ΑΣΚΗΣΗ 5

ΔΗΜΙΟΥΡΓΙΑ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΠΟΛΙΤΙΚΗΣ ΟΜΑΔΑΣ ΧΡΗΣΤΩΝ

ΣΚΟΠΟΣ: Όταν πραγματοποιήσεις αυτή την άσκηση θα πρέπει να μπορείς...

- Να δημιουργείς και να διαχειρίζεσαι πολιτικές ομάδων χρηστών.

ΧΡΗΣΙΜΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

Ίσως από την πρώτη άσκηση δημιουργίας χρηστών αλλά και στις επόμενες ασκήσεις, σας έκανε εντύπωση η επιλογή **Active Directory** Users And Computers που τόσο συχνά χρησιμοποιήσατε. Είναι η ώρα να κάνουμε μια σύντομη αναφορά στην έννοια του Active Directory.

Κατά την διάρκεια της εγκατάστασης των Windows 2003 Server (θα μας απασχολήσει σε αντίστοιχη άσκηση) η πρώτη σημαντική διαφορά που θα αντιληφθείτε μετά το τέλος της, είναι ότι τότε αρχίζουν όλα, με πρώτο την ενεργοποίηση και διαμόρφωση του Ενεργού Καταλόγου (Active Directory). Ίσως να έχετε ήδη καταλάβει την σπουδαιότητα του Active Directory κατά την διάρκεια εκτέλεσης των προηγούμενων ασκήσεων, αλλά σίγουρα όχι στις πραγματικές της διαστάσεις.

Με λίγα λόγια μπορούμε να πούμε ότι το Active Directory είναι ένα σύνολο υπηρεσιών, που επιτρέπει την ύπαρξη ενός μοναδικού σημείου διαχείρισης για όλους τους πόρους του δικτύου: των χρηστών, των Η/Υ, των εκτυπωτών, των αρχείων, των περιφερειακών συσκευών, των βάσεων δεδομένων, της πρόσβασης στον Ιστό κα. Το Active Directory αντικατέστησε επιτυχώς την υπηρεσία καταλόγου των Windows NT, προσφέροντας μεγάλη κλιμάκωση, επέκταση και ασφάλεια, χρησιμοποιώντας ένα συνδυασμό υπηρεσιών και πρωτοκόλλων, όπως την γνωστή από το Internet υπηρεσία DNS (Domain Name System - Σύστημα Ονομάτων Περιοχών), την DHCP (Dynamic Host Configuration Protocol) το πρότυπο X.500 το LDAP (Lightweight Directory Access Protocol - Ελαφρό Πρωτόκολλο Προσπέλασης Καταλόγου), και το πρωτόκολλο ασφάλειας kerberos. Το σημαντικότερο είναι ότι η υπηρεσία Active Directory είναι μια ενοποιημένη υλοποίηση μιας συλλογής υπηρεσιών σε ένα σημείο, σχεδιασμού και διαχείρισης δικτύων.

