Διερεύνηση πιθανότητας και δυνατότητας υιοθέτησης του FreeIPA/IDM στο Τμήμα Πληροφορικής

Περίληψ03Β7

Σκοπός του έργου είναι να εξετάσει τις προσφερόμενες δυνατότητες του FreeIPA (αναφέρεται ως IDM στην πλατφόρμα RedHat/Centos) και εάν η υιοθέτηση του στο Τμήμα Πληροφορικής μπορεί να βελτιώσει τις προσφερόμενες υπηρεσίες όσον αφορά την δημιουργία και διαχείριση χρηστών, την εφαρμογή πολιτικής πρόσβασης σε χρήστες και σε μηχανές (authorization/policy access), και την δυνατότητα sigle-sign-on.

Υπάρχουσα υποδομή

Στο Τμήμα Πληροφορικής λειτουργεί εδώ και χρόνια η υπηρεσία καταλόγου LDAP, και η υπηρεσία Windows Active Directory. Οι δύο αυτές υπηρεσίες, εξυπηρετούν την πρόσβαση των χρηστών σε Linux και Windows clients αντίστοιχα, και σχετίζονται μεταξύ τους όσον αφορά τον συγχρονισμό των συνθηματικών των χρηστών. Η δημιουργία χρηστών γίνεται και στα δύο συστήματα, όπως και η διαχείριση τους. Όσον αφορά την πρόσβαση των χρηστών σε υπηρεσίες που χρειάζεται η πιστοποίηση χρηστών (authetication) αυτή γίνεται μέσω του καταλόγου LDAP.

Όσον αφορά την επιτρεπόμενη πρόσβαση χρηστών σε μηχανών και τον καθορισμό πολιτικής αυτή γίνεται προς το παρόν μόνο σε μεμονωμένες μηχανές/εξυπηρετητές που διαχειρίζεται η ΟΤΥ, ξεχωριστά σε κάθε μηχανή, και όχι σε όλες τις μηχανές του τμήματος.

Τι είναι και τι μπορεί να προσφέρει το FreeIPA/IDM

Το FreeIPA (**Free I**dentity,**P**olicy,**A**udit) είναι μια ολοκληρωμένη λύση διαχείρισης ασφάλειας πληροφοριών που συνδυάζει Linux (Fedora) , 389 Directory Server , MIT Kerberos , NTP , DNS , Dogtag Certificates (Πιστοποιητικό Συστήματος) . Η διαχείριση των πληροφοριών μπορεί να γίνει μέσω web

interface αλλά και από την γραμμή εντολών (command line)

Το FreeIPA είναι μια ολοκληρωμένη λύση ταυτότητας και ταυτοποίησης για Linux/UNIX δικτυωμένα περιβάλλοντα. Ένας server FreeIPA αποθηκεύει όλες τις πληροφορίες που σχετίζονται με τους λογαριασμούς πρόσβασης των χρηστών και των ομάδων χρηστών, αποθηκεύει πληροφορίες πελατών (hosts) ουτωσώστε να παρέχεται η πρόσβαση των χρηστών σε αυτούς , και δίνει την δυνατότητα δημιουργίας πολιτικής πρόσβασης σε μηχανές και υπηρεσίες(services) που τρέχουν στις μηχανές που υπάρχουν σε ένα FreeIPA domain.

FreeIPA είναι χτισμένο στην κορυφή γνωστών συστατικών Open Source και πρότυπα πρωτόκολλα με μια πολύ ισχυρή έμφαση στην ευκολία διαχείρισης και αυτοματοποίησης των εργασιών εγκατάστασης και ρύθμισης.
Σε ένα FreeIPA Domain η εγκατάσταση του FreeIPA, μπορεί να γίνει σε πάνω από πολλούς εξυπηρετητές ουτωσώστε να υπάρχει πλεονασμός. Η σύνδεση με το Windows Active Directory μπορεί να γίνει, σε επίπεδο χρηστών και είναι μονής κατεύθυνσης (από το Windows Active Directory προς το FreeIPA, και όχι αντίστροφα.)

