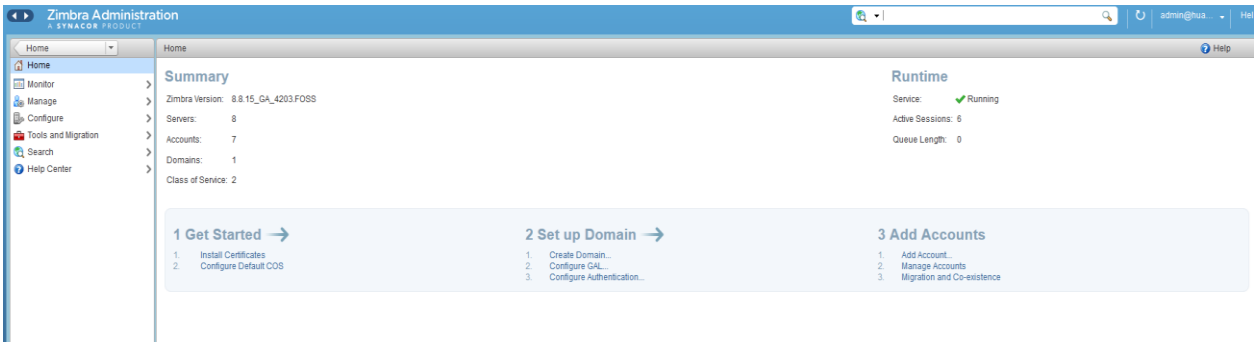
*Απόσπασμα εντολών 7: συγχρονισμός όλων των εξυπηρετητων με τον zimbra logger*

Πλέον μπορουμε να συνδεθούμε στο πίνακα ελέγχου διαχειριστή για να δούμε εάν λειτουργούν οι server μας και όλες τις άλλες υπηρεσίες που μας παρέχει.

https://proxy.huadit.eu:9071
https://proxy1.huadit.eu:9071

user : admin
password: (ο κωδικός που δημιουργήσαμε για τον admin@huadit.eu)

Η παρακάτω εικόνα είναι ενδεικτική και είναι η αρχική εικόνα από τον πίνακα ελέγχου του Zimbra το οποίο είναι διαθέσιμο από την θύρα 9071 πλέον.




*Εικόνα 16: πίνακας ελέγχου διαχειριστή zimbra*

### 2.7.2 Mta trusted networks

Στη δική μας περίπτωση που όλοι οι εξυπηρετητές μας δεν ανήκουν στο ίδιο δίκτυο θα χρειαστεί να ρυθμίσουμε το postfix, ώστε να επιτρέπει το σύστημα μας να στέλνει και να λαμβάνει εξωτερικά μηνύματα . Σε εγκαταστάσεις Zimbra με πολλούς εξυπηρετητές το postfix επιτρέπει μόνο την τοπική ανταλλαγή μηνυμάτων . Για το σκοπό αυτό θα χρειαστεί στους δυο mta server που διαθέτουμε να ενεργοποιήσουμε την αναμετάδοση αλληλογραφίας από απομακρυσμένα δίκτυα. (de la Cruz, 2014)

Οι ρυθμίσεις και για τους δύο mta θα είναι ίδιες όποτε θα πρέπει να εκτελέσουμε τις παρακάτω εντολές και στους δύο mta ξεχωριστά:

```
1. su – zimbra
2. zmprov ms mta01.huadit.eu zimbraMtaMyNetworks '127.0.0.0/8 5.182.33.0/24
   185.241.151.39 185.230.138.207 185.190.142.65 194.163.145.237 173.212.253.146
   173.249.51.17'
3. postfix reload
```

*Απόσπασμα εντολών 8: mta trusted networks*

Πλέον είμαστε έτοιμοι να στείλουμε και να λάβουμε μηνύματα από εξωτερικούς διακομιστές στο email μας. (de la Cruz, 2014)

### 2.7.3 Sender policy record

Το spf ή αλλιώς sender policy record είναι μια εγγραφή στην ζώνη του dns ενός domain , και ορίζει ποιοι εξυπηρετητές έχουν δικαίωμα να στείλουν email για το εκάστοτε domain και στη δική μας περίπτωση για το huadit.eu.

Στην ουσία όταν θα στείλουμε ένα ηλεκτρονικό μήνυμα προς τον παραλήπτη Β , τότε ο διακομιστής του Β θα ρωτήσει το dns του αποστολέα εάν η διεύθυνση ip του αποστολέα συμπίπτει με τις ip διευθύνσεις που ορίζονται στο spf record του εκάστοτε domain . Εάν συμπίπτει τότε το μήνυμα θα προωθηθεί για περεταίρω έλεγχο όπως το spamassassin εάν όμως δεν συμπίπτει τότε το μήνυμα θα απορριφθεί.

Η spf εγγραφή θα πρέπει να γίνει για τους δύο mta server που διαθέτουμε και θα είναι μια txt εγράφη. (RBDurgin, 2015)

**Spf records:**

| Recource record | ttl | type | priority | data |
|---|---|---|---|---|
| huadit.eu | 86400 | txt | 0 | v=spf1 mx -all |

*Πίνακας 8: spf record*

Με αυτή την εγγραφή δηλώνουμε ότι τα μηνύματα μας στέλνονται μόνο από τους server που έχουν μια mx εγγραφή , και εμείς έχουμε mx εγγραφή μόνο για τους mta01.huadit.eu και mta01.huadit.eu

### 2.7.4 DKIM και DMARC εγγραφές

Το dkim ή αλλιώς domain key identidfied mail είναι ένας έλεγχος ταυτότητας και χρησιμοποιεί ένα κλειδί κρυπτογράφησης ως ψηφιακή υπογραφή.

Χρειάζεται λοιπόν να δημιουργήσουμε το dkim κλειδί για το domain μας και να το προσθέσουμε στην εγγραφή dns. Το Zimbra μας παρέχει **zmdkimkeyutil** εργαλείο για τη δημιουργία του κλειδιού αυτου, το οποίο βρίσκεται μέσα στους mta εξυπηρετητές. Οπότε στον mta01 θα συνδεθούμε σαν root χρήστες και θα εκτελέσουμε την παρακάτω εντολή: (RBDurgin, 2015)

```
1. /opt/zimbra/libexec/zmdkimkeyutil -a -d huadit.eu
```

*Απόσπασμα εντολών 9: Δημιουργία κλειδιού για το domain μας*

Εφόσον εκτελέσουμε την εντολή θα δούμε στο τερματικό μας το παρακάτω κλειδί. (RBDurgin, 2015)


*Εικόνα 17: δημιουργία κλειδιού για το domain*

**Οπότε η εγγραφή μας στο dns θα είναι το περιεχόμενο :** (RBDurgin, 2015)

| Recource record | ttl | type | priority | data |
|---|---|---|---|---|
| 1ad10ec6-5f3d-11ec-8e74-222b0e039fca._domainkey.huadit.eu | 14400 | TXT | 0 | v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzBifX0LSU+tmsR158igBGZWO7p9Wwa3n5Xn1xrC4EsR9IwwPp3ctqcv2nPt+ wsFkMRLoSgQVfa9LAun60RyP7NLXQ7ElC80itGaO1xBJClyZsoC84/GGPBJUfa7XqTF4UFC83QleFh3hqHcsfXDgSnN52OGy5F7zbPV3C2L5b4KXNV2JT xJ7C1lSaddK/i9Pq12i676FMqRC3rr7+GlTNgLI2uDJULoNzq/zh/te6IZumMMCfd37oo2ORAjJ4wqo+ZUa8t4aP/xFvMWWp6cAzjzldiqRY4hqZC50gT87vtse9qu9s/JJRqiJ nCMnGb1mdfufcWSnHDYBLJEEF5fzvQIDAQAB |

*Πίνακας 9: dkim record*

**Το DMARC διασφαλίζει ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου είναι συμβατά με SPF και DKIM πριν σταλούν**. (RBDurgin, 2015)

Οπότε στο dns record θα έχουμε :

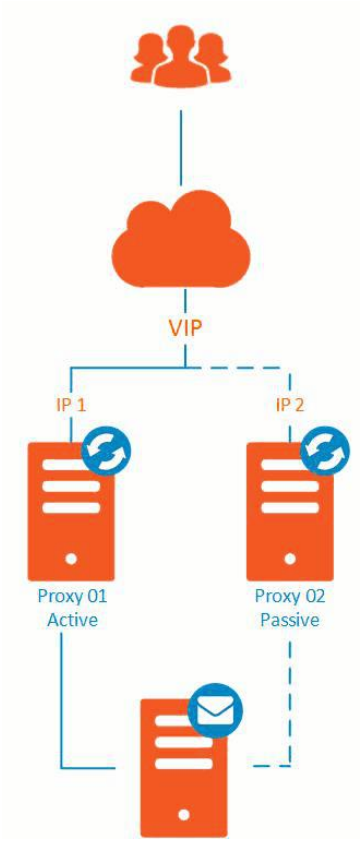
| Recource record | ttl | Type | priority | data |
|---|---|---|---|---|
| _dmarc.huadit.eu | 14400 | TXT | 0 | v=DMARC1; p=quarantine; rua=mailto:dmarc@huadit.eu; ruf=mailto:dmarc@huadit.eu; sp=quarantine |

*Πίνακας 10: dmarc record*

# Κεφάλαιο 3ο: High availability

## 3.1 High availability

Το high availability ή αλλιώς μεγάλη διαθεσιμότητα έχει ως σκοπό να προσφέρει υψηλή διαθεσιμότητα στους χρήστες μας να μπορούν να συνδεθούν , να στέλνουν μηνύματα και οτιδήποτε άλλο πραγματοποιείται μέσα από τον διακομιστή μας. Μέχρι τώρα η σύνδεση γινόταν είτε μέσω του https://proxy.huadit.eu είτε μέσω του https://proxy1.huadit.eu όμως χρειαζόμαστε ένα κοινό url για να συνδέονται οι χρήστες το οποίο θα είναι το https://mail.huadit.eu και στόχος του είναι να προσφέρει υψηλή διαθεσιμότητα, για να επιτευχθεί αυτή χρειάζεται να εγκαταστήσουμε στους δυο proxy server μας το εργαλείο keepalived , αλλα επιπλέον θα χρειαστούμε μια στατική ip και στην περίπτωση μας έχω την : **144.91.126.9/18**. Με λίγα λόγια η Ip αυτή θα είναι κοινή για τους δυο proxy και μέσω του εργαλείου keepalived θα την μοιράζονται. Το παρακάτω διάγραμμα θα μας βοηθήσει να δούμε πως λειτουργεί. (Maussion, 2015)




*Εικόνα 18: high avalabiliry*

λειτουργέι ως εξής : (Maussion, 2015)

- Ο proxy έχει την vip 144.91.126.9
- Στη συνέχεια ο proxy δεν είναι διαθέσιμος
- Έτσι η vip περνάει στον proxy1 ο οποίος είναι διαθέσιμος

Θα χρειαστούμε επιπλέον A record για την vip και θα είναι το εξής :

| Recource record | Ttl | Type | Priority | Data |
|---|---|---|---|---|
| mail.huadit.eu | 14400 | A | 0 | 144.91.126.9 |

*Πίνακας 11: A record για την failover ip*

### 3.1.1 Προσθήκη της επιπλέον ip

Στα centos η διεπαφή του δικτύου είναι στον κατάλογο /etc/sysconfig/network-scripts όπου μέσα περιέχει πολλά αρχεία , το ifcfg -eth0 είναι το βασικό αρχείο που μέσα περιέχει πληροφορίες του δικτύου. Εμείς για να προσθέσουμε την ip 144.91.126.9 πρέπει για proxy και proxy1 να δημιουργήσουμε στον κατάλογο /etc/sysconfig/network-scripts το αρχείο το ifcfg-eth0:1 . (Tobias, 2021)

| **Για τον proxy το ifcfg-eth0:1 περιέχει τα εξης:** | **Για τον proxy1 το ifcfg-eth0:1 περιέχει τα εξης:** |
|---|---|
| TYPE=Ethernet<br>PROXY_METHOD=none<br>BROWSER_ONLY=no<br>BOOTPROTO=none<br>DEFROUTE=yes<br>IPV4_FAILURE_FATAL=no<br>IPV6INIT=yes<br>IPV6_AUTOCONF=yes<br>IPV6_DEFROUTE=yes<br>IPV6_FAILURE_FATAL=no<br>IPV6_ADDR_GEN_MODE=stable-privacy<br>NAME=eth0:1<br>UUID=eb2cb6c2-e69d-4b1d-8942-54725333c161<br>ONBOOT=no<br>DEVICE=eth0:1<br>IPADDR=144.91.126.9<br>PREFIX=18<br>GATEWAY=144.91.64.1<br>DNS1=1.1.1.1 | BOOTPROTO=none<br>DEFROUTE=yes<br>DEVICE=eth0:1<br>GATEWAY=144.91.64.1<br>HWADDR=00:50:56:44:de:2e<br>IPADDR=144.91.126.9<br>PREFIX=18<br>IPADDR6=2a02:c207:2077:1273:0000:0000:0000:0001/64<br>IPV6ADDR=2a02:c207:2077:1273:0000:0000:0000:0001/64<br>IPV6INIT=yes<br>IPV6_DEFAULTGW=fe80::1<br>NETMASK=255.255.192.0<br>ONBOOT=no<br>STARTMODE=auto<br>TYPE=Ethernet<br>USERCTL=no |

*Πίνακας 12: προσθήκη της failover ip*

Τέλος θα κάνουμε επανεκκίνηση τους δύο proxy εξυπηρετητές μας.

### 3.1.2 Λήψη εργαλείου keepalived στους δυο proxy

Το keepalived είναι το εργαλείο που θα μας βοηθήσει να εκτελέσουμε το failover. Λειτουργεί ως εξής ο ένας proxy θα είναι ο master και ο άλλος θα είναι ο backup. Εάν ο ένας από τους δύο δεν είναι διαθέσιμος τότε το keepalived θα προωθήσει την virtual ip στον επόμενο proxy και έτσι το σύστημα μας θα είναι διαθέσιμο. ("Introduction — Keepalived 1.2.15 documentation", n.d.)

Σε κάθε proxy server θα εκτελέσουμε ξεχωριστά την παρακάτω εντολή σαν root χρηστης . Εφόσον ολοκληρωθεί η εγκατάσταση στον proxy.huadit.eu και proxy1.huadit.eu θα τροποποιήσουμε το αρχείο keepalived.conf .

```
1. yum -y install keepalived  #εγκατάσταση keepalived
2. nano /etc/keepalived/keepalived.conf
```

*Απόσπασμα εντολών 10: keepalived εργαλείο*

**και το αρχείο αυτό θα έχει μέσα :** (Maussion, 2015)

```
vrrp_script chk_zimbra_nginx {
  script "pidof nginx"      # ελέγχει το zimbra nginx
  interval 2                # κάθε  2 δευτερόλεπτα
}

vrrp_instance VI_1 {
  interface eth0              #η διεπαφή του
  state MASTER                #MASTER ο proxy, BACKUP ο proxy1
  virtual_router_id 51
  priority 101                  #101 στο proxy, 100 στο proxy1
  virtual_ipaddress {
   144.91.126.9/18
  }
  track_script {
    chk_zimbra_nginx
  }
}
```

*Πίνακας 13: keepalived.conf στον proxy*

**Και στο proxy1 το keepalived.conf θα έχει ως εξής:** (Maussion, 2015)

```
vrrp_script chk_zimbra_nginx {
  script "pidof nginx"                    # ελεγχει το zimbra nginx process
  interval 2                              # κάθε 2 δευτερόλεπτα

}

vrrp_instance VI_1 {
  interface eth0
  state BACKUP          #MASTER ο proxy, BACKUP ο proxy1
  virtual_router_id 51
  priority 100                #101 ο proxy, 100 ο proxy1
  virtual_ipaddress {
    144.91.126.9/18
  }
  track_script {
    chk_zimbra_nginx
  }
}
```

*Πίνακας 14: keepalived.conf στον proxy1*

Στη συνέχεια θα πρέπει να ενεργοποιήσουμε την προώθηση ipv4 και στους δύο server ώστε όταν ο ένας δεν είναι διαθέσιμος η virtual ip να εξυπηρετεί τον διαθέσιμο server μας με την παρακάτω εντολή :

```
1. echo "net.ipv4.ip_forward = 1" | sudo tee -a /etc/sysctl.conf
2. sudo systemctl enable keepalived   #ενεργοποίηση keepalived
3. sudo systemctl start keepalived      #εκκίνηση keepalived
```

*Απόσπασμα εντολών 11: λειτουργία keepalived*

Για να συμπεράνουμε ότι λειτουργεί θα κλείσουμε τον έναν proxy για να δούμε εάν το https://mail.huadit.eu είναι προσβάσιμο και η ίδια διαδικασία θα επαναληφθεί και για τον άλλον proxy server και θα δούμε πως λειτουργεί έτσι όπως θα θέλαμε.