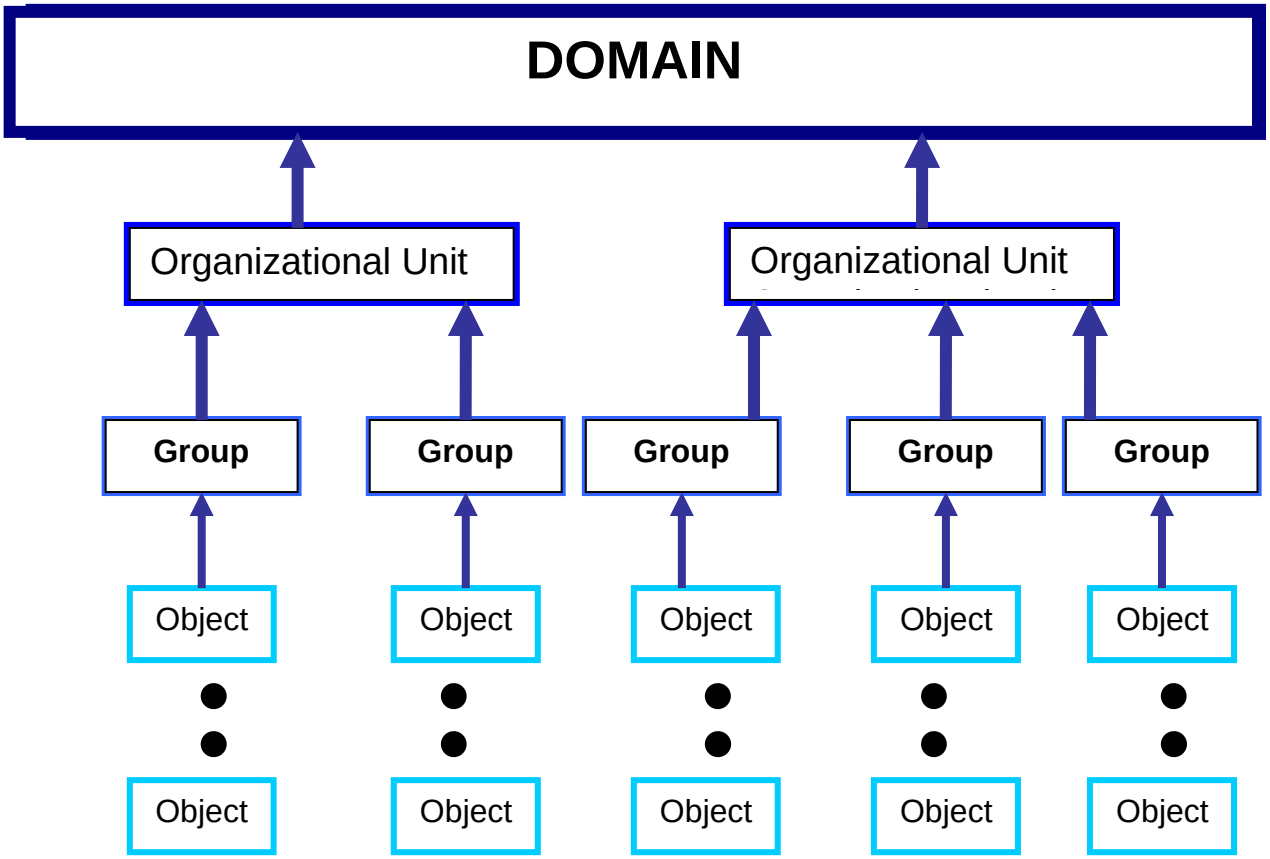
Ο σχεδιασμός ενός δικτύου Η/Υ είναι πολύ σημαντικός, ειδικά όταν αναφερόμαστε σε μεγάλου μεγέθους δίκτυα. Τα Windows 2003 Server στις διάφορες εκδόσεις τους, μπορούν να υποστηρίξουν γιγαντιαία δίκτυα Η/Υ. Θα περιοριστούμε όμως στην απλή περίπτωση τυπικού εταιρικού δικτύου μιας περιοχής. Ήδη αναφέρθηκε και ήδη έχετε συναντήσει στις προηγούμενες ασκήσεις την έννοια της περιοχής (**Domain**).

Το Domain είναι στην κορυφή της ιεραρχίας του Active Directory και ταυτόχρονα είναι ο πυρήνας λειτουργίας του. Όλα τα αντικείμενα του δικτύου, είναι τμήματα που συνθέτουν το Domain και υπακούουν στην πολιτική του, μέχρι ο Administrator να την τροποποιήσει για κάποιο από αυτά. Η λειτουργία και ο έλεγχος στο Domain εφαρμόζεται από έναν τουλάχιστον Η/Υ που ονομάζεται **Domain Controller** (Ελεγκτής Περιοχής) και πιο συνηθισμένα Server, Γράφτηκε «τουλάχιστον έναν

Η/Υ» γιατί οι Domain Controller μπορεί να είναι και περισσότεροι, ανάλογα με τα χαρακτηριστικά του κάθε δικτύου, αλλά είναι όλοι ισότιμοι μεταξύ τους. Έτσι αν τεθεί εκτός λειτουργίας κάποιος, οι υπόλοιποι συνεχίζουν να διαχειρίζονται το Domain. Όποια ενέργεια ή αλλαγή κάνει ο Domain Controller στην περιοχή αυτή αναπαράγεται (Replicated) σε ολόκληρο το Domain.