Το FreeIPA δίνει την δυνατότητα ενοποίησης των εξής λειτουργιών, με δυνατότητα κεντρικής διαχείρισης :

- Λειτουργία αυθεντικοποίησης και ταυτοποίησης χρηστών (Identity and authorization service) με δυνατότητα χρήσης Kerberos και KDC για εφαρμογή του single-sign on. Η λειτουργία βασίζεται σε ένα backend LDAP server, ο οποίος παρέχει όλες τις πληροφορίες για τους χρήστες, τις ομάδες, κτλ
- DNS Service
- NTP Service
- Certificate Service

Πιο κάτω θα πρέπει να εξεταστούν οι επιμέρους λειτουργίες και πως αυτές θα πρέπει να αλλάξουν αν χρειαστεί, ουτωσώστε να μην επηρεαστεί η λειτουργία του τμήματος.

Σχεδιασμός και υλοποίηση της υποδομής	
Στην φάση αυτή πρέπει να εξεταστεί ο σχεδιασμός της υπηρεσίας σε σχέση με το υπάρχον περιβάλλον, σε τεχνικό επίπεδο	
Σημεία προς εξέταση	**Παρατηρήσεις**
Υποδομή σε φυσικές ή ιδεατές μηχανές.	Εάν θα επιλεγεί να προσφερθεί το NTP service, τότε δεν πρέπει να είναι σε ιδεατή μηχανή. Εάν θα επιλεγούν φυσικές μηχανές να εξεταστεί η δυνατότητα τοποθέτησης τους και σε άλλο δωμάτιο εκτός του 002
Καθορισμός αριθμού μηχανών (master/slave operation, replicans in FreeIPA terminology)	Το FreeIPA επιτρέπει την δημιουργία πολλαπλών εξυπηρετητών για δημιουργία υποδομής για replication, με δυνατότητα ρύθμισης του load balancing.

Καθορισμός FreeIPA domain name σε σχέση με το DNS domain, και Windows AD domain name	Σημαντική παράμετρος στην οποία βασίζεται η όλη λειτουργία του λογισμικού
Hardware and Software Requirements Hardware requirements: • 2GB of RAM and 1GB swap space Software : centos 6.5 (Freeipa ver. 3.0.0) Centos 7 (Freeipa ver. 3.2.0)	Centos 6.4 or Centos 7. (FreeIPA on Centos 7 will provide support to define trust with AD 2012)
Τρόποι διαχείρησης του FreeIPA: 1. Web GUI 2. Command line (cli) 3. Υπάρχει η δυνατότητα για πρόσβαση στα αρχεία από το linux	Επίσης παρέχεται η δυνατότητα delegation για διάφορα επίπεδα admins

Υπηρεσία LDAP (Θα εξεταστεί σε βάθος από τον υπεύθυνο λειτουργίας. Πιο κάτω αναφέρονται επιγραμματικά κάποια στοιχεία που εντοπίστηκαν)	
Πρέπει να εξεταστεί η διαδικασία που θα ακολουθηθεί σε σχέση με την μετάβαση στο FreeIPa, ουτωσώστε να μην χρειαστεί οι χρήστες να αλλάξουν usernames, password, directory ownership etc...	
Password Policy – Πρέπει να εξεταστεί η δυνατότητα καθορισμού του υφιστάμενου password policy και κατά πόσο θα μπορεί να εφαρμοστεί και στο Windows AD	Μπορεί να εφαρμοστεί γενικά για όλους τους χρήστες αλλά και κατά ομάδες χρηστών. Επιτρέπει ακόμα την δυνατότητα καθορισμού αυτόματου κλειδώματος του λογαριασμού σε περίπτωση Brute-force
Πρέπει να εξεταστεί εάν είναι δυνατόν ο administrator να μπορεί να δει το LDAP schema και θα πρέπει να μπορεί να το τροποποιεί ανάλογα των απαιτήσεων που θα προκύψουν view/extend/modify schema	Η διαδικασία επεξηγείται στο ακόλουθο link, για το FreeIPA 3.3 http://www.freeipa.org/images/5/5b/FreeIPA33-extending-freeipa.pdf

