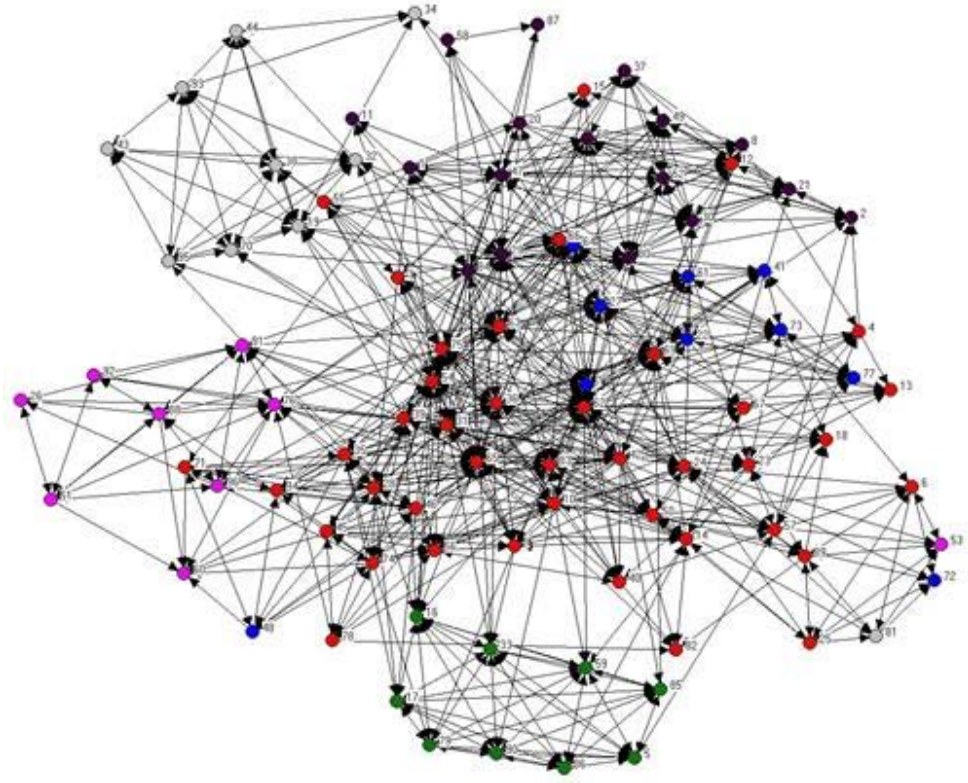
ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ Τεχνολογικών Εφαρμογών
ΤΜΗΜΑ Μηχανικών Πληροφορικής
ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΤΩΝ ΣΠΟΥΔΑΣΤΩΝ

«ΔΙΒΑΝΗ ΗΛΙΑ - ΛΑΦΗ ΓΕΩΡΓΙΟΥ»

ΘΕΜΑ

« Ανάπτυξη συστήματος κεντρικής διαχείρησης των ηλεκτρονικών υπηρεσιών του τμήματος πληροφορικής. »



Επιβλέπων καθηγητής
Δρ. Περικλής Χατζημίσιος
Αναπληρωτής Καθηγητης ΑΤΕΙΘ

..περίληψη

Σκοπός αυτής της εργασίας είναι η ανάπτυξη και ο συνδυασμός υπηρεσιών που θα απλουστεύσουν και θα κάνουν αποτελεσματικότερη τη διαχείριση των πόρων του δικτύου του Τμήματος Πληροφορικής.

Κυρίαρχο ρόλο για τη διευκόλυνση του έργου των διαχειριστών του οργανισμού, παίζουν οι υπηρεσίες καταλόγου της Microsoft (***Active Directory Services***) που επιτρέπουν τη διαχείριση του δικτύου από ένα σημείο και κάνουν πολύ ευκολότερη την επιτήρηση του όσο οι ανάγκες του οργανισμού αυξάνονται.

Το Active Directory είναι μια βάση δεδομένων στην οποία αποθηκεύονται όλες οι πληροφορίες του δικτύου. Τέτοιες πληροφορίες μπορεί να 'ναι χρήστες, ομάδες χρηστών, κοινόχρηστοι φάκελοι ή και ακόμα φυσικές συσκευές (πχ εκτυπωτές δικτύου).

Σημαντικό, χαρακτηριστικό γνώρισμα του Active Directory είναι η ενιαία σύνδεση (***Single Sign On***) όπου κάθε χρήστης αφού έχουν ταυτοποιηθεί τα στοιχεία του έχει πρόσβαση ανάλογα με τα δικαιώματα που του έχουν δοθεί, στους πόρους και τις υπηρεσίες του δικτύου.

Ο συνδυασμός του Active Directory με τις υπηρεσίες που περιγράφονται στα παρακάτω κεφάλαια (***WDS,PXELINUX, HYPER-V, DHCP, DNS, Mail Services***) αλλά και η δυνατότητα σύνδεσης του με συστήματα Linux δίνει την ευχέρεια στους διαχειριστές να ελέγχουν και να συντηρούν το δίκτυο , αποτελεσματικότερα , με ευελιξία , με μικρότερο χρηματικό και χρονικό κόστος και να μπορούν να το επεκτείνουν όσο οι ανάγκες του Τμήματος Πληροφορικής μεγαλώνουν.

..περιεχόμενα

ΚΕΦΑΛΑΙΟ 1. ACTIVE DIRECTORY

Με τον όρο *'Υπηρεσίες Καταλόγου'* αναφερόμαστε σε μια κατανεμημένη βάση δεδομένων η οποία επιτρέπει την αποθήκευση πληροφοριών που σχετίζονται με τους πόρους του δικτύου μας, με σκοπό να διευκολύνεται ο εντοπισμός και η διαχείρισή αυτών. Μια υλοποίηση της Microsoft των υπηρεσιών καταλόγου για τις εκδόσεις λογισμικού Windows Server είναι το Active Directory. Ο Ενεργός Κατάλογος (Active Directory) παρέχει τα μέσα για την διαχείριση των οντοτήτων – ταυτοτήτων και των σχέσεων που υπάρχουν σε έναν οργανισμό.

Το Active Directory βασίζεται στον πρωτόκολλο LDAP και παρέχεται ως υπηρεσία (Role) του λειτουργικού συστήματος Windows Server, ενώ περιέχει όλα εκείνα τα χαρακτηριστικά τα οποία είναι απαραίτητα για την κεντρική διαχείριση των οντοτήτων, των χρηστών και των εφαρμογών ενός συστήματος. Με το Active Directory απλοποιείται σε μεγάλο βαθμό η διαχείριση των χρηστών και των υπολογιστών, καθίσταται εφικτή η λειτουργία της «μοναδικής εγγραφής» (single sign on), αποκτώντας με αυτόν τον τρόπο πρόσβαση σε πόρους του δικτύου και βελτιώνεται η ιδιωτικότητα και ασφάλεια των πληροφοριών και επικοινωνιών.

Το Active Directory συμπεριλαμβάνεται αποκλειστικά στις Server εκδόσεις του λειτουργικού της Microsoft, 'Microsoft Windows Server' και πρωτοεμφανίζεται ως υπηρεσία στην έκδοση 2000 αποτελούμενο από κάποιες βασικές λειτουργίες οι οποίες αναβαθμίζονταν ή συμπληρώνονταν από νέες σε κάθε νέα έκδοση του λειτουργικού. Ήδη από την έκδοση των Windows Server 2003, έχει αποδειχτεί ως μια αποτελεσματική και ιδιαίτερα ισχυρή υπηρεσία καταλόγου. Στην έκδοση 2008 η υπηρεσία του Active Directory παρουσιάζεται βελτιωμένη με την προσθήκη νέων χαρακτηριστικών τα οποία μειώνουν το διαχειριστικό κόστος αυξάνοντας την αποδοτικότητα και την παραγωγικότητα του οργανισμού – συστήματος. Στα Windows Server 2008 το AD αποτελεί την πιο πολύπλοκη λειτουργία του λειτουργικού.

Τα βασικά χαρακτηριστικά του AD τα οποία και θα αναλυθούν στη συνέχεια ώστε να γίνει το δυνατόν πιο προσιτή και κατανοητή η σημασία και το μοναδικά οφέλη της υπηρεσίας αυτής είναι τα εξής :

- Λογική Δομή
- Φυσική Δομή
- Αυθεντικοποίηση
- Group Policy
- Roaming Profiles
- Redirected Folders
- Restricted Groups

1.1 ΛΟΓΙΚΗ ΔΟΜΗ

Το AD, απαρτίζεται από ένα σύνολο υπηρεσιών, γνωστές ως υπηρεσίες τομέα του AD (Active Directory Domain Services ή AD DS) οι οποίες αποθηκεύουν πληροφορίες για χρήστες, υπολογιστές, αλλά και για άλλες συσκευές του δικτύου, ενώ βοηθούν τους διαχειριστές αυτού να διαχειρίζονται με ασφάλεια τις πληροφορίες από ένα κεντρικό σημείο διευκολύνοντας επίσης το διαμοιρασμό των πόρων του δικτύου και τη συνεργασία μεταξύ των χρηστών.