Στο παρακάτω επίπεδο υπάρχει η έννοια (εμφανίστηκε στα Windows 2003 Server) της Οργανωτικής Μονάδας (**Organizational Unit**). Έχει κάποια χαρακτηριστικά από το Domain αλλά ούτε απαιτεί πόρους (δεν χρειάζεται Domain Controller) αλλά και δεν εμπλέκεται στην διαδικασία αναπαραγωγής (Replication). Αυτό την καθιστά βολικό και ενδεδειγμένο διαχειριστικό όριο. Όποια πολιτική εφαρμοστεί σε Organizational Unit επηρεάζει μόνο τα αντικείμενα που αυτό περιέχει και όχι το υπόλοιπο Domain. Συνοψίζοντας το Domain περιέχει Organizational Unit, και αυτά με την σειρά τους μπορεί να περιέχουν είτε άλλα Organizational Unit, είτε ομάδες (Group) αντικειμένων, όπως π.χ. την ομάδα χρηστών που δημιουργήσατε, είτε και μεμονωμένα αντικείμενα αν και αυτό δεν ενδείκνυται . Με τον όρο «αντικείμενα» συνήθως εννοούμε Η/Υ ή Users.

Πιθανά, αντιλαμβάνεστε πόσο σημαντικό είναι, πριν την υλοποίηση ενός δικτύου Η/Υ να έχει προηγηθεί ένας προσεκτικός σχεδιασμός του. Συνοψίζοντας μια λογική και απλή δομή ενός Domain είναι περίπου όπως το παρακάτω σχήμα.



σχήμα 5.1

Θα δούμε με συντομία, ένα ακόμη ζήτημα: τις **άδειες (permissions)** και τα **δικαιώματα (rights)** που μπορούν να διατεθούν στους χρήστες.

Το τι μπορούν και το τι δεν μπορούν να κάνουν οι χρήστες, είτε είναι μέλη μιας ομάδας είτε είναι μεμονωμένοι εξαρτάται από τα δικαιώματα και τις άδειες που έχουν χορηγηθεί σε αυτούς ή στις ομάδες που ανήκουν. Εδώ πρέπει να ξεκαθαρίσουμε τις έννοιες δικαιωμάτων και αδειών :

Οι άδειες χαρακτηρίζουν την πρόσβαση που έχει ένας χρήστης ή ομάδα χρηστών σε συγκεκριμένα αντικείμενα όπως αρχεία, φακέλους ή εκτυπωτές. Για παράδειγμα η εκτύπωση για ένα χρήστη από έναν δικτυακό εκτυπωτή ή το άνοιγμα ενός φακέλου που βρίσκεται στον Server του Domain, είναι αποτέλεσμα της αντίστοιχης άδειας που διαθέτει αυτός ο χρήστης

Τα δικαιώματα ισχύουν γενικά για το σύνολο του συστήματος που παραχωρούνται ή αφαιρούνται από τον διαχειριστή (πχ η δυνατότητα λήψης αντιγράφων ή η σύνδεση σε ένα Server). Τα **δικαιώματα** διακρίνονται στα **προνόμια (privileges)** και στα **δικαιώματα σύνδεσης (logon rights)**.

Τα προνόμια, όπως αναφέρει και η λέξη είναι κάτι που δύσκολα παραχωρείται σε κάποιον (όπως πχ η δυνατότητα εξαναγκαστικού τερματισμού λειτουργίας από απομακρυσμένο σύστημα ή η ικανότητα ελέγχων ασφάλειας).

Τα δικαιώματα σύνδεσης επίσης κάνουν αυτό που λέει το όνομα τους, δηλαδή καθορίζουν την ικανότητα σύνδεσης σε έναν Η/Υ με συγκεκριμένους τρόπους (πχ το δικαίωμα σύνδεσης Logon locally επιτρέπει την σύνδεση στον Η/Υ τοπικά, ενώ το Access this computer from the network, επιτρέπει σε όποιον χρήστη παραχωρείται ή σε όποια ομάδα το έχει εξ ορισμού την σύνδεση στον Η/Υ μέσω του δικτύου.

Γενικά υπάρχουν δύο πρακτικοί κανόνες που πρέπει να ακολουθείτε σαν διαχειριστές δικτύων, στην χορήγηση αδειών και δικαιωμάτων :

- ✓ Για λόγους απλούστευσης της διαχείρισης του δικτύου, είναι προτιμότερο να χορηγείτε άδειες και δικαιώματα ανά Ομάδες, είτε καλύτερα ανά Οργανωτικές Μονάδες παρά ανά χρήστες.
- ✓ Ο βασικός σκοπός ενός δικτύου είναι να εξασφαλίζει ότι οι χρήστες, θα έχουν ότι τους χρειάζεται για να εκτελέσουν τις εργασίες τους και τίποτα που δεν χρειάζονται. Αυτό που σίγουρα δεν χρειάζονται είναι να συναντούν προβλήματα στο να κάνουν αυτό που πραγματικά χρειάζεται.