# Κεφάλαιο 4ο: Τεχνικές ασφάλειας συστήματος

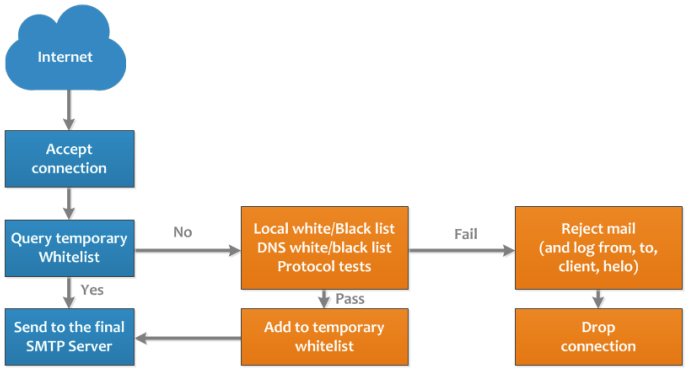
## 4.1 Τεχνικές anti-spam

Ο Zimbra διακομιστής έχει δικό του spamassassin το οποίο το έχουμε εγκαταστήσει το έχουμε εγκαταστήσει στους δύο mta υξυπηρετητές. Τα πακέτα που έχουμε εγκαταστήσει στους mta server είναι το antispam, postfix , amavisd , clamAV και antivirus. Ειδικότερα το postfix είναι υπεύθυνο για να δέχεται και να παραδίδει ηλεκτρονικά μηνύματα σε άλλους διακομιστές αλληλογραφίας. Το amavisd είναι επεξεργάζεται μηνύματα μέσω του spamassassin και του clamAV πριν επιτρέψει στο postfix να τα παραδώσει. Το spamassassin είναι ένα ισχυρό εργαλείο το οποίο εκτελεί δοκιμές σε ένα ηλεκτρονικό μήνυμα κάθε αποτέλεσμα δοκιμές επιστρέφει μια βαθμολογία καλή ή κακή στο τέλος προσθέτει τις βαθμολογίες από όλες τις δοκιμές για να λάβει την τελική βαθμολογία . Η τελική βαθμολογία που είναι πάνω από ένα συγκεκριμένο όριο έχει ως αποτέλεσμα να επισημάνει ένα email ως ανεπιθύμητο πριν το παραδώσει στο χρήστη ή την οριστική διαγραφή του ανάλογα με τις ρυθμίσεις μας. Το clamAv είναι η μηχανή προστασίας από ιούς η οποία είναι ρυθμισμένη να ενημερώνει τον εαυτό της

### 4.1.1 Αποκλεισμός με postscreen

Το Zimbra postscreen είναι ενεργοποιημένο ήδη από το Zimbra 8.7 και μέτα , και εμείς έχουμε εγκαταστήσει το Zimbra 8.8.x. Είναι μία διαδικασία που η οποία διαχειρίζεται τις εισερχόμενες συνδέσεις smtp και αποφασίζει ποιοι πελάτες μπορούν να μιλήσουν με το postfix. Διατηρεί μακριά ανεπιθύμητα μηνύματα και έτσι αφήνει περισσότερες διεργασίες διαθέσιμες στον smtp server μας και καθυστερεί την έναρξη των συνθηκών υπερφόρτωσης του διακομιστή μας. (Koranga, 2016)

Ας δούμε τη ροή της postscreen διεργασίας :




*Εικόνα 19: λειουργία postscreen αποκλεισμού*

**Τα χαρακτηριστικά του Zimbra για το postscreen έιναι**: (Koranga, 2016)

| Όνομα | Περιγραφή: τιμές | Επιλογές |
|---|---|---|
| **zimbraMtaPostscreenAccessList** | **postscreen_access_list**. Single valued, commas,separated list. | |
| **zimbraMtaPostscreenBareNewlineAction** | **postscreen_bare_newline_action** | ignore,enforce, drop |
| **zimbraMtaPostscreenBareNewlineEnable** | **postscreen_bare_newline_enable**. | yes,no |
| **zimbraMtaPostscreenBareNewlineTTL** | **postscreen_bare_newline_ttl**. | |
| **zimbraMtaPostscreenBlacklistAction** | **postscreen_blacklist_action** | ignore,enforce, drop |
| **zimbraMtaPostscreenCacheCleanupInterval** | **postscreen_cache_cleanup_interval** | |
| **zimbraMtaPostscreenCacheRetentionTime** | **postscreen_cache_retention_time** | |
| **zimbraMtaPostscreenCommandCountLimit** | **postscreen_command_count_limit** | |
| **zimbraMtaPostscreenDnsblAction** | **postscreen_dnsbl_action** | ignore,enforce, drop |
| **zimbraMtaPostscreenDnsblSites** | **postscreen_dnsbl_sites** | |
| **zimbraMtaPostscreenDnsblThreshold** | **postscreen_dnsbl_threshold** | |
| **zimbraMtaPostscreenDnsblTTL** | **postscreen_dnsbl_ttl** | |
| **zimbraMtaPostscreenDnsblWhitelistThreshold** | **postscreen_dnsbl_whitelist_threshold** | |
| **zimbraMtaPostscreenGreetAction** | **postscreen_greet_action** | ignore,enforce, drop |
| **zimbraMtaPostscreenGreetTTL** | **postscreen_greet_ttl** | |
| **zimbraMtaPostscreenNonSmtpCommandAction** | **postscreen_non_smtp_command_action** | ignore,enforce, drop |
| **zimbraMtaPostscreenNonSmtpCommandEnable** | **postscreen_non_smtp_command_enable** | yes,no |
| **zimbraMtaPostscreenNonSmtpCommandTTL** | **postscreen_non_smtp_command_ttl** | |
| **zimbraMtaPostscreenPipeliningAction** | **postscreen_pipelining_action** | ignore,enforce, drop |
| **zimbraMtaPostscreenPipeliningEnable** | **postscreen_pipelining_enable** | yes,no |
| **zimbraMtaPostscreenWatchdogTimeout** | **postscreen_watchdog_timeout** | |
| **zimbraMtaPostscreenWhitelistInterfaces** | **postscreen_whitelist_interfaces** | |
| **zimbraMtaPostscreenDnsblMinTTL** | **postscreen_dnsbl_min_ttl** | 60s |
| **zimbraMtaPostscreenDnsblMaxTTL** | **postscreen_dnsbl_max_ttl** | tbd |
| **zimbraMtaPostscreenUpstreamProxyProtocol** | **postscreen_upstream_proxy_protocol** | |

*Πίνακας 15: λίστα Zimbra postscreen*

Εφόσον είναι ήδη ενεργοποιημένο εμείς θα χρειαστεί να κάνουμε τροποποιήσεις ανάλογα με το τι είναι καλύτερο στην περίπτωση μας.

```
1. zmprov mcf zimbraMtaPostscreenDnsblSites 'b.barracudacentral.org=127.0.0.2*7'
2. zmprov mcf zimbraMtaPostscreenDnsblAction enforce
3. zmprov mcf zimbraMtaPostscreenGreetAction enforce
4. zmprov mcf zimbraMtaPostscreenNonSmtpCommandAction drop
5. zmprov mcf zimbraMtaPostscreenPipeliningAction enforce
6. zmprov mcf   zimbraMtaPostscreenDnsblTTL5m
```

*Απόσπασμα εντολών 12: Αποκλεισμός με postscreen*

### 4.1.2 Αποκλεισμός με ελέγχους πρωτοκόλλου DNS

Οι εξυπηρετητές που προσπαθούν να μας στείλουν μηνύματα θα πρέπει να συμπεριφέρονται κατάλληλα και να διαμορφώνονται σχετικά με τα αποδεκτά πρότυπα. Το Zimbra postfix μα επιτρέπει να ελέγξουμε έναν αριθμό από αυτά τα προτυπα μέσω ρυθμίσεων στην κονσόλα του διαχειριστή (Home > Configure > Global Settings > MTA) .Οι έλεγχοι αυτοί μπορούν να δημιουργήσουν ψευδώς θετικά στοιχεία. Οι δύο έλεγχοι που μπορούν να μπλοκάρουν αρκετά ανεπιθύμητα είναι οι παρακάτω: (Thomvanderboon, 2014)

- **reject_non_fqdn_sender** → Ο έλεγχος θα απορρίψει το email εάν το MAIL FROM δεν είναι μια σωστά διαμορφωμένη διεύθυνση email.

- **reject_unknown_sender_domain** → εκτελεί ορισμένους ελέγχους για να διασφαλίσει εάν το domain του αποστολέα υπάρχει όντως σε public dns , εάν δεν υπάρχει το μήνυμα δεν γίνεται αποδεκτό.

Οι παραπάνω έλεγχοι γίνονται στους mta εξυπηρετητές και για να τους ενεργοποιήσουμε θα πρέπει να συνδεθούμε στους δυο αυτους server και σαν Zimbra χρήστης να εκτελέσουμε τις παρακάτω εντολές. (Thomvanderboon, 2014)

```
1. zmprov mcf +zimbraMtaRestriction reject_non_fqdn_sender
2. zmprov mcf +zimbraMtaRestriction reject_unknown_sender_domain
```

*Απόσπασμα εντολών 13: αποκλεισμός με πρωτόκολλο ελέγχου dns*

### 4.1.3 Αποκλεισμός κακών διακοσμητών αποστολής

Εδώ χρησιμοποιούμε λίστες αποκλεισμού στο postfix και υπάρχουν δυο είδη : οι RBL λίστες αποκλεισμού IP και οι RHSBL λίστες domain. Οι δωρεάν λίστες που μπορούμε να χρησιμοποιήσουμε είναι: (Rnoti, 2014)

| RBL |
| --- |
| b.barracudacentral.org |
| psbl.surriel.com |
| zen.spamhaus.org |

*Πίνακας 16: λίστες με κακούς διακομιστές αποστολής*

Οπότε για να ενεργοποιήσουμε τις λίστες αποκλεισμού rbl θα συνδεθούμε σαν Zimbra χρήστης στους mta εξυπηρετητές και θα εκτελέσουμε τις παρακάτω εντολές : (Rnoti, 2014)

```
1. zmprov mcf +zimbraMtaRestriction "reject_rbl_client b.barracudacentral.org"
2. zmprov mcf +zimbraMtaRestriction "reject_rbl_client zen.spamhaus.org"
```

*Απόσπασμα εντολών 14: αποκλεισμός κακών διακομιστών αποστολής*

### 4.1.4 Αποκλεισμός ορισμένων συνημμένων

Από προεπιλογή, το Zimbra δεν αποκλείει επικίνδυνα συνημμένα email, όπως δέσμες ενεργειών της Visual Basic, επεξεργασίες μητρώου των Windows κ.λπ. Επομένως, πρέπει να αποκλείσουμε αυτά τα συνημμένα και να ειδοποιήσουμε τους διαχειριστές του συστήματος και τους παραλήπτες ότι το κάναμε. Το Zimbra αποκλείει επίσης τα κρυπτογραφημένα συνημμένα από προεπιλογή, αλλά είναι πλέον πιο συνηθισμένο για πολλούς χρήστες να στέλνουν μεταξύ τους αρχεία που προστατεύονται με κωδικό πρόσβασης, επομένως στο σύστημά μας το επιτρέπουμε. (Amolmistry, 2020)

Για ενεργοποίηση θα χρειαστεί να τρέξουμε τις παρακάτω εντολές σας χρήστης Zimbra στους mta εξυπηρετητές :

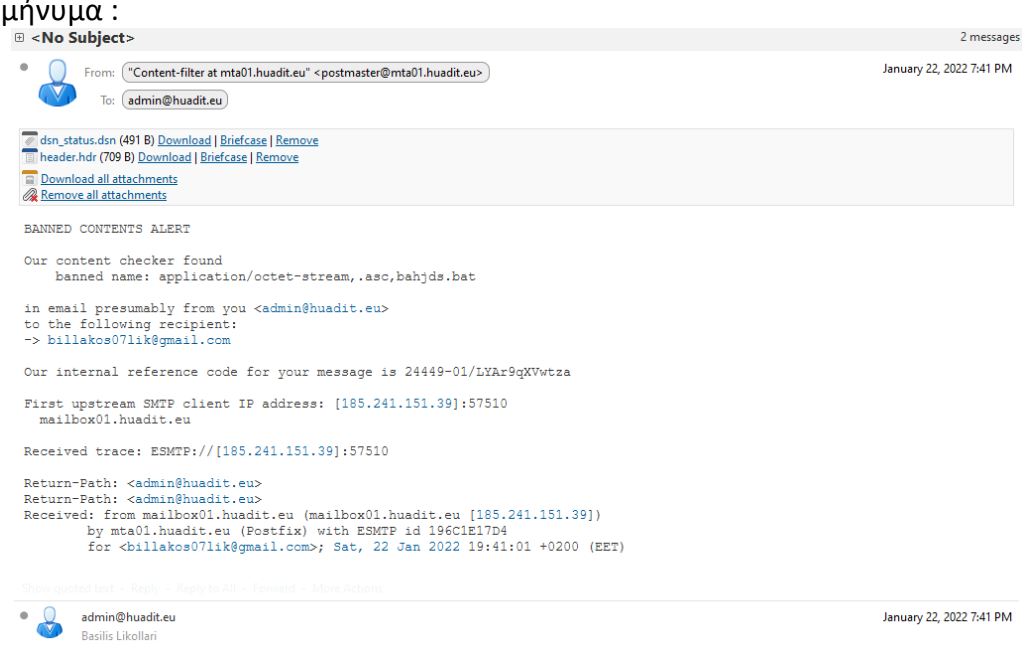
**zmprov mcf +zimbraMtaBlockedExtension {ονομα}**

1. zmprov mcf +zimbraMtaBlockedExtension vbx
2. zmprov mcf zimbraMtaBlockedExtensionWarnAdmin TRUE
3. zmprov mcf zimbraMtaBlockedExtensionWarnRecipient TRUE
4. zmprov mcf zimbraVirusBlockEncryptedArchive FALSE

*Απόσπασμα εντολών 15: αποκλεισμός συνημμενων*

Επίσης θα χρειαστεί να αποκλείσουμε και τα παρακάτω συννημένα:
**vxd,wsf,wsh,xl,asd,bat,cab,chm,cmd,com,cpl,cpgz,dll,ocx,pif,reg,scr,shb,shm,shs,vbe,do,exe,hlp,hta,html,js,jse,lnk**

Τέλος για δοκιμή προσπάθησα να στέιλω ένα αρχείο .bat σε ένα δικό μου email και λάβαμε αυτό το μήνυμα :




*Εικόνα 20: μήνυμα φίλτρου ελέγχου*

Οπότε διαπιστώνουμε ότι λειτουργεί.!