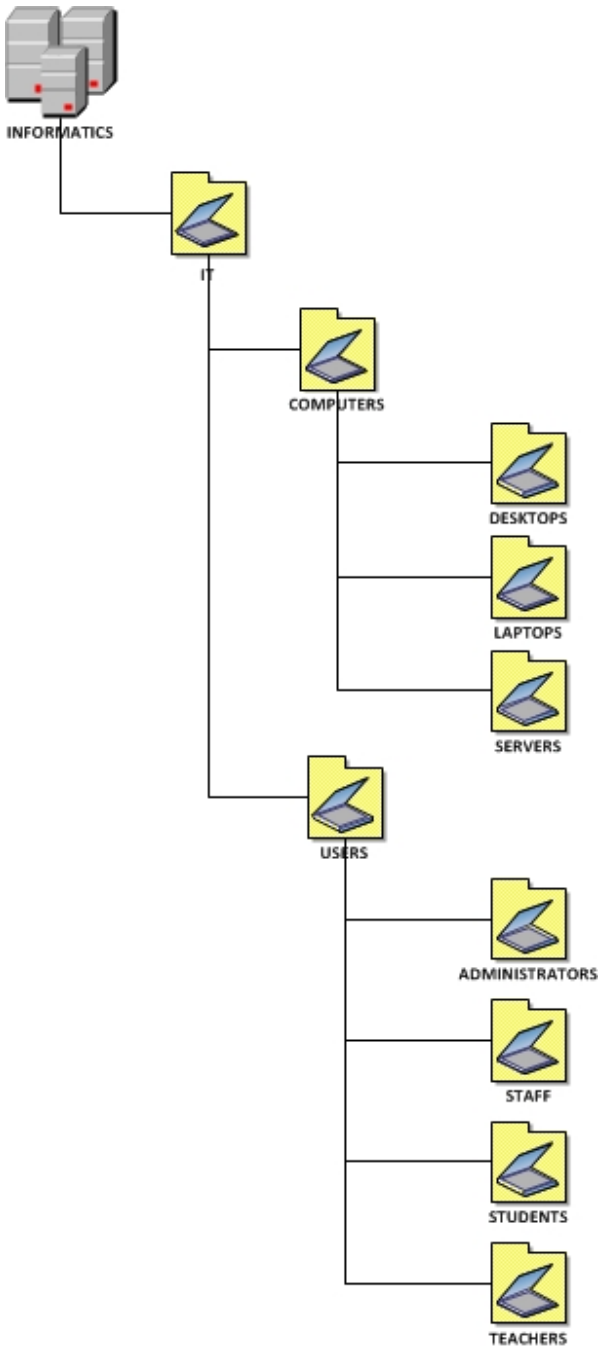
Η βασική δομική μονάδα μιας υπηρεσίας καταλόγου Active Directory είναι ένα αντικείμενο, ένα διακριτό, επώνυμο σύνολο ιδιοτήτων που αντιπροσωπεύει έναν πόρο δικτύου. Οι ιδιότητες αντικειμένων είναι χαρακτηριστικά αντικειμένων στον κατάλογο. Τα αντικείμενα μπορούν να οργανωθούν σε κλάσεις, οι οποίες είναι λογικές ομαδοποιήσεις αντικειμένων. Οι *χρήστες*, *ομάδες* και *υπολογιστές* είναι κάποια χαρακτηριστικά παραδείγματα διαφορετικών κλάσεων αντικειμένων. (screenshot)

Στο λειτουργικό σύστημα Windows Server 2008 οι AD DS περιέχουν μια δομή οργάνωσης και παρακολούθησης των διαφόρων οντοτήτων του συστήματος η οποία επιτρέπει στους διαχειριστές να κατηγοριοποιούν με τον βέλτιστο δυνατό τρόπο την ιεραρχία του δικτύου τους και να βλέπουν με μεγαλύτερη ευκολία τις ενέργειες που λαμβάνουν χώρα μέσα στον τομέα (domain). Η δομή αυτή οργάνωσης ονομάζεται Δεντρο (Domain Tree) και ο κεντρικός

υπολογιστή κάθε τομέα στον οποίο είναι εγκατεστημένα και τα AD DS είναι ο Ελεγκτής Τομέα (Domain Controller).

Ένας Domain Controller ελέγχει και διαχειρίζεται ένα πλήθος υπολογιστών οι οποίοι αποτελούν μέλη του εκάστοτε τομέα, ενώ χαρακτηριστικό του γνώρισμα είναι το ότι μπορεί να προσπελαστεί αποκλειστικά και μόνο από χρήστη του συστήματος ο οποίος φέρει την ιδιότητα του διαχειριστή (administrator). Κανένας χρήστης ο οποίος δεν έχει την ιδιότητα του διαχειριστή δεν μπορεί να επέμβει και να μεταβάλλει τη λειτουργία ενός domain controller. Θα πρέπει να σημειώσουμε ότι με την εγκατάσταση του AD σε κάποιον τομέα πραγματοποιείται εγκατάσταση μιας βάσης δεδομένων στην οποία μέσω των υπηρεσιών του αποθηκεύονται οι όποιες εισαγωγές, μεταβολές ή αφαιρέσεις των οντοτήτων (χρήστες, υπολογιστές, συσκευές κτλ.) του δικτύου. Το AD υποστηρίζει την ταυτόχρονη ύπαρξη περισσοτέρων από έναν Domain Controller στον ίδιο (subdomain) αλλά και σε διαφορετικό τομέα. Η ύπαρξη περισσοτέρων domain controllers προϋποθέτει την εννοιολογική σύνδεση μεταξύ τους μέσω της σχέσης γονέα-παιδιού (parent-child). Το σύνολο των Domain Controllers, Domain Trees καθώς και οι εξαρτήσεις μεταξύ τους μας συνθέτουν την έννοια του Δάσους (Domain Forest) Παρακάτω παρουσιάζεται σχηματικά η απεικόνιση της έννοιας του Δάσους. (screenshot)

Η ταυτόχρονη ύπαρξη πολλών domain σε έναν οργανισμό δημιουργεί αυτόματα την ανάγκη ύπαρξης του ίδιου αριθμού domain controllers πράγμα που με τη σειρά του μπορεί να οδηγήσει σε ένα μεγάλου μεγέθους domain forest με χιλιάδες (ή ακόμα και εκατομμύρια) αντικείμενα προς διαχείριση. Όπως μπορεί να γίνει εύκολα κατανοητό η διαχείριση όλου αυτού του όγκου των αντικειμένων χωρίς κάποιο είδος διαχωρισμού τους ή ταξινόμησής τους είναι σχεδόν ανέφικτη. Διέξοδο σε αυτό το πρόβλημα δίνεται με τις οργανωτικές μονάδες (organizational units – OU). Οι OU έχουν σχεδιαστεί για να μειώνουν την κλίμακα διαχείρισης των AD DS. Σκοπός τους είναι να κάνουν τη διαχείριση του κάθε domain ξεχωριστά πιο αποδοτική δημιουργώντας σε κάθε ένα ξεχωριστά μια ιεραρχική δομή των αντικειμένων που το απαρτίζουν. Η παρακάτω εικόνα απεικονίζει τον τρόπο με το πώς μια δομή οργανωτικών μονάδων μπορεί να δείχνει.

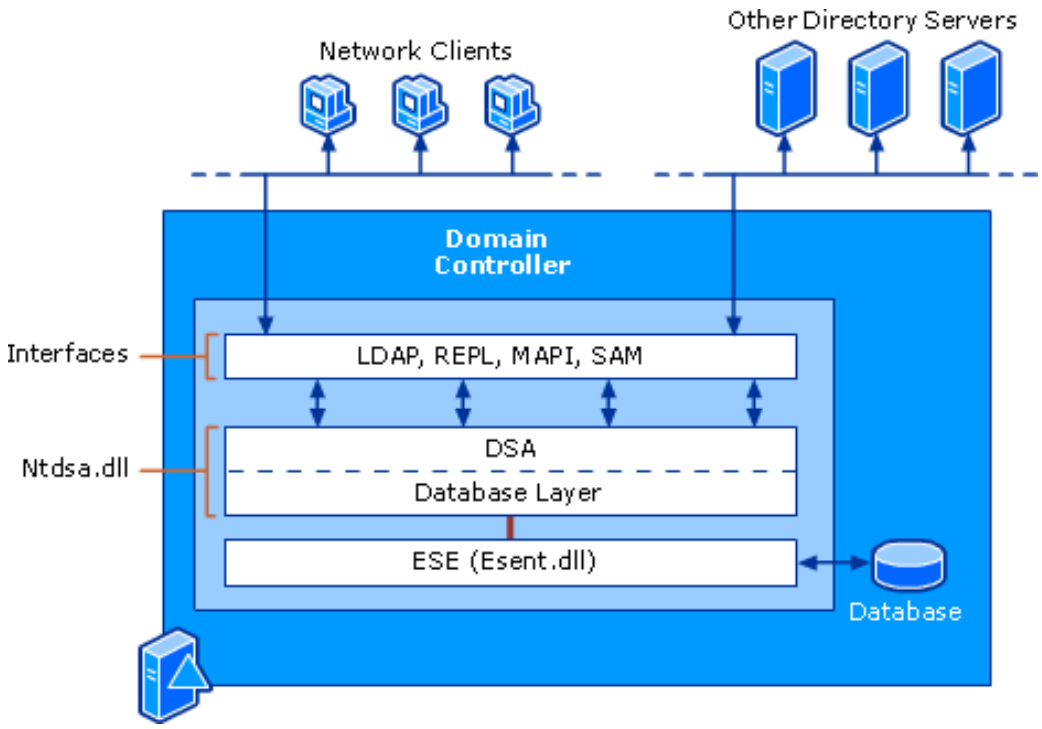


Κύριος διαχωρισμός OU σε υπολογιστές και χρήστες

1.2 ΦΥΣΙΚΗ ΔΟΜΗ

Όλα δεδομένα των AD DS καταχωρούνται σε μία ξεχωριστή βάση δεδομένων η οποία βρίσκεται στον εκάστοτε Domain Controller. Μέσω του Domain Controller μπορεί να την προσπελάσει ο διαχειριστής και να εφαρμόσει, σε χρήστες και υπολογιστές, λειτουργίες που