Η πολιτική ομάδας χρηστών δικτύου δημιουργείται στον Server του δικτύου και με τη χρήση ενός λογαριασμού Administrator. Όπως διαβάσατε και παραπάνω, ενδεδειγμένο διαχειριστικό όριο είναι η Οργανωτική Μονάδα (ΟΜ). Αυτό δεν σημαίνει ότι δεν υπάρχει η δυνατότητα υλοποίησης πολιτικής σε αντικείμενο (χρήστη) ή ομάδα αντικειμένων, αλλά αυτό είναι αντίθετο στην φιλοσοφία του Active Directory και δεν συμβάλλει στην προσπάθεια απλοποίησης της διαχείρισης του δικτύου.

ΠΟΡΕΙΑ ΕΡΓΑΣΙΑΣ

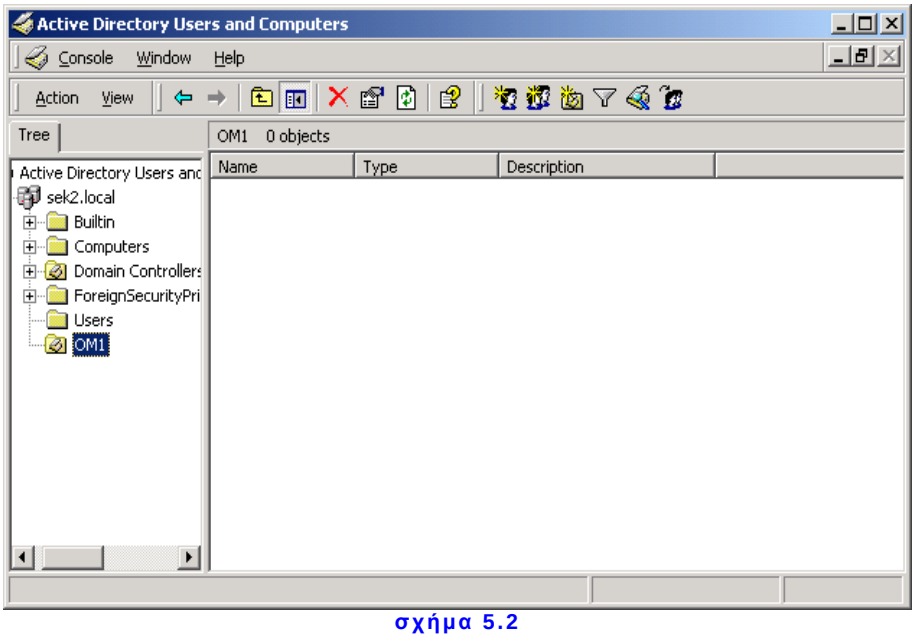
1. Να ελέγξετε την επικοινωνία των Η/Υ του δικτύου σας και να την αποκαταστήσετε αν χρειάζεται.

2. Αφού συνδεθείτε στον Server του δικτύου με έναν λογαριασμό Administrator δημιουργήστε μια Οργανωτική Μονάδα ως εξής:

Από Start → Programs → Administrative Tools → Active Directory Users and Computers και επιλέξτε το Domain σας (στο σχήμα 5.2 που ακολουθεί είναι το sek2).

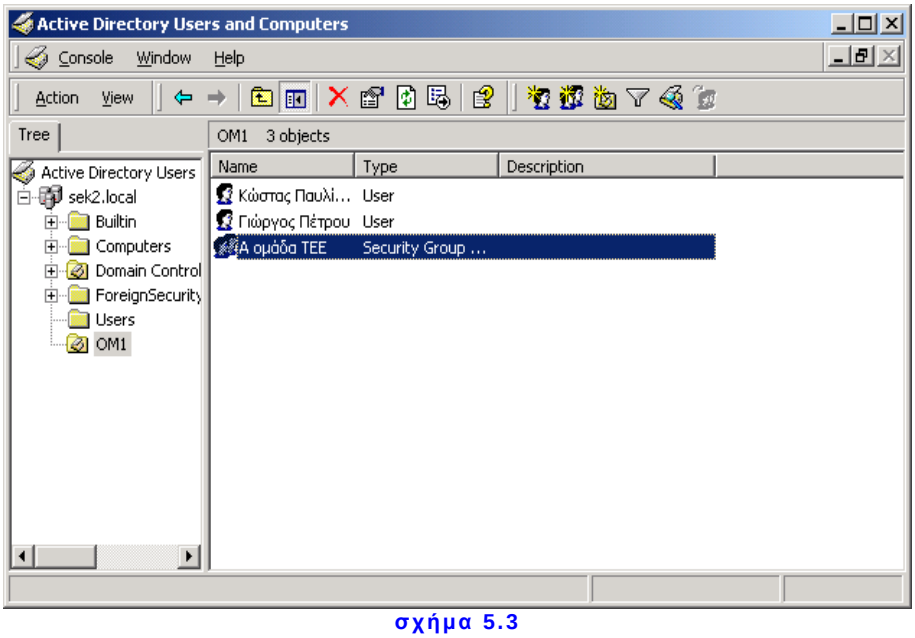
3. Κάνετε δεξί κλικ σε αυτό και επιλέξτε New → Organizational Unit. Ονομάστε την **OMx** (όπου x ο αριθμός της ομάδας εργασίας σας).

