ΑΣΚΗΣΗ 4

ΘΕΜΑ : ΔΗΜΙΟΥΡΓΙΑ ΧΡΗΣΤΩΝ ΔΙΚΤΥΟΥ ΙΔΙΟΤΗΤΕΣ ΧΡΗΣΤΩΝ

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

- **Να δημιουργείς χρήστες δικτύου:**
- **Να τους κάνεις μέλη στις κατάλληλες ομάδες**
- **Να ρυθμίζεις τις ιδιότητες τους.**

ΧΡΗΣΙΜΕΣ ΠΛΗΡΟΦΟΡΙΕΣ – ΕΛΑΧΙΣΤΕΣ ΑΠΑΙΤΟΥΜΕΝΕΣ ΓΝΩΣΕΙΣ

Πριν πραγματοποιήσεις αυτή την άσκηση θα πρέπει να γνωρίζεις :

- ✓ Τις διαφορές μεταξύ τοπικών και δικτυακών χρηστών.
- ✓ Γενικά που και πως δημιουργείται ένας νέος λογαριασμός δικτυακού χρήστη και την περιοχή λειτουργίας του.
- ✓ Τα βασικά χαρακτηριστικά των ήδη δημιουργημένων ομάδων χρηστών στα Windows 2012 Server.
- ✓ Το εργαλείο Active Directory Users and Computers.

ΠΟΡΕΙΑ ΕΡΓΑΣΙΑΣ

1. Αφού έχετε δημιουργήσει το δίκτυο και έχετε κάνει μέλη του τους Η/Υ που πρέπει, ένα από τα πρώτα καθήκοντά σας, ως διαχειριστές δικτύου, είναι να δημιουργήσετε τους λογαριασμούς των χρηστών που θα δουλεύουν σε αυτό το δίκτυο. Για να το δούμε διαφορετικά, σκεφτείτε το ως εξής:

   Η εταιρεία ΕΚ4PER στεγάζεται σε ένα πενταόροφο κτίριο και εσείς αναλάβατε την εγκατάσταση αρχικά και έπειτα την διαχείριση και την συντήρηση του δικτύου της. Έτσι λοιπόν δημιουργήσατε το ομώνυμο Domain στον Domain Controller της (Server) και έπειτα πήγατε στα διάφορα γραφεία της και εντάξατε όλους τους Η/Υ της στο Domain ΕΚ4PER, με τον τρόπο που είδαμε στις προηγούμενες ασκήσεις. Τώρα έχετε παραλάβει μια λίστα με τα ονόματα των υπαλλήλων της εταιρείας και την ιδιότητα του καθενός καθώς και τα επιμέρους τμήματα της εταιρείας που είναι:

   Πωλήσεις – Μάρκετινγκ – Λογιστήριο – Διοίκηση - Τεχνικό τμήμα.

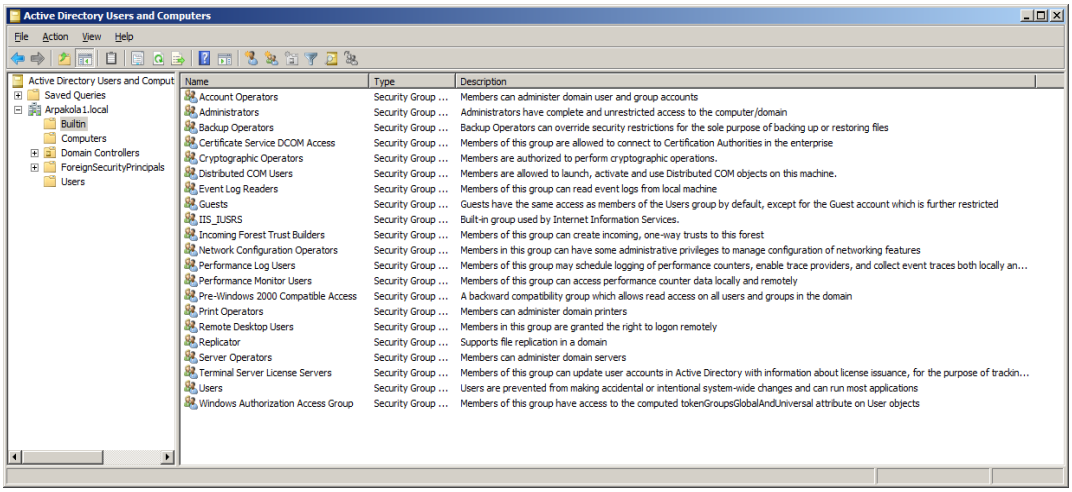
   Τώρα πρέπει να δημιουργήσετε ένα ατομικό λογαριασμό για τον κάθε υπάλληλο της εταιρείας, ώστε να μπορεί να χρησιμοποιεί τους πόρους του δικτύου αλλά και να ελέγχεται κεντρικά για την χρήση αυτή, ανάλογα με την ιδιότητά του μέσα στην εταιρεία και πιθανά με την πολιτική της εταιρείας σε αυτά τα θέματα. Υπάρχει περίπτωση η ΕΚ4PER σε αντίθεση με το όνομά της να τηρεί μια αυστηρή στάση σε τέτοια ζητήματα, όπως για παράδειγμα να μην μπορεί κανείς υπάλληλος ή κάποιοι υπάλληλοι να συνδέονται στο δίκτυο πέρα από το ωράριο εργασίας τους ή πιο απλά να μην μπορούν να

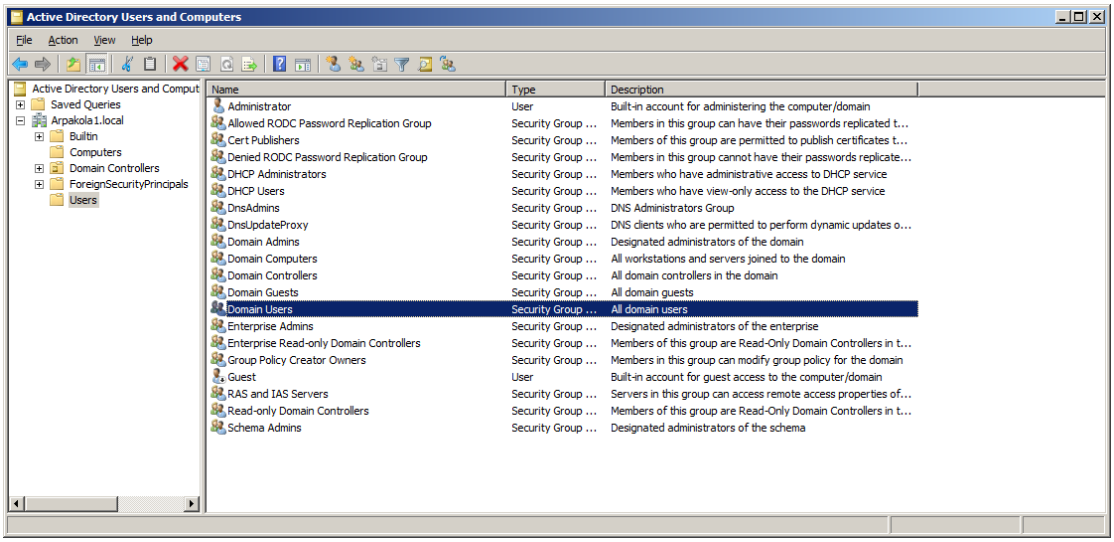
κάνουν εκτυπώσεις ή οτιδήποτε άλλο. Εμείς από την πλευρά μας θα πρέπει να γνωρίζουμε τις δυνατότητες των Server (των 2012 Server εδώ), για να μπορούμε να υλοποιούμε σε κάθε περίπτωση τα ζητούμενα. Ίσως αντιλαμβάνεστε τώρα ότι είναι σημαντικό να σχεδιάσετε αρχικά την τακτική σας σε αυτό το θέμα, για να μην αναγκαστείτε εκ των υστέρων σε τροποποιήσεις ή και διαγραφές χρηστών. Στη συγκεκριμένη περίπτωση της εταιρείας EK4PER, με τα πέντε διακριτά τμήματα υπαλλήλων, καλό θα ήταν να δημιουργήσετε πέντε ομάδες (Groups) χρηστών ή ακόμα καλύτερα πέντε οργανωτικές μονάδες (Organizational Units) χρηστών. Τις έννοιες Ομάδας και Οργανωτικής Μονάδας, θα τις δούμε σε άλλο σημείο.

Είναι πιθανό να δημιουργηθούν κάποια ερωτήματα κατά την διάρκεια της εκτέλεσης αυτής της άσκησης, που θα οφείλονται σε κάποια «κενά» θεωρητικών γνώσεων σχετικά με την δομή των Windows 2012 Server. Είναι σίγουρο όμως, ότι αυτά δεν μπορούν άμεσα να καλυφθούν, αλλά θα αρχίσετε σταδιακά να κατανοείτε τις σχετικές έννοιες, κατά την διάρκεια εκτέλεσης των επόμενων ασκήσεων.

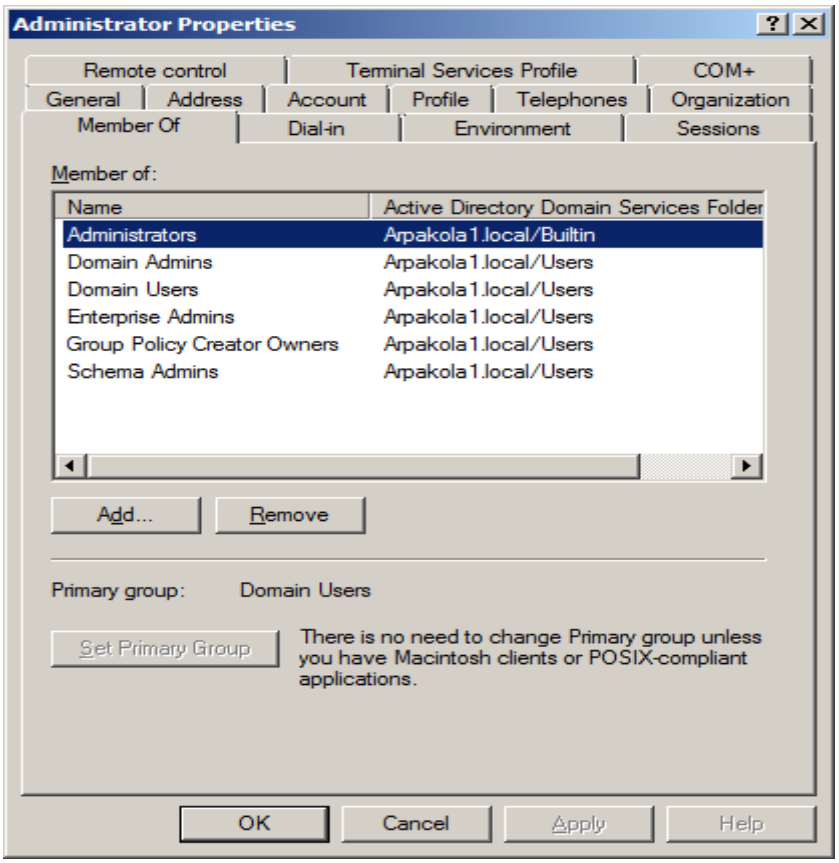
Τα βασικά σημεία που πρέπει να κατανοήσετε πριν εκτελέσετε την άσκηση είναι τα εξής:

Οι λογαριασμοί χρηστών δικτύου δημιουργούνται **μόνο** στον Server του Domain και με χρήση ενός λογαριασμού επιπέδου Administrator ή κάποιου λογαριασμού που έχει την δυνατότητα αυτή (περισσότερα για το θέμα αυτό θα δούμε σε παρακάτω άσκηση). Για τον λόγο αυτό, την άσκηση θα την πραγματοποιήσετε στους Η/Υ που εκτελούν χρέη Server δικτύου που διαθέτει το εργαστήριο σας. Πρέπει να γνωρίζετε ότι οι χρήστες του δικτύου που θα δημιουργήσετε είναι χρήστες περιοχής (Domain Users) με περιορισμένα δικαιώματα (μόνο αυτά που διαθέτει η ομάδα τους). Για λόγους ασφάλειας ο κάθε αρχικός χρήστης τοποθετείται σε αυτή την ομάδα. Ήδη πρέπει να αντιληφθήκατε ότι υπάρχουν κάποιες αρχικές ομάδες χρηστών (και Η/Υ) του συστήματος. Αυτές δημιουργήθηκαν κατά την εγκατάσταση του AD DS και είναι απαραίτητες για την λειτουργία του Server.





Στο παραπάνω σχήμα εκτός του λογαριασμού του αρχικού Administrator και του αρχικά απενεργοποιημένου λογαριασμού Guest (για λόγους ασφάλειας), οι υπόλοιπες είναι οι αρχικές ομάδες του συστήματος. Ο κάθε λογαριασμός μπορεί να ανήκει σε περισσότερες από μία ομάδες, όπως για παράδειγμα ο αρχικός administrator (κοίτα την παρακάτω εικόνα).