παρέχονται από τις υπηρεσίες καταλόγου όπως η αυθεντικοποίηση (authentication) και η εξουσιοδότηση (authorization). Όταν υλοποιούμαι τις AD DS μπορούμε να προσθέσουμε όσους Domain Controllers χρειάζεται, ώστε να μπορούν να υποστηρίξουν τις υπηρεσίες καταλόγου που χρειάζεται ο οργανισμός. Το αρχείο στο οποίο αποθηκεύονται τα δεδομένα της βάσης των AD DS είναι το Ntds.dit και μαζί με τα transaction logs του Domain Controller βρίσκονται στον %SystemRoot%\NTDS φάκελο στον Domain Controller. Τα αρχεία αυτά περιέχουν όλες τις πληροφορίες καταλόγου για τον εκάστοτε τομέα καθώς και πληροφορίες που διαμοιράζονται από όλους τους Domain Controllers σε κάθε οργανισμό. Η καταχώρηση δεδομένων (Data Store) των AD DS υλοποιείται σε κάθε τομέα ενός Domain Forest. Παρακάτω παρουσιάζονται σχηματικά τα στάδια από τα οποία αποτελείται η διαδικασία καταχώρησης δεδομένων των AD DS. (screenshot)



Συστατικά στοιχεία του Data Store των AD DS.

Interfaces (διεπαφές): Οι υπολογιστές πελάτες (clients), οι διαχειριστές καθώς και οι Domain Controllers δεν μπορούν να επικοινωνήσουν απευθείας με τη βάση δεδομένων. Η

καταχώρηση δεδομένων υποστηρίζει τα παρακάτω Interfaces για clients και servers ώστε να υλοποιείται η επικοινωνία μεταξύ αυτών και του Data Store.

- LDAP -Lightweight Directory Access Protocol-
- REPL –Replication and Domain Controller Management Interface-
- MAPI –Messaging API-
- SAM -Security Accounts Manager-

DSA (Directory Service Management): Το DSA είναι ο δεσμός μεταξύ της βάσης και των χρηστών. Είναι το εργαλείο αυτό που επιλέγει ποιο από τα παραπάνω interfaces θα χρησιμοποιηθούν για πρόσβαση των clients ή servers στη βάση. Στο σύστημα το DSA εμφανίζεται ως Ntdsai.dll.

Database Layer : Το Database Layer είναι μια διεπαφή προγραμματισμού εφαρμογών (API) η οποία βρίσκεται στο αρχείο ntdsa.dll και παρέχει μια εσωτερική διεπαφή μεταξύ των εφαρμογών και της βάσης δεδομένων του directory, για την προστασία των δεδομένων από την άμεση αλληλεπίδραση με τις εφαρμογές. Όλες οι εφαρμογές οι οποίες προσπαθούν να αποκτήσουν πρόσβαση στη βάση, το κάνουν διαμέσου του Database Layer.

ESE (Extensible Storage Engine) : Το ESE είναι ένα συστατικό (component) των Windows το οποίο χρησιμοποιείται από τις AD DS καθώς εξίσου και από άλλα συστατικά των windows ως διεπαφή προς τη βάση. Το έχει τρέχει ως Esent.dll και είναι υπεύθυνο για τη διαχείριση των πινάκων της βάσης του καταλόγου.

1.3 ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ

Υπάρχουν κάποιες βασικές έννοιες τις οποίες πρέπει να κατανοήσουμε για να καταλάβουμε το πως λειτουργεί η ασφάλεια των AD DS σε ένα δίκτυο Windows Server 2008. Η

ασφάλεια απαρτίζεται από 2 τύπους αντικειμένων και των αλληλεπιδράσεων μεταξύ αυτών. Το πρώτο αντικείμενο είναι μια *μονάδα ασφαλείας* (security principal) ή αλλιώς ένα αντικείμενο το οποίο αναπαριστά έναν χρήστη, ένα γκρουπ χρηστών ή κάποιον μεμονωμένο υπολογιστή ό οποίος ζητάει πρόσβαση σε κάποιο πόρο του δικτύου. Το δεύτερο αντικείμενο είναι ο ίδιος ο πόρος του δικτύου στο οποίο η μονάδα ασφαλείας ζητάει πρόσβαση. Για να παρέχει το σωστό επίπεδο ασφάλειας οι AD DS προϋποθέτει να έχουν κάποια μέθοδο που να καθορίζει την ταυτότητα της μονάδας ασφαλείας και κατά συνέπεια να δίνει το σωστό επίπεδο πρόσβασης στους πόρους του δικτύου.

Οι μονάδες ασφαλείας είναι τα μοναδικά αντικείμενα των AD DS στα οποία μπορεί να τους επιτραπεί η άδεια για να προσπελάσουν πόρους του δικτύου. Σε κάθε μονάδα ασφαλείας εκχωρείται ένα αναγνωριστικό ασφαλείας (Security Identifier – SID) το οποίο αποτελείται από δύο μέρη. Το πρώτο είναι το αναγνωριστικό τομέα (domain identifier) το οποίο το έχουν κοινό όλες οι μονάδες ασφαλείας που ανήκουν στον ίδιο τομέα και το άλλο είναι το σχετικό αναγνωριστικό (Relative Identifier – RID) το οποίο είναι και μοναδικό για κάθε μονάδα ασφαλείας στον τομέα. Η έλεγχος για την αποδοχή ή μη της πρόσβασης σε μια μονάδα ασφαλείας στο σύστημα γίνεται ελέγχοντας το SID της μονάδας αυτής και όχι το όνομά της. Πράγμα που σημαίνει ότι σε περίπτωση που γίνει αλλαγή στην ονομασία της δεν επηρεάζεται η όλη διαδικασία.

Το άλλο συστατικό το οποίο περιλαμβάνεται στην ασφάλεια των AD DS είναι το αντικείμενο το οποίο η μονάδα ασφαλείας προσπαθεί να προσπελάσει. Το αντικείμενο αυτό μπορεί να είναι μια οργανωτική μονάδα, ένας εκτυπωτής ή ακόμα και κάποια άλλη μονάδα ασφαλείας. Το αντικείμενο μπορεί επίσης να είναι κάποιος πόρος όπως κάποιο αρχείο σε κάποιον Server που τρέχει Windows Server 2008 ή ακόμα και κάποιο mailbox σε κάποιον Mail Server (πχ Microsoft Exchange Server 2010). Τα δικαιώματα (permissions) τα οποία έχουν αποδοθεί σε αυτά τα αντικείμενα είναι όλα καταχωρημένα σε μια λίστα ελέγχου πρόσβασης (Access Control List – ACL). Κάθε αντικείμενο στις AD DS συνοδεύεται από κάποιον περιγραφέα ασφάλειας (security descriptor). Ο περιγραφέας ασφάλειας περιλαμβάνει το SID της μονάδας ασφάλειας στην οποία ανήκει. Αντίθετα κάθε αντικείμενο έχει δύο ξεχωριστές λίστες ελέγχου πρόσβασης. Μια διακριτική λίστα (Discretionary Access Control List – DACL) και μία λίστα

συστήματος (System Access Control List – SACL). Η διακριτική λίστα καταχωρεί τις μονάδες ασφαλείας που έχουν εκχωρήσει δικαιώματα στο εκάστοτε αντικείμενο καθώς και το επίπεδο των δικαιωμάτων που έχουν εκχωρηθεί σε κάθε μονάδα ασφαλείας. Η λίστα συστήματος καταγράφει τις μονάδες ελέγχου των οποίων η πρόσβαση στους πόρους που ζητάει να προσπελάσει, χρειάζεται να ελεγχθεί. Ο συνδετικός κρίκος μεταξύ του SID της μονάδας ελέγχου και της λίστας ελέγχου πρόσβασης ονομάζεται σημείο πρόσβασης (access token)