4. Τώρα η νέα OM είναι έτοιμη να εποικιστεί με άλλα αντικείμενα, όπως χρήστες, ομάδες χρηστών, Η/Υ ή και άλλες OM. Να εντοπίσετε τους λογαριασμούς σας στον αποδέκτη Users του Domain και με δεξί κλικ → move να τους μετακινήσετε στην OM σας.



σχήμα 5.2

5. Δημιουργήστε **μέσα στην OM** σας, την δική σας ομάδα (Group) χρηστών, όπως και στην προηγούμενη άσκηση, και να τοποθετήσετε τους λογαριασμούς σας ως μέλη της ομάδας όπως φαίνεται και στο σχήμα 5.3.

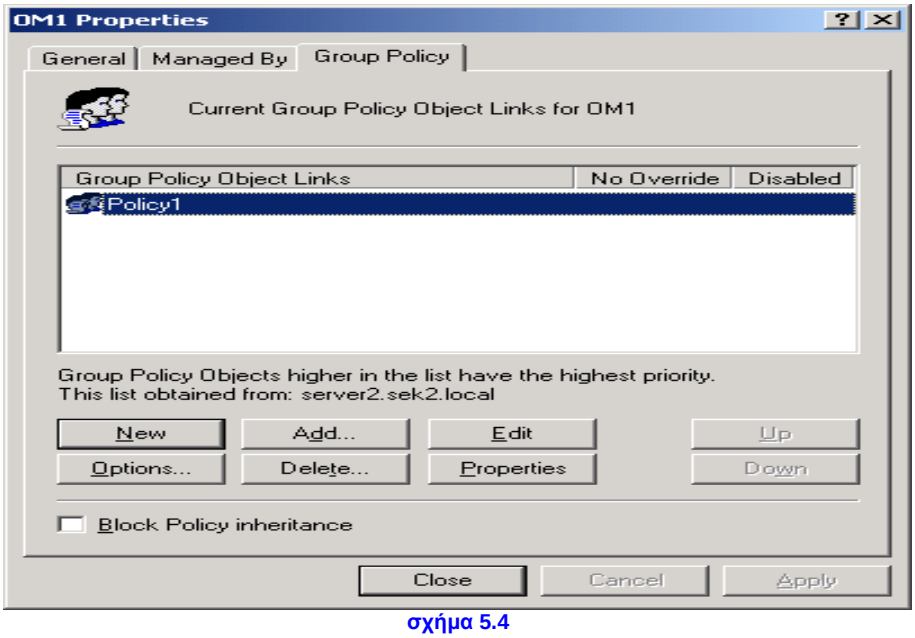


σχήμα 5.3

Παρατήρηση:

Πρέπει να είσαστε προσεκτικοί και να μην υπάρχουν χρήστες σε διαφορετικούς αποδέκτες ταυτόχρονα. Για παράδειγμα αν στον αποδέκτη Users είχατε δημιουργήσει μια ομάδα και ενσωματώνατε κάποιους χρήστες σε αυτήν, και έπειτα μετακινούσατε την ομάδα σε μια άλλη ΟΜ, οι χρήστες θα υπήρχαν ταυτόχρονα και στον αποδέκτη Users αλλά και στην νέα ΟΜ. Το πιθανότερο είναι έτσι, να υπάρξει σύγκρουση πολιτικών και να είναι αμφίβολο το τι θα ισχύσει κάθε φορά.