Υπηρεσία Δημιουργίας και Διαχείρισης Χρηστών	
Πρέπει να εξεταστεί η διαδικασία δημιουργίας χρηστών και κατά πόσο θα μπορεί να απλοποιηθεί η διαδικασία π.χ 1. Σχέση linux users/windows users, και κατά πόσον θα πρέπει οι χρήστες να δημιουργούνται και στα windows ή και στο Linux (δες πιο κάτω) 2. Δημιουργία πολλών χρηστών από αρχείο 3. Αυτόματη διανομή uid/gid στην δημιουργία χρηστών 4. Εύκολη δημιουργία group 5. Αυτόματη εισαγωγή χρηστών σε group , (κατά την δημιουργία χρηστών να εισάγεται και στο group. Στο FreeIPa αυτό γίνεται με την δυνατότητα το **automembership**, για χρήστες και μηχανές, κατά την διαδικασία δημιουργίας τους) 6. Δημιουργία userhome directory/mail /extraspace κατά την δημιουργία χρηστών 7. Εύκολη ρύθμιση quotas στο homedir/email 8. Διαγραφή χρηστών και δεδομένων τους ταυτόχρονα 9. Enable/disable users για login σε συστήματα, για παραλαβή emails	Σήμερα η διαδικασία δημιουργίας λογαριασμού χρηστών απαιτεί το λιγότερο 8 διεργασίες, σε 4-6 διαφορετικούς εξυπηρετητές(hermes,kronos,atlas,proteas,Softera, AD users and groups, κτλ), όπως περιγράφεται εδώ https://wiki.cs.ucy.ac.cy/index.php/OTY_Internal:User_accounts Το ζητούμενο είναι να μπορούμε να δημιουργούμε λογαριασμούς χρηστών (και κατά πόσο θα μπορούμε να δημιουργούμε λογαριασμούς σε μια μόνο πλατφόρμα π.χ Linux και να ενημερώνεται ταυτόχρονα και η άλλη πλατφόρμα ή ανάποδα) με λιγότερες διαδικασίες όσον πιο αυτοματοποιημένα μπορούμε, για αποφυγή λαθών Επίσης θα πρέπει να διευκολυνθεί η διαχείριση των χρηστών (π.χ διαγραφή χρηστών και δεδομένων τους). Η δημιουργία και διαχείριση στο FreeIPA μπορεί να γίνει είτε μέσω cli (αυτό θα ευκολύνει στην περίπτωση που έχουμε batch files) και μέσω webgui, για εύκολη διαχείρηση ενός ή πολλών χρηστών.
Users and Autofs	
Θα πρέπει να παρέχεται η δυνατότητα του autofs στα home directories	Υπάρχουν ορισμένες προϋποθέσεις π.χ εάν το nfs export θα γίνεται με Kerberos κτλ.
FreeIPA and Samba	
Κατά πόσον επηρεάζεται η λειτουργία της sambas από την εισαγωγή του FreeIPa	Οι χρήστες θα πρέπει να μπορούν να έχουν πρόσβαση στο U:\ στον προσωπικό τους χώρο (και σε άλλους χώρους p.x O:\ Drive το οποίο αντιστοιχεί σε χώρο για το opnet) από τα Windows
FreeIPA and Windows Active Directory	Εξαιρετικά σημαντική σχέση, η οποία πρέπει να μελετηθεί σε βάθος γιατί βασίζεται όλη η λειτουργία του Τμήματος.