Για να μπορέσει ένας χρήστης να κάνει χρήση των λειτουργιών του τομέα του AD θα πρέπει αρχικά με κάποιο τρόπο να αποκτήσει πρόσβαση στο δίκτυο. Βασικά ο κάθε χρήστης ο οποίος επιχειρεί σύνδεση στο δίκτυο, πρέπει να μπορεί να αποδείξει ότι είναι αυτός που ισχυρίζεται ώστε να του επιτραπεί η είσοδος από τον domain controller. Η διαδικασία αυτή ονομάζεται Αυθεντικοποίηση (authentication). Η διαδικασία της αυθεντικοποίησης λαμβάνει χώρα κατά την αρχική διαδικασία εισόδου ενός client-user σε ένα υπολογιστή ο οποίος είναι μέλος ενός AD DS τομέα. Τα ακριβή βήματα εισόδου ποικίλουν ανάλογα με το λειτουργικό σύστημα του υπολογιστή από τον οποίο επιχειρείται η είσοδος. Στα λειτουργικά Windows 2000, Windows XP Professional ή Windows Server 2003 η σύνδεση επιτυγχάνεται πατώντας τον συνδυασμό πλήκτρων alt+ctrl+del, και βάζοντας τα απαραίτητα Username και Password αλλά και το όνομα του τομέα στα αντίστοιχα πεδία. Η διαδικασία αυτή υλοποιείται μέσω της βιβλιοθήκης δυναμικής σύνδεσης GINA (Graphic Identification and Authentication), η οποία στο σύστημα ‘τρέχει’ ως Msgina.dll. Τα Windows Vista, Windows 2008 Server και Windows 7 δεν κάνουν χρήση αυτής της βιβλιοθήκης. Αντίθετα έχουν στο λειτουργικό τους σύστημα ενσωματωμένη λειτουργία απευθείας καταχώρησης και ελέγχου των στοιχείων του χρήστη που προσπαθεί να εισέλθει στο σύστημα χώρις την ενδιάμεση κλήση κάποιου ‘μεσολαβητικού’ .dll. Για την ταυτοποίηση των στοιχείων του χρήστη τα Windows Server 2008 έχουν δύο *παρόχους ασφαλούς υποστήριξης (Security Support Providers – SSP).* Τον Kerberos SSP και τον NT LAN Manager (NTLM) SSP. Αν ο client από τον οποίο επιχειρείται η σύνδεση (και κατά συνέπεια η αυθεντικοποίηση) χρησιμοποιεί λειτουργικό σύστημα Windows 2000 ή νεότερο τότε γίνεται χρήση του Kerberos SSP σε αντίθετη περίπτωση γίνεται χρήση του NTLM SSP.

1.4 GROUP POLICY

Επειδή με την πάροδο του χρόνου το πλήθος των υπολογιστών σε κάποιος οργανισμό συνεχώς αυξανόταν γινόταν ολοένα και δυσκολότερη η διαχείριση, η εποπτεία καθώς και διαμόρφωση των ρυθμίσεων του καθενός ξεχωριστά. Οι συνθήκες αυτές δημιουργούσαν συχνά προβλήματα σε μεγάλους οργανισμούς καθώς απαιτούσαν περισσότερο τεχνικό προσωπικό ώστε να αποφεύγονται τα απρόοπτα που μπορούσε να δημιουργήσει η (εσκεμμένα ή μη) λανθασμένη χρήση των υπολογιστών από τους χρήστες τους. Τη λύση σε αυτό το πρόβλημα (αλλά και σε άλλα πολλά) έρχεται να δώσει το Group Policy.

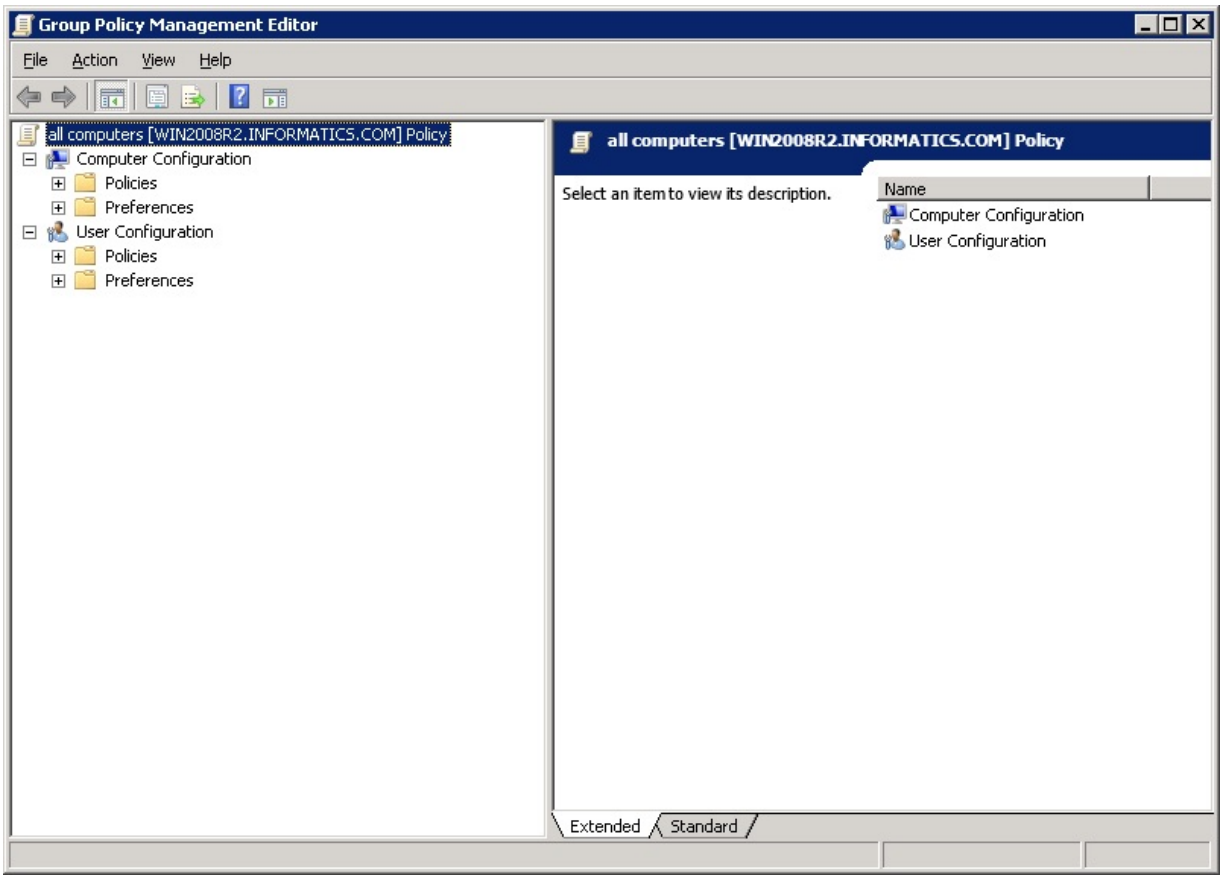
Το Group Policy είναι ένας μηχανισμός ο οποίος μας επιτρέπει την κεντρική διαχείριση των υπολογιστών και των χρηστών που ανήκουν σε έναν τομέα. Με την υπηρεσία αυτή των Windows Server 2008 παρέχονται τεράστιες δυνατότητες διαχείρισης των ρυθμίσεων διαμόρφωσης (configuration settings) που σχετίζονται με τους υπολογιστές αλλά και τους χρήστες στο περιβάλλον του active Directory. Αναφέρουμε επιλεκτικά κάποιες από τις δυνατότητες του Group Policy.

- *Εγκατάσταση Λογισμικού και Διαχείριση* : μέσω του Group Policy για το AD μπορεί να πραγματοποιηθεί εγκατάσταση, αναβάθμιση ή και απεγκατάσταση προγραμμάτων σε επιλεγμένους υπολογιστές μέλη της δομής του AD.
- *Scripts* : μπορεί να πραγματοποιηθεί η εκτέλεση κάποιου script κατά την έναρξη – τερματισμό ενός υπολογιστή ή και κατά τη σύνδεση – αποσύνδεση ενός χρήστη.
- *Ρυθμίσεις Ασφαλείας* : υπάρχει ένας τεράστιος αριθμός από ρυθμίσεις ασφαλείας οι οποίες μπορούν να διαμορφωθούν ανάλογα για υπολογιστές αλλά και χρήστες.
- *Folder Redirection* : μπορεί να γίνει επαναφορά κάποιων τμημάτων του περιβάλλοντος εργασίας του χρήστη, όπως ο φάκελος *'Τα Έγγραφά μου'*, το '*Start Menu'* ή η *'Επιφάνεια Εργασίας' σε* προεπιλεγμένη (default) κατάσταση.