6. Θα δημιουργήσετε πολιτική τώρα που θα έχει ισχύ στην ομάδα σας (δηλ στους λογαριασμούς σας) μόνο. Να κάνετε δεξί κλικ στην ΟΜ σας και να επιλέξετε properties. Επιλέξτε τώρα την καρτέλα Group Policy και ιδρύστε την πολιτική σας πατώντας New στις επιλογές που βλέπετε και ονομάστε την Policy x (όπου x ο αριθμός της ομάδας σας).



σχήμα 5.4

7. Προσέξτε τώρα ένα βασικό σημείο. Έχοντας υπ όψιν την δομή και την ιεραρχία του Active Directory, όπως περίπου δείχνει το σχήμα 5.1, πρέπει να υπολογίσετε κατά τον σχεδιασμό της πολιτικής σας και το θέμα της κληρονομικότητας. Οι ρυθμίσεις πολιτικής μεταβιβάζονται από τους γονικούς στους θυγατρικούς αποδέκτες. Αυτό σημαίνει για παράδειγμα ότι η εξ΄ ορισμού πολιτική της περιοχής (Default Domain Policy), μεταβιβάζεται σε όλες τις ΟΜ που είναι κάτω από αυτήν και βέβαια και στην δική σας. Στην περίπτωση της σύγκρουσης των δύο πολιτικών, η πρακτική των Windows 2003 Server είναι να επικρατεί αυτή του θυγατρικού αποδέκτη. Στην περίπτωση που οι δύο πολιτικές συμπληρώνονται, τότε εφαρμόζονται και οι δύο. Με άλλα λόγια, όταν δημιουργείτε μια νέα πολιτική σε ΟΜ, όπως κάνατε τώρα, στην ουσία κληρονομείτε την πολιτική του Domain και στην συνέχεια την τροποποιείτε. Υπάρχουν πάντως τρόποι παράκαμψης της κληρονομικότητας, που αξίζει να τους αναφέρουμε. Όπως φαίνεται στο σχήμα 5.4 αν κάνετε δεξί κλικ στο όνομα της πολιτικής σας (Policy x) και επιλέξετε **No Override**, τότε οι θυγατρικοί αποδέκτες δεν μπορούν να παρακάμψουν την πολιτική αυτή. Αν δηλαδή η Default Domain Policy στο επίπεδο του Domain χαρακτηρισθεί No Override, καμιά πολιτική ΟΜ δεν θα ισχύσει. Στο κάτω αριστερό μέρος της οθόνης σας (το

βλέπετε και στο σχήμα 5.4) υπάρχει η επιλογή **Block Policy Inheritance** (Μπλοκάρισμα της κληρονομημένης πολιτικής). Αν αυτή ενεργοποιηθεί ο θυγατρικός αποδέκτης δεν κληρονομεί καμιά πολιτική από τους γονικούς αποδέκτες. Για παράδειγμα, αν στο σχήμα 5.4 επιλέγει Block Policy Inheritance, τότε «μπλοκάρεται» η γονική πολιτική του Domain sek2.local σε αυτή την περίπτωση. Αν υπάρχει διένεξη των δύο πολιτικών τότε επικρατεί η No Override.

8. Επιλέξτε την πολιτική σας και πατήστε Edit. Να τροποποιήσετε τις καταχωρήσεις, ώστε η οθόνη σας να μοιάζει με αυτή του σχήματος 5.5. Παρατηρήστε ότι υπάρχουν δύο βασικοί κόμβοι:

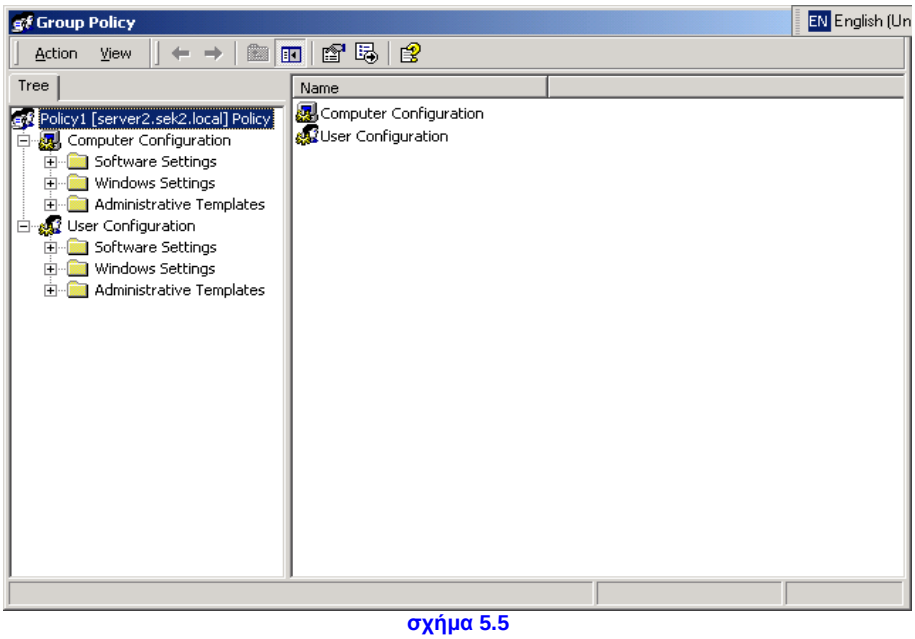
- Computer Configuration (Διευθέτηση Η/Υ) και
- User Configuration (Διευθέτηση χρήστη)