Σε κάθε περίπτωση ο κάθε νέος δικτυακός χρήστης είναι μέλος μόνο της ομάδας Domain Users και στη συνέχεια μπορούμε αν το κρίνουμε σωστό να τον κάνουμε μέλος και σε άλλες ομάδες. Για παράδειγμα αν και οι χρήστες δημιουργούνται στον Server του δικτύου, δεν έχουν δικαίωμα σύνδεσης σε αυτόν αλλά μόνο στους σταθμούς εργασίας που αυτός

ελέγχει στο Domain του. Για να μπορέσουν να συνδεθούν στον Server, όπως θα δούμε στην πορεία των ασκήσεων θα πρέπει να γίνουν μέλη της ομάδας Server Operators. Με άλλα λόγια το τι μπορεί και το τι δεν μπορεί να κάνει ένας χρήστης εξαρτάται από δύο παράγοντες:

- ❖ Σε ποια ομάδα χρηστών από τις ενσωματωμένες των Windows 2012 Server ανήκει.
- ❖ Τι ορίζει η πολιτική ομάδας που δημιούργησε ο Administrator (αν έχει δημιουργήσει). Την πολιτική (Policy) του δικτύου θα την δούμε παρακάτω.

Ας δούμε τώρα κάποια βασικά σημεία για τις ομάδες χρηστών.

Σε γενικές γραμμές μια ομάδα χρηστών είναι συνήθως μια συλλογή χρηστών ενός δικτύου υπολογιστών. Στόχος της ύπαρξης των ομάδων είναι να απλοποιήσουν την διαχείριση, επιτρέποντας στον διαχειριστή να δίνει δικαιώματα και άδειες ή γενικά να εφαρμόζει πολιτικές, σε ομάδες και όχι σε μεμονωμένους χρήστες.

Σε πολύ γενικές γραμμές μπορούμε να κάνουμε με διάφορα κριτήρια τις εξής κατηγοριοποιήσεις:

- Στα WINDOWS 2012 Server υπάρχουν γενικά δύο τύποι ομάδων :
- ➢ οι ομάδες ασφαλείας (security groups) και
- ➢ οι ομάδες διανομής (distribution groups).

Βασικά όμως οι ομάδες ασφαλείας είναι οι μόνες που μπορούν να πάρουν άδειες αλλά και να χρησιμοποιηθούν και για άλλους σκοπούς (όπως η ομαδική αποστολή email).

- Ένα άλλο χαρακτηριστικό που διακρίνει τις ομάδες είναι η **εμβέλεια** τους και με βάση το κριτήριο αυτό υπάρχουν τρεις κατηγορίες ομάδων :

❑ ***Οι Τοπικές Ομάδες Περιοχής (Local Domain Group).*** Οι άδειες που δίνονται σε αυτές τις ομάδες, αφορούν **μόνο** πόρους της περιοχής τους. Τα μέλη όμως της ομάδας μπορεί να προέρχονται από **οποιαδήποτε** περιοχή.

❑ ***Οι Ομάδες Καθολικής Εμβέλειας (Global Scope Group).*** Τα μέλη αυτής της κατηγορίας προέρχονται **μόνο** από την περιοχή δημιουργίας της ομάδας ενώ άδειες στις ομάδες αυτές μπορούν να αποδοθούν για πόρους **οποιασδήποτε** περιοχής.

❑ ***Οι Οικουμενικές Ομάδες Ασφάλειας (Universal Security Group).*** Τα μέλη της ομάδας αυτής μπορεί να προέρχονται από **οποιαδήποτε** περιοχή και να δοθούν άδειες σε αυτά για πόρους **οποιασδήποτε** περιοχής.

- Όπως όμως ήδη αναφέραμε υπάρχουν και οι ενσωματωμένες ομάδες των Windows 2012 Server.

Και στην περίπτωση αυτή υπάρχει μια κατηγοριοποίηση:

➢ Σε ομάδες που έχουν ως μέλη διαχειριστές **(administrators)** του δικτύου. Κάθε τύπος Administrator έχει αυξημένη έως πλήρη πρόσβαση στους πόρους του δικτύου. Γενικά η ιδιότητα μέλους της ομάδας Administrator δεν πρέπει να παρέχεται εύκολα σε χρήστες δικτύου. Οι βασικές ομάδες διαχείρισης είναι:

- ✓ **Domain Administrators** (Διαχειριστές περιοχής).

- ✓ **Enterprise Administrators** (Διαχειριστές επιχείρησης).
- ✓ **Schema Administrators** (Διαχειριστές Σχήματος).

Οι λογαριασμοί Administrators δίνουν την δυνατότητα σύνδεσης και διαχείρισης σε τοπικούς Η/Υ του δικτύου. Όταν συνδεθούν στον ελεγκτή περιοχής (1ο Server) εκτελούν διαχείριση περιοχής (Domain Administrators). Σε δίκτυα με περισσότερες από μία περιοχές οι λογαριασμοί της ομάδας Enterprise Administrators εκτελούν διαχείριση όλων των περιοχών. Τέλος οι διαχειριστές σχήματος κάνουν διαχείριση στο σύνολο των δασών (Forest) που αποτελούν ένα σχήμα.

➢ Σε ομάδες που έχουν ως μέλη χειριστές **(operators)** του δικτύου. Σε αυτούς παραχωρούνται συγκεκριμένα προνόμια που θα τους βοηθήσουν στην εκτέλεση συγκεκριμένων διαχειριστικών εργασιών. Τέτοιες ομάδες είναι:

- ✓ **Account Operators** (Χειριστές λογαριασμών). Τα μέλη της ομάδας αυτής έχουν προνόμια (περιορισμένα) δημιουργίας λογαριασμών. Έχουν δικαίωμα σύνδεσης στον ελεγκτή περιοχής, μπορούν να δημιουργούν λογαριασμούς χρηστών περιοχής (domain user), αλλά όχι και να τροποποιούν τα δικαιώματα τους. Επίσης δεν μπορούν να δημιουργήσουν λογαριασμούς τύπου Operator και Administrator.
- ✓ **Backup Operators** (Χειριστές αντιγράφων ασφαλείας). Όπως δηλώνει η ονομασία της ομάδας αυτής, τα μέλη της μπορούν να πάρουν αντίγραφα ασφαλείας φακέλων ή αρχείων από Η/Υ του δικτύου, αλλά και να επαναφέρουν τα αρχεία αυτά.
- ✓ **Print Operators** (Χειριστές εκτυπωτών). Τα μέλη της ομάδας αυτής μπορούν να εγκαθιστούν κοινόχρηστους εκτυπωτές στο δίκτυο (ή να διακόπτουν την κοινοχρησία) και να χορηγούν ή να αφαιρούν δικαιώματα εκτύπωσης στους χρήστες.
- ✓ **Server Operators** (Χειριστές Διακομιστών). Τα μέλη της ομάδας αυτής έχουν δικαίωμα σύνδεσης στον Server της περιοχής τους και να εκτελούν βασικές διαχειριστικές εργασίες.

➢ Σε ομάδες που χρησιμοποιούνται από χρήστες **(users)** του δικτύου

- ✓ **Domain Users** (Χρήστες περιοχής). Συνήθως περιορίζονται μόνο στον Η/Υ που εργάζονται, χωρίς δικαίωμα σύνδεσης σε άλλο Η/Υ του δικτύου. ΄Έχουν μάλλον περισσότερους περιορισμούς παρά προνόμια (σκεφτείτε ότι δεν μπορούν ούτε να αλλάξουν την ώρα στον Η/Υ τους). Τέτοιοι είναι οι λογαριασμοί που δημιουργήσατε.
- ✓ **Domain Guest** (Επισκέπτες περιοχής). Οι λογαριασμοί αυτοί σπάνια χρησιμοποιούνται λόγω των πολλών περιορισμών της ομάδας αυτής.

➢ Τέλος υπάρχει η δυνατότητα δημιουργίας ομάδων χρηστών από τον Administrator, οι οποίες είναι προσαρμοσμένες στα χαρακτηριστικά του εκάστοτε δικτύου. Για παράδειγμα ο Administrator ενός εταιρικού δικτύου θα μπορούσε να δημιουργήσει μια ομάδα χρηστών που αφορά τους υπαλλήλους του τμήματος πωλήσεων, μια άλλη για τους υπαλλήλους του διαφημιστικού τμήματος, μια για το λογιστήριο κοκ. Αυτό θα τον διευκολύνει πιθανά στην διαχείριση του συνολικού δικτύου. Σε κάθε περίπτωση οι «χειροποίητες» ομάδες που δημιουργούνται από τον Administrator μπορούν όπως θα δείτε στην εκτέλεση της άσκησης να συνδυαστούν με τις ενσωματωμένες ομάδες των Windows 2012 Server και οι χρήστες τους να αποκτήσουν μαζικά τις ιδιότητες και τα δικαιώματα της ενσωματωμένης ομάδας. Κάθε τύπος αυτών των ομάδων έχει ένα

προκαθορισμένο σύνολο δικαιωμάτων χρηστών. Υπάρχει οπότε η δυνατότητα κάθε χρήστης που τοποθετείται σε μία από αυτές τις ομάδες να αποκτά αυτόματα αυτά τα δικαιώματα.

ΠΟΡΕΙΑ ΕΡΓΑΣΙΑΣ

Α. ΔΗΜΙΟΥΡΓΙΑ ΧΡΗΣΤΩΝ ΔΙΚΤΥΟΥ

1. Να ελέγξετε την επικοινωνία των Η/Υ του δικτύου σας και να την αποκαταστήσετε αν χρειάζεται. (Start → Network).

2. Αφού συνδεθείτε στον Server του δικτύου με έναν λογαριασμό Administrator, θα πραγματοποιήσετε τα παρακάτω βήματα.

3. Από Start → Administrative Tools → Active Directory Users and Computers.

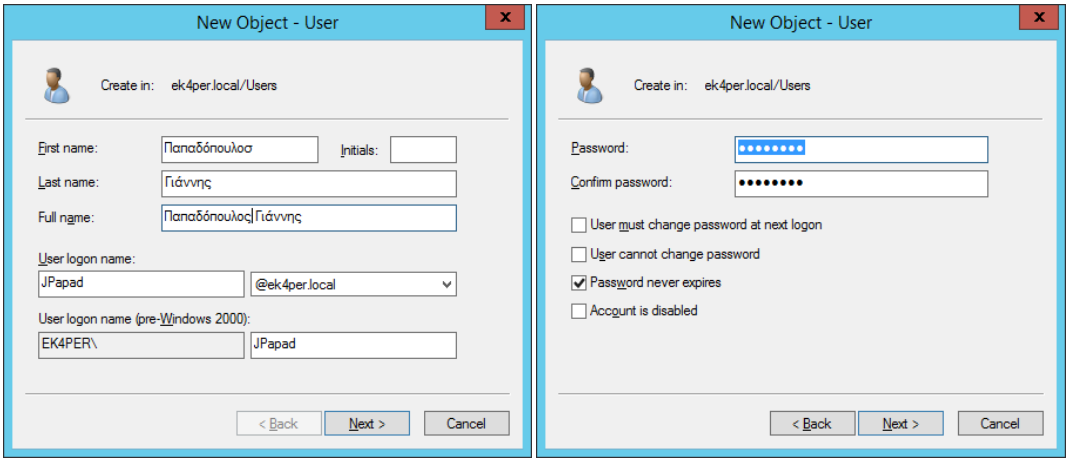
4. Επιλέξτε την περιοχή του δικτύου σας (είναι EK4PER.local) και έπειτα τον αποδέκτη (Container) Users. Με δεξί κλικ επιλέξτε New User.

5. Να δώσετε τα ζητούμενα στοιχεία όπου :

First Name : το μικρό σας όνομα.

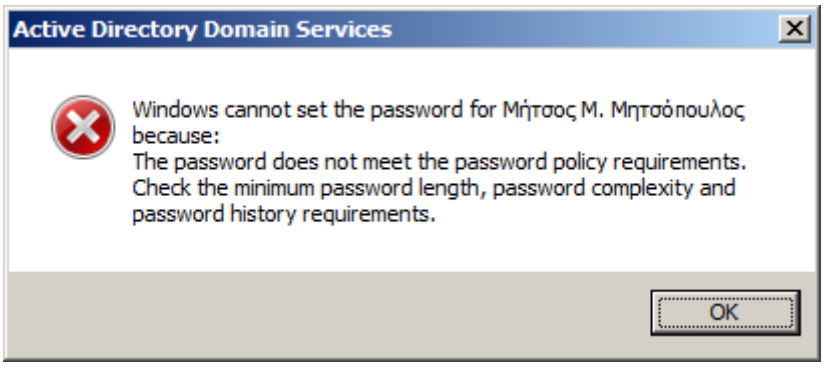
Last Name : το επίθετό σας

User Logon Name : θα δώσετε το επίθετο σας (αγγλικά).