- *Internet Explorer Settings* : μπορεί να γίνει χρήση του Group Policy για να διαχειριστούμε τα menu, τα toolbars, τις ρυθμίσεις σύνδεσης, τα αγαπημένα και τα security features του Internet Explorer.
- *Administative Templates* : Μέσω των Administrative Templates μπορούμε να διαχειριστούμε ένα μεγάλο πλήθος από GUI στοιχείων, όπως οι ρυθμίσεις του *Πίνακα Ελέγχου*, οι ρυθμίσεις της *Επιφάνειας Εργασίας* καθώς και τις ρυθμίσεις του *Μενού Έναρξης* αλλά και της *Μπάρας Εργασίας.* Αυτές οι ρυθμίσεις επεμβαίνουν στη Registry και περιορίζουν τις αλλαγές τις οποίες μπορεί να πραγματοποιήσει κάποιος χρήστης στον Υπολογιστή του.
- *Preferences* : παρέχεται η δυνατότητα διαχείρισης ενός πλήθους επιλογών που σχετίζονται με ρυθμίσεις των Windows, drive mappings, μεταβλητές περιβάλλοντος, κοινή χρήση στο δίκτυο, τοπικούς χρήστες και γκρουπ χρηστών, συκευές και άλλα..
- *Εκτυπωτές* : Οι διαχειριστές έχουν τη δυνατότητα τώρα πια να επιτρέπουν ή να απαγορεύουν στους χρήστες να κάνουν εγκατάσταση κάποιου νέου εκτυπωτή (καθώς και άλλων συσκευών) μέσω του Group Policy.
- *Απαγόρευση Εγκατάστασης Συσκευής* : Μπορεί να απαγορευτεί εξ' ολοκλήρου η εγκατάσταση κάποιας συσκευής στο δίκτυο μας. Μπορούν να δημιουργηθούν πολιτική ρυθμίσεων για την πρόσβαση σε συσκευές όπως USB drives, μονάδες DVD καθώς και άλλα αφαιρούμενα μέσα.
- *Ρυθμίσεις Διαχείρισης Ενέργειας* : Όλες οι ρυθμίσεις Διαχείρισης Ενέργειας μπορούν να ελεγχθούν μέσω του Group Policy παρέχοντας έτσι ένα μεγάλο κέρδος σε κάποιον οργανισμό μέσω της εξοικονόμησης ενέργειας.

Όπως μπορεί να παρατηρηθεί και από τα παραπάνω οι ρυθμίσεις του Group Policy (οι οποίες αξίζει να σημειωθεί πως είναι περίπου 1500 στον αριθμό) χωρίζονται, ανάλογα στο αντικείμενο στο οποίο εφαρμόζονται, σε δύο μέρη : User Configuration και Computer Configuration. Όλες οι ρυθμίσεις που αφορούν τον χρήστη (User Configuration) εφαρμόζονται κάθε φορά που ο χρήστης εισέρχεται στον λειτουργικό σύστημα (user logon) ενώ οι ρυθμίσεις

που αφορούν τους υπολογιστές (Computer Configuration) εφαρμόζονται κάθε φορά που ξεκινά τη λειτουργία του ο υπολογιστής (computer start up). Κάθε φορά που εισέρχεται ένας client στο σύστημα κατεβάζει τις ρυθμίσεις από τον Domain Controller και τις εφαρμόζει τοπικά. Το σύνολο των ρυθμίσεων είναι αποθηκευμένο στη βάση δεδομένων του AD.



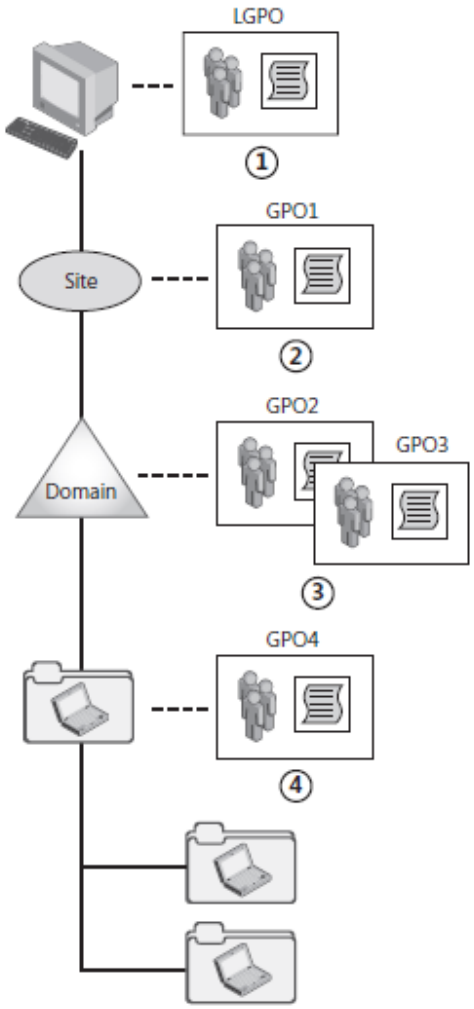
Κονσόλα διαχείρησης του group policy

Οι ρυθμίσεις στο Group Policy συναντώνται στο σύστημα σε μορφή αντικειμένων (Group Policy Object – GPO) και είναι συνδεδεμένα με διάφορα επίπεδα της δομής του AD όπως ο τομέας ή η οργανωτική μονάδα (OU). Η ιεραρχική δομή του AD παρέχει τη δυνατότητα σε ρυθμίσεις του Group Policy οι οποίες εφαρμόζονται σε αντικείμενα ψηλά στη δομή του AD να κληρονομούνται από αντικείμενα που βρίσκονται χαμηλότερα. Κατά την αρχική δημιουργία ενός τομέα Active Directory, δημιουργούνται παράλληλα δύο GPOs και συνδέονται με το Active Directory. Το αντικείμενο Default Domain Policy και το Default Domain Controllers Policy. Το

πρώτο εφαρμόζεται σε επίπεδο τομέα και θέτει το αρχικό επίπεδο ασφάλειας καθώς και τους περιορισμούς των κωδικών για όλον τον τομέα. Από την άλλη, το Default Domain Controllers Policy χρησιμοποιείται για να ρυθμιστούν οι αρχικές ρυθμίσεις ασφαλείας των Domain Controllers.

Σε παλαιότερα λειτουργικά συστήματα (Windows XP, Windows Server 2003), Η χρήση των ρυθμίσεων γινόταν από ένα τοπικό αντικείμενο Group Policy (Local Group Policy Object - LGPO), το οποίο επηρέαζε όλους τους χρήστες που εισέρχονταν στον υπολογιστή. Στα πιο σύγχρονα λειτουργικά συστήματα (Windows Vista, Windows 7, Windows Server 2008) παρουσιάζεται πάλι η ύπαρξη ενός μόνο GPO αλλά παρέχεται η δυνατότητα δημιουργίας περισσοτέρων για πρόσθετες διαχειριστικές δυνατότητες, αλλά και πρόσθετους περιορισμούς ασφαλείας στο σύστημα μας.

Αν η χρήση του LGPO είναι επιλεγμένη στο σύστημα, τότε αυτή εκτελείται και πρώτη και στους stand-alone αλλά και στους υπολογιστές μέλη του AD τομέα. Στη συνέχεια εκτελείται η LGPO που έχει ανατεθεί στο επίπεδο του domain και θα έχει επίπτωση μόνο στους υπολογιστές και τους χρήστες που είναι μέλη αυτού του domain. Τέλος εκτελούνται τυχόν LGPO’s έχουν ανατεθεί σε επίπεδο Οργανωτικών μονάδων (OU level) . Αυτές με τη σειρά τους θα έχουν επίδραση σε υπολογιστές και χρήστες που ανήκουν σε αυτές τις μονάδες καθώς επίσης θα κληρονομηθούν από τυχόν μονάδες παιδιά (child OU) των αρχικών μονάδων.



Ιεραρχία εκτέλεσης LGPO

Ένα Group Policy αντικείμενο του Active Directory αποτελείται από δύο βασικά συστατικά (components) τα οποία παρουσιάζουν τη φυσική και λογική δομή του αντικειμένου. Το συστατικό της λογικής δομής είναι καταχωρημένο μέσα στη βάση του Active Directory και ονομάζεται Group Policy Container (GPC) ενώ το συστατικό της φυσικής δομής είναι βρίσκεται στον αναπαραγόμενο σε κάθε Domain Controller φάκελο, με όνομα SYSVOL, και ονομάζεται Group Policy Template (GPT).

Όταν δημιουργείται ένα νέο αντικείμενο Group Policy το GPC δημιουργείται στη βάση του Active Directory. Το GPC στο σύστημα εμφανίζεται με ένα καθολικά μοναδικό αναγνωριστικό

για όνομα και περιέχει γνωρίσματα που περιγράφουν διάφορους τύπους πληροφοριών για το Group Policy αντικείμενο. Κάποιοι από τους τύπους αυτούς είναι :

- Το όνομα του Group Policy αντικειμένου
- Η διαδρομή για το Group Policy Template
- Ο αριθμός έκδοσης
- Η κατάσταση του Group Policy αντικειμένου (enabled – disabled)

Τις λεπτομέρειες αυτές μπορούμε να τις δούμε μέσω της επιλογής Active Directory Users And Computers ή μέσω του εργαλείου ADSI Edit που έχουμε αναφέρει ξανά σε προηγούμρνη ενότητα.