### 4.1.5 Postfix PCRE bot spam killer

Η hardware freak.com συντηρεί μια pcre λίστα με κακόβουλα εύρη ip. Η λίστα αυτή είναι δωρεάν να χρησιμοποιηθεί και απορρίπτει μεγάλα ποσά από bot , τα οποία θα στείλουν μηνύματα .Η λήψη της λίστας θα γίνει και στους δύο mta server που έχουμε . Θα συνδεθούμε σαν root χρήστης στον mta01 και mta02 και θα εκτελέσουμε : (de la Cruz, 2015)

```
1. su – Zimbra
2. cd /opt/Zimbra/conf   # ο κατάλογος με όλες τις ρυθμίσεις
3. wget
   https://raw.githubusercontent.com/stevejenkins/hardwarefreak.comfqrdns.pcre/master/fqrdns.pcre   # λήψη της λίστας
4. zmprov mcf
   +zimbraMtaRestriction'check_reverse_client_hostname_accesspcre:/opt/zimbra/conf/fqrdns.pcre'    # ενεργοποίηση της λίστας
```

*Απόσπασμα εντολών 16: pcre bot spam killer*

## 4.2 Ενεργοποίηση cbpolicyd και παραμετροποίηση

Το cbPolicyD είναι μια υπηρεσία πολιτικών για τους Zimbra MTA. Το cbpolicyd έχει σχεδιαστεί κυρίως για μεγάλα περιβάλλοντα φιλοξενίας αλληλογραφίας. Ο κύριος στόχος είναι να εφαρμοστούν όσο το δυνατόν περισσότερες επιλογές συμμόρφωσης με ανεπιθύμητα μηνύματα και email, διατηρώντας παράλληλα τη φορητότητα, τη σταθερότητα και την απόδοση που απαιτούνται για τη σημερινή κρίσιμη φιλοξενία email. (Shaikh, n.d.)

### 4.2.1 Ενεργοποίηση και εγκατάσταση cbpolicyd

Η ενεργοποίηση και εγκατάσταση θα πρέπει να γίνει σέ όσους mta εξυπηρετητές έχουμε , εμείς εχουμε δυο , το mta01.huadit.eu και mta02.huadit.eu
Συνδεδεμένοι σαν υπερχρήστες θα συνδεθούμε στους mta01 και mta02:

**Εντολές**

```
1. su - zimbra -c 'zmprov ms `zmhostname`' +zimbraservicelnstalledcbpolicyd'
2. su - zimbra -c 'zmprov ms `zmhostname`' +zimbraServiceEnabledcbpolicyd'
```

*Απόσπασμα εντολών 17: ενεργοποίηση cbpolicyd*

#με τις παραπάνω εντολές ενεργοποιούμε και εγκαθιστουμε το cbpolicyd στο Zimbra

Για να έχουμε πρόσβαση στο πίνακα ελέγχου το policyd θα χρειαστεί να εγκαταστήσουμε τα παρακάτω πακέτα

**Εντολές**

```
1. yum -y install httpd php php-sqlite php-pdo      #httpd για να εμφανιστεί ο πίνακας
2. cd /var/www/html && ln -s /opt/zimbra/common/share/webui    #webui ο καταλογος της πολιτικής μας
3. cp  -p /opt/zimbra/common/share/webui/includes/config.php /opt/zimbra/common/share/webui/includes/config.php.ori          # επειδή θα τροποποιήσουμε τον config.php θα αποθηκεύσουμε τις ρυθμίσεις του στο config.php.ori ώστε να τις έχουμε σε περίπτωση που χρειαστούμε.
4.  nano /opt/zimbra/common/share/webui/includes/config.php # θα τροποποιήσουμε το αρχείο config.php
```

*Απόσπασμα εντολών 18: εγκατάσταση httpd webui για το policy*

και Μέσα σε αυτό το αρχείο θα αλλάξουμε τις παρακάτω γραμμες
**#$DB_DSN="mysql:host=localhost;dbname=cluebringer";**
**$DB_DSN="sqlite:/opt/zimbra/data/cbpolicyd/db/cbpolicyd.sqlitedb";**

```
1. chmod 777 -R /opt/zimbra/data/cbpolicyd/db
2. cp -p /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.ori  #ομοίος με config.php
3. sed -i 's/Listen 80/Listen 8880/' /etc/httpd/conf/httpd.conf    #αλλαγή θύρας πρόσβασης πίνακα ελεγχου της πολιτικής από 80 σε 8880
4. systemctl restart httpd
```

*Απόσπασμα εντολών 19: αλλαγή θύρας webui*

Επομένως η πρόσβαση στον πίνακα ελέγχου της πολιτικής θα γίνεται:

| URL |
|---|
| **http://mta01.huadit.eu:8880/webui** |
| **http://mta02.huadit.eu:8880/webui** |

*Πίνακας 17: url για σύνδεση στο πίνακα ελέγχου των policy*

Όμως θα χρειαστεί να ορίσουμε **χρήστη** και **κωδικό** για τον διαχειριστή της πολιτικής ώστε να μην μπορεί ο καθένας να έχει πρόσβαση στο πίνακά ελέγχου της.

**Δημιουργία κωδικού**

```
1. touch /opt/zimbra/common/share/webui/.htaccess  #δημιουργία αρχείου htaccess
2. nano /opt/zimbra/common/share/webui/.htaccess  # θα βαλουμε τα παρακάτω
```

*Απόσπασμα εντολών 20: Αρχείο htaccess*

**Αρχείο htaccess**

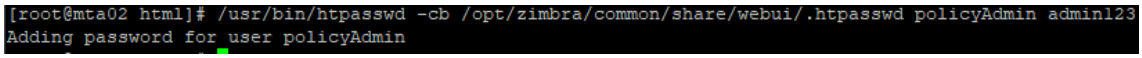
```
AuthUserFile /opt/zimbra/common/share/webui/.htpasswd
AuthGroupFile /dev/null
AuthName "User and Password"
AuthType Basic
<LIMIT GET>
require valid-user
</LIMIT>
```

*Πίνακας 18: περιεχόμενο htaccess αρχείο*

```
1. touch /opt/zimbra/common/share/webui/.htpasswd    #δημιουργία αρχείου htpasswd
2. /usr/bin/htpasswd -cb /opt/zimbra/common/share/webui/.htpasswd policyAdmin
   admin123
```

*Απόσπασμα εντολών 21: δημιουργία κωδικου και χρήστη για την είσοδο στο πίνακα ελέγχου policyd*

policyAdmin είναι ό χρήστης και admin123 ο κωδικός




*Εικόνα 21: δημιουργία κωδικού και δαχειριστή πολιτικών*

```
1. touch /etc/httpd/conf.d/cbpolicyd.conf  #δημιουργία cbpolicyd.conf
2. nano  /etc/httpd/conf.d/cbpolicyd.conf #παρακάτω προσθέσουμε μας ρυθμίσεις μας
```

*Απόσπασμα εντολών 22: δημιουργία ρυθμίσεων για cbpolicy.conf*

**Αρχέιο cbpolicy.conf**

```
Alias /webui /opt/zimbra/common/share/webui/
<Directory /opt/zimbra/common/share/webui/>
AllowOverride AuthConfig
Order Deny,Allow
Allow from all
</Directory>
```

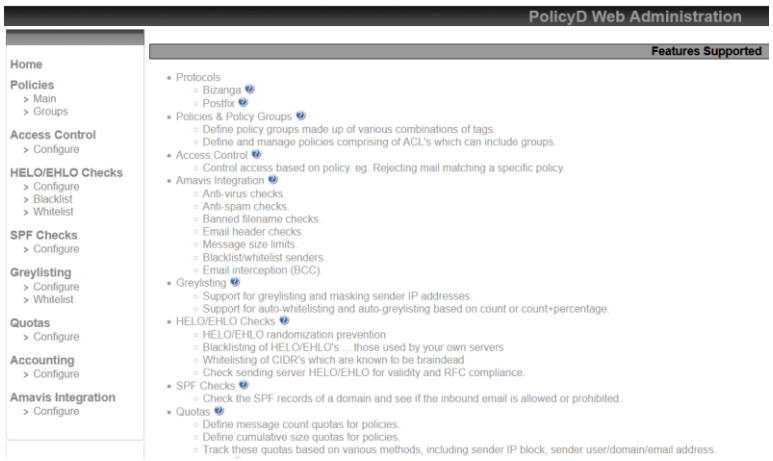
*Πίνακας 19: cbpolicy.conf αρχείο*

```
1. chmod 777 -R /opt/zimbra/data/cbpolicyd/db
2. systemctl enable httpd
3. systemctl restart httpd
```

*Απόσπασμα εντολών 23: Ενεγροποίηση httpd*

Πλέον μπορούμε να συνδεθούμε στον πίνακα ελεγχου του policyd admin με τους κωδικούς μας.

### 4.2.2 Παραμετροποίηση και εφαρμογή policyd

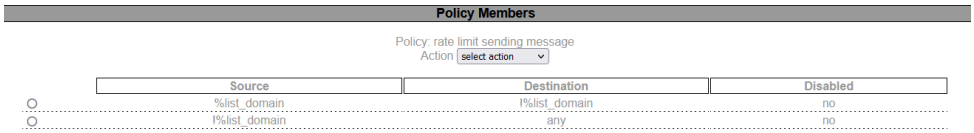



*Εικόνα 22: πίνακας ελέγχου πολιτικής*

**Δημιουργία πολιτικής**

Στο **policies>groups** θα δημιουργήσουμε το list_domain και αφού το επιλέξουμε στη συνέχεια θα βάλουμε disabled=no , στη συνέχεια θα ξαναεπιλέξουμε το list_domain στο select action θα πατήσουμε στο members και θα προσθέσουμε το @huadit.eu , και θα το ενεργοποιήσουμε αλλάζοντας το disabled από yes σε no.

Στη συνέχεια στο policies>main θα δημιουργήσουμε το rate limit sending message και θα το ενεργοποιήσουμε , στα μέλη του θα έχουμε τα παρακάτω:




*Εικόνα 23: list domain ρυθμίσεις*

*Εφόσον κάναμε τα παραπάνω βήματα θα πάμε στο quotas>configure*


*Εικόνα 24: rate limit πολιτική*

Στη συνέχεια θα προσθέσουμε πολιτική στο **policies>main** με το όνομα check-spf , και members

| Source | Destination |
|---|---|
| !%list_domain | %list_domain |

*Πίνακας 20: check-spf ρυθμίσεις members*

Τέλος στο **spf checks > configure** θα δημιουργήσουμε το spf-check
Με όνομα check-spf , link to policy check-spf και όλες τις υπόλοιπες επιλογές σε yes.
Αφού δημιουργήσουμε όλες τις πολιτικές μας για να ενεργοποιηθούν οι ρυθμίσεις θα πρέπει μέσω του τερματικού να εκτελέσουμε τις παρακάτω εντολές.

```
1. su – Zimbra
2. zmprov ms `zmhostname` zimbraCBPolicydCheckSPFEnabled TRUE
3. zmcbpolicydctl restart
```

*Απόσπασμα εντολών 24: ενεργοποίση ελέγχους για spf*

**Εφόσον τελειώσουμε την δημιουργία των policy που χρειαζόμαστε θα χρειαστεί να κλείσουμε την θύρα 8880 μέσω του firewald ώστε να έχουμε περισσότερη ασφάλεια στους Mta εξυπηρετητές μας.**

## 4.3 Τείχος προστασίας

Πριν μιλήσουμε για το τείχος προστασίας ιδιαίτερη σημασία πρέπει να μιλήσουμε για τις ssh συνδέσεις που θα έχουμε στο σύστημά μας. Η θύρα 22 χρησιμοποιείται κυρίως για τις ssh συνδέσεις και οι περισσότερες επιθέσεις γίνονται στη θύρα αυτή , με χρήστη τον root τα bot που μας επιτίθονται γνωρίζουν θύρα, χρήστη οπότε το μόνο που τους λείπει είναι ο κωδικός που θα προσπαθήσουν να τον βρουν. Για να αποφύγουμε μία τέτοια επίθεση θα χρειαστεί να :

- απενεργοποιήσουμε τις συνδέσεις root χρήστη / υπερχρήστη
- και να αλλάξουμε την θύρα του ssh από 22 σε 2020
- να κρατήσουμε τους εξυπηρετητές αναβαθμισμένους
- να απενεργοποιήσουμε θύρες που δεν χρησιμοποιούμε
- να ρυθμίσουμε το τείχος προστασίας.
- να κάνουμε προσβάσιμες τις θύρες 9071, 7071 **μόνο** από συγκεκριμένες ip διευθύνσεις όπως την ip του διαχειριστή ή μέσα από το δίκτυο της σχολής ώστε να μην είναι ευάλωτες.

Η κυκλοφορία ρέει μέσα και έξω από τους εξυπηρετητές μέσω των θυρών που καλούμε. Τα τείχη προστασίας ελέγχουν τι επιτρέπεται και τι δεν επιτρέπεται να περάσει μέσα από αυτές τις πόρτες. Μπορείτε να το σκεφτείτε σαν ένας φύλακας που στέκεται στην πόρτα και ελέγχει την ταυτότητα όλων των πληροφοριών που προσπαθούν να εισαγάγουν ή να βγουν. Για το λόγο αυτό χρειάζεται να κλείσουμε κάποιες θύρες και να αφήσουμε ανοιχτές μόνο όσες χρειάζονται και μας προτείνει και ο Zimbra. (Jhurley, 2006)

Στον παρακάτω πίνακα θα δούμε τις θύρες για εξωτερική σύνδεση στους διακομιστές μας :

| θύρα | πρωτόκολλο | Zimbra υπηρεσία | περιγραφή |
|---|---|---|---|
| 25 | smtp | mta | Εισερχόμενα μηνύματα στο postfix |
| 80 | http | mailbox / proxy | web mail client (απενεργοποιημένο μετρά 8.0) |
| 110 | pop3 | mailbox / proxy | POP3 |
| 143 | imap | mailbox / proxy | IMAP |
| 443 | https | mailbox / proxy - web mail client | HTTP over TLS |
| 465 | smtps | mta | Εισερχόμενη αλληλογραφία σε postfix μέσω TLS |
| 587 | smtp | mta | Υποβολή αλληλογραφίας μέσω TLS |
| 993 | imaps | mailbox / proxy | IMAP μέσω TLS |
| 995 | pop3s | mailbox / proxy | POP3 μέσω TLS |
| 3443 | https | proxy | Θύρα σύνδεσης πιστοποιητικού χρήστη (προαιρετικό |
| 5222 | xmpp | mailbox | Προεπιλεγμένη θύρα διακομιστή |
| 5223 | xmpp | mailbox | Προεπιλεγμένη θύρα SSL παλαιού τύπου |
| 9071 | https | proxy admin console | HTTP μέσω TLS (προαιρετικό) |

*Πίνακας 21: εξωτερικές θύρες zimbra*

### 4.3.1 Απενεργοποίηση root σύνδεσης , αλλαγή ssh θύρας

Αρχικά θα πρέπει να δημιουργήσουμε έναν χρήστη με προνόμια sudo. Το όνομά του δεν πρέπει να έχει καμία σχέση με τον server μας πχ δεν θα τον ονομάσουμε mail, client κτλ. Θα δώσουμε ένα τυχαίο όνομα πχ liki ώστε να μην είναι εύκολο να το βρούν. Η δημιουργία του χρήστη liki θα γίνει και στους 8 εξυπηρετητές που διαθέτουμε και θα είναι ο χρήστης που θα χρησιμοποιήσουμε για να συνδεθούμε στους εξυπηρετητές μας στην καινούρια θύρα 2020. Πάμε να δημιουργήσουμε το χρήστη και να του δώσουμε sudo προνόμια με τις παρακάτω εντολές.

```
1. adduser liki    #προσθήκη χρήστη με όνομα liki
2. passwd liki      # δημιουργία κωδικού πρόσβασης για τον χρήστη liki
3. usermod -aG wheel liki  #στο centos τα μέλη του wheel έχουν sudo προνομία
```