με τις ίδιες επεκτάσεις:

- ✓ Software Settings (Ρυθμίσεις λογισμικού)
- ✓ Windows Settings (Ρυθμίσεις των Windows)
- ✓ Administrative Templates (Διαχειριστικά πρότυπα)

Στον κόμβο Computer Configuration προσαρμόζουμε πολιτικές για τους Η/Υ του δικτύου και αυτές τίθενται σε ισχύ όταν ξεκινά ο Η/Υ και γίνεται εκκίνηση του λειτουργικού συστήματος. Αυτές εφαρμόζονται σε οποιοδήποτε χρήστη που συνδέεται στον Η/Υ.

Στον κόμβο User Configuration προσαρμόζουμε πολιτικές για χρήστες του δικτύου και εφαρμόζονται μόνο όταν οι συγκεκριμένοι χρήστες συνδέονται στο δίκτυο.

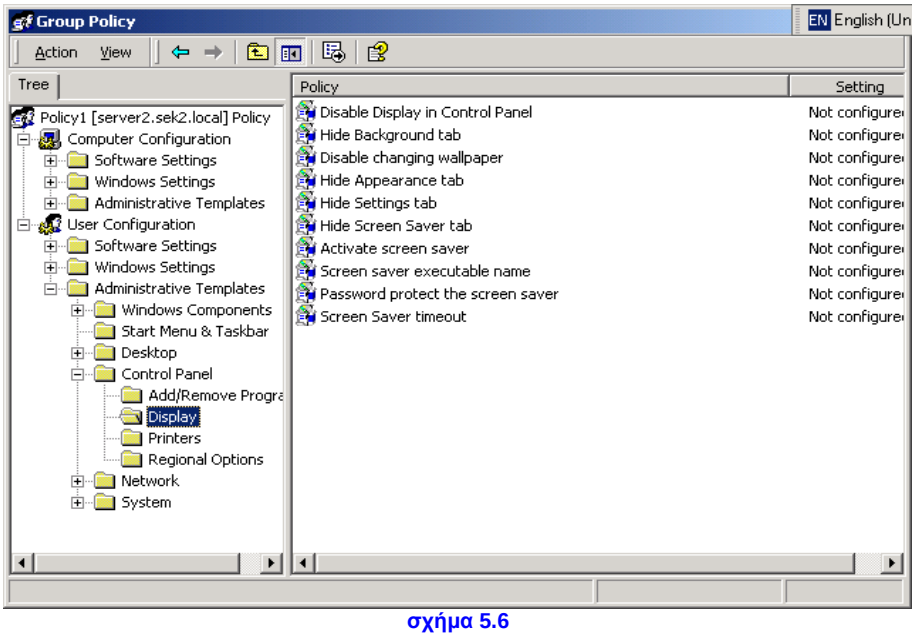


σχήμα 5.5

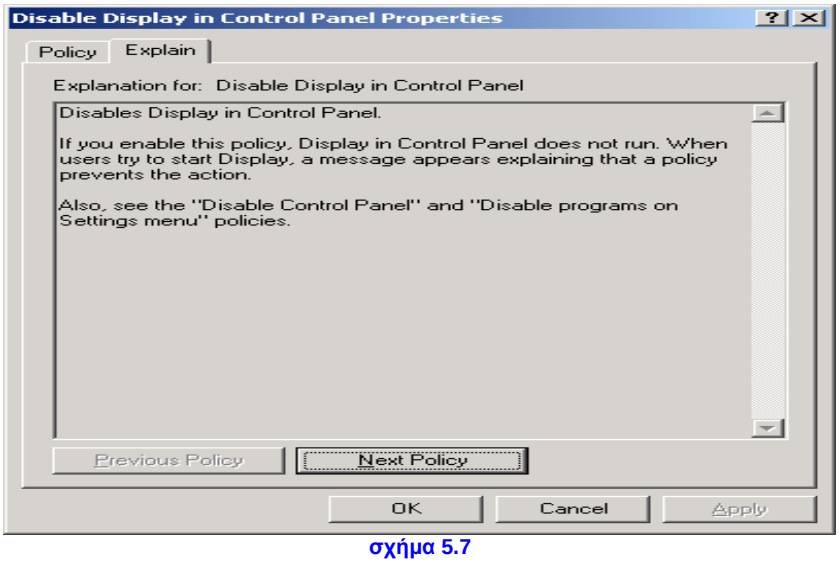
9. Επιλέξτε διαδοχικά User Configuration → Administrative Templates → Control Panel →Display → διπλό κλικ στο Disable Display In Control Panel (σχήμα 5.6). Στην εικόνα που έχετε τώρα μπροστά σας, μπορείτε να δείτε αρχικά κάποιες επεξηγήσεις της συγκεκριμένης ρύθμισης από την καρτέλα Explain (σχήμα 5.7). Στην καρτέλα Policy, οι επιλογές σας είναι τρεις :

- ⇒ Not Configured (που είναι και κληρονομικά επιλεγμένη)
- ⇒ Enable (Ενεργοποίηση της ρύθμισης)
- ⇒ Disable (Απενεργοποίηση της ρύθμισης)

Επιλέξτε Enable και πατήστε OK.



σχήμα 5.6



σχήμα 5.7

10. Συνδεθείτε σε ένα Workstation του Domain με έναν λογαριασμό της ομάδας εργασίας σας (αν ήδη είστε συνδεδεμένοι να κάνετε Log Off και μετά Log On). Δοκιμάστε με δεξί κλικ στην επιφάνεια εργασίας των Windows να αλλάξετε ταπετσαρία. Σχολιάστε το αποτέλεσμα.