Από την άλλη μεριά τώρα, με τη δημιουργία του αντικειμένου Group Policy δημιουργείται και το αντίστοιχο Group Policy Template στον φάκελο %System Root%\SYSVOL του κάθε τομέα. Το GPT περιλαμβάνει τις πιο πολλές από τις ρυθμίσεις του αντικειμένου καθώς και ένα πλήθος από φακέλους και αρχεία διαμόρφωσης. Οι φάκελοι και τα αρχεία που περιλαμβάνει το κάθε GPT είναι τα εξής:

- Adm (φάκελος) : δε χρησιμοποιείται στις καινούριες εκδόσεις λειτουργικών συστημάτων.
- USER (φάκελος) : περιέχει όλες τις ρυθμίσεις για τη διαμόρφωση χρήστη (user configuration)
- MACHINE (φάκελος) : αντίθετα με τον φάκελο USER περιέχει όλες τις ρυθμίσεις για τη διαμόρφωση υπολογιστή (computer configuration)
- Gpt.ini (αρχείο) : στο αρχείο αυτό είναι αποθηκευμένος ο αριθμός έκδοσης του GPT καθώς και το όνομα του συνεργαζόμενου αντικειμένου Group Policy.

1.5 ROAMING PROFILES

Μια συνήθης πρόκληση για τους διαχειριστές των δικτύων είναι η διαχείριση των δεδομένων των χρηστών και οι ρυθμίσεις των προφίλ τους. Αυτό παρατηρείται διότι οι τελικοί χρήστες πάντα περιμένουν ότι το περιβάλλον εργασίας του υπολογιστή τους θα είναι πάντα το ίδιο καθώς και ότι τα δεδομένα τους θα είναι εξίσου διαθέσιμα ανεξάρτητα το πώς ή το πότε εισέρχονται στο δίκτυο. Στο περιβάλλον των Windows Server 2008 και στην αυτή η 'απαίτηση' μπορεί να γίνει εφικτή με τη χρήση των *φορητών προφίλ χρηστών* (roaming user profiles). Τα roaming profiles μπορούν να υλοποιηθούν κάνοντας χρήση του Active Directory και κάποιες από τις ρυθμίσεις για τον έλεγχο τους και τη συμπεριφορά τους μπορούν να ρυθμιστούν μέσω του Group Policy. Δίνουν τη δυνατότητα στους χρήστες που ανήκουν σε έναν τομέα να έχουν πρόσβαση στο προσωπικό τους προφίλ από οποιονδήποτε υπολογιστή του ίδιου τομέα. Με τον όρο *προσωπικό προφίλ* εννοούμε τις προσωπικές ρυθμίσεις και προτιμήσεις του χρήστη (θέματα επιφάνειας εργασίας, μενού, μπάρα εργασίας, εικονίδια κλπ) και τα αρχεία που αποθηκεύει στους φακέλους του προφίλ του (τα έγγραφα μου, η μουσική μου, οι λήψεις μου κλπ)

Τα roaming profiles καταχωρούνται σε ένα κοινόχρηστο τμήμα του δικτύου έτσι ώστε το προφίλ να είναι διαθέσιμο ανεξάρτητα από τον υπολογιστή που θα εισέλθει ο τελικός χρήστης. Επειδή στις καινούριες εκδόσεις των windows έχουν πραγματοποιηθεί αρκετές αλλαγές στη δομή του φακέλου που αποθηκεύονται οι ρυθμίσεις και τα δεδομένα του προφίλ σε σχέση με τις παλαιότερες εκδόσεις, θα πρέπει να είμαστε αρκετά προσεκτικοί όταν πρόκειται να εργαστούμε σε περιβάλλον όπου τα λειτουργικά των υπολογιστών που απαρτίζουν το δίκτυο ποικίλουν. Για παράδειγμα: Ένα roaming profile το οποίο έχει δημιουργηθεί για κάποιον υπολογιστή πελάτη με Windows 7 δεν είναι συμβατό σε έναν υπολογιστή με Windows XP.

Από προεπιλογή κάθε φορά που κάποιος χρήστης εισέρχεται για πρώτη σε κάποιον υπολογιστή, δημιουργείται ένα τοπικό προεπιλεγμένο προφίλ (Local Default Profile). Το αρχικό αυτό προφίλ βασίζεται σε ένα 'κρυφό' προφίλ με ονομασία *Default* και είναι στον φάκελο %SystemDrive%\Users. Όταν ένας χρήστης του οποίου το roaming profile έχει ρυθμιστεί ως

προφίλ χρήστη Windows Vista, εισέλθει σε κάποιον υπολογιστή για πρώτη φορά, τότε μπορεί να συμβεί ένα από τα παρακάτω :

- Να δημιουργηθεί ένα προφίλ ως αντίγραφο κάποιου ήδη κατασκευασμένου και ρυθμισμένου με συγκεκριμένες ρυθμίσεις προφίλ, που βρίσκεται αποθηκευμένο στον NETLOGON φάκελο του Domain Controller. Να σημειωθεί ότι το προεγκατεστημένο αυτό προφίλ πρέπει να έχει δημιουργηθεί σε λειτουργικό σύστημα Windows Vista ή νεότερο και να έχει γίνει αντιγραφή του στον κοινοχρηστο NETLOGON με την ονομασία Default User.v2. Το επίθεμα v2 δηλώνει ότι χρησιμοποιείται από Windows Vista ή νεότερο λογσμικό.
- Να δημιουργηθεί ένα τοπικό προεπιλεγμένο προφίλ σε περίπτωση που ο υπολογιστής δεν είναι συνδεδεμένος στον τομέα ή δεν υπάρχει ο φάκελος Default User.v2 στον κοινόχρηστο NETLOGON.

Όταν ο χρήστης αποσυνδεθεί από τον υπολογιστή του, όλες οι αλλαγές που γίναν κατά τη διάρκεια της παραμονής του σε αυτόν, αξιολογούνται και αντιγράφονται στον κοινόχρηστο NETLOGON στον Domain Controller. Όταν ο χρήστης εισέλθει και πάλι με τα στοιχεία του σε κάποιον άλλο υπολογιστή, οι τελευταίες αποθηκευμένες ρυθμίσεις του προφίλ του, θα φορτωθούν από τον Domain Controller και σαν αποτέλεσμα αυτού ο χρήστης θα μπορεί να έχει το περιβάλλον το οποίο είχε ο ίδιος προηγούμενα ορίσει.

1.6 REDIRECTED FOLDERS

Με τη χρήση των roaming profiles εξασφαλίζεται στον χρήστη ότι ανεξάρτητα από τον υπολογιστή με τον οποίο θα εισέλθει στο δίκτυο, το περιβάλλον εργασίας του θα είναι το πάντα το ίδιο και πάντα με βάση τις δικές του επιλογές. Παρόλα αυτά όμως τα roaming profiles έχουν και κάποιους περιορισμούς. Το πιο συχνό στην εμφάνιση του πρόβλημα είναι ότι το προφίλ του χρήστη μπορεί σε κάποιες περιπτώσεις να ..'ξεφύγει' σε μέγεθος. Ο χρήστης για παράδειγμα μπορεί να κρατάει ένα πλήθος αρχείων στα έγγραφά μου ή να αποθηκεύσει κάποια μεγάλου μεγέθους αρχεία στα βίντεο μου και στην επιφάνεια εργασίας. Αν υπολογίσουμε τον, μερικές

φορές, τεράστιο αριθμό χρηστών ενός οργανισμού και τον μεγάλο όγκο δεδομένων που μπορεί να επιθυμεί να αποθηκεύει ο κάθε ένας στο προφίλ του τότε οδηγούμαστε στην ανάγκη ύπαρξης πολλαπλάσιου αποθηκευτικού χώρου στον Domain Controller, ώστε να είναι δυνατόν να εξυπηρετηθούν όλοι οι χρήστες. Επίσης επειδή το προφίλ του χρήστη φορτώνεται κάθε φορά κατά την είσοδο του στο σύστημα αλλά και αντιγράφεται στον Domain Controller κάθε φορα που αποσυνδέεται ο χρήστης, αυτό οδηγεί σε καθυστέρηση φόρτωσης του προφίλ, ανάλογη με το μέγεθος των δεδομένων που πρόκειται να μεταφερθούν, αλλά και μεγάλο φόρτο στην κίνηση του δικτύου μας (network traffic).

Τη λύση σε αυτό το πρόβλημα τη δίνει το group policy μέσω της λειτουργίας ανακατεύθυνσης φακέλων (redirected folders). Με τη λειτουργία αυτή δίνεται η δυνατότητα χρήσης των roaming profiles χωρίς την ανησυχία υπερφόρτωσης του δικτύου μας αλλά και καθυστέρησης εισόδου στο σύστημα. Με την ενεργοποίηση της ανακατεύθυνσης ενός φακέλου, ο οποίος είναι τμήμα του τοπικού προφίλ ενός χρήστη, ο φάκελος ανακατευθύνεται εκτός του προφίλ μας και αποθηκεύεται σε έναν κοινόχρηστο φάκελο του δικτύου μας. Έτσι κάθε φορά που θα επιχειρείται προσπέλαση του φακέλου αυτού, θα γίνεται ουσιαστικά προσπέλαση του κοινόχρηστου φακέλου που βρίσκεται στο δίκτυο, ενώ όταν επιχειρείται αποθήκευση ενός αρχείου στον φάκελο αυτόν, το αρχείο θα αποθηκεύεται και πάλι στον κοινόχρηστο που θα έχουμε εμείς ορίσει. Η λειτουργία της ανακατεύθυνσης δεν γίνεται αντιληπτή από τον χρήστη παρά μόνο αν επιχειρήσει να δει την διαδρομή του φακέλου στην καρτέλα των ιδιοτήτων του.