Στην ενότητα αυτή θα πρέπει να εξεταστεί η σχέση του FreeIPA και του Windows AD. • Υπάρχει θέμα με το FreeIPA version (Freeipa on centos 6.5, ver 3.0) • Support AD 2012 trust στο ver 3.1.0	Στο https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Windows_Integration_Guide/trust-requirements.html αναφέρεται μόνο στο Windows 2008 R2, παρόλο που στο http://www.freeipa.org/page/Releases/3.1.0 αναφέρεται σε windows 2012 trust
Στο RH7, υπάρχει η δυνατότητα authenticate των linux clients με sssd στο Active Directory	Αυτό σημαίνει κατάργηση του LDAP, που μάλλον απορρίπτεται εξαρχής!!!!
Υπάρχει επίσης η δυνατότητα δημιουργίας “trust” μεταξύ IDM και Windows Active Directory. • Η δημιουργία είναι μονομερής, δηλαδή η ενημέρωση γίνεται από το Windows AD προς τον IDM, και αφορά τις ομάδες χρηστών. Στον IDM, οι ομάδες χρηστών που προέρχονται από το AD, τους δίνεται πρόσβαση σε επίπεδο group και εφαρμόζονται τα access policies/rules etc	Αυτό συνήθως εφαρμόζεται σε περιβάλλοντα όπου οι windows users δεν υπάρχουν στον IDM. Θα πρέπει να εξεταστεί εάν στην δική μας περίπτωση εξυπηρετεί .
Υπάρχει επίσης η δυνατότητα συγχρονισμού μεταξύ IDM και Windows AD, υπό προϋποθέσεις.(Cross-realm forest trust) Ο συγχρονισμός είναι 2-way synchronization(παρόλο που μπορεί να ρυθμιστεί για να είναι 1-way). • Υπάρχει αντιστοιχία μεταξύ των attributes του LDAP και των attributes του AD, αλλά υπάρχουν και εξαιρέσεις (The `uidNumber` and `gidNumber` attributes defined and used in Identity Management are not the same `uidNumber` and `gidNumber` attributes defined and used in the Active Directory entry, and the numbers are not related.) • Υπάρχει ξεχωριστή διαδικασία για password synchronization. Password Sync Service είναι λογισμικό το οποίο θα πρέπει να εγκατασταθεί στους AD controllers, για να επιτρέπει το password synchronization μεταξύ των δύο πλατφόρμων.	Αυτό προϋποθέτει την δημιουργία χρηστών στα windows και μεταφορά τους στον IDM. Αλλαγές στους λογαριασμούς χρηστών μπορεί να γίνονται και στις 2 πλατφόρμες και θα μεταφέρονται οι αλλαγές.

FreeIPA and freeipa-clients	
1. Η εγκατάσταση του freeipa-client σε linux μηχανές, μπορεί να γίνει με διάφορους τρόπους π.χ yum install ipa-client, add host entry from from web gui	Το FreeIP προϋποθέτει σωστά DNS records για να μπορεί να γίνεται η επικοινωνία με τον FreeIP server

2. Ο administrator μπορεί να διαχειριστεί τις μηχανές με την ίδια φιλοσοφία όπως τους χρήστες. Δηλαδή μπορεί να κάμει disable/enable hosts που σημαίνει ότι η μηχανή βρίσκεται στο freeipa domain, αλλά οι χρήστες δεν μπορούν να κάνουν login. 3. Μπορεί να δημιουργήσει ομάδες μηχανών με βάση δικά του κριτήρια και να δώσει προνόμια πρόσβασης ή μη σε ομάδες χρηστών	
4. Μια από τις βασικές λειτουργίες του λογισμικού είναι η σχέση χρηστών και μηχανών και η δημιουργία policies	
5. Οι windows μηχανές μπορούν να κάνουν login σε FreeIPA domain, υπό προϋποθέσεις, παρόλο που δεν συστήνεται (Σε περιβάλλοντα που υπάρχει AD καλύτερα να γίνει trust μεταξύ τους)	http://pgina.org/ είναι πρόγραμμα, που επιτρέπει την σύνδεση windows clients με FreeIPA domain