11. Να ανοίξετε με τον ίδιο τρόπο την πολιτική του Domain: δεξί κλικ στο Domain → Properties → Group Policy → Default Domain Policy → Edit και να φτάσετε στην ίδια ρύθμιση όπως και στο βήμα 9 (Disable Display In Control Panel). Λογικά θα την βρείτε στην κατάσταση Not Configured. Να την κάνετε Disable και να την εφαρμόσετε. Να επαναλάβετε το προηγούμενο βήμα, και να σχολιάσετε το αποτέλεσμα.

12. Επιλέξτε στην πολιτική του Domain, με δεξί κλικ στο Default Domain Policy την επιλογή No Override. Να επαναλάβετε τα βήματα 8,9,10 και11. Να σχολιάσετε το αποτέλεσμα.

13. Επιλέξτε στην πολιτική της ΟΜ σας την επιλογή Block Policy Inheritance. Να επαναλάβετε τα βήματα 8,9,10 και11. Να σχολιάσετε το αποτέλεσμα.

14. Να αφαιρέσετε την ένδειξη No Override από την Default Domain Policy, και να προσπαθήσετε να ορίσετε τα παρακάτω στην πολιτική της ομάδας σας:

Παρατήρηση:
Όταν κάνετε αλλαγές σε πολιτικές (στον κόμβο User Configuration) αυτές εφαρμόζονται κατά την σύνδεση του χρήστη).

- Να αφαιρέσετε για τους χρήστες σας την επιλογή Run από το Start Menu.
- Να προσθέσετε την επιλογή Log Off στο Start Menu.
- Να αφαιρέσετε την επιλογή Shut Down από το Start Menu.
- Να αφαιρέσετε τον Internet Explorer από το Desktop.
- Να απενεργοποιήσετε μετά το πάτημα των Ctrl + Alt + Delete τις επιλογές Task Manager – Lock Computer – Change Password – Log Off.
- Να απομακρύνετε όλα τα εικονίδια από το Desktop.

15. Ολοκληρώνοντας τα παραπάνω να μεταφέρετε τους λογαριασμούς σας στον αποδέκτη Users και έπειτα να διαγράψετε την Ο.Μ. που δημιουργήσατε στο βήμα 3, για τις ανάγκες αυτής της άσκησης.