Ένας άλλος τρόπος που μπορεί να φανεί η χρησιμότητα της ανακατεύθυνσης των φακέλων είναι η δυνατότητα που σου δίνει να δημιουργήσεις για ένα σύνολο χρηστών, ένα μη μεταβαλλόμενο τμήμα του προφίλ που εσύ επιθυμείς. Για παράδειγμα την επιφάνεια εργασίας. Μπορούμε να ρυθμίσουμε ένα γκρουπ χρηστών ώστε να κάνουν όλοι χρήση του φάκελο Desktop τον οποίο έχουμε ανακατευθύνει σε μια κοινόχρηστη τοποθεσία του δικτύου μας. Δίνοντας σε όλους του χρήστες δικαιώματα *μόνο για ανάγνωση* σε αυτόν τον φάκελο αυτόματα καταφέρνουμε να μην μπορεί να πραγματοποιηθεί καμία αλλαγή στην επιφάνεια εργασίας.

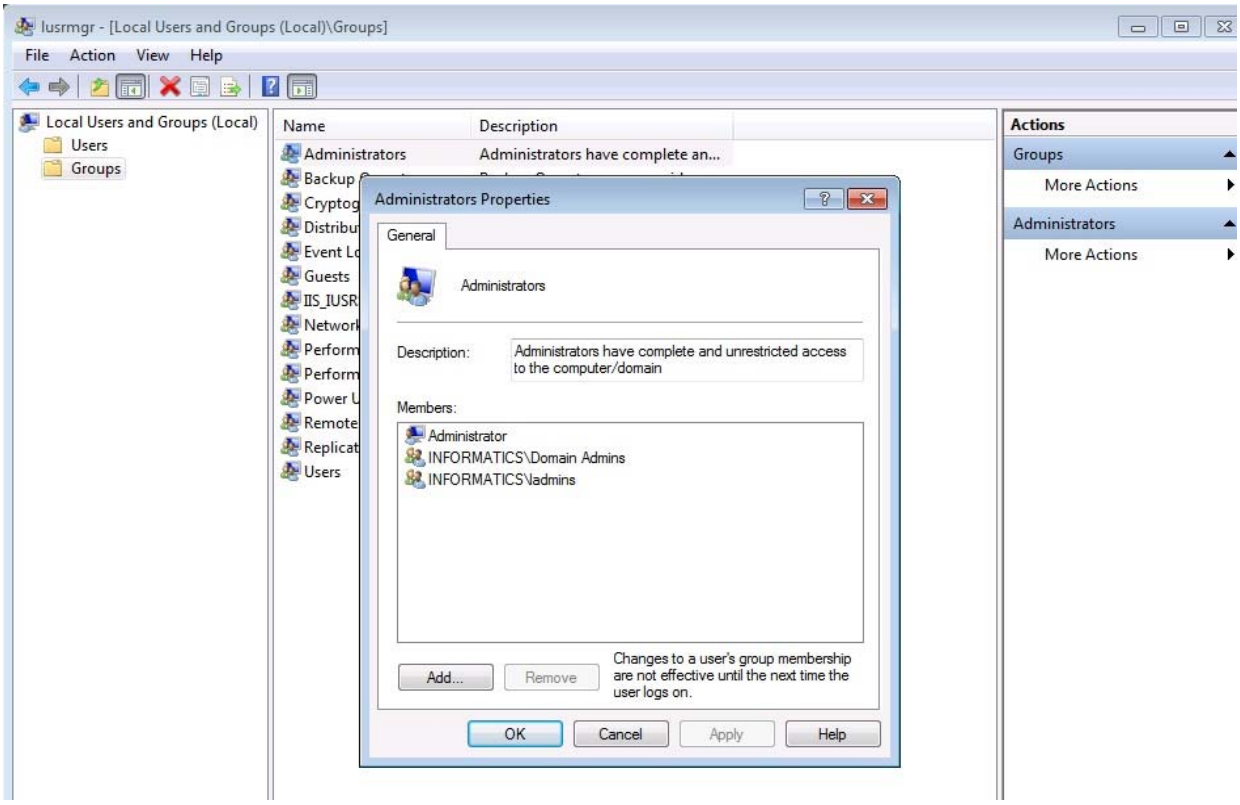
1.7 RESTRICTED GROUPS

Αναφερόμενοι στα restricted groups, κάνουμε λόγο για γκρουπ χρηστών με δικαιώματα διαχειριστή (χωρίς δικαιώματα στον Domain Controller), στους υπολογιστές που ανήκουν στο ίδιο domain. Κατά την δημιουργία ενός νέου χρήστη στο active directory, αυτός έχει εξ' ορισμού περιορισμένα δικαιώματα ανεξάρτητα με το ποιον υπολογιστή του τομέα θα χρησιμοποιήσει. Με τα χρήση των Restricted Groups μπορούμε να ορίσουμε το ποιοι χρήστες ή ποιες ομάδες χρηστών θα μπορούν να έχουν πρόσβαση στους υπολογιστές του τομέα με δικαιώματα διαχειριστή.

Υπάρχει η δυνατότητα δυο διαφορετικών υλοποιήσεων των Restricted Groups:

- Αντικατάσταση του τοπικού γκρουπ διαχειριστών με το γκρουπ ή τα γκρουπ χρηστών που θα ορίσουμε από το group policy.
- Πρόσθεση χρηστών στο ήδη υπάρχον τοπικό γκρουπ διαχειριστών.

Στην παρακάτω φωτογραφία φαίνεται ξεκάθαρα η πρώτη υλοποίηση. Οι τοπικοί διαχειριστές έχουν αντικατασταθεί από τα γκρουπ που ορίσαμε Domain Admins και ladmins (ο χρήστης administrator δημιουργείται με την εγκατάσταση του λειτουργικού συστήματος και είναι ανενεργός).

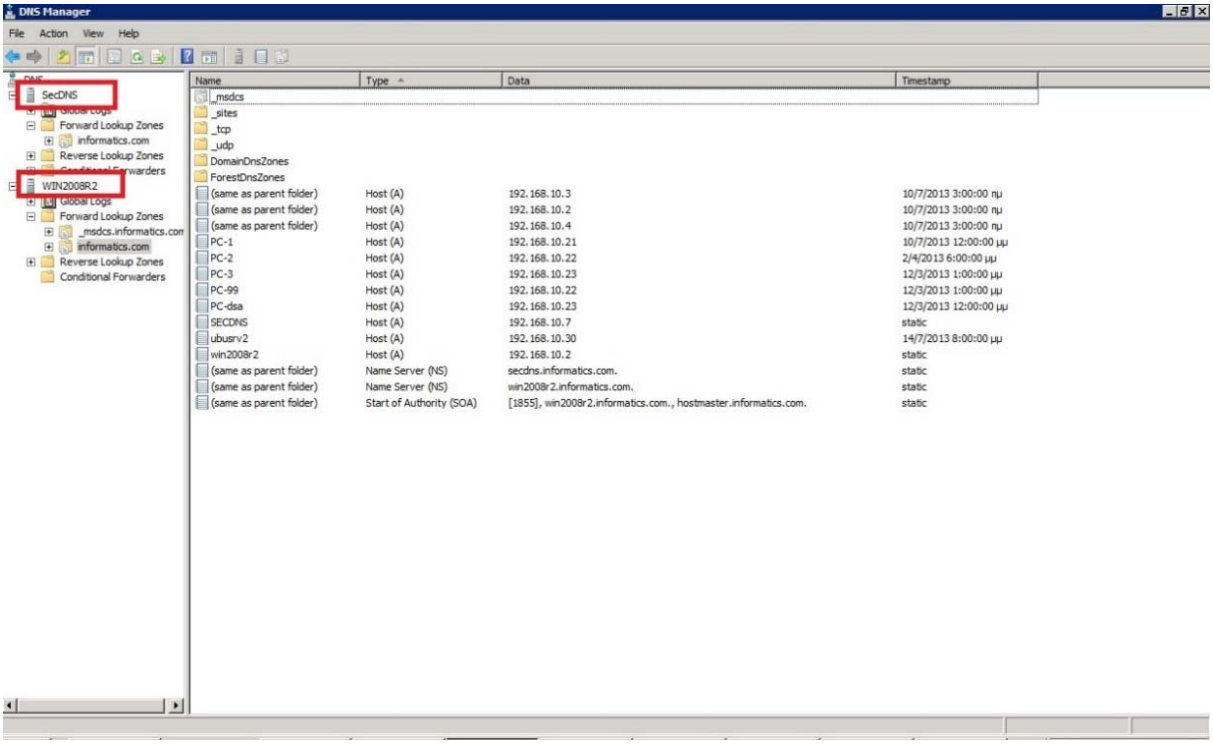

lusrmgr - [Local Users and Groups (Local)\Groups]
File Action View Help
Local Users and Groups (Local)
Users
Groups
Name
Description
Administrators
Administrators have complete an...
Guests
Actions
Groups
More Actions
Administrators
More Actions
Administrators Properties
General
Administrators
Description:
Administrators have complete and unrestricted access to the computer/domain
Members:
Administrator
INFORMATICS\Domain Admins
INFORMATICS\ladmins
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help

ΚΕΦΑΛΑΙΟ 2. DOMAIN NAME SYSTEM (DNS)

Η υλοποίηση του active directory και των AD DS προϋποθέτει την ύπαρξη κάποιων βοηθητικών υπηρεσιών όπως αυτή του DNS. Το Domain Name System ή DNS είναι ένα ιεραρχικό σύστημα ονοματοδοσίας για δίκτυα υπολογιστών, που χρησιμοποιούν το πρωτόκολλο IP. Το σύστημα DNS μπορεί και αντιστοιχίζει ονόματα με διευθύνσεις IP ή άλλα ονόματα στο Διαδίκτυο ή κάποιο άλλο δίκτυο.