CA Certificate	Το FreeIPA βασίζει την λειτουργία του και την επικοινωνία μεταξύ των λειτουργιών του, στην ύπαρξη server certificates ουτωσώστε να μπορεί να επιτυχάνεται ασφαλής επικοινωνία
Υπάρχουν 2 τρόποι δημιουργίας Certificate Certificate Authority που θα πρέπει να εξεταστούν : 1. The Dogtag Certificate System can sign *its own* certificate 2. The Dogtag Certificate System CA can be signed by an externally-hosted CA 3. Να μην εγκατασταθεί καθόλου και να χρησιμοποιηθούν certificates ανεξάρτητα	Η επιλογή της μεθόδου που θα χρησιμοποιηθεί πρέπει να γίνει εξαρχής πριν από την εγκατάσταση γιατί δεν θα είναι δυνατή η μετάβαση από την μια μέθοδο στην άλλη όταν ολοκληρωθεί η εγκατάσταση όλου του λογισμικού
DNS server setup (BIND 9.9) (Θα εξεταστεί σε βάθος από τον υπεύθυνο λειτουργίας. Πιο κάτω αναφέρονται επιγραμματικά κάποια στοιχεία που εντοπίστηκαν)	Το FreeIPA βασίζει την λειτουργία του στα DNS records, ειδικά για τις λειτουργίες όπως το LDAP directory services, Kerberos, and Active Directory integration.
1. Εγκατάσταση και λειτουργία	Επειδή η ύπαρξη και η λειτουργία του DNS service είναι πολύ σημαντική στην όλη λειτουργία του τμήματος θα πρέπει να εξεταστεί εξαρχής τι σημαίνει η υιοθέτηση ή όχι αυτής της λειτουργίας, και τι επιπτώσεις θα έχει εάν επιλεγεί η μη εγκατάσταση της.

2. Θα πρέπει να εξεταστεί πιο πρωτόκολλο χρησιμοποιεί	
3. Θα πρέπει να εξεταστεί ο τρόπος διαχείρισης του DNS service	

sudo and FreeIPa	Με την linux εντολή sudo, ο υπεύθυνος της μηχανής επιτρέπει σε χρήστες να εκτελούν συγκεκριμένες εντολές που μόνο ο root έχει το προνόμιο να τις εκτελεί
1. Επιτρέπει την δημιουργία σχέσεων μεταξύ μηχανών-χρηστών-εντολών	Στην δική μας περίπτωση θα μπορεί να εξυπηρετήσει την ομάδα της ΟΤΥ, αφού θα περιορίσει την χρήση του root. Θα μπορεί να εφαρμοστεί και σε μηχανές και χρήστες των ερευνητικών εργαστηρίων, όπου ζητούν root priviledges

Host-based access control	Με την δυνατότητα αυτή ο IDM μπορεί να ελέγχει ποιος (χρήστης), τι μπορεί να τρέχει (service), πού (σε ποια μηχανή που ανήκει στο domain)
1. Για την λειτουργία αυτή θα πρέπει να εξεταστούν πιθανοί τρόποι αξιοποίησης της δυνατότητας που προσφέρεται.	Πιθανές εφαρμογές στα διδακτικά και ερευνητικά εργαστήρια, και σε μηχανές της ΟΤΥ, οι οποίες είναι στην DMZ
2. Θα πρέπει να μελετηθεί κατά πόσον μπορούν να προστεθούν και άλλες λειτουργίες (services) που πιθανόν να μην περιλαμβάνονται ήδη	

FreeIPA, Web Applications, https	
1. Υπηρεσίες όπως webmail, moodle, helpdesk, OATS, wireless authentication, VPN κτλ, θα πρέπει να συνεχίσουν απρόσκοπτα να λειτουργούν και με το FreeIPA	Δεδομένου ότι αυτές οι υπηρεσίες δουλεύουν με authentication μέσω OpenLdap, δεν φαίνεται να υπάρχει πρόβλημα όμως θα πρέπει να εξεταστεί
2. Δυνατότητα single-sign on	Παρόλο που αναφέρεται στο κείμενα, θα πρέπει να εξεταστεί τι πραγματικά σημαίνει, κατά πόσον εφαρμόζεται και ποιες αλλαγές προϋποθέτει στις εφαρμογές.

Βιβλιογραφία

Linux Domain Identiry,Authentication and Policy Guide

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html

Identity Management Guide

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Identity_Management_Guide/index.html

Windows Integration Guide

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Windows_Integration_Guide/Preface.html

RED HAT ENTERPRISE LINUX:IDENTITY MANAGEMENT, Technical Brief

https://access.redhat.com/site/sites/default/files/pages/attachments/rhel_7_identity_management_techbrief_12069297_0414jcs_web_0.pdf