*Απόσπασμα εντολών 25: δημιουργία χρήστη liki με sudo προνόμοια*

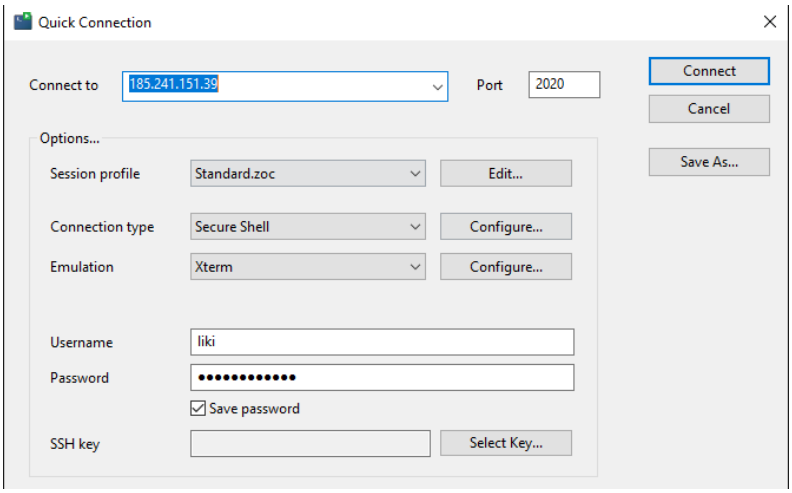
Η εικόνα της δημιουργίας του χρήστη:

```
[root@proxy1 ~]# passwd liki
Changing password for user liki.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

*Εικόνα 25: δημιουργία κωδικού για τον χρήστη liki*

Στη συνέχεια θα πάμε να απενεργοποιήσουμε τα root logins και να αλλάξουμε την θύρα ssh από 22 σε 2020 **προσοχή** πρέπει η θύρα αυτή να μην χρησιμοποιείτε .θα μεταβούμε στο αρχείο **/etc/ssh/sshd_config** και θα αλλάξουμε το PermitRootLogin από yes σε no . Τέλος θα αλλάξουμε το default port από 22 σε 2020.

Παράδειγμα σύνδεσης στο σύστημα μετά τις αλλαγές.




*Εικόνα 26: δοκιμή σύνδεσης στην θύρα 2020*

Και στη συνέχεια θα εκτελέσουμε την εντολή :
**netstat -tulpn** για να δούμε τις θύρες του εξυπηρετητή μας

```
[root@proxy1 ~]# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      1587/nginx: master
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN      1587/nginx: master
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN      1587/nginx: master
tcp        0      0 127.0.0.1:7171          0.0.0.0:*               LISTEN      1275/java
tcp        0      0 0.0.0.0:2020            0.0.0.0:*               LISTEN      24010/sshd
tcp        0      0 0.0.0.0:11211           0.0.0.0:*               LISTEN      1559/memcached
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN      1587/nginx: master
tcp        0      0 0.0.0.0:9071            0.0.0.0:*               LISTEN      1587/nginx: master
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN      1587/nginx: master
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      618/rpcbind
tcp6       0      0 :::2020                 :::*                    LISTEN      24010/sshd
tcp6       0      0 :::11211                :::*                    LISTEN      1559/memcached
tcp6       0      0 :::111                  :::*                    LISTEN      618/rpcbind
udp        0      0 127.0.0.1:323           0.0.0.0:*                           631/chronyd
udp        0      0 0.0.0.0:37364           0.0.0.0:*                           1275/java
udp        0      0 0.0.0.0:780             0.0.0.0:*                           618/rpcbind
udp        0      0 0.0.0.0:33961           0.0.0.0:*                           937/rsyslogd
udp        0      0 0.0.0.0:55734           0.0.0.0:*                           937/rsyslogd
udp        0      0 0.0.0.0:60298           0.0.0.0:*                           937/rsyslogd
udp        0      0 0.0.0.0:111             0.0.0.0:*                           618/rpcbind
udp6       0      0 ::1:323                 :::*                                631/chronyd
udp6       0      0 :::780                  :::*                                618/rpcbind
udp6       0      0 :::111                  :::*                                618/rpcbind
[root@proxy1 ~]#
```

*Εικόνα 27: έλεγχος για την αλλάγη θύρας sshd*

Και θα δούμε ότι όντως η θύρα 22 δεν λειτουργεί και πως η θύρα 2020 έχει πάρει τη θέση της.

### 4.3.2 Τείχος προστασίας FirewallD

Ο σκοπός της εγκατάστασης ενός τείχους προστασίας είναι η πρόληψη και η αντιμετώπιση επιθέσεων στο τοπικό δίκτυο. Ωστόσο, τα τείχη προστασίας μπορεί να αποδειχθούν άχρηστα εάν έχουν ρυθμιστεί εσφαλμένα. Είναι καλύτερο να διαμορφώσετε το τείχος προστασίας σας ώστε να απορρίπτει συνδέσεις εκτός από αυτές που θα επιτραπούν από εμάς (default-deny).

Το firewalld είναι ένα ανοιχτού κώδικα τείχος προστασίας που παρέχει μεγάλη προστασία από διάφορα σενάρια επίθεσης. Μπορεί να εγκατασταθεί σε πολλά λειτουργικά συστήματα όπως και στο δικό μας που είναι το centos7. (Firewall - Βικιπαίδεια, n.d.)

**Εγκατάσταση firewalld σέ όλους τους εξυπηρετητές μας:** (Firewall - Βικιπαίδεια, n.d.)

Η εγκατάσταση είναι πολύ απλή και θα χρειαστεί να εκτελέσουμε μια εντολή και στους 8 εξυπηρετητές μας, και θα την ενεργοποιήσουμε

**Εντολή**

```
1. sudo yum -y install firewalld      #εγκατάσταση firewalld
2. sudo systemctl enable firewalld    #ενεργοποίηση firewalld
```

*Απόσπασμα εντολών 26: εγκατάσταση firewalld*

Στη συνέχεια , στο πιο απαιτητικό κομμάτι θα πρέπει να θέσουμε τους κανόνες / ρυθμίσεις σε κάθε εξυπηρετητή ξεχωριστά. (Mhammett, 2007)

**Για τους ldap server θα έχουμε τις εξής ρυθμίσεις:**

| **Ldap01 και ldap02** |
|---|
| sudo firewall-cmd --add-service={http,https,smtp,smtps,imap,imaps,pop3,pop3s} --permanent |
| sudo firewall-cmd --add-port=389/tcp --permanent |
| sudo firewall-cmd --add-port=636/tcp --permanent |
| sudo firewall-cmd --reload |

*Πίνακας 22: ρυθμίσεις firewald για ldap*

**Για τους mta server θα έχουμε τις εξής ρυθμίσεις:**

| **mta01 και mta02** |
|---|
| sudo firewall-cmd --add-service={http,https,smtp,smtps,imap,imaps,pop3,pop3s} --permanent |
| sudo firewall-cmd --add-port=25/tcp --permanent |
| sudo firewall-cmd --add-port=465/tcp --permanent |
| sudo firewall-cmd --add-port=587/tcp --permanent |
| sudo firewall-cmd --reload |

*Πίνακας 23: ρυθμίσεις firewall για τους mta εξυπηρετητές*

**Για τους proxy server θα έχουμε τις εξής ρυθμίσεις:**

| **Proxy και proxy1** |
|---|
| sudo firewall-cmd --add-service={http,https,smtp,smtps,imap,imaps,pop3,pop3s} --permanent |
| sudo firewall-cmd --add-port=11211/tcp --permanent |
| sudo firewall-cmd --add-port=9071/tcp --permanent |
| sudo firewall-cmd --reload |

*Πίνακας 24: ρυθμίσεις firewall για τους proxy εξυπηρετητές*

**Για τους mailbox server θα έχουμε τις εξής ρυθμίσεις:**

| **Mailbox01 και mailbox02** |
|---|
| sudo firewall-cmd --add-service={http,https,smtp,smtps,imap,imaps,pop3,pop3s} --permanent |
| sudo firewall-cmd --add-port=7071/tcp --permanent |
| sudo firewall-cmd --add-port=7025/tcp --permanent |
| sudo firewall-cmd --add-port=7443/tcp --permanent |
| sudo firewall-cmd --reload |

*Πίνακας 25: ρυθμίσεις firewald για τους zimbra mailbox*

# Κεφάλαιο 5ο: Διαχείριση με γραμμές εντολών

Η διαχείριση με εντολές τερματικού είναι απαραίτητη σε ένα ολοκληρωμένο σύστημα διακομιστή ηλεκτρονικού ταχυδρομείου και μπορεί να υλοποιηθεί με τις εντολές που ορίζει ο Zimbra.

Όλες οι εντολές του τερματικού για την διαχείριση του Zimbra υπάρχουν στον κατάλογο **/opt/Zimbra/bin** . Παρακάτω παραθέτω μια λίστα με τις εντολές αυτές και μια σύντομη περιγραφή τους. (Zimbra CLI Commands, 2010)

| **Εντολές** | **Περιγραφή** |
|---|---|
| antispam-mysqladmin | βοηθητικό πρόγραμμα διαχείρισης διακομιστή SQL κατά των ανεπιθύμητων μηνυμάτων |
| antispam-mysql | anti-spam SQL client |
| antispam-mysql.server | Έναρξη, διακοπή του anti-spam SQL instance |
| ldap | Σταματά, ξεκινάει ή βρίσκει την κατάσταση του Zimbra LDAP |
| ldapsearch | Εκτελεί αναζήτηση σε έναν ldap server |
| logmysqladmin | Στέλνει τις mysqladmin εντολές στο logger του SQL instance |
| mysql | Εισάγει διαδραστική γραμμή εντολών για το mailbox SQL instance |
| mysql.server | Σταματά, ξεκινάει το mailbox SQL instance |
| mysqladmin | Στέλνει εντολές διαχειριστή στο mailbox SQL instance |
| postconf | Postfix εντολή για να δει ή να επεξεργαστεί τις postfix ρυθμίσεις. |
| postfix | Έναρξη, διακοπή, επαναφόρτωση, έκπλυση, έλεγχος, αναβάθμιση για τις ρυθμίσεις του postfix |
| qshape | Εξετάζει την postfix ουρά σε σχέση με την ώρα του αποστολέα/παραλήπτη |
| zmaccts | Παραθέτει τους λογαριασμούς και δίνει την κατάσταση των λογαριασμών για το domain |

| | |
|---|---|
| zmamavisdctl | Έναρξη, διακοπή, επανεκκίνηση ή εύρεση της κατάστασης του Amavis-D |
| zmantispamctl | Έναρξη, διακοπή, επανεκκίνηση ή εύρεση της κατάστασης της anti-spam υπηρεσίας. |
| zmantivirusctl | Έναρξη, διακοπή, επανεκκίνηση ή εύρεση της κατάστασης της υπηρεσίας anti-virus |
| zmantispamdbpasswd | Αλλάζει τον κωδικό της βάσης δεδομένων anti-spam SQL |
| zmapachectl | Έναρξη, διακοπή, επαναφόρτωση ή έλεγχος της κατάστασης της υπηρεσίας Apache (για έλεγχο spell) |
| zmarchiveconfig | Εντολή για προβολή, τροποποίηση ή διαμόρφωση αρχειοθέτησης |
| zmarchivectl | Έναρξη, διακοπή, επαναφόρτωση, ή έλεγχος της κατάστασης για αρχειοθέτηση |
| zmarchivesearch | Αναζήτηση αρχειοθετημένων στο λογαριασμό |
| zmauditswatchctl | Έναρξη, διακοπή, επανεκκίνηση, επαναφόρτωση, ή έλεγχός κατάσταση του auditswatch |
| zmbackup | Εκτελεί πλήρη και σταδιακά αντίγραφα ασφαλείας για έναν καθορισμένο κεντρικό υπολογιστή αλληλογραφίας. |
| zmbackupabort | Διακόπτει ένα αντίγραφο ασφαλείας που βρίσκεται σε διαδικασία. |
| zmbackupquery | Βρίσκει ένα συγκεκιμένο σύνολο πλήρους αντίγραφου ασφαλείας. |
| zmblobchk | Ελέγχει τη συνοχή του Zimbra blob store |
| zmcalchk | Ελέγξτε τη συνέπεια των ραντεβού και των συμμετεχόντων στο ημερολόγιο του Zimbra |
| zmcbpolicydctl | Σταματά, ξεκινάει και επανεκκινεί την υπηρεσία policyd, εάν είναι ενεργοποιημένη. |
| zmconfigdctl | Εκκίνηση, διακοπή, οριστική διακοπή, επανεκκίνηση της κατάστασης του mta . |
| zmcertmgr | Διαχειρίζεται αυτο-υπογεγραμμένα και εμπορικά πιστοποιητικά |
| zmclamdctl | Έναρξη, διακοπή ή εύρεση της κατάστασης του Clam AV |

| | |
|---|---|
| zmcleaniplanetics | Διαγράφει τα αρχεία ημερολογίου iPlanet ICS |
| zmcontrol | Εκκινεί , σταματάει, επανεκκινέι , ευρεσή κατάστασης από τους Zimbra servers. Επίσης μπορεί να βρει ποια έκδοση έχουμε εγκατεστημένη. |
| zmdevicesstats | Αριθμός μοναδικών αναγνωριστικών συσκευής ActiveSync ανά διακομιστή |
| zmgsautil | Βοηθητικό πρόγραμμα συγχρονισμού Global Address Book (GAL). Δημιουργία, διαγράφη του λογαριασμού συγχρονισμού GAL και εκκίνηση μη αυτόματους συγχρονισμούς. |
| zmhostname | Βρείτε το όνομα κεντρικού υπολογιστή του διακομιστή Zimbra |
| zmitemdatafile | Εξάγει και δημιουργεί tgz αρχεία {product-abbrev} χρησιομοποιούνται για REST εισαγωγή/εξαγωγή. |
| zmjava | Εκτελεί Java με ρυθμίσεις περιβάλλοντος ειδικά για το Zimbra |
| zmjavaext | Εκτελεί υθμίσεις περιβάλλοντος ειδικά για Java και Zimbra, συμπεριλαμβανομένων jar extention. |
| zmldappasswd | Αλλάζει τον κωδικό LDAP |
| zmlicense | Εμφανίζει και εκτελεί εγκατάσταση της άδειας Zimbra |
| zmlmtpinject | Εργαλείο δοκιμής |
| zmlocalconfig | Χρησιμοποιείται για τη ρύθμιση ή λήψη της τοπικής διαμόρφωσης ενός διακομιστή Zimbra |
| zmloggerctl | Έναρξη, διακοπή, επαναφόρτωση ή εύρεση της κατάστασης της Zimbra logger υπηρεσίας |

| | |
|---|---|
| zmloggerhostmap | Χρησιμοποιείται για τη μη αυτόματη αντιστοίχιση ενός ονόματος κεντρικού υπολογιστή DNS σε zmhostname. |
| zmlogswatchctl | Έναρξη, διακοπή, κατάσταση του δείγματος που παρακολουθεί την καταγραφή |
| zmmailbox | Εκτελεί εργασίες διαχείρισης γραμματοκιβωτίου |
| zmmailboxdctl | Έναρξη, διακοπή, επαναφόρτωση ή εύρεση της κατάστασης των στοιχείων του mailbox (zmmailboxd, MariaDB, convert) |
| zmmboxsearch | (Cross Mailbox Search) Αναζήτηση στα γραμματοκιβώτια για να βρείτε μηνύματα και συνημμένα |
| zmmboxmove | 7.1.3 και μετά. Χρησιμοποιείται για τη μετακίνηση επιλεγμένων γραμματοκιβωτίων από έναν διακομιστή Zimbra σε έναν άλλο. |
| zmmboxmovequery | 7.1.3 και μετά.. Χρησιμοποιείται για την αναζήτηση κινήσεων γραμματοκιβωτίου σε εξέλιξη σε έναν διακομιστή |
| zmpurgeoldmbox | 7.1.3 και μετά.. Καθαρίζει ένα γραμματοκιβώτιο από τον παλιό διακομιστή μετά από μια μετακίνηση γραμματοκιβωτίου |
| zmmemcachedctl | Εναρξη, διακοπή ,επανεκκίνηση |
| zmmetadump | Εργαλείο υποστήριξης που απορρίπτει τα μεταδεδομένα ενός στοιχείου σε μορφή αναγνώσιμη από τον άνθρωπο |

| | |
|---|---|
| zmmilterctl | Εκκινήστε, σταματήστε και επανεκκινήστε τον διακομιστή milter Zimbra εάν είναι ενεργοποιημένος |
| zmmtactl | Ξεκινήστε, σταματήστε ή βρείτε την κατάσταση του MTA |
| zmmypasswd | Αλλαγή κωδικών πρόσβασης SQL |
| zmmysqlstatus | Κατάσταση mailbox SQL instance |
| zmnginxconf | Εξαγωγή της αντίστροφης διαμόρφωσης διακομιστή μεσολάβησης |
| zmnginxctl | Ξεκινήστε, σταματήστε και επανεκκινήστε τον αντίστροφο διακομιστή μεσολάβησης Zimbra |
| zmprov | Εκτελεί όλες τις εργασίες παροχής στο Zimbra LDAP, συμπεριλαμβανομένης της δημιουργίας λογαριασμών, τομέων, λιστών διανομής και ψευδωνύμων. |
| zmproxyconfgen | Δημιουργεί διαμόρφωση για τον διακομιστή μεσολάβησης nginx |
| zmproxyctl | Έναρξη, διακοπή, επανεκκίνηση και εύρεση της κατάστασης της υπηρεσίας διακομιστή μεσολάβησης IMAP |
| zmproxypurge | Εκκαθαρίζει τις πληροφορίες δρομολόγησης POP/IMAP από έναν ή περισσότερους διακομιστές memcached |
| zmpython | Δυνατότητα εγγραφής σεναρίων Python που έχουν πρόσβαση σε βιβλιοθήκες Java Zimbra. Ορίζει τη διαδρομή κλάσης Zimbra και ξεκινά τον διερμηνέα Jython. |
| zmredodump | Εργαλείο υποστήριξης για την απόρριψη περιεχομένου ενός αρχείου redolog για σκοπούς εντοπισμού σφαλμάτων |

| | |
|---|---|
| zmrestore | Εκτελεί πλήρεις επαναφορές και σταδιακές επαναφορές για καθορισμένο κεντρικό υπολογιστή αλληλογραφία |
| zmrestoreldap | Επαναφορά λογαριασμών από το αντίγραφο ασφαλείας LDAP |
| zmrestoreoffline | (Επαναφορά εκτός σύνδεσης) Εκτελεί πλήρη επαναφορά όταν ο διακομιστής Zimbra (δηλ. η διαδικασία γραμματοκιβωτίου) είναι εκτός λειτουργίας |
| zmsaslauthdctl | Έναρξη, διακοπή ή εύρεση της κατάστασης του saslauthd (έλεγχος ταυτότητας) |
| zmschedulebackup | Προγραμματίστε αντίγραφα ασφαλείας και προσθέστε την εντολή στον πίνακα cron |
| zmskindeploy | Αναπτυξή skins |
| zmsoap | τυπώστε πληροφορίες αλληλογραφίας, λογαριασμού και διαχειριστή σε μορφή SOAP |
| zmspellctl | Ξεκινήστε, σταματήστε ή βρείτε την κατάσταση του διακομιστή ορθογραφικού ελέγχου |
| zmsshkeygen | δημιουργία κλειδιώνκρυπτογράφησης SSH Zimbra |
| zmstat-chart | Δημιουργήστε γραφήματα από δεδομένα zmstat που συλλέγονται σε έναν κατάλογο |
| zmstat-chart-config | Εξάγει μια διαμόρφωση XML που περιγράφει την τρέχουσα κατάσταση των δεδομένων που συλλέγονται από το zmstat-chart για τη δημιουργία γραφημάτων στην Κονσόλα διαχείρισης. |
| zmstatctl | Έναρξη, διακοπή, έλεγχος κατάστασης ή περιστροφή αρχείων καταγραφής των συλλεκτών δεδομένων zmstat |
| zmstorectl | Ξεκινήστε, σταματήστε ή βρείτε την κατάσταση των υπηρεσιών Zimbra store |
| zmswatchctl | Ξεκινήστε, σταματήστε ή βρείτε την κατάσταση της διαδικασίας Swatch, η οποία χρησιμοποιείται στην παρακολούθηση. |

| | |
|---|---|
| zmtlsctl | Ρυθμίστε τη λειτουργία διακομιστή Web στις επιλογές πρωτοκόλλου επικοινωνίας: HTTP, HTTPS ή μικτή |
| zmtrainsa | Χρησιμοποιείται για την εκπαίδευση του φίλτρου anti-spam ώστε να αναγνωρίζει τι είναι spam ή ham |
| zmtzupdate | Παρέχει μηχανισμό για την επεξεργασία αλλαγών ζώνης ώρας |
| zmupdateauthkeys | Χρησιμοποιείται για την ανάκτηση των κλειδιών κρυπτογράφησης ssh που δημιουργούνται από το zmsshkeygen |
| zmvolume | Διαχειριστείτε τους όγκους αποθήκευσης στον διακομιστή γραμματοκιβωτίου Zimbra |
| zmzimletctl | Αναπτύξτε και διαμορφώστε τα Zimlets |

*Πίνακας 26: οι διαθέσιμες zimbra εντολές*

## 5.1 Εντολές Διαχείρισης Λογαριασμών

Η εντολή zmprov εκτελεί όλες τις εργασίες παροχής στο Zimbra LDAP, συμπεριλαμβανομένης της δημιουργίας λογαριασμών, τομέων, λιστών διανομής και ψευδωνύμων. (De Graaff, 2017)

Η εντολή zprov Θα έχει την εξής μορφή:

**zmprov εντολη σύνταξη**

παράδειγμά για την δημιουργία του χρήστη user1 θα εκτελέσω την παρακατώ εντολή.