Password : να το επιλέξετε εσείς. Προσέξτε σε αυτό το σημείο, γιατί η αρχική πολιτική ασφάλειας προβλέπει για τους κωδικούς κάποια ελάχιστα απαιτούμενα για να είναι αποδεκτοί. Χρησιμοποιήστε πεζά και κεφαλαία γράμματα μαζί με αριθμούς και σημεία στίξης. Το ελάχιστο αποδεκτό μήκος κωδικού είναι 7 χαρακτήρες. Μια καλή πρακτική είναι να επιλέγετε μια λέξη και να αντικαθιστάτε τα «προφανή» γράμματα με σημεία στίξης ή και αριθμούς. Για παράδειγμα στον χρήστη που είδατε στις εικόνες παραπάνω δόθηκε ο κωδικός της λέξης Μητσάκος, η οποία όμως έγινε M1ts@k0$. Αν

δεν ακολουθήσετε τον κανόνα, θα δείτε ένα προειδοποιητικό μήνυμα και ο χρήστης δεν θα δημιουργηθεί.



Στα παράθυρα ιδιοτήτων που ακολουθούν να κάνετε τις επιλογές όπως περιγράφονται παρακάτω και φαίνονται στο σχήμα παραπάνω:

- **User must change password at next logon** (Ο χρήστης πρέπει να αλλάξει κωδικό στην επόμενη σύνδεση του).

Δεν το ενεργοποιείτε.

- **User cannot change password** (Ο χρήστης δεν μπορεί να αλλάξει τον κωδικό του).

Δεν το ενεργοποιείτε.

- **Password never expires** (Ο κωδικός δεν λήγει ποτέ).

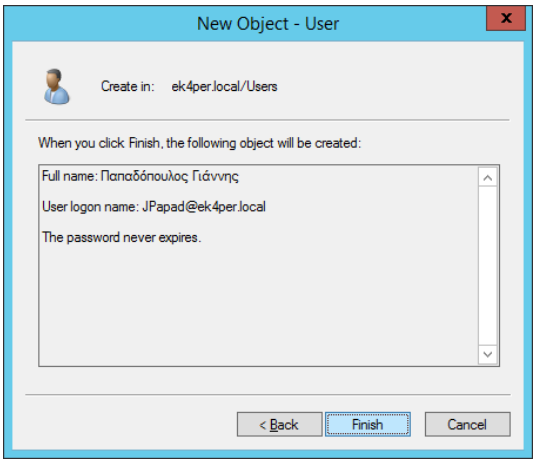
Το ενεργοποιείτε.

- **Account is disabled** (Ο λογαριασμός είναι απενεργοποιημένος).

Δεν το ενεργοποιείτε.

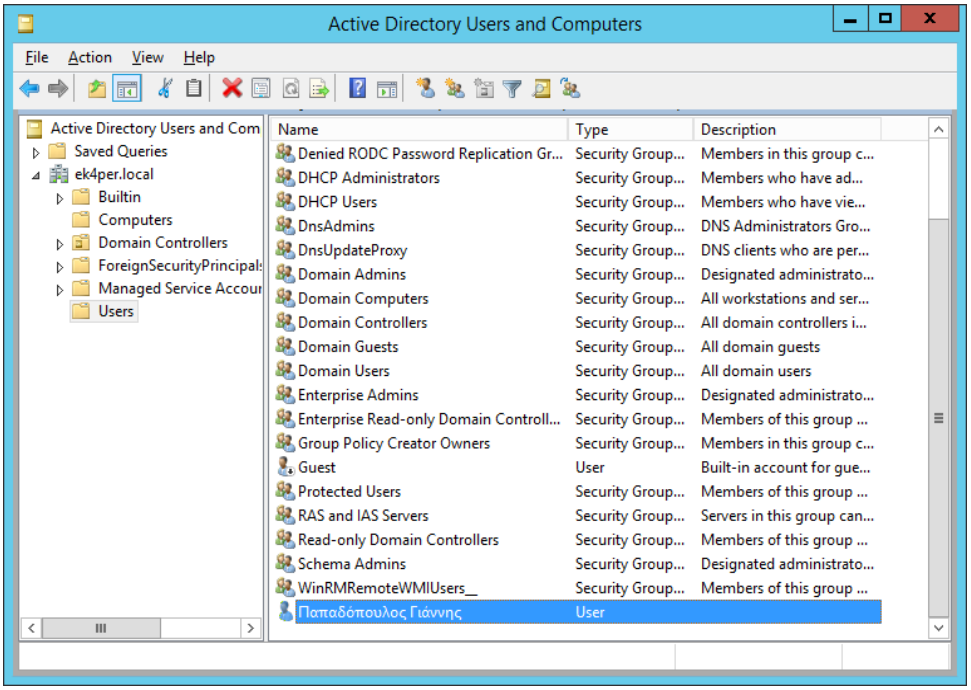
Κλικ στο Next.

Εδώ βλέπετε συγκεντρωμένες τις βασικές ιδιότητες του λογαριασμού σας.

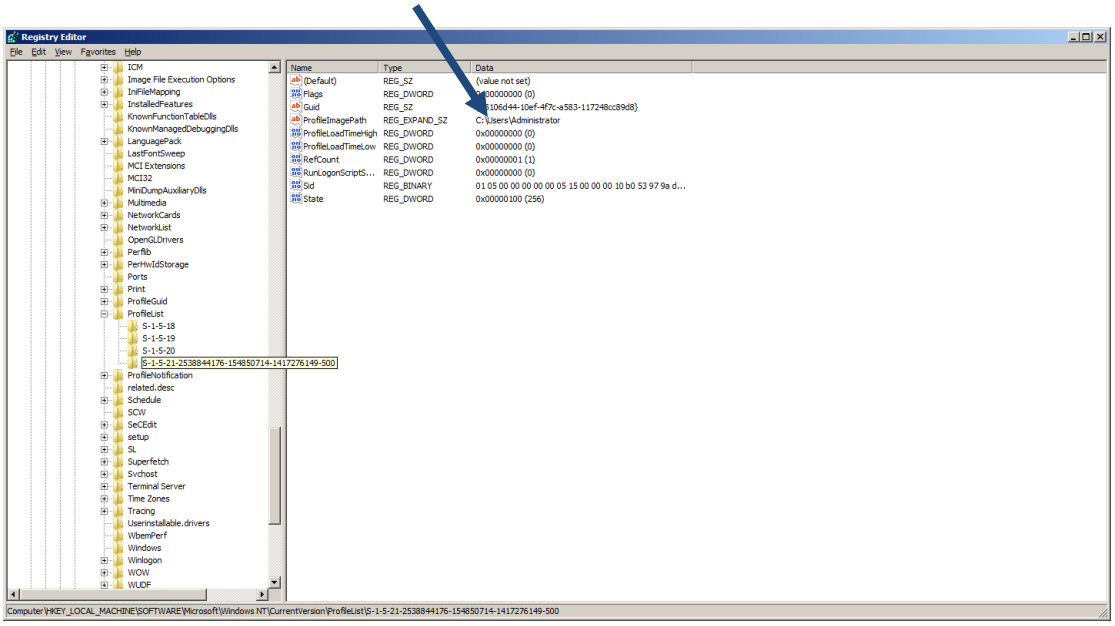


Αν δεν χρειάζεται κάποια διόρθωση να κάνετε κλικ στο Finish. Σε αντίθετη περίπτωση να κάνετε κλικ στο Back και να κάνετε τις απαραίτητες διορθώσεις.

Να ελέγξετε στην λίστα των χρηστών αν εμφανίζεται ο λογαριασμός σας.



6. Αξίζει να δούμε λίγο τι γίνεται στα Windows όταν δημιουργείται ένας νέος χρήστης. Κάθε φορά που δημιουργείται ένας νέος χρήστης τα Windows του αποδίδουν έναν μοναδικό **αναγνωριστικό ασφάλειας** (**S**ecurity **Id**entifier – **SID**). Αυτό το αναγνωριστικό θα συνοδεύει από εδώ και πέρα τον χρήστη, με τις όποιες μεταβολές του. Ανοίξτε το μητρώο των Windows 2012 Server (από Start → πληκτρολογήστε **regedit**) και διαδοχικά ανοίξτε τις καταχωρήσεις HKEY_ LOCAL_MACHINE →SOFTWARE → Microsoft →Windows NT → CurrentVersion→ ProfileList. Εδώ βλέπετε τα SID που ήδη υπάρχουν. Τα τρία πρώτα είναι τα βασικά προϋπάρχοντα (ένα για τοπικούς χρήστες, ένα για δικτυακούς και ένα του συστήματος), ενώ το τέταρτο και μεγαλύτερο είναι το SID του Administrator, του μοναδικού μέχρι στιγμής χρήστη.



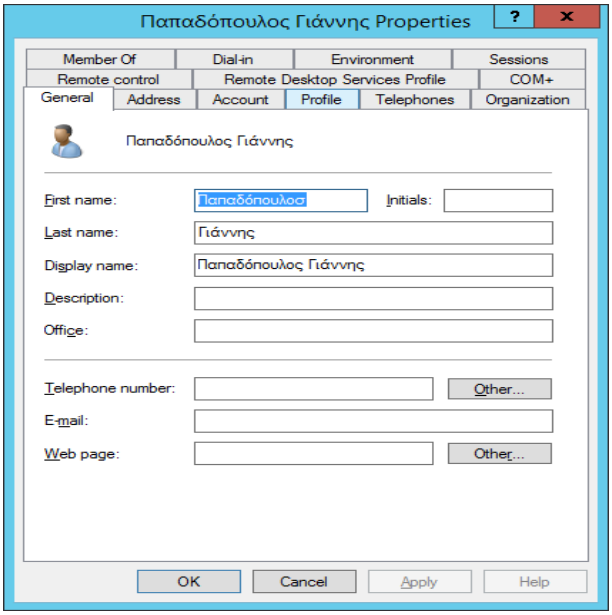
Το SID είναι αυτό που ακολουθεί σε όλο το δίκτυο τον κάθε χρήστη και καθορίζει την πρόσβασή του στους πόρους του δικτύου αλλά και τους περιορισμούς που του έχουν επιβληθεί . Όταν διαγράφεται ένας χρήστης, διαγράφεται και το SID του, γι αυτό μια συνηθισμένη τακτική που ακολουθούμε στις εταιρείες σε περίπτωση που φύγει ένας υπάλληλος και αντικαθίσταται από άλλον είναι η εξής: Αν διαγραφεί ο λογαριασμός του παλιού υπάλληλου, διαγράφεται μαζί με το SID του και όλο το πακέτο δυνατοτήτων, προσβάσεων και περιορισμών του υπαλλήλου. Ακόμα και αν φτιάξουμε πάλι τον ίδιο λογαριασμό, επειδή αποδίδεται σε αυτόν νέο SID, όλα αυτά πρέπει να επαναπροσδιοριστούν. Έτσι απλά ο παλιός λογαριασμός απενεργοποιείται και γίνεται μετονομασία για τον νέο υπάλληλο.

7. Τελικά θα πρέπει όλοι να δημιουργήσετε ένα λογαριασμό δικτυακού χρήστη. Να δοκιμάσετε να συνδεθείτε με τον λογαριασμό σας στον Η/Υ που τον δημιουργήσατε αλλά και σε έναν οποιοδήποτε άλλο Η/Υ που ανήκει στο ίδιο Domain. Σχολιάστε το αποτέλεσμα αυτού του βήματος.

Β. ΙΔΙΟΤΗΤΕΣ ΛΟΓΑΡΙΑΣΜΩΝ ΧΡΗΣΤΩΝ ΔΙΚΤΥΟΥ

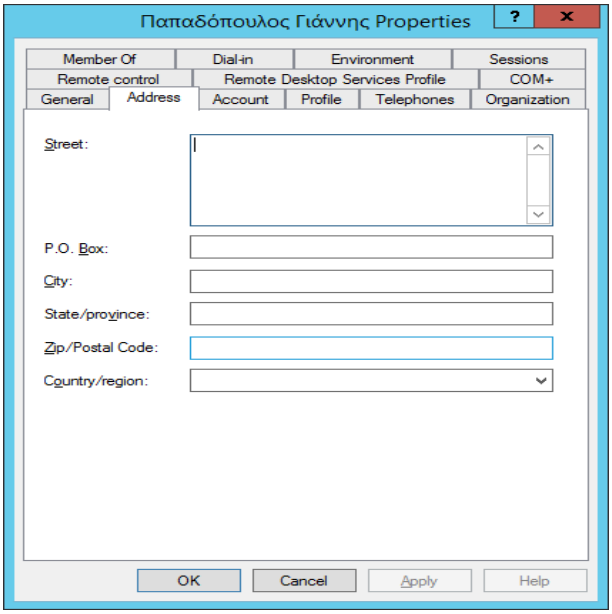
Έχουμε πλέον δημιουργήσει τους δικτυακούς χρήστες που χρειάζονται για το προσωπικό της εταιρείας. Είδατε ότι η διαδικασία έγινε μέσα στον Ενεργό Κατάλογο. Για να χρησιμοποιήσετε τις δυνατότητες που προσφέρει ο Ενεργός Κατάλογος, θα πρέπει να συμπληρώσετε ή να ρυθμίσετε τις ιδιότητες των χρηστών. Πηγαίνετε λοιπόν μέσα από το εργαλείο Administrative Tools και κάνετε δεξί κλικ →Properties για να δούμε τις βασικές ιδιότητες:

1. Η κάρτα **General**



Αυτή είναι η κάρτα γενικών πληροφοριών του κάθε χρήστη. Τα πεδία δεν απαιτούν κάποια ιδιαίτερη εξήγηση, αλλά η συμπλήρωσή τους θα φανεί ιδιαίτερα χρήσιμη για την διαχείριση του δικτύου, όταν θελήσετε να στείλετε email στους χρήστες ή όταν αναζητήσετε μέσα από τον Ενεργό Κατάλογο μια κατηγορία χρηστών, πχ όσους εργάζονται στον 1ο όροφο της εταιρείας, ή τους υπάλληλους του Λογιστηρίου για οποιοδήποτε λόγο. Να συμπληρώσετε τα πεδία αυτά.