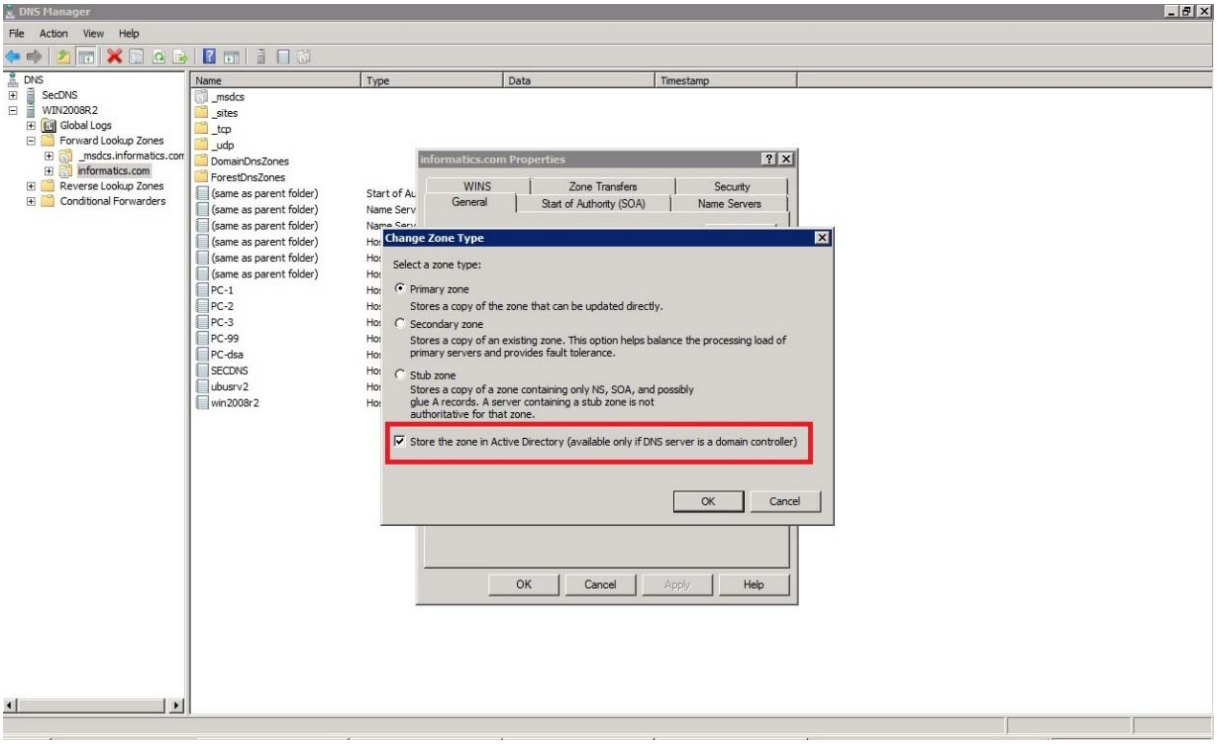
Οι Microsoft Windows Server 2008 Active Directory Domain Name Services απαιτούν DNS ώστε να εντοπίσουν πόρους του δικτύου. Ο DNS παρέχει τις πληροφορίες που χρειάζεται ο κάθε υπολογιστής μέλος του δικτύου μας, ώστε να εντοπίσει τον Domain Controller. Χωρίς τη χρήση μιας αξιόπιστης υποδομής DNS, η δημιουργία αντιγράφου AD DS μεταξύ των domain controller σε ένα δίκτυο θα αποτύχει, οι clients δε θα μπορούν να εισέλθουν (logon) στο δίκτυο και κάποιος Microsoft Exchange Server δε θα δύναται να στείλει mail. Ουσιαστικά αν η υλοποίηση του DNS μας δεν είναι σταθερή και διαθέσιμη, το Windows Server 2008 δίκτυό μας θα πέσει.

Λόγω της σημαντικότητας του DNS έχουν υλοποιηθεί δυο συστήματα DNS (primary και secondary). Το secondary απλά είναι ένα αντίγραφο του primary(read only) και περιέχει ακριβώς τις ίδιες εγγραφές με τον primary. Παρακάτω φαίνονται οι 2 DNS (SecDns και Win2008R2)

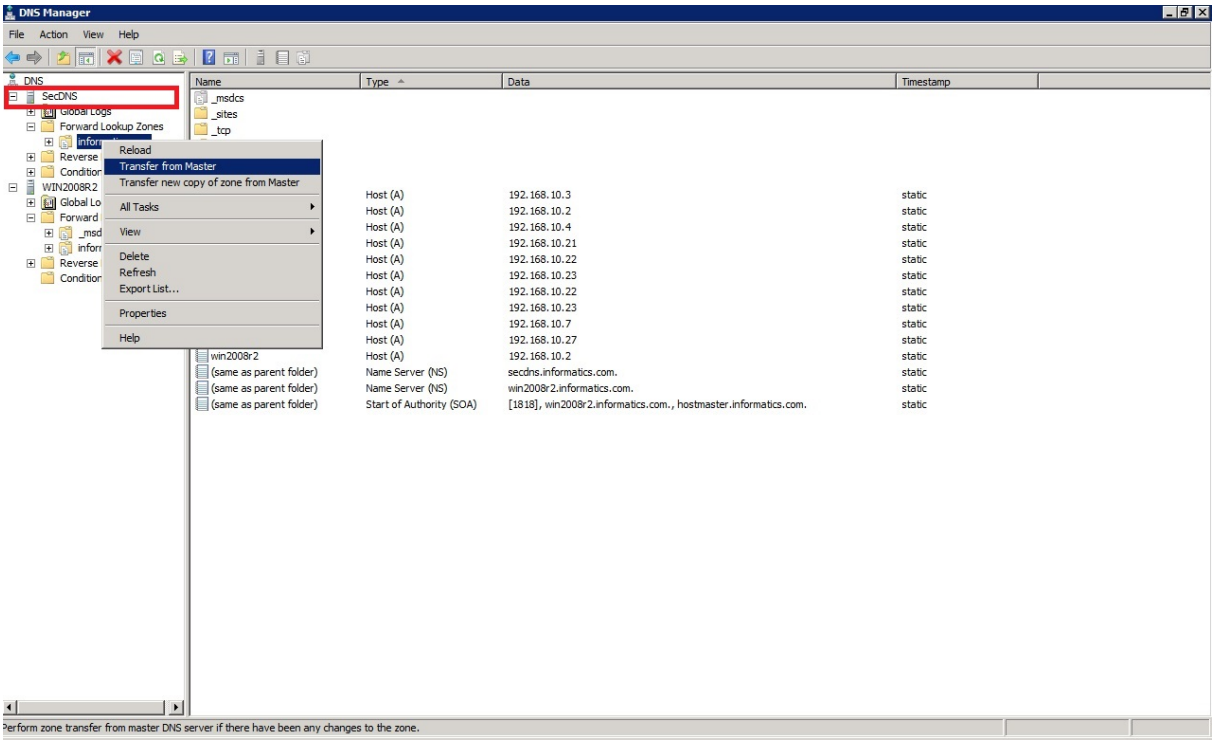


Οι 2 DNS του συστήματος μας (WIN2008R2 & SecDNS)

Ο πρωτεύον DNS(WIN2008R2) είναι ενσωματωμένος με το AD. Αυτό σημαίνει ότι οι ζώνες του είναι αποθηκευμένες στη βάση δεδομένων του AD. Αντίθετα ο δευτερεύον DNS (SecDns)έχει υλοποιηθεί ξεχωριστά σε εικονική μηχανή και ενημερώνεται απλά με τις εγγραφές του πρώτου.



Καταχώρηση ζωνών στη βάση του AD



Αντιγραφή δεδομένων από τον κεντρικό DNS στον δευτερεύων

Οι AD DS σχετίζονται με τον DNS με διάφορους τρόπους. Πρώτ' απ' όλα όλοι οι υπολογιστές με λειτουργικό σύστημα Microsoft Windows 2000 ή νεότερο χρησιμοποιούν τον DNS για να εντοπίσουν κάποιον