```
1. zmprov ca user1@huadit.eu {passwd} displayName user1 # δημιουργία χρήστη user1
2. zmprov da user1@huadit.eu                            # διαγραφή χρήστη user1
```

*Απόσπασμα εντολών 27:Παράδειγμα εντολών διαχείρισης χρηστών*

Στο πεδίο **{passwd}** θα ορίσουμε τον κωδικό για τον χρήστη user1.

Παραθέτω παρακάτω όλες τις διαθέσιμες εντολές για την διαχείριση των λογαριασμών. (De Graaff, 2017)

| Εντολή | Σύνταξη | παραδείγματα |
|---|---|---|
| addAccountAlias (aaa) | {name@domain \| id \| adminName} {alias@domain} | zmprov aaa user@domain.com user.user@alias.domain.com |
| checkPasswordStrength (cps) | {name@doman \| id} {password} | zmprov cps user@domain.com test123 |
| createAccount (ca) | {name@domain} {password} [attr1 value1]… | zmprov ca user@domain.com test123 displayName user |
| createDataSource (cds) | {name@domain} {ds-type} {ds-name} zimbraDataSourceEnabled {TRUE \| FALSE} zimbraDataSourceFolderId {folder-id} [attr1 value1 [attr2 value2]…] | |
| createIdentity (cid) | {name@domain} {identity-name} [attr1 value1 [attr2 value2]…] | |
| createSignature (csig) | {name@domain} {signature-name} [attr1 value1 [attr2 value2]…] | |
| deleteAccount (da) | {name@domain \| id \| adminName} | zmprov da user@domain.com |

| | | |
|---|---|---|
| deleteDataSource (dds) | {name@domain \| id} {ds-name \| ds-id} | |
| deleteIdentity (did) | {name@domain \| id} {identity-name} | |
| deleteSignature (dsig) | {name@domain \| id} {signature-name} | |
| getAccount (ga) | {name@domain \| id \| adminName} | zmprov ga user@domain.com |
| getAccountMembership (gam) | {name@domain \| id} | |
| getAllAccounts (gaa) | [-v] [domain] | Πρέπει να περίεχει την παράμετρο -l/--ldap<br><br>zmprov -l gaa<br><br>zmprov -l gaa -v domain.com |
| getAllAdminAccounts (gaaa) | | zmprov gaaa |
| getDataSources (gds) | {name@domain \| id} [arg1 [arg2]…] | |
| getIdentities (gid) | {name@domain \| id} [arg1 [arg2]…] | |
| getSignatures (gsig) | {name@domain \| id} [arg1 [arg2]…] | |
| modifyAccount (ma) | {name@domain \| id \| adminName} [attr1 value1]… | zmprov ma user@domain.com zimbraAccountStatus maintenance |
| modifyDataSource (mds) | {name@domain \| id} {ds-name \| ds-id} [attr1 value1 [attr2 value2]…] | |
| modifyIdentity (mid) | {name@domain \| id} {identity-name} [attr1 value1 [attr2 value 2]…] | |
| modifySignature (msig) | {name@domain \| id} {signature-name \| signature-id} [attr1 value1 [attr2 value2]…] | |
| removeAccountAlias (raa) | {name@domain \| id \| adminName} {alias@domain} | zmprov raa user@domain.com user.user@alias.domain.com |
| renameAccount (ra) | {name@domain \| id} {newname@domain} | zmprov ra user@domain.com newUser@domain.com<br>αφού μετανομάσουμε έναν λογαριασμό μετά πρέπει να πάρουμε ένα αντίγραφο ασφαλείας για αυτόν τον λογαριασμό |

| | | |
|---|---|---|
| | | zmbackup -f -s <servername.com> -a <newaccountname@servername.com> |
| setAccountCOS (sac) | {name@domain \| id \| adminName} {cos-name \| cos-id} | zmprov sac tech@domain.com FieldTechnician |
| setPassword (sp) | {name@domain \| id \| adminName} {password} | zmprov sp tech@domain.com test321 |

*Πίνακας 27: εντολές διαχείρησης λογαριασμών*

## 5.2 Εντολές διαχείρισης server

Σε περίπτωση που αλλάξουμε εξυπηρετητή ή προσθέσουμε νέο εξυπηρετητή ή οτιδήποτε αλλαγή χρειαστεί να κάνουμε σε επίπεδο server θα χρειαστούμε τις παρακάτω εντολές. (De Graaff, 2017)

Η σύνταξη των εντολών είναι απλή και είναι της εξής μορφής:

- **zmprov εντολή συντάξη**

| Εντολή | Σύνταξη | παράδειγμα |
|---|---|---|
| createServer (cs) | {name} [attr1 value1]… | |
| deleteServer (ds) | {name \| id} | zmprov ds domain.com |
| getServer (gs) | {name \| id} | zmprov gs domain.com |
| getAllServers (gas) | [-v] | zmprov gas |
| modifyServer (ms) | {name \| id} [attr1 value1]… | zmprov ms domain.com zimbraVirusDefinitionsUpdateFrequency 2h |
| getAllMtaAuthURLs (gamau) | | Χρησιμοποιείται για τη δημοσίευση στο saslauthd.conf ποιοι διακομιστές πρέπει να χρησιμοποιούνται για το saslauthd.conf MTA auth |
| getAllMemcachedServers (gamcs) | | Χρησιμοποιείται για τη λίστα διακομιστών memcached (για χρήση nginix). |

*Πίνακας 28: εντολές διαχείρησης διακομιστών zimbra*

## 5.3 Mailbox εντολές

Σε επίπεδο αλληλογραφίας οι εντολές είναι της μορφής

- zmprov εντολή

παραθέτω μερικά παραδείγματα. (De Graaff, 2017)