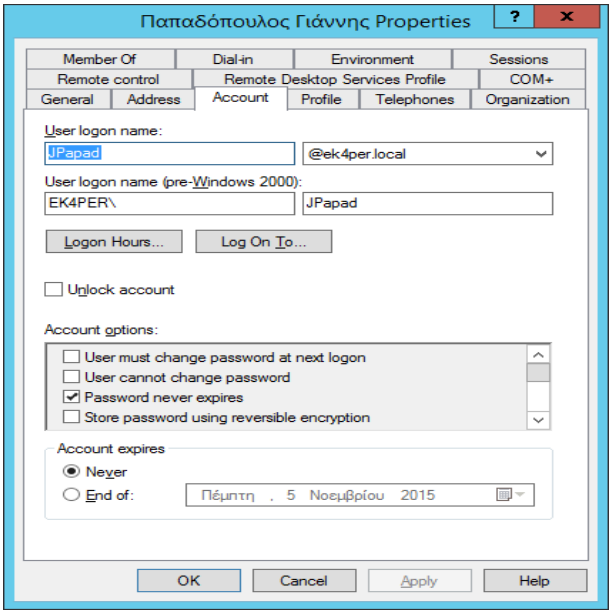
2. Η κάρτα **Address**



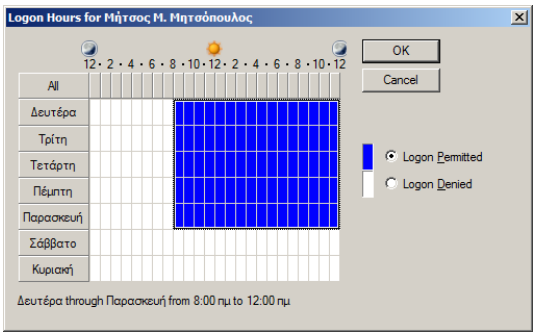
Στις περισσότερες περιπτώσεις δεν χρειάζεται να συμπληρωθεί. Βρίσκει χρήση περισσότερο σε ιντερνετικά δίκτυα εταιρειών που έχουν παραρτήματα σε διάφορες πόλεις ή χώρες και στα πεδία αυτά συμπληρώνονται τα τοπικά στοιχεία κάθε παραρτήματος.

Αφήστε την κενή.

3. Η κάρτα **Account**



Η πρώτη επιλογή αυτής της κάρτας είναι το όνομα σύνδεσης που μπορεί να αλλάξει σε κάποιο άλλο. Ακολουθεί η επιλογή Logon Hours, στην οποία μπορείτε να ορίσετε τις επιτρεπτές εβδομαδιαίες ώρες σύνδεσης στο δίκτυο για τον χρήστη αυτόν.



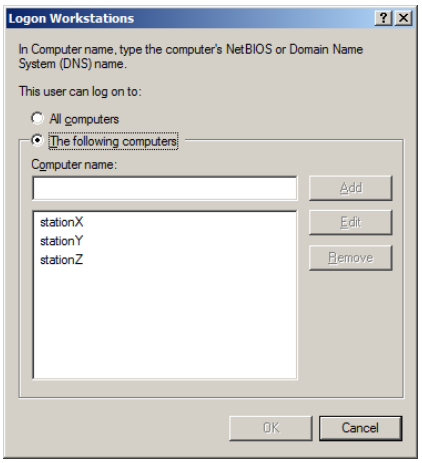
Ένα πρώτο ερώτημα είναι τι θα συμβεί αν ο χρήστης είναι ήδη συνδεδεμένος στο δίκτυο και παρέλθει η επιτρεπτή ώρα σύνδεσης. Μπορεί τότε να συμβούν τα εξής δύο πράγματα:

- ✓ Ο χρήστης να συνεχίσει να εργάζεται αλλά αν χρειαστεί νέα σύνδεση στο δίκτυο δεν θα γίνει. Αυτή είναι η αρχικά προσαρμοσμένη ρύθμιση των Windows 2012 Server.
- ✓ Ο χρήστης αποσυνδέεται αναγκαστικά. Αυτό θα συμβεί μόνο μετά από κατάλληλη ρύθμιση της πολιτικής του δικτύου (Domain Policy), όπως θα δούμε παρακάτω, από τον διαχειριστή του δικτύου.

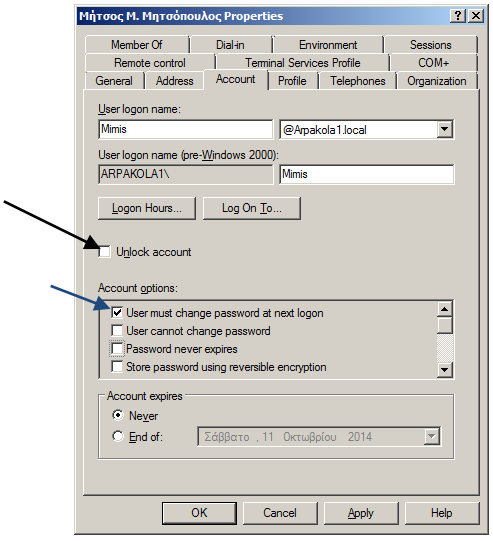
Ρυθμίστε τους λογαριασμούς σας για επιτρεπτές ώρες σύνδεσης αυτές του μαθήματος εκτός από έναν που θα τον ρυθμίσετε για απαγόρευση τις ώρες αυτές. Δοκιμάστε να συνδεθείτε με αυτόν σε ένα σταθμό εργασίας και παρατηρήστε το μήνυμα που εμφανίζεται.

Ακολουθεί η επιλογή Log On To… Εδώ ανάλογα με την περίπτωση μπορείτε να αφήσετε την προεπιλογή να συνδέεται ο χρήστης στο δίκτυο από όλους τους Η/Υ του δικτύου ή να τον περιορίσετε να συνδέεται στο δίκτυο από κάποιον ή κάποιους Η/Υ (πιθανά τους Η/Υ

του τμήματός του μόνο). Αυτό μπορεί να είναι η επιθυμία της εταιρείας αλλά ταυτόχρονα αυξάνει και την ασφάλεια του δικτύου.



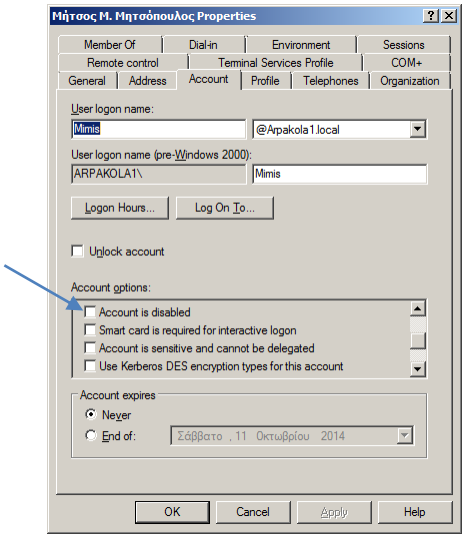
Πάμε τώρα να δούμε τις υπόλοιπες επιλογές στο κάτω μέρος της καρτέλας Account :



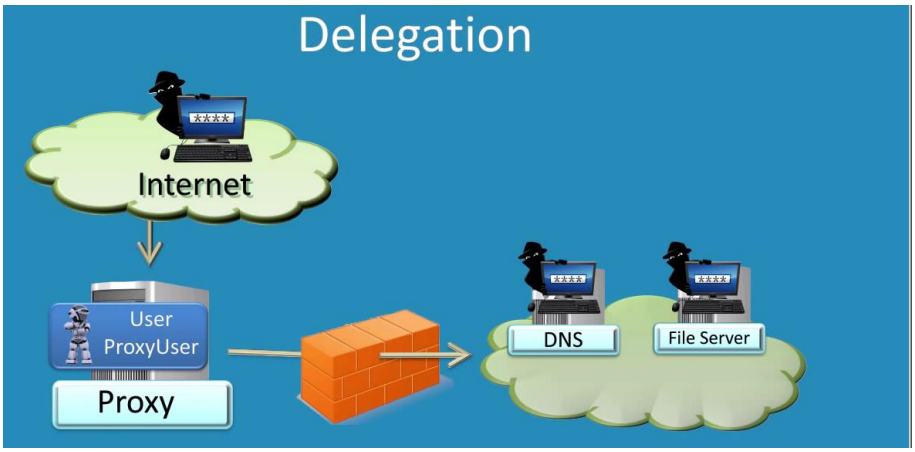
- Το check button **Unlock account** το χρησιμοποιείτε για να ξεκλειδώσετε τον χρήστη που έχει κλειδωθεί εκτός δικτύου. Αυτό μπορεί να συμβεί μετά από κάποιο αριθμό αποτυχημένων προσπαθειών σύνδεσης του χρήστη, λόγω λανθασμένης εισαγωγής του Username ή του Password του χρήστη. Υπάρχει ανάλογη ρύθμιση της πολιτικής του δικτύου όπως θα δούμε (Domain Policy), που ορίζει πόσες θα είναι αυτές οι προσπάθειες αλλά και για πόσο χρόνο θα κλειδωθεί εκτός δικτύου ο χρήστης. Όταν συμβεί κάτι τέτοιο, εσείς ως διαχειριστές μπορείτε με αυτή την επιλογή να τον ξεκλειδώσετε άμεσα.
  - **User must change password at next logon.** Η επιλογή αυτή αναγκάζει τους χρήστες να αλλάξουν τον κωδικό τους στην επόμενη σύνδεση τους στο δίκτυο (θα δουν αναγκαστική προτροπή).
  - **User cannot change password.** Η επιλογή αυτή αφαιρεί από τον χρήστη την δυνατότητα να αλλάξει τον κωδικό του.
  - **Password never expires.** Σε δίκτυα με μεγάλο αριθμό χρηστών που συνδυάζονται με έντονη κινητικότητα υπαλλήλων, υπάρχει ο κίνδυνος συσσώρευσης «νεκρών»

λογαριασμών. Για το λόγο αυτό η πολιτική των Windows 2012 Server ορίζει με την δημιουργία κάθε νέου χρήστη αυτόματα και την διάρκεια ζωής του που είναι 30 ημέρες. Αν δεν κάνουμε κάτι εμείς ως διαχειριστές, οι χρήστες θα λαμβάνουν τις τελευταίες ημέρες, κατά την σύνδεσή τους μήνυμα ότι σε Χ ημέρες ο λογαριασμός τους θα λήξει και αυτό πραγματικά θα γίνει. Ενεργοποιώντας αυτή την επιλογή ο λογαριασμός τους δεν θα λήξει ποτέ, αλλά θα πρέπει να μεριμνήσουμε να μην συμβεί τελικά αυτή η συσσώρευση «νεκρών» λογαριασμών.

- **Store Password Using Reversible Encryption.** Η επιλογή αυτή προκαλεί την αποθήκευση του κωδικού ως απλό κρυπτογραφημένο κείμενο.



- **Account is disabled**. Απενεργοποιεί τον συγκεκριμένο λογαριασμό και τον αποκλείει από το δίκτυο.
- **Smart card is required for interactive logon**. Στην περίπτωση αυτή ο χρήστης συνδέεται στο δίκτυο με την χρήση έξυπνης κάρτας.
- **Account is Sensitive And Cannot Be Delegated.** (ο λογαριασμός είναι ευαίσθητος και δεν επιτρέπεται η μεταβίβαση διαπιστευτηρίων). Αυτή η επιλογή όταν ενεργοποιηθεί σημαίνει ότι επειδή ο συγκεκριμένος χρήστης χαρακτηρίζεται σημαντικός έχοντας αυξημένη πρόσβαση σε πόρους, το πρωτόκολλο ασφάλειας (Kerberos), δεν θα επιτρέπει την μεταβίβαση διαπιστευτηρίων σε άλλες περιοχές.