| Εντολή | Σύνταξη | Παραδείγματα |
|---|---|---|
| getMailboxInfo (gmi) | {account} | |
| getQuotaUsage (gqu) | {server} | |
| recalculateMailboxCounts (rmc) | {name@domain \| id} | Όταν ο αριθμός των μη αναγνωσμένων μηνυμάτων και η χρήση του ορίου δεν συγχρονίζονται με τα δεδομένα στο γραμματοκιβώτιο, χρησιμοποιήστε αυτήν την εντολή για να υπολογίσετε ξανά αμέσως τη χρήση του ορίου του γραμματοκιβωτίου και τον αριθμό των μη αναγνωσμένων μηνυμάτων. Σημαντικό Ο επανυπολογισμός της χρήσης του ορίου γραμματοκιβωτίου και του αριθμού μηνυμάτων θα πρέπει να προγραμματίζεται για να εκτελείται σε ώρες εκτός αιχμής και να χρησιμοποιείται σε ένα γραμματοκιβώτιο κάθε φορά. |
| reIndexMailbox (rim) | {name@domain \| id} {start \| status \| cancel} [type \| id]… | |
| compactIndexMailbox (cim) | {name@domain \| id} {start \| status} | |
| verifyIndex (vi) | {name@domain \| id} | |
| getIndexStats (gis) | {name@domain \| id} | |
| selectMailbox (sm) | {account-name} [{zmmailbox commands}] | |
| unlockMailbox (ulm) | {name@domain \| id} [hostname] | Καθορίστε την παράμετρο ονόματος κεντρικού υπολογιστή μόνο όταν ξεκλειδώνετε ένα γραμματοκιβώτιο μετά από μια αποτυχημένη προσπάθεια μετακίνησης. |

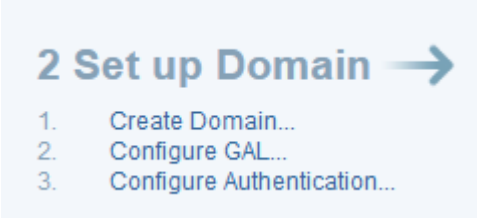
*Πίνακας 29 : εντολές διαχείρησης αλληλογραφίας*

# Κεφάλαιο 6ο: Σύνδεση με τον ήδη υπάρχον κατάλογο χρηστών και μετάβαση από άλλους διακομιστές

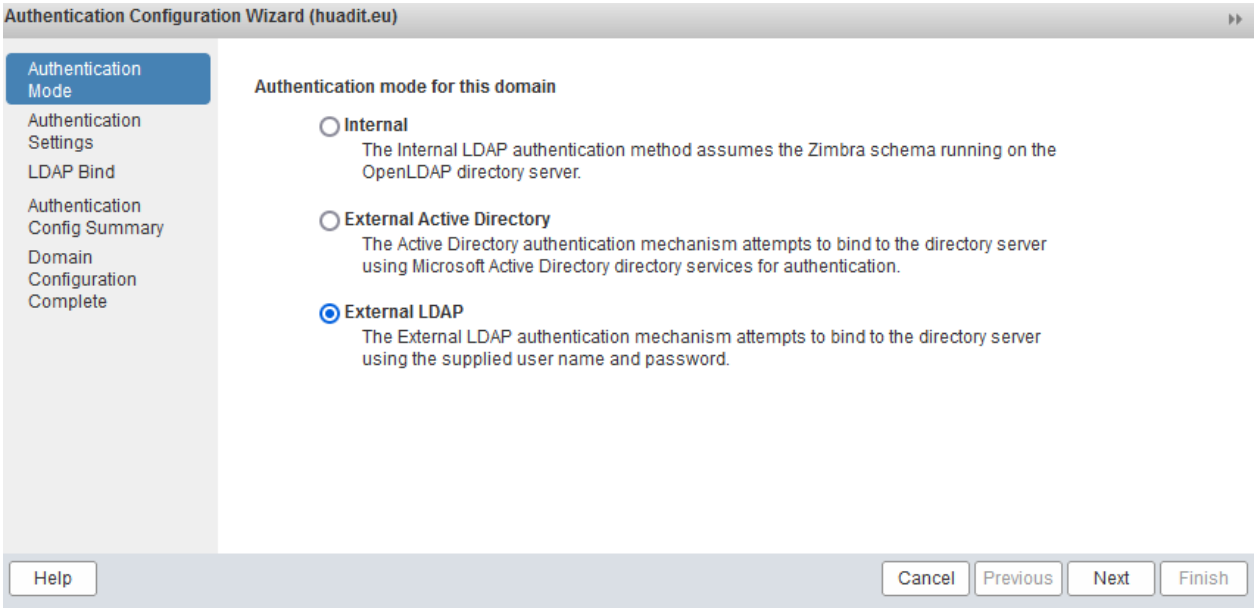
## 6.1 Διασύνδεση με τον κατάλογο χρηστών της σχολής

Η διασύνδεση με τον κατάλογο χρηστών της σχολής είναι εφικτή, και μπορεί να επιτευχθεί μέσα από τον πίνακα ελέγχου του διαχειριστή. Στον πίνακα ελέγχου στην αρχική σελίδα στην ενότητα set up domain, έχει την επιλογή configure authentication. Η δοκιμή έγινε στον κατάλογο ssaml2.hua.gr στη θύρα 389 , με uid=%u,ou=People.dc=hua.dc=gr. Ο Έλεγχος εάν όντως λειτουργεί έγινε με το δικό μου όνομα χρήστη , και κωδικο.

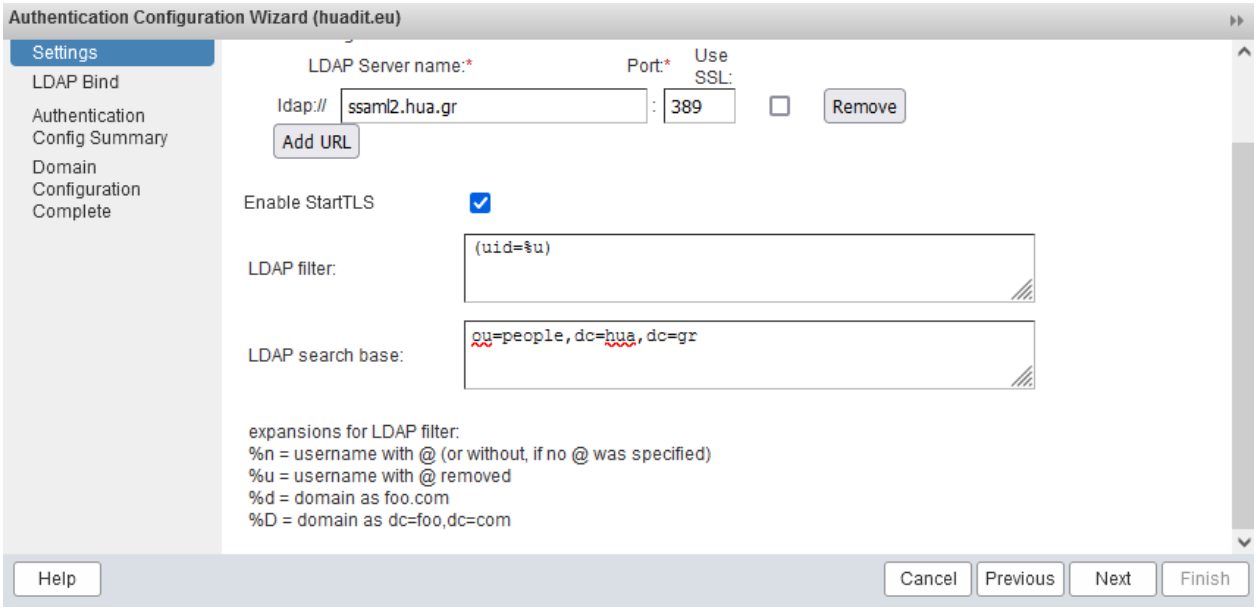
Στις παρακάτω εικόνες θα δείξω τα βήματα ελέγχου της σύνδεσης.



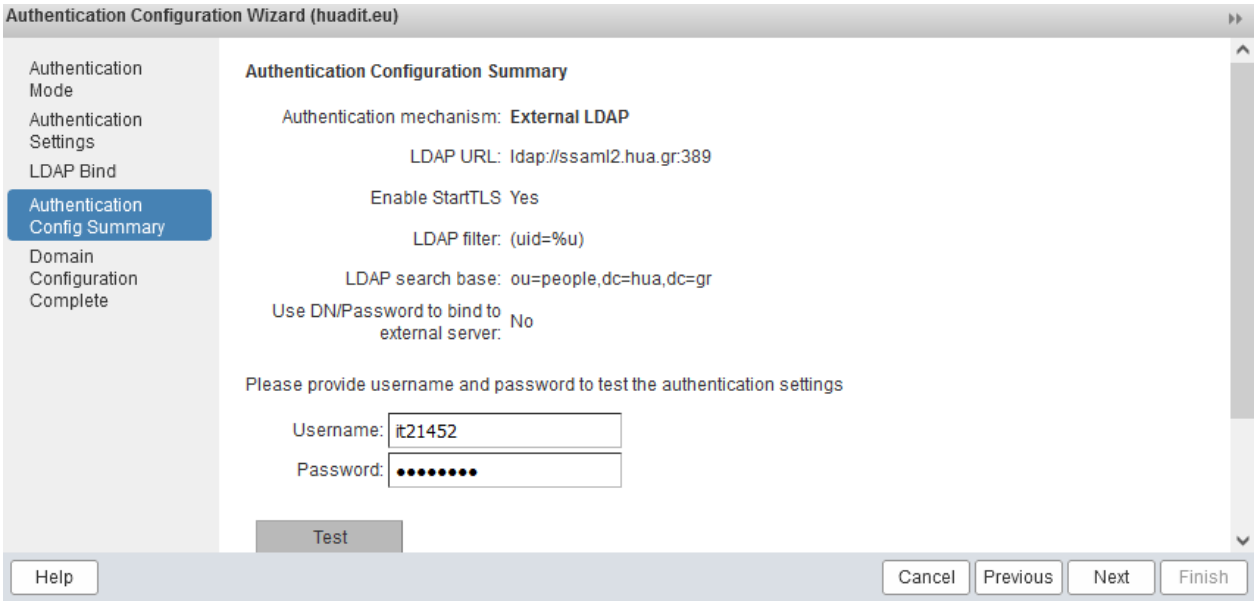

*Εικόνα 28: βημα 1 για την σύνδεση*



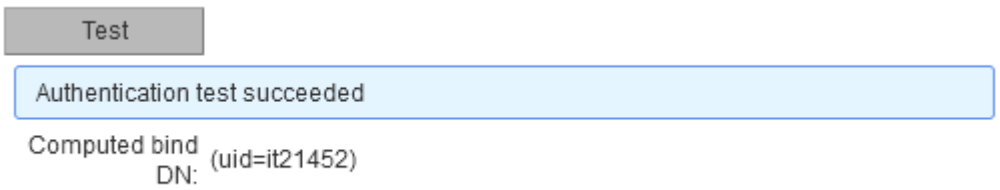

*Εικόνα 29: βήμα 2 για τη σύνδεση*




*Εικόνα 30: βημα 3 για την σύνδεση*




*Εικόνα 31: βήμα 4 για την σύνδεση*



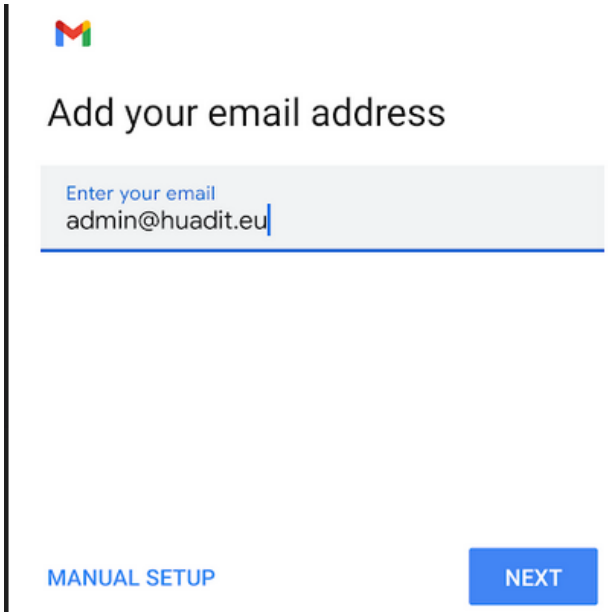

*Εικόνα 32: επιτυχής σύνδεση στον κατάλογο*

## 6.2 Μετάβαση από άλλους διακομιστές στο mailbox μας

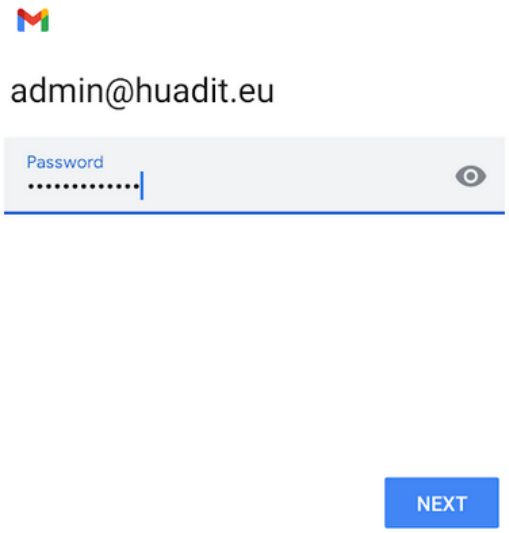
Σημαντική είναι η ανάγκη για να μπορέσουμε να συνδεθούμε στη αλληλογραφία μας και από άλλους διακομιστές όπως gmail , ή outlook. Παρακάτω θα δείξουμε πώς μπορούμε να συνδεθούμε από το κινητό μας μέσω του gmail στην αλληλογραφία μας. Στην προσθήκη λογαριασμού στο gmail θα επιλέξουμε το personal(IMAP).

| **Ρυθμίσεις** | **όνομα** |
|---|---|
| Incoming mail server | mail.huadit.eu |
| Outgoing mail server | smtp.huadit.eu |

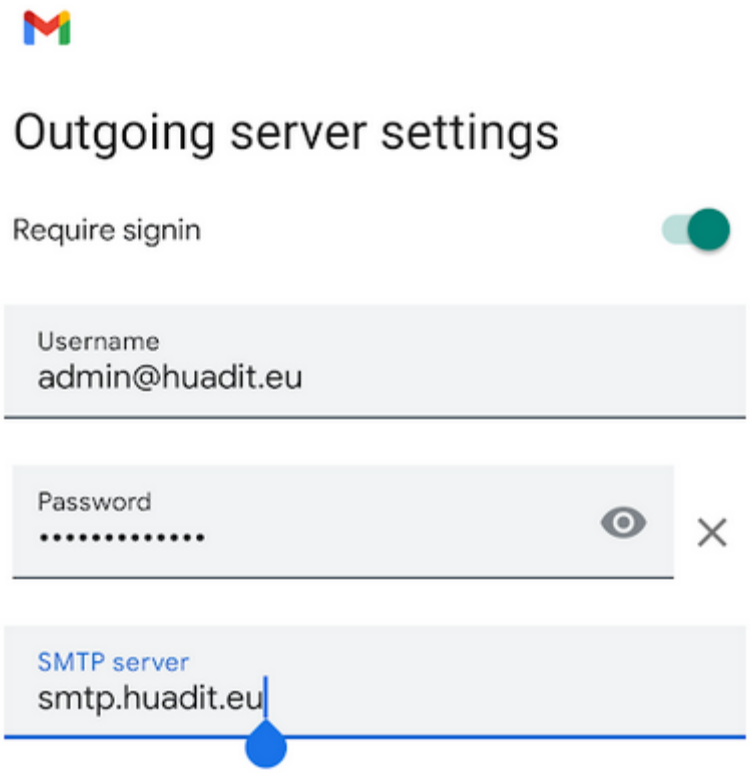
*Πίνακας 30: Ρυθμίσεις σύνδεσης gmail/outlook*



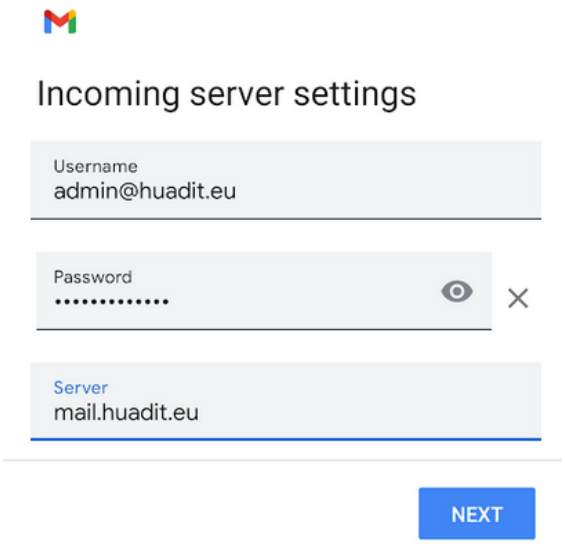

*Εικόνα 33: μετάβαση στο gmail*



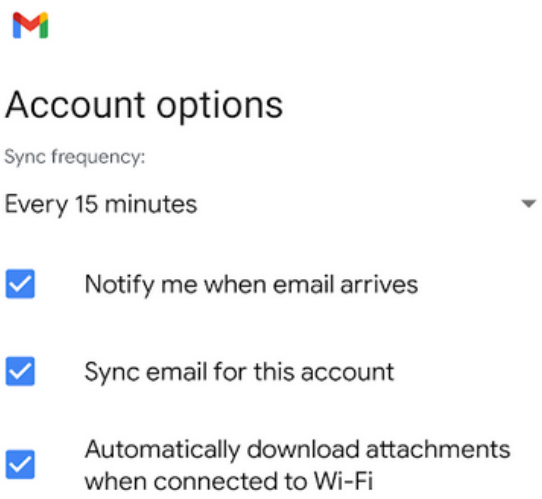

*Εικόνα 34: κωδικός χρήστη*




*Εικόνα 35: εισαγωγή smtp εξυπηρετητή*



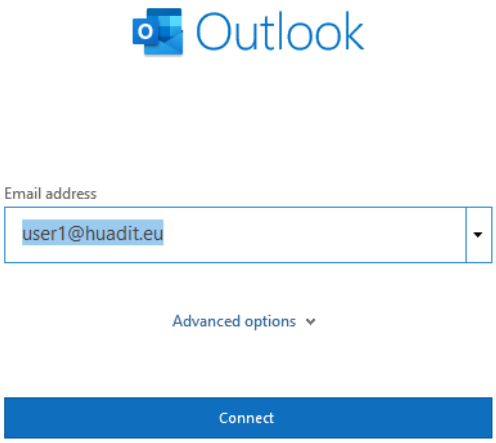

*Εικόνα 36: εισαγωγή εξυπηρετητή εισερχομένων*



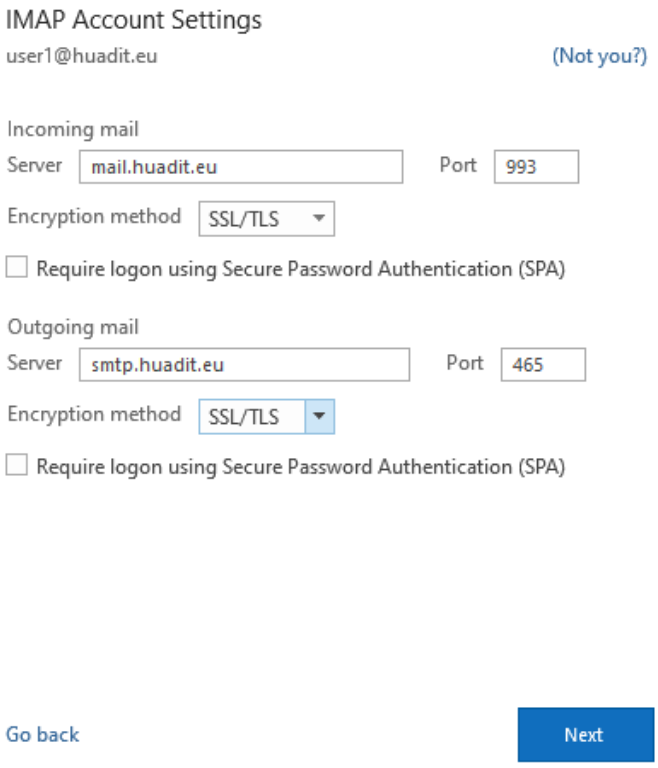

*Εικόνα 37: τελικές ρυθμίσεις*

**Πλέον μπορούμε να στείλουμε και να λάβουμε τα mail μας μέσω του gmail.**

Για σύνδεση στο **outlook** θα πατήσουμε προσθήκη λογαριασμού και στη συνέχεια θα ανοίξει το παράθυρο διαλόγου για να δώσουμε τις τελικές ρυθμίσεις.Στο email address: θα βάλουμε το mail που θέλουμε να συνδεθούμε, και πατάμε connect.

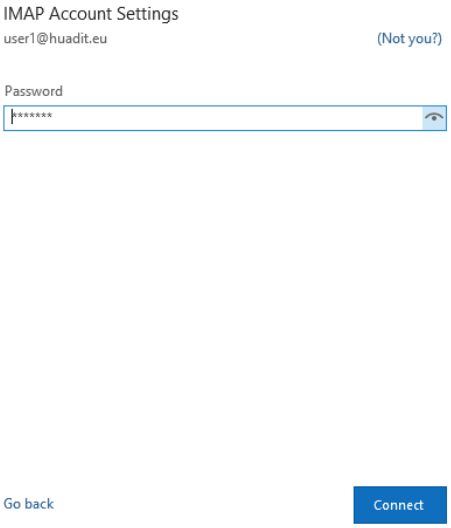



*Εικόνα 38: email σύνδεσης*



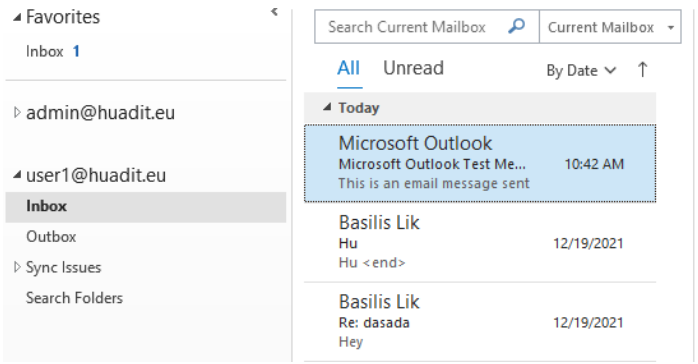

*Εικόνα 39: imap ρυθμίσεις*

Αφού δώσουμε τα παραπάνω στοιχεία σύνδεσης , με θύρες 993 για το mail και 465 για το smtp, και μέθοδος encryption sll/tls θα πατήσουμε το next.



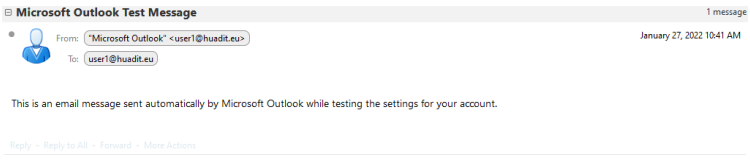

*Εικόνα 40: κωδικός χρήστη*

Και αφού δώσουμε το σωστό κωδικό χρήστη είμαστε πλέον έτοιμοι να συνδεθούμε στην αλληλογραφία μας.




*Εικόνα 41: Η αλληλογραφία μας*

Εφόσον συνδεθούμε με επιτυχία η Microsoft θα στείλει ένα μήνυμα δοκιμής στο λογαριασμό μας για να μας ενημερώσει ότι δοκιμάζει τη σύνδεση .




*Εικόνα 42: μήνυμα δοκιμής σύνδεσης*

**Πλέον λαμβάνουμε και στέλνουμε τα μηνύματα μας μέσω του outlook.**

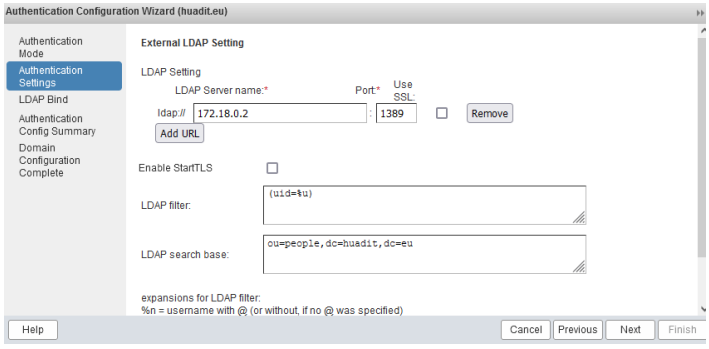
# Κεφάλαιο 7ο: Ιδέες προς υλοποίηση

## 7.1 Zimbra Open Source Two Factor Authentication

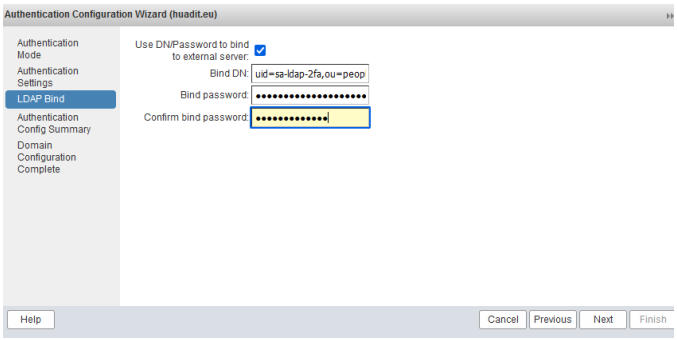
Το open source Zimbra δεν σου παρέχει από μόνο του το 2fa , είναι διαθέσιμο μόνο στο network edition που είναι το επί πληρωμή Zimbra. Για το λόγο αυτό το privacyIDEA είναι ένα ανοιχτού κώδικα λογισμικό που θα τροφοδοτεί το 2fa στο Zimbra μας . Το privacyIDEA θα εκτελείται σε ένα docker container στον διακομιστή μας mailbox01 ή οποίον άλλο θέλουμε εμείς. Τεχνικά αυτό κάνει το Zimbra να υποστηρίζει όλα τα διακριτικά 2fa που υποστηρίζει το pivacyIDEA περιλαμβάνοντας HOTP, TOTP και Yubikey. (De Graaff, 2021)

Αυτό το έργο χρησιμοποιεί έναν διακομιστή μεσολάβησης ldap που παρέχεται από το privacyIDEA . Έτσι τα ονόματα χρήστη , οι κωδικοί τους θα διαβαστούν στον privacyIDEA μέσα από το Zimbra ldap . Και τα διακριτικά 2FA διαβάζονται από τη βάση δεδομένων PrivacyIDEA. Ο χρήστης μπορεί να συνδεθεί χρησιμοποιώντας το 2FA πληκτρολογώντας το όνομα χρήστη, τον κωδικό πρόσβασης και το διακριτικό. Ή απλώς με όνομα χρήστη/κωδικό πρόσβασης εάν ο χρήστης δεν έχει ακόμη διακριτικό.

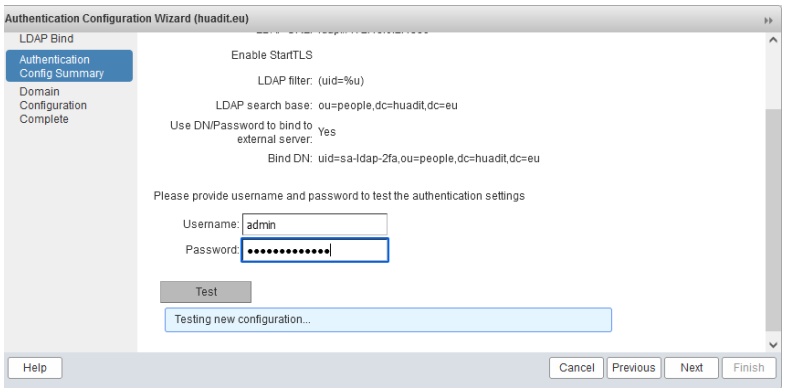
Το privacyIDEA παρέχει δικό του πίνακα ελεγχου το οποιό θα είναι σε κάποια θύρα πχ. 5000. Όταν το εγκαταστήσουμε και το ρυθμίσουμε στη συνέχεια θα πρέπει στο Zimbra control panel να δημιουργήσουμε την διασταύρωση των χρηστών όπως θα δείτε παρακάτω




*Εικόνα 43: εξωτερική αυθεντικοποίηση χρήστη*

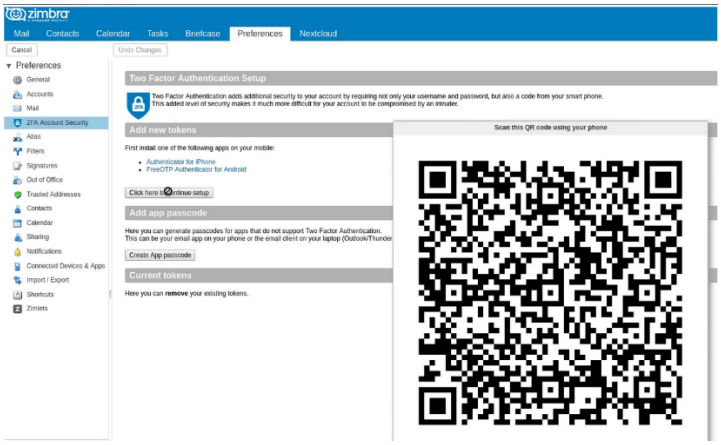



*Εικόνα 44: ldap bind*




*Εικόνα 45: έλεγχος αυθεντικοποίησης*

Τέλος αφού ρυθμίσουμε την διαστάυρωση των χρηστών μπορούμε να ενεργοποιήσουμε το από email μας το 2 factor authenticator.



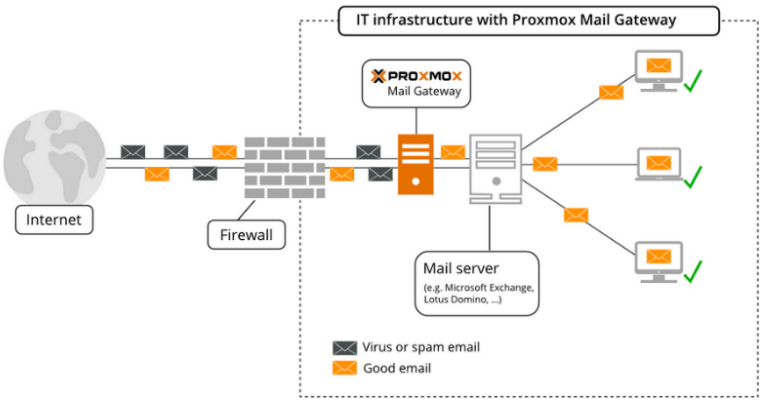

*Εικόνα 46: 2factor qr code*

## 7.2 Proxmox mail gateway

Το Proxmox Mail Gateway είναι η κορυφαία λύση ασφάλειας email ανοιχτού κώδικα που βοηθά στην προστασία των διακομιστών αλληλογραφίας σας από όλες τις απειλές email από τη στιγμή που εμφανίζονται. Μια ευέλικτη αρχιτεκτονική σε συνδυασμό με μια φιλική προς το χρήστη διεπαφή διαχείρισης που βασίζεται στον ιστό που μας επιτρέπει να ελέγχουμε εύκολα όλα τα εισερχόμενα και εξερχόμενα email και να προστατεύουν τους χρήστες τους από ανεπιθύμητα μηνύματα, ιούς, phishing και παραβιάσεις Trojans. (Proxmox, 2014)

Οργανισμοί οποιουδήποτε μεγέθους μπορούν εύκολα να αναπτύξουν και να εφαρμόσουν μια πλατφόρμα anti-spam και anti-virus μέσα σε λίγα λεπτά. Ένας διακομιστής αλληλογραφίας με πλήρεις δυνατότητες αναπτύσσεται μεταξύ του τείχους προστασίας και του εσωτερικού διακομιστή αλληλογραφίας, επιτρέποντάς σας να ελέγχετε όλη την κίνηση email από μία μόνο πλατφόρμα. Το Proxmox μας βοηθά να διατηρήσουμε εύκολα ασφαλείς και επαγγελματικές επικοινωνίες μέσω email, να ικανοποιήσουμε την ανάγκη για περισσότερη ασφάλεια και ικανοποίηση των χρηστών.

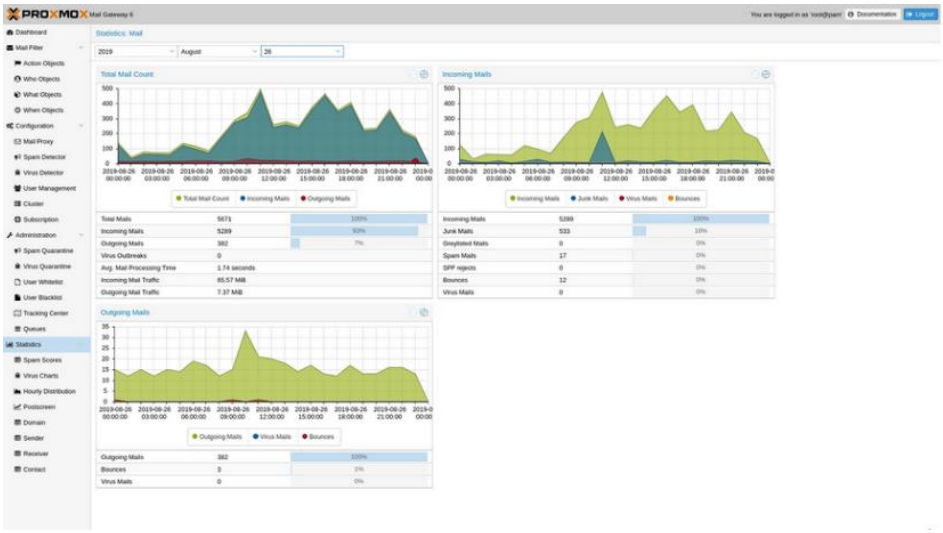
Το proxmox mail gateway είναι στην ουσία ένα εικονικό περιβάλλον, βασιζόμενο κυρίως σε Debian. Για την εγκατάσταση του θα πρέπει να κατεβάσουμε το αρχείο μορφής .iso που βρίσκεται στην επίσημη σελίδα του. (Proxmox, 2014)




*Εικόνα 47: proxmox σενάριο*

Πώς λειτουργεί : ο διακομιστής που θα έχει εγκατεστημένο τον proxmox mail gateway θα είναι στην ουσία μπροστά από τους δύο Zimbra mta και αφού κρίνει ότι το μήνυμα είναι μη κακόβουλο τότε θα το προωθήσει με τη σειρά του στους mta μας, και αυτά με τη σειρά τους αφού το εξετάσουν θα το προωθήσουν στην αλληλογραφία μας.(Proxmox, 2014)

Παρέχει επίσης στατιστικά στοιχεία:



*Εικόνα 48: στατιστικά proxmox mail gateway*

## 7.3 Fail2Ban

Το fail2ban είναι ένα χρήσιμο εργαλείο το οποίο σαρώνει τα αρχεία καταγραφής (/var/log/auth.log, /var/log/apache/access.log, κτλ) έτσι ώστε όταν εντοπίσει πολλές αποτυχημένες προσπάθειες κωδικού πρόσβασης , κακόβουλες προθέσεις, ή πάρα πολλά αιτήματα σε μικρό χρόνο τότε απαγορεύει τις ip αυτές. Το fail2ban είναι ικανό να μειώσει τις λανθασμένες απόπειρες εισόδου, όμως αυτό δεν σημαίνει ότι οι απόπειρες αυτές θα μηδενιστούν . Το fail2ban σε συνδυασμό με το two factor authentication είναι μια πολύ καλή λύση για την προστασία τους συστήματος μας. (Koranga, 2020)

**Προ απαιτούμενα εγκατάστασης fail2ban στο Zimbra.**