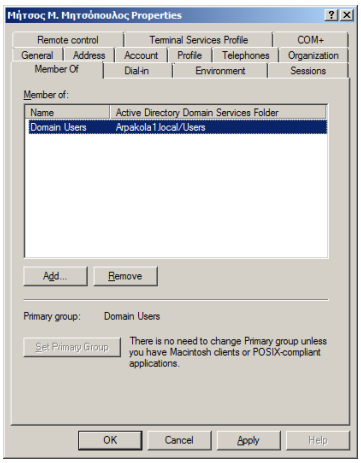


Για να το καταλάβουμε αυτό λίγο καλύτερα ας δούμε το παραπάνω σχήμα. Έστω ότι υπάρχει εξωτερική εισβολή (hacking) στον Proxy Server του δικτύου. Μεταξύ του Proxy Server και του υπόλοιπου δικτύου υπάρχει τείχος προστασίας (firewall) που προστατεύει το δίκτυο. Αν ο hacker χρησιμοποιήσει έναν λογαριασμό του δικτύου για την εισβολή που έχει διαχειριστικές ιδιότητες, με την χρήση των διαπιστευτηρίων του περνά το τείχος, με την συναίνεση του Kerberos, φτάνει στους υπόλοιπούς Server του δικτύου και από εκεί και πέρα είναι ανεξέλεγκτος.

Οι υπόλοιπες επιλογές αφορούν την κρυπτογράφηση των λογαριασμών. Τα βασικά σημεία που πρέπει να γνωρίζουμε είναι ότι όσο ισχυρότερη είναι η κρυπτογράφηση, κερδίζουμε σε ασφάλεια, αλλά επιβαρύνουμε αρκετά την κίνηση δεδομένων στο δίκτυο. Το πρότυπο DES (Data Encryption Standard – Πρότυπο Κρυπτογράφησης Δεδομένων), υποστηρίζεται από παλαιότερες εκδόσεις των Windows και όταν έχουμε τέτοιους πελάτες στο δίκτυο αυτό πρέπει να χρησιμοποιούμε , αλλά το AES (Advanced Encryption Standard – Πρότυπο Βελτιωμένης Κρυπτογράφησης) είναι το νεότερο και ισχυρότερο πρωτόκολλο κρυπτογράφησης. Έτσι λοιπόν έχουμε:

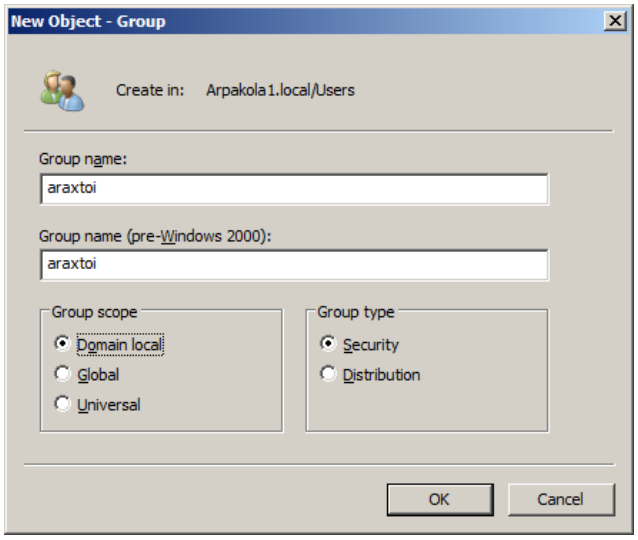
- **Use Kerberos DES Encryption Types For This Account.** Να χρησιμοποιηθεί στο πρωτόκολλο ασφάλειας Kerberos η DES κρυπτογράφηση για αυτόν τον λογαριασμό.
- **This Account Supports Kerberos AES 128 bit.** Αυτός ο λογαριασμός υποστηρίζει κρυπτογράφηση AES 128 bit στο πρωτόκολλο Kerberos.
- **This Account Supports Kerberos AES 256 bit.** Αυτός ο λογαριασμός υποστηρίζει κρυπτογράφηση AES 256 bit στο πρωτόκολλο Kerberos.
- **Do Not Require Kerberos Pre authentication.** Αυτός ο λογαριασμός δεν χρειάζεται προέγκριση από το πρωτόκολλο ασφάλειας Kerberos για να προσπελάσει τους πόρους του δικτύου. Στην ουσία αυτή η ρύθμιση απενεργοποιεί την ασφάλεια του δικτύου για αυτόν τον χρήστη.
- **Account Expires.** Στην περίπτωση αυτή ορίζουμε εμείς την επιθυμητή ημερομηνία λήξης του λογαριασμού. Η επιλογή αυτή είναι ιδιαίτερα χρήσιμη όταν έχουμε περιπτώσεις υπαλλήλων που έχουν συμβάσεις ορισμένου χρόνου.

4. Η κάρτα **Member Of**

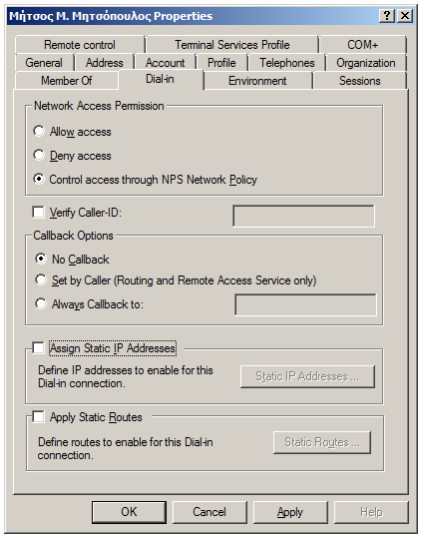


Σε αυτή την κάρτα έχουμε την δυνατότητα για κάθε χρήστη, να τον κάνουμε μέλος σε μία ή περισσότερες ομάδες. Οι ομάδες αυτές μπορεί να είναι είτε από τις αρχικές των Windows 2012 Server, είτε από αυτές που δημιουργήσαμε εμείς. Για παράδειγμα έστω ότι θέλουμε ο χρήστης να συνδέεται στον Server για να εκτελεί βασικές εργασίες (όχι διαχειριστικές), τότε θα τον εντάξουμε ως μέλος της ομάδας Server Operators.

Να δημιουργήσετε μια ομάδα χρηστών και να εντάξετε σε αυτήν τους λογαριασμούς σας. Ο τύπος της ομάδας να είναι Security και η εμβέλειά της Domain Local. Έπειτα να εντάξετε την ομάδα σας στην υπάρχουσα ομάδα Server Operators των Windows 2012 Server.



5. Η κάρτα **Dial-in**



Σε αυτή τη κάρτα ρυθμίζουμε για αυτόν τον χρήστη την δυνατότητα και τον τρόπο της πρόσβασης με τηλεφωνική κλήση. Στην έκδοση που χρησιμοποιείτε (Standard) υπάρχει ένα όριο 50 τέτοιων συνδέσεων (στην έκδοση WEB δεν υπάρχει καθόλου η δυνατότητα, ενώ στις εκδόσεις Datacenter και Enterprise δεν υπάρχει όριο συνδέσεων). Ενημερωτικά για να χρησιμοποιηθεί αυτή η δυνατότητα θα πρέπει πρώτα να γίνουν τα εξής :

- ✓ Να προστεθούν δύο ακόμα Roles από την κονσόλα Server Manager: Network Policy και Access Services.
- ✓ Αν δεν θέλουμε να έχουν συνολικά όλοι οι χρήστες του δικτύου το προνόμιο αυτό, τότε αυτοί που το έχουν καλό θα είναι να συγκεντρωθούν σε μια Οργανωτική Μονάδα. Στη συνέχεια με χρήση της GPO (Group Policy Object) δηλαδή της Πολιτικής που θα εφαρμοστεί στον Τομέα η στην Οργανωτική Μονάδα ανάλογα, πρέπει να γίνουν οι απαραίτητες διευθετήσεις.
  Δεν έχουμε ακόμα ασχοληθεί με τα θέματα πολιτικής στο δίκτυο, απλά αναφέρουμε ότι οι ρυθμίσεις αυτές γίνονται στον κόμβο User Configuration → Administrative Templates → Network → Network connections. Όμοια στην πολιτική Routing And Remote Access στον κόμβο Computer Management → Services And Applications → Routing And Remote Access θα πρέπει να διευθετήσουμε την δρομολόγηση.

Αφού έχουν προηγηθεί οι διευθετήσεις, τώρα μπορούμε να ρυθμίσουμε τις υπόλοιπες παραμέτρους της κάρτας Dial-In της τηλεφωνικής κλήσης.
Αρχικά ενδεδειγμένη επιλογή στην περιοχή **Network Access Permission** είναι η Control Access through NPS (Network Policy Server) Network Policy. Οι παρακάτω επιλογές είναι:

- Verify Caller ID (Επαλήθευση Αναγνωριστικού Καλούντος). Αυτή η επιλογή ενεργοποιείται όταν ο χρήστης καλεί μόνο από έναν συγκεκριμένο αριθμό, τον οποίο και θα καταχωρήσουμε στο διπλανό πεδίο.
- No Callback (Χωρίς απαντητική κλήση). Στην περίπτωση αυτή ο χρήστης τηλεφωνεί, συνδέεται και παραμένει συνδεδεμένος.
- Set By Caller (Ορισμός από τον καλούντα). Σε αυτή την περίπτωση ο χρήστης καλεί μέσω τηλεφώνου και δίνει ο ίδιος τον τηλεφωνικό αριθμό που θέλει. Στη συνέχεια αποσυνδέεται και ο Server τον καλεί σε αυτόν τον αριθμό για επανασύνδεση. Η χρησιμότητα αυτής της επιλογής είναι ότι τα τέλη της τηλεφωνικής σύνδεσης τα χρεώνεται η εταιρεία.
- Always Callback To: (Πάντα Απαντητική Κλήση στο:). Είναι παρόμοια με την προηγούμενη επιλογή, μόνο που εδώ ο απαντητικός αριθμός προκαθορίζεται και καταχωρείται στο διπλανό πεδίο.

Τέλος υπάρχει η δυνατότητα απομακρυσμένης πρόσβασης με δρομολόγηση στατικής IP.

6. Η κάρτα **Profiles**

Με τον όρο προφίλ χρήστη εννοούμε ένα σύνολο προσωπικών χαρακτηριστικών, ιδιαίτερων για κάθε χρήστη. Τα σπουδαιότερα από αυτά είναι :

- ❑ Η επιφάνεια εργασίας
- ❑ Ο φάκελος My Documents
- ❑ Το μενού Start
- ❑ Ο φάκελος Favorites
- ❑ Οι φάκελοι Templates, Local Settings, Cookies, Recent κ.α.

Υπάρχουν τρία είδη προφίλ χρηστών στα WINDOWS 2012 :

- **Το τοπικό προφίλ (Local Profile).**

Δημιουργείται σε κάθε υπολογιστή την πρώτη φορά που συνδέεται ένας χρήστης σε αυτόν. Δημιουργείται και παραμένει τοπικά στον συγκεκριμένο υπολογιστή στον σκληρό του δίσκο και ενημερώνεται τοπικά με τις εκάστοτε αλλαγές που προκαλεί ο ίδιος χρήστης.

- **Το προφίλ περιαγωγής(Roaming Profile).**

Δημιουργείται **μόνο** από έναν Administrator και αποθηκεύεται σε ένα Server δικτύου. Το προφίλ αυτό ακολουθεί τον χρήστη σε οποιοδήποτε Η/Υ του δικτύου.(με την προϋπόθεση ότι οι Η/Υ έχουν λειτουργικά Microsoft, από 2000 και μετά). Οι όποιες αλλαγές στα στοιχεία του προσωπικού του προφίλ, κάνει ο χρήστης, αποθηκεύονται στον Server και τον ακολουθούν σε όποιο υπολογιστή συνδέεται.

- **Το υποχρεωτικό προφίλ (Mandatory profile).**

Δημιουργείται και αυτό **μόνο** από ένα Administrator και αποθηκεύεται σε ένα Server δικτύου. Η διαφορά του με το προηγούμενο είναι στο γεγονός ότι **μόνο** κάποιος Administrator μπορεί να κάνει αλλαγές στο προφίλ. Οι αλλαγές που κάνει ο χρήστης δεν αποθηκεύονται.

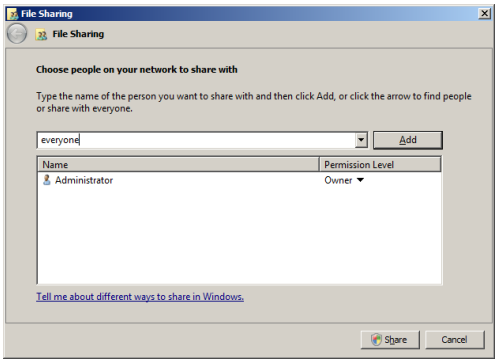
Όπως εύκολα καταλαβαίνουμε, για να δημιουργηθούν τα δύο τελευταία είδη Profile (Roaming και Mandatory), απαιτείται κοινόχρηστος χώρος αποθήκευσης στο δίκτυο και αν κάποια στιγμή αυτός δεν είναι διαθέσιμος τα προφίλ δεν θα λειτουργήσουν. Θα δοκιμάσετε να δημιουργήσετε τέτοια προφίλ.

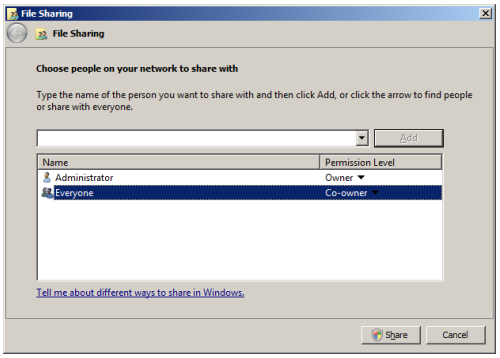
ΠΟΡΕΙΑ ΕΡΓΑΣΙΑΣ

Δημιουργία Περιπλανώμενου Προφίλ (Περιαγωγής) - Roaming Profile

Στην άσκηση αυτή θα δημιουργήσετε για τον λογαριασμό σας ένα προφίλ περιαγωγής (Roaming profile). Επειδή υπάρχει η ανάγκη τα διάφορα προφίλ των χρηστών του δικτύου να αποθηκεύονται σε κάποιο φάκελο του Server, αρχικά θα πρέπει αυτός να δημιουργηθεί. Έτσι :

1. Να δημιουργηθεί στον σκληρό δίσκο του Server ένας νέος φάκελος και να ονομαστεί pro (τυχαία ονομασία). Ο φάκελος αυτός να γίνει γενικά κοινόχρηστος (δεξί κλικ στον φάκελο και επιλέξτε Share → Προσθέστε την ομάδα everyone → Στην επιλογή Access Level να την ορίζετε ως Co-Owner → Ok).





2. Να επιλέξετε τον λογαριασμό σας, να κάνετε δεξί κλικ σε αυτόν και επιλέξτε properties.

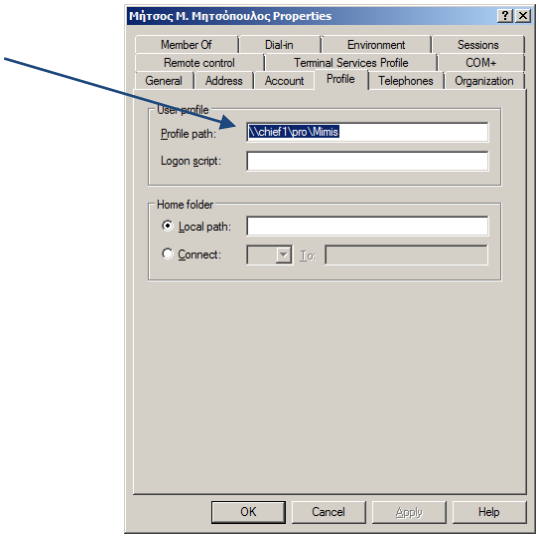
Παρατήρηση:

Μην ξεχάσετε, για να μπορέσετε να δοκιμάσετε το προφίλ σας να δώσετε στον λογαριασμό σας δικαίωμα πρόσβασης και σε κάποιον ακόμη Η/Υ του Domain. (Account → Log On Το κλπ)

3. Στην καρτέλα Profile του λογαριασμού σας, στο πεδίο Profile Path πληκτρολογήστε την διαδρομή προς τον κοινόχρηστο φάκελο ως εξής :

***ServerComputerName*\pro\username**

Όπου username βάζετε το δικό σας όπως στην εικόνα:



Πατήστε Apply → OK.

Αν δεν θέλουμε να ψάχνουμε το username του κάθε χρήστη, τότε αντί γι αυτό πληκτρολογούμε την μεταβλητή %username% και τα Windows την αντικαθιστούν αυτόματα με το username του κάθε χρήστη.

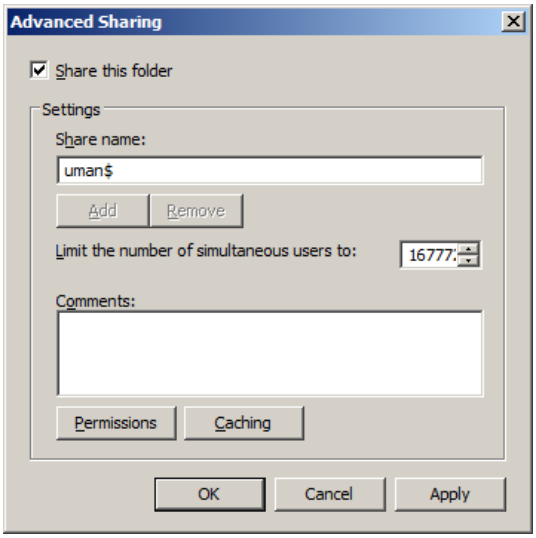
4. Να συνδεθείτε με τον λογαριασμό σας σε ένα οποιοδήποτε workstation και να δημιουργήσετε έναν νέο φάκελο στην επιφάνεια εργασίας (ονομάστε τον όπως θέλετε).

5. Να κάνετε Restart στον Η/Υ σας **πρώτα** και να συνδεθείτε πάλι με τον ίδιο λογαριασμό σε οποιοδήποτε άλλο workstation που έχετε πρόσβαση έπειτα, επαληθεύοντας ότι πράγματι το προφίλ σας είναι περιπλανώμενο (roaming).

Δημιουργία Υποχρεωτικού Προφίλ - Mandatory Profile

Υπάρχουν περισσότεροι του ενός τρόποι για να δημιουργήσουμε υποχρεωτικά προφίλ χρηστών. Ο πιο απλός και σύντομος είναι ο εξής:

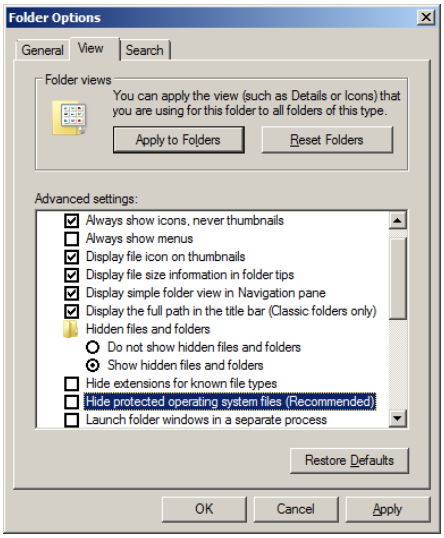
1. Δημιουργούμε στον Server ένα φάκελο όπου θα αποθηκεύονται τα υποχρεωτικά προφίλ. Έστω ότι τον ονομάζουμε uman. Τον κάνουμε κοινόχρηστο (από Properties → Sharing → Advanced Sharing → γράφουμε για λόγους στο τέλος του ονόματός του το $ και έτσι γίνεται κρυφός στην εξερεύνηση του δικτύου.



1. Ανοίγουμε την καρτέλα Permissions και απομακρύνουμε την ομάδα των everyone. Προσθέτουμε την ομάδα των πιστοποιημένων χρηστών (Authenticated Users) και την ομάδα των Administrators, στην οποία δίνουμε Full Control ενώ στους Authenticated Users μόνο Read.
   Μέσα στον φάκελο αυτό δημιουργούμε ένα ακόμα, έστω ότι τον ονομάζουμε mandatory με κατάληξη .v2, δηλαδή mandatory.v2 (αυτή είναι η κατάληξη προφίλ που υποστηρίζουν τα 2012 Server και τα Win 7 και μεταγενέστερα).
2. Πηγαίνουμε σε ένα σταθμό εργασίας και συνδεόμαστε με λογαριασμό administrator. Ανοίγουμε τα προφίλ των χρηστών του και διαλέγουμε το Default (Προεπιλεγμένο) προφίλ. Πατάμε **Copy to** (Αντιγραφή σε…) και στο **Copy profile to** (Αντιγραφή προφίλ σε …) γράφουμε το μονοπάτι αποθήκευσης : \\ServerName\Φάκελος Προφίλ\Υποφάκελος Υποχρεωτικού Προφίλ δηλαδή στο παράδειγμά μας: **\\Chief1\uman$\mandatory.v2.** Πιο κάτω στο πεδίο Permitted to use… (Μπορείτε να χρησιμοποιήσετε…) πατάμε Change (Αλλαγή) και επιλέγουμε την ομάδα των Everyone.

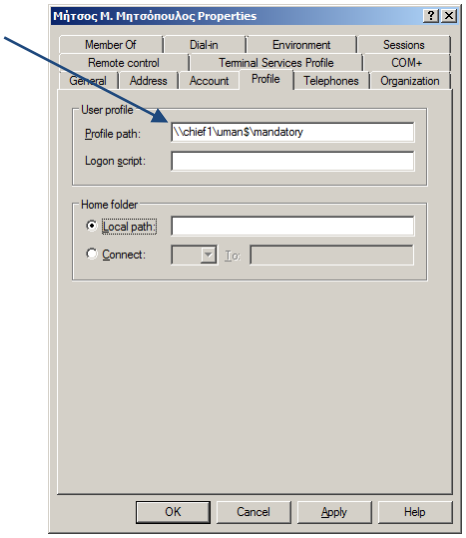
3. Αποσυνδεόμαστε και συνδεόμαστε στον Server με λογαριασμό διαχειριστή. Ανοίγοντας τον φάκελο uman→mandatory.v2, Ρυθμίζουμε την προβολή φακέλων και αρχείων για εμφάνιση κρυφών αρχείων Organize → Folder and search options

→ View → View hidden files και αποεπιλέγουμε το Hide protected operating system files και το Hide extension for Known file types.



Εντοπίζουμε το αρχείο NTUSER.DAT και το μετονομάζουμε σε NTUSER.MAN.

4. Τώρα μπορούμε να επιλέξουμε όποιον χρήστη θέλουμε να του δώσουμε υποχρεωτικό προφίλ εύκολα ως εξής: Πηγαίνουμε στην κάρτα Profile και στο Profile Path δίνουμε την διαδρομή : \\ServerName\Φάκελος Προφίλ\Υποφάκελος Υποχρεωτικού Προφίλ δηλαδή στο παράδειγμά μας: **\\Chief1\uman$\mandatory (χωρίς την κατάληξη .v2).**



5. Την διαδικασία απόδοσης προφίλ μπορούμε να την κάνουμε μαζικά σε χρήστες, αν τους επιλέξουμε όλους μαζί και με δεξί κλικ στην μαζική επιλογή δίνουμε στο κοινό πλέον πεδίο του path του προφίλ το μονοπάτι του φακέλου, όπως πιο πάνω.

6. Να δημιουργήσετε τρεις νέους χρήστες και ονομάστε τους όπως θέλετε. Ακολουθώντας την παραπάνω διαδικασία να τους αποδώσετε υποχρεωτικό προφίλ ως εξής: στον 1ο χρήστη να κάνετε την απόδοση του προφίλ ατομικά ενώ στους άλλους δύο ταυτόχρονα.

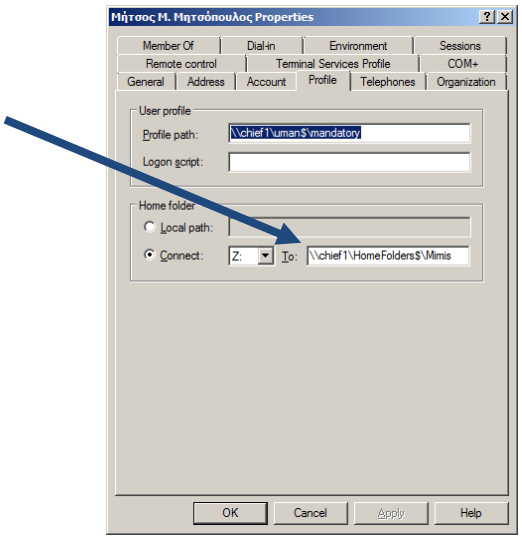
7. Να συνδεθείτε σε ένα σταθμό και με τους τρεις και να δοκιμάσετε να αλλάξετε την ταπετσαρία, να δημιουργήσετε φακέλου ή αρχεία στην επιφάνεια εργασίας

και στα έγγραφα του κάθε χρήστη. Να κάνετε έπειτα διαδοχικές αποσυνδέσεις και επανασυνδέσεις με αυτούς τους χρήστες και να διαπιστώσετε την υποχρεωτικότητα των προφίλ τους. Στη συνέχεια να συνδεθείτε στον Server με λογαριασμό διαχειριστή και να οδηγηθείτε στον φάκελο αποθήκευσης των προφίλ (mandatory στο παράδειγμα), να ανοίξετε τον φάκελο desktop και να δημιουργήσετε μέσα του αρχεία και φακέλους. Το ίδιο να κάνετε και στον φάκελο Documents. Έπειτα συνδεθείτε με τους χρήστες σας σε ένα σταθμό και παρατηρήστε την ύπαρξη αυτών των φακέλων στην επιφάνεια εργασίας και στα έγγραφα του κάθε χρήστη.

Δημιουργία Home Folder

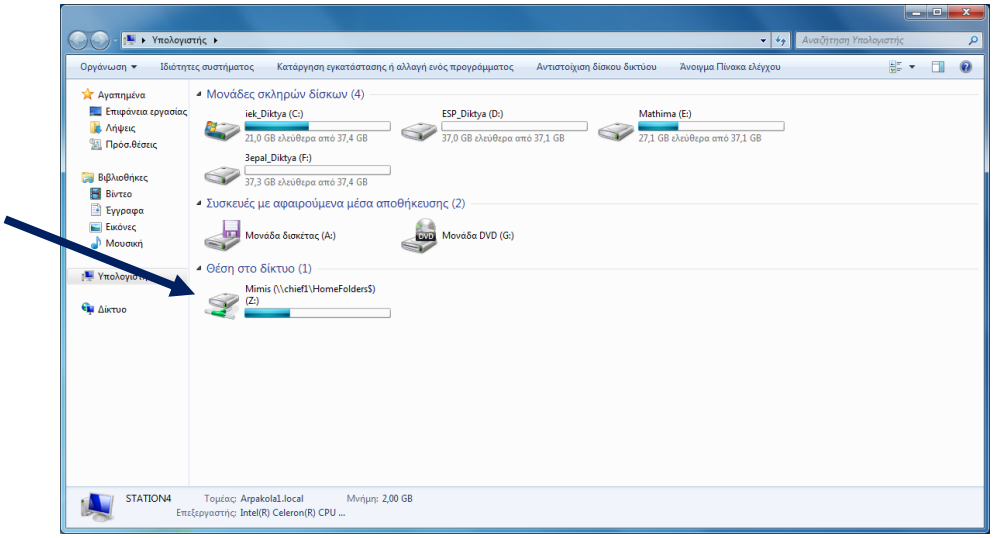
Η επιλογή Home Folder (Αρχικός φάκελος), σας δίνει την δυνατότητα να ορίσετε για κάθε χρήστη έναν φάκελο για την αποθήκευση των προσωπικών του αρχείων. Αυτός ο φάκελος μπορεί να βρίσκεται στον Η/Υ που ο χρήστης εργάζεται (επιλογή Local Path – Τοπική διαδρομή), δείτε το σχήμα 3.4, ή μπορεί να είναι κοινόχρηστος κάπου στο δίκτυο (επιλογή Connect). Προτιμότερη είναι η δεύτερη περίπτωση, γιατί δίνει την ευχέρεια στον χρήστη, να χρησιμοποιεί τον φάκελο του από οποιοδήποτε Η/Υ του δικτύου, αφού ο Server είναι πάντα σε λειτουργία (Εναλλακτικά και προτιμότερη λύση είναι η χρήση ενός NAS Server για αυτές τις διαδικασίες).

Μια τακτική είναι η εξής: Δημιουργήστε σε έναν δίσκο του Server ένα φάκελο και ονομάστε τον όπως νομίζετε πχ UsersFolder. Να τον κάνετε κοινόχρηστο και **κρυφό**. Να δώσετε στις άδειες (permissions) πλήρη έλεγχο στους everyone. Στην συνέχεια στην καρτέλα profile του λογαριασμού σας, επιλέξτε Connect και αφήστε το γράμμα Z ως γράμμα μονάδας. (Μπορείτε να επιλέξετε άλλο γράμμα ως γράμμα μονάδας, αρκεί να μην χρησιμοποιείται από κάποια άλλη μονάδα δίσκου. Το Z είναι μια καλή επιλογή.).



Στο πεδίο ***To*** γράψτε την διαδρομή προς τον φάκελο σας ως εξής: ***\\ServerComputerName\UsersFolder\username*** όπως φαίνεται στην εικόνα9 (μην ξεχάσετε το $ τέλος του ονόματος του αρχείου).

Συνδεθείτε στον Η/Υ σας και να κάνετε διπλό κλικ στο My Computer. Παρατηρήστε τον δικτυακό σας δίσκο.



Κάποιες ακόμη παρατηρήσεις:

8. Αν σας μπερδεύει το username στην γραφή της διαδρομής των προφίλ ή των προσωπικών φακέλων (ειδικά όταν σαν Administrator, τους κατασκευάζετε για πολλούς χρήστες), μπορείτε να γράφετε σε όλους αντί του username τους την μεταβλητή: **%username%** και τα Windows θα το αντικαθιστούν αυτόματα με το πλήρες username του κάθε χρήστη. Ιδιαίτερα χρήσιμη είναι η χρήση της μεταβλητής αυτής στην περίπτωση μαζικής απόδοσης Home Folder. Αν βάλουμε την μεταβλητή %username% τότε τα Windows θα κάνουν τις κατάλληλες ατομικές αντικαταστάσεις ονομάτων αυτόματα και μαζικά.

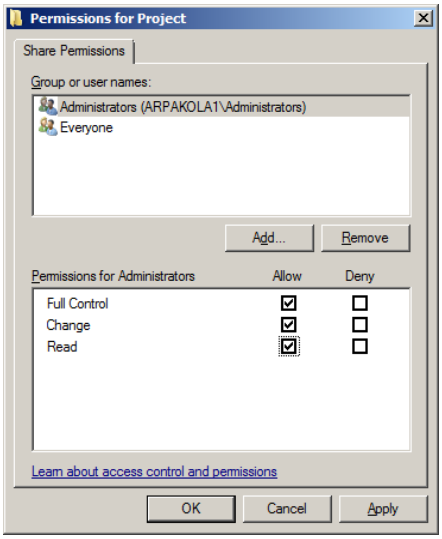
- Έγινε λόγος παραπάνω για την κοινοχρησία φακέλων στο δίκτυο, όπως επίσης για άδειες και ασφάλεια κοινόχρηστων φακέλων. Δεχτείτε προς το παρόν απλά τις έννοιες αυτές και θα τις αναλύσουμε διεξοδικά σε παρακάτω άσκηση.

Δημιουργία Σεναρίου Σύνδεσης – Logon Script

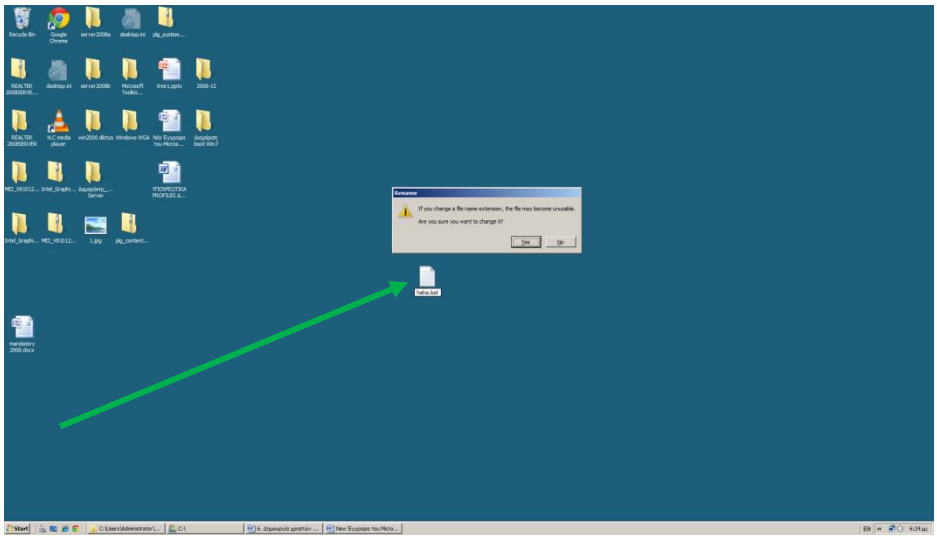
Τα σενάρια σύνδεσης είναι διαταγές που πρέπει να εκτελούνται κάθε φορά που συνδέεται ο χρήστης ή οι χρήστες που τους τα έχουμε επιβάλλει. Η χρησιμότητά τους ποικίλει και θα μπορούσαν να χρησιμοποιηθούν για παράδειγμα για τον ορισμό της ώρας του συστήματος ή για την σύνδεση του χρήστη σε έναν εκτυπωτή ή ακόμα και για την δημιουργία ενός Home Folder όπως της προηγούμενης περίπτωσης που είδαμε. Τα σενάρια

σύνδεσης μπορεί να είναι αρχεία κατάληξης .bat ή .vbs (visual basic script) ή .exe (Αν και γενικά δεν είναι όμως ο καλύτερος τρόπος για να εκκινούμε προγράμματα. Αν θέλουμε κάτι τέτοιο ο καλύτερος τρόπος είναι να βάλουμε την συντόμευση της εφαρμογής στον φάκελο Startup του χρήστη). Ας δούμε ένα παράδειγμα δημιουργίας σεναρίου σύνδεσης το οποίο θα δίνει στους χρήστες έναν Home Folder, στον Server (έστω για αποθήκευση των εργασιών τους σε αυτόν). Θα τον ονομάσουμε Project.

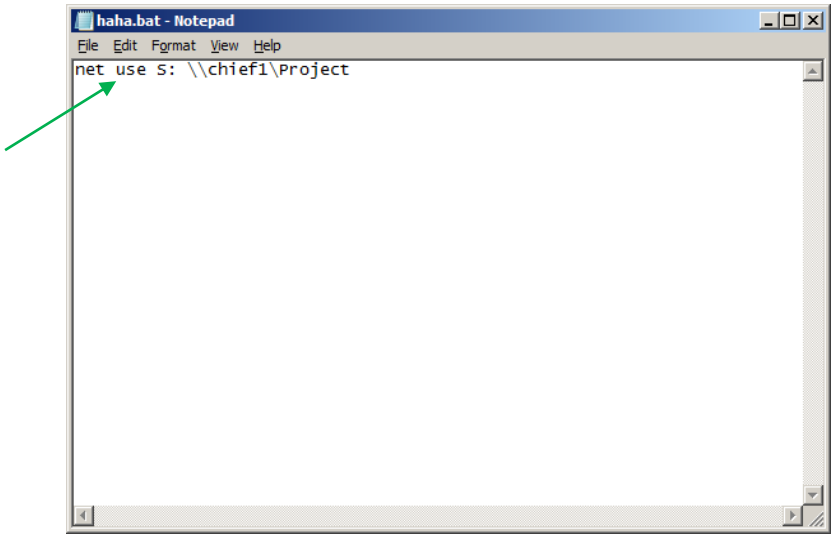
1. Αρχικά δημιουργούμε τον φάκελο στον Server (στο root) και τον κάνουμε κοινόχρηστο δίνοντας επιπλέον άδειες (permissions) στην ομάδα των Administrators πλήρη έλεγχο.



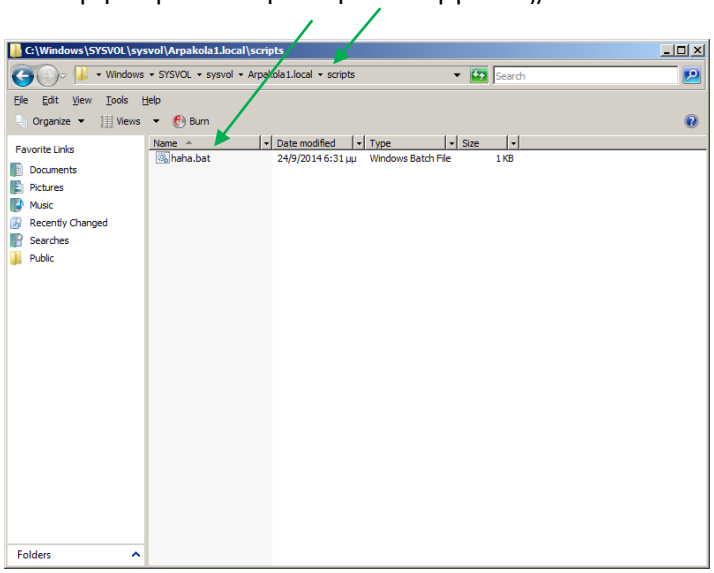
2. Στην επιφάνεια εργασίας δημιουργούμε ένα νέο αρχείο κειμένου το ονομάζουμε όπως θέλουμε (έστω haha) και αλλάζουμε την κατάληξη του από .txt σε .bat, αγνοώντας την προειδοποίηση των Windows.



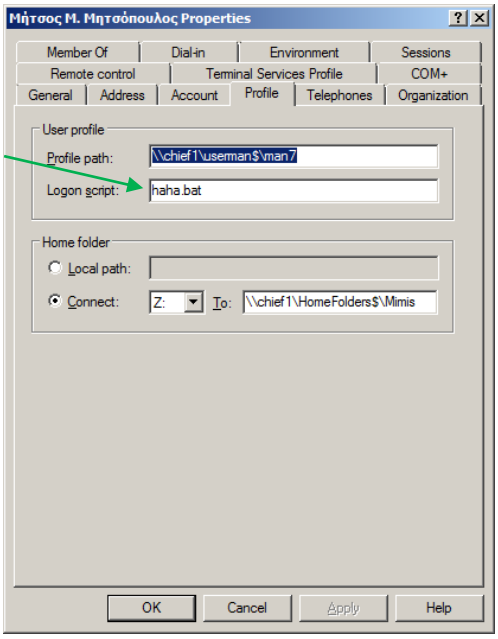
3. Με δεξί κλικ στο αρχείο haha.bat επιλέγουμε edit και γράφουμε : **net use S: \\chief1\Project** και το σώζουμε (Το S θα είναι το γράμμα δίσκου, εδώ είναι τυχαία επιλογή και μπορεί να χρησιμοποιηθεί οποιοδήποτε διαθέσιμο γράμμα.

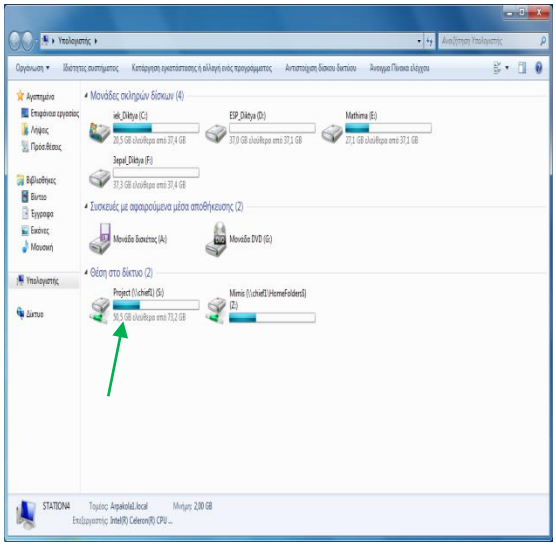


Ανοίγουμε διαδοχικά : C (τον δίσκο που είναι το λειτουργικό μας) → Windows → SYSVOL → sysvol → EK4PER1 (το domain μας) → scripts → και κάνουμε μέσα στον φάκελο scripts επικόλληση το αρχείο .bat που δημιουργήσαμε προηγούμενα. (Το αρχείο δεν θα μας χρειαστεί ξανά και το σβήνουμε από την επιφάνεια εργασίας).

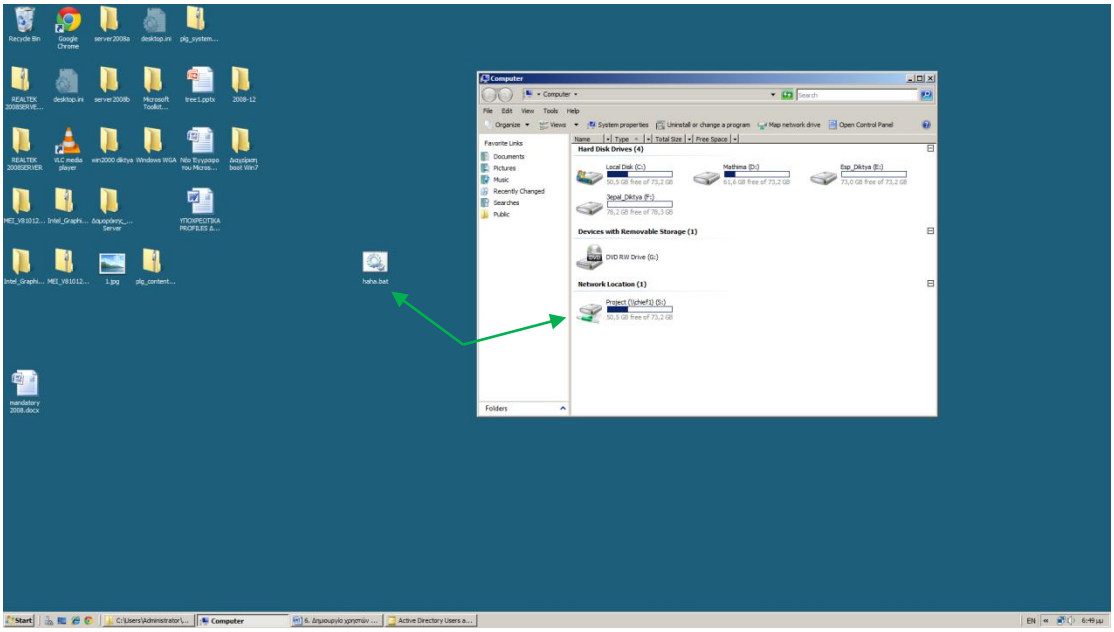


Πηγαίνουμε στον ή στους χρήστες που θέλουμε να τους δώσουμε το σενάριο, και στην κάρτα Profile → Logon script γράφουμε το όνομα (και την κατάληξη του αρχείου .bat).

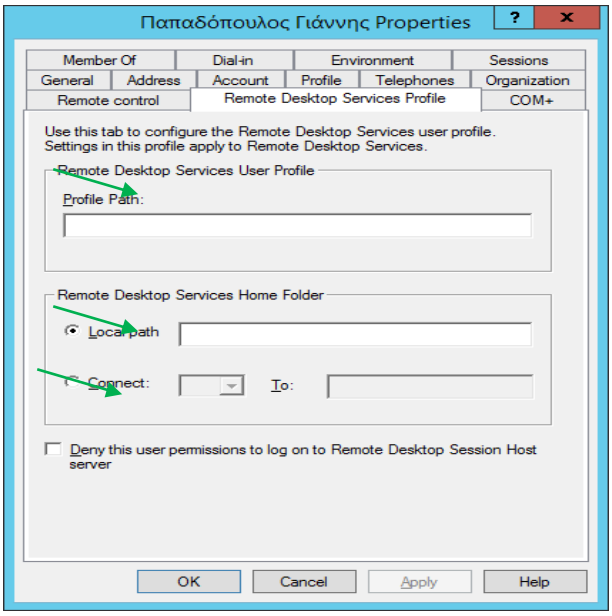




Μια παρατήρηση: καλό θα είναι τα script που δημιουργούμε να τα δοκιμάζουμε πριν τα εφαρμόσουμε στους χρήστες. Στην περίπτωσή μας θα μπορούσαμε να «τρέξουμε» το script στον Server και θα βλέπαμε άμεσα την δημιουργία του δίσκου Project.

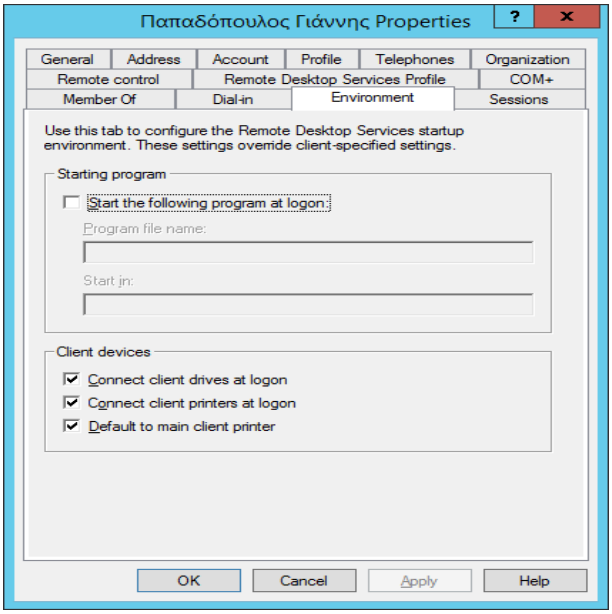


7. Η κάρτα **Terminal Services Profiles**



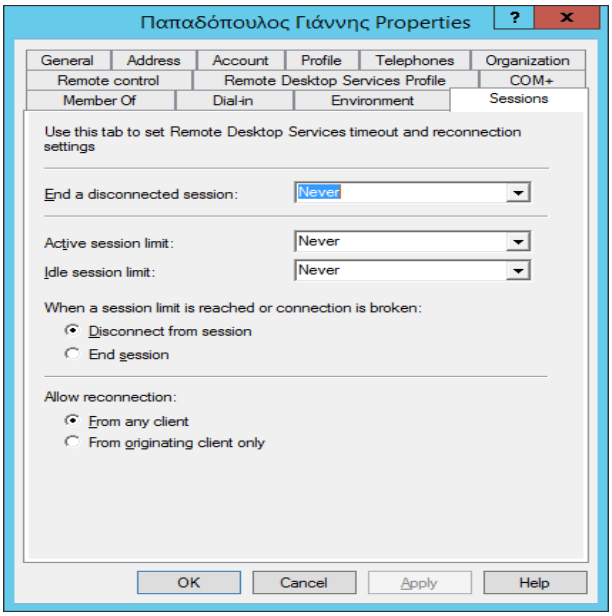
Αρχικά πρέπει να πούμε ότι η κάρτα αυτή έχει χρήση και νόημα μόνο αν έχουμε διαμορφώσει κάποιον Terminal Server, δηλαδή έχουμε εγκαταστήσει τα Terminal services και το Terminal Service Role. Κατά τα υπόλοιπα για κάθε χρήστη μπορούμε να ορίσουμε αν θα έχει γενικά πρόσβαση στην υπηρεσία αυτή, τσεκάροντας ή όχι το αντίστοιχο chek button (Terminal Server χρησιμοποιούμε για να εκτελούν από αυτόν κάποιες εφαρμογές οι χρήστες, οι οποίες είναι εγκατεστημένες στον Terminal Server και όχι στα τοπικά μηχανήματα). Τώρα προαιρετικά μπορούμε να ορίσουμε path για το profile του terminal user και path για το Home Folder αυτού του χρήστη με διαδικασία όμοια με αυτή που είδαμε στην κάρτα Profiles. Αν δεν ορίσουμε Profile ή Home Folder στην κάρτα Terminal Services Profile, τότε χρησιμοποιείται αυτό που ορίσαμε στην κάρτα Profiles, αν όμως έχουμε ορίσει και στις δύο κάρτες, τότε υπερισχύει αυτό της κάρτας Terminal Services Profile για τους Terminal Users.

8. Η κάρτα **Environment**



Και αυτή η κάρτα συνδέεται με τις παροχές του Terminal Server. Όταν καθορίσουμε το πρόγραμμα που θα εκτελείται στο πεδίο Program file name, τότε κατά τη σύνδεση αυτού του Terminal User στον Terminal Server, θα εκτελείται **μόνο** αυτό το πρόγραμμα και όταν ο χρήστης το κλείνει αυτόματα θα αποσυνδέεται από τον Terminal Server. Αν επιπλέον θέλουμε να ορίσουμε και συγκεκριμένο φάκελο εργασίας τότε δίνουμε το Path του στο πεδίο Start in. Στις παρακάτω επιλογές ορίζουμε ότι ο τοπικός δίσκος και εκτυπωτής του χρήστη θα είναι διαθέσιμος κατά την σύνδεση (οι δύο πρώτες επιλογές) και αν ο προεπιλεγμένος εκτυπωτής θα είναι επίσης ο προεπιλεγμένος κατά την απομακρυσμένη σύνδεση.

9. Η κάρτα **Sessions**



Και αυτή η κάρτα συνδέεται με τις παροχές του Terminal Server. Συγκεκριμένα στην επιλογή:

- **End a disconnected session** επιλέγουμε τον χρόνο (μέσα από προκαθορισμένες τιμές), που θα μείνει ενεργό το πρόγραμμα που δούλευε ο χρήστης στον Terminal Server **μετά** την αποσύνδεσή του. Αν επιλέξουμε Never τότε το συγκεκριμένο πρόγραμμα θα μείνει ενεργό χωρίς όριο χρόνου και μετά την αποσύνδεση του χρήστη, ή αλλιώς επιλέγουμε μια τιμή χρόνου που θα κλείσει.
- **Active session limit** επιλέγουμε τον χρόνο (μέσα από προκαθορισμένες τιμές), που θα μείνει ενεργό το πρόγραμμα που μπορεί να δουλέψει ο χρήστης στον Terminal Server. Δυο λεπτά πριν την λήξη αυτού του χρόνου, ο χρήστης θα πάρει σχετικό μήνυμα, ώστε να μπορέσει να κάνει αποθηκεύσεις.
- **Idle session limit ε**πιλέγουμε τον χρόνο (μέσα από προκαθορισμένες τιμές), που θα μείνει αδρανές το πρόγραμμα χωρίς ο χρήστης να είναι συνδεδεμένος, πριν τι πρόγραμμα κλείσει. Και σε αυτή την περίπτωση αποστέλλεται στον χρήστη σχετικό μήνυμα δυο λεπτά πριν.
- **When a session limit is reached or connection is broken.** Στην περίπτωση αυτή της κλεισίματος του προγράμματος εργασίας του Terminal user (ως αποτέλεσμα των παραπάνω ρυθμίσεων ή της απώλειας της σύνδεσής του, έχουμε δυο επιλογές να ορίσουμε: **να τον αποσυνδέσουμε από το πρόγραμμα**, ενώ αυτό θα συνεχίσει να είναι ενεργό (Disconnect from session) ή **να τον αποσυνδέσουμε τελείως από τον Terminal Server** (End Session), οπότε θα χρειαστεί να επανασυνδεθεί αν θέλει να συνεχίσει.

- **Allow reconnection**. Εδώ δεν έχουμε να σκεφτούμε πολλά γιατί τα Windows 2012 server υποστηρίζουν μόνο την πρώτη επιλογή, δηλαδή επιτρέπουν την επανασύνδεση του χρήστη από οποιονδήποτε Η/Υ και δεν τον περιορίζουν σε συγκεκριμένο.

10. Η κάρτα **Remote Control**

Συνεχίζουμε με την υπηρεσία Terminal Services. Εδώ καθορίζονται τα επίπεδα πρόσβασης του Terminal User τα οποία κυμαίνονται από απλή παρατήρηση του Terminal server ή κατόπιν άδειας από τον χρήστη ή αλληλεπιδραστικά με αυτόν (επίδραση πληκτρολογίου και ποντικιού στο περιβάλλον εργασίας του χρήστη).