```
1. su - zimbra
2. zmprov mcf +zimbraHttpThrottleSafeIPs 185.241.151.39    # IP του Mailbox01}
3. zmprov mcf +zimbraHttpThrottleSafeIPs  185.230.138.207  #{IP του Mailbox02}
4. zmprov mcf +zimbraMailTrustedIP 173.212.253.146         # {IP του Proxy}
5. zmprov mcf +zimbraMailTrustedIP  173.249.51.17          #{IP του Proxy1}
6. zmcontrol restart
```

*Απόσπασμα εντολών 28: προαπαιτούμενα fail2ban*

**Εγκατάσταση fail2ban.**

```
1. yum install epel-release -y
2. yum install fail2ban -y
```

*Απόσπασμα εντολών 29: εγκατάσταση fail2ban*

Στη συνέχεια θα δημιουργήσουμε το αρχείο "/etc/fail2ban/jail.local" και στο "ignoreip=" Θα προσθέσουμε όλες τις ip που θέλουμε να εξαιρεθούν από τον έλεγχο. Οπότε εφόσον έχουμε υλοποιήσει την εγκατάσταση Zimbra σε 8 εξυπηρετητές θα προσθέσουμε τις ip για τους 8 αυτούς εξυπηρετητές.

```
1. nano /etc/fail2ban/jail.local
```

*Απόσπασμα εντολών 30: δημιουργία αρχείου jail.local*

**Αρχείο jail.local .**

```
[DEFAULT]
# "ignoreip" μπορεί να περιέχει IP διευθύνεις, CIDR masks ή DNS hosts.
# το Fail2ban δεν θα κάνει ban τις ip αυτές
#ignoreip = 127.0.0.1/8 ::1 10.137.26.29/32
ignoreip = 127.0.0.1/8  5.182.33.217/24  5.182.33.219/24 173.212.253.146/24
173.249.51.17/24 185.190.142.65/32 194.163.145.237/32 185.241.151.39/32
185.230.138.207/32

banaction = route


# 10 λεπτά  (σε δευτερόλεπτα)
#findtime  = 600

# "bantime" ο αριθμός σε δευτερόλεπτα που ο εξυπηρετητής γίνεται ban
# 10 ώρες(σε δευτερόλεπτα)
bantime  = 36000

# "maxretry" ο αριθμός των αποτυχιών μέχρι να γίνει ban.
maxretry = 5
```

*Πίνακας 31: αρχείο jail.local*

**Δημιουργία αρχείου για τις Zimbra υπηρεσίες "Zimbra.local".**

```
1.  nano etc/fail2ban/jail.d/zimbra.local
```

*Απόσπασμα εντολών 31: δημιουργία zimbra.local αρχείου*

```
[zimbra-smtp]
enabled = true
filter = zimbra-smtp
port = 25,465,587
logpath = /var/log/zimbra.log
maxretry = 3
findtime = 600
bantime = 3600

[zimbra-webmail]
enabled = true
filter = zimbra-webmail
port = 80,443
logpath = /opt/zimbra/log/mailbox.log
```

```
maxretry = 3
findtime = 600
bantime = 3600

[zimbra-admin]
enabled = true
filter = zimbra-admin
port = 7071,9071
logpath = /opt/zimbra/log/mailbox.log
maxretry = 3
findtime = 600
bantime = 3600
```

*πίνακας 32: zimbra.local αρχείο*

**Δημιουργία sshd.local αρχείου για ssh συνδέσεις.**

```
1. nano /etc/fail2ban/jail.d/sshd.local
```

*Απόσπασμα εντολών 32: δημιουργία αρχείου sshd.local*

```
[sshd]
enabled = true
port = 2020
maxretry = 3
findtime = 600
bantime = 3600
```

*πίνακας 33: αρχείο sshd.local*

Τέλος θα χρειαστεί να δημιουργήσουμε τα φίλτρα για τις Zimbra υπηρεσίες. Τα Αρχεία που θα δημιουργήσουμε θα βρίσκονται μέσα στον κατάλογο "/etc/fail2ban/filter.d" και θα είναι τα παρακάτω.

- **zimbra-webmail.conf**
- **zimbra-smtp.conf**
- **zimbra-admin.conf**

**Το αρχείο zimbra-webmail.conf θα περιέχει.**

```
[Definition]
#
failregex = \[oip=<HOST>;.* SoapEngine - handler exception: authentication failed for .*,
account not found$
        INFO .*;oip=<HOST>;.* SoapEngine - handler exception: authentication failed for .*,
invalid password$

ignoreregex =
```

*πίνακας 34: zimbra-webmail.conf*

**Το αρχείο zimbra-smtp.conf θα είναι της μορφής.**

```
[Definition]
#
failregex = postfix\/submission\/smtpd\[\d+\]: warning: .*\[<HOST>\]: SASL \w+
authentication failed: authentication failure$
        postfix\/smtps\/smtpd\[\d+\]: warning: .*\[<HOST>\]: SASL \w+ authentication failed:
authentication failure$

ignoreregex =
```

*πίνακας 35: zimbra-smtp.conf*

**Το αρχείο zimbra-admin.conf θα είναι της μορφής.**

```
[Definition]
#
failregex = INFO .*;ip=<HOST>;.* SoapEngine - handler exception: authentication failed for .*,
invalid password$
        INFO .*ip=<HOST>;.* SoapEngine - handler exception: authentication failed for .*,
account not found$

ignoreregex =
```

*πίνακας 36: zimbra-admin.conf*

**Εντολές εκκίνησης fail2ban.**

```
1. systemctl restart fail2ban  #επαννεκίνηση
2. systemctl status fail2ban   #κατάσταση
3. systemctl enable fail2ban  #ενεργοποίηση
```

*Απόσπασμα εντολών 33: εντολές fail2ban*

# Κεφάλαιο 8ο: Συμπεράσματα

Από την παραπάνω μελέτη και υλοποίηση της εγκατάστασης και παραμετροποίησης του διακομιστή ηλεκτρονικού ταχυδρομείου Zimbra , συμπεραίνουμε ότι πρόκειται για ένα ολοκληρωμένο διακομιστή ηλεκτρονικής αλληλογραφίας, αρκετά τροποποιήσιμο ως προς την εγκατάσταση όλων των πακέτων του σέ έναν εξυπηρετητή ή και να τον διαχωρίσουμε σε πολλαπλούς εξυπηρετητές. Αποτελεί μια κορυφαία λύση ανοιχτού λογισμικού διακομιστή , οπού μπορεί να ανταπεξέλθει σε όλες τις ανάγκες που χρειάζονται την σημερινή εποχή. Σε επίπεδο πανεπιστημίου, μπορεί να ανταπεξέλθει σε όλες τις ανάγκες και να αντικαταστήσει τον υπάρχον διακομιστή και ανάλογα με τους εξυπηρετητές που μπορούν να διατεθούν μπορούμε να προσθέσουμε κι άλλους ή και ακόμα να αντικαταστήσουμε κάποιους αρκετά εύκολα.

Αξιοσημείωτο είναι πως ο διακομιστής Zimbra είναι ολοκληρωμένος, μας παρέχει από εργαλεία καταγραφής συστήματος μέχρι ξεχωριστό διαχειριστή ανεπιθύμητης αλληλογραφίας και antivirus φίλτρα για βελτιστοποίηση της ασφάλειας του συστήματος. Φυσικά όλα τα παραπάνω την σημερινή εποχή δεν αρκούν και ποτέ δεν θα είναι αρκετά για την ασφάλεια, ωστόσο με τις κατάλληλες αλλαγές που πραγματοποιήσαμε μπορούμε να πούμε με σιγουριά ότι έχουμε ένα καλό επίπεδο ασφάλειας συστήματος και με τη συνεχή συντήρηση του μπορούμε να το τροποποιούμε ώστε να είμαστε σε υψηλά επίπεδα ασφάλειας.

Κλείνοντας αξίζει να αναφέρουμε ότι η διασύνδεση με τον κατάλογο χρηστών της σχολής που πραγματοποιείτε μέσω του Zimbra και η προσθήκη νέων χρηστών όχι μόνο μέσω του τερματικού αλλά και μέσω του πίνακα ελέγχου για τον διαχειριστή του συστήματος μας, μέσω xml αρχείων. Επίσης η μετάβαση από άλλους εμπορικούς διακομιστές είναι εφικτή , όμως δεν είναι απαραίτητη αφού ο Zimbra διαθέτει μια μοντέρνα διεπαφή χρηστών που δεν διαφέρει σε κάτι από τους επώνυμους διακομιστές αλληλογραφίας. Τέλος η υλοποίηση της καλύτερης διαχείρισης των μηνυμάτων και της μεγάλης διαθεσιμότητας ώς προς τους χρήστες του ηλεκτρονικού ταχυδρομείου το καθιστούν τον τέλειο διακομιστή για την σχολή μας.

# Βιβλιογραφία


IMAP - Βικιπαίδεια. (2022). Retrieved 4 February 2022, from https://el.wikipedia.org/wiki/IMAP

Open Source Email Platform - Zimbra Collaboration Open Source Edition. (2022). Retrieved 4 February 2022, from https://www.zimbra.com/open-source-email-overview/

Zimbra Collaboration Multi-Server Installation Guide. (2019). Retrieved 4 February 2022, from https://zimbra.github.io/installguides/8.8.15/multi.html

List of DNS record types - Wikipedia. Retrieved 4 February 2022, from https://en.wikipedia.org/wiki/List_of_DNS_record_types

Zimbra Collaboration Multi-Server Installation Guide. (2019). Retrieved 4 February 2022, from https://zimbra.github.io/installguides/8.8.15/multi.html#multiple_server_install

Koranga, H. (2014). Configuring-Logger-Host - Zimbra :: Tech Center. Retrieved 4 February 2022, from https://wiki.zimbra.com/wiki/Configuring-Logger-Host

RBDurgin. (2015). Best Practices on Email Protection: SPF, DKIM and DMARC - Zimbra :: Tech Center. Retrieved 4 February 2022, from https://wiki.zimbra.com/wiki/Best_Practices_on_Email_Protection:_SPF,_DKIM_and_DMARC

Maussion, F. (2015). Zimbra Proxy HA - Zimbra :: Tech Center. Retrieved 4 February 2022, from https://wiki.zimbra.com/wiki/Zimbra_Proxy_HA

Tobias. (2021). Configuring Additional IP Addresses - Blog - Contabo. Retrieved 4 February 2022, from https://contabo.com/blog/configuring-additional-ip-addresses/

Introduction — Keepalived 1.2.15 documentation. Retrieved 4 February 2022, from https://keepalived.readthedocs.io/en/latest/introduction.html

de la Cruz, J. (2014). ZimbraMtaMyNetworks - Zimbra :: Tech Center. Retrieved 4 February 2022, from https://wiki.zimbra.com/wiki/ZimbraMtaMyNetworks

de la Cruz, J. (2015). Add hardware freak's pcre spam blocker in zimbra - Zimbra :: Tech Center. Retrieved 4 February 2022,
from https://wiki.zimbra.com/wiki/Add_hardware_freak%27s_pcre_spam_blocker_in_zimbra

Thomvanderboon. (2014). Anti-spam Strategies - Zimbra :: Tech Center. Retrieved 4 February 2022, from https://wiki.zimbra.com/wiki/Anti-spam_Strategies

Rnoti. (2014). Customized spam score for RBL listed senders - Zimbra :: Tech Center. Retrieved 4 February 2022,
from https://wiki.zimbra.com/wiki/Customized_spam_score_for_RBL_listed_senders

Koranga, H. (2016). Zimbra Collaboration Postscreen - Zimbra :: Tech Center. Retrieved 4 February 2022, from https://wiki.zimbra.com/wiki/Zimbra_Collaboration_Postscreen

Amolmistry. (2020). *Preventing Spamming - Zimbra :: Tech Center*. Wiki.zimbra.com. Retrieved 4 February 2022, from https://wiki.zimbra.com/wiki/Preventing_Spamming.

Shaikh, D. *CBPolicyD Management - Zimbra :: Tech Center*. Wiki.zimbra.com. Retrieved 4 February 2022, from https://wiki.zimbra.com/wiki/CBPolicyD_Management.

*Firewall - Βικιπαίδεια*. El.wikipedia.org. Retrieved 4 February 2022, from https://el.wikipedia.org/wiki/Firewall.

Mhammett. (2007). *Firewall Configuration - Zimbra :: Tech Center*. Wiki.zimbra.com. Retrieved 4 February 2022, from https://wiki.zimbra.com/wiki/Firewall_Configuration.

*Zimbra CLI Commands*. Docs.zimbra.com. (2010). Retrieved 4 February 2022, from http://docs.zimbra.com/docs/ne/6.0.8/administration_guide/A_app-command-line.20.03.html.

De Graaff, B. (2017). *adminguide/cmdlineutils.adoc at develop · Zimbra/adminguide*. GitHub. Retrieved 4 February 2022,
from https://github.com/Zimbra/adminguide/blob/develop/cmdlineutils.adoc.

De Graaff, B. (2021). *GitHub - Zimbra-Community/zimbra-foss-2fa: Two factor authentication for Zimbra Open Source (beta)*. GitHub. Retrieved 4 February 2022, from https://github.com/Zimbra-Community/zimbra-foss-2fa.

Koranga, H. (2020). *Configure Fail2Ban for Zimbra Server with route instead of iptables to block IPs - Zimbra :: Tech Center*. Wiki.zimbra.com. Retrieved 4 February 2022, from https://wiki.zimbra.com/wiki/Configure_Fail2Ban_for_Zimbra_Server_with_route_instead_of_iptables_to_block_IPs.

*Try Zimbra Collaboration Open Source Edition*. Zimbra. Retrieved 4 February 2022, from https://www.zimbra.com/try/zimbra-collaboration-open-source/.

Jhurley. (2006). *Ports - Zimbra :: Tech Center*. Wiki.zimbra.com. Retrieved 4 February 2022, from https://wiki.zimbra.com/wiki/Ports.

Proxmox. (2014). Proxmox mail gateway. Retrieved 4 February 2022, from https://www.proxmox.com/en/proxmox-mail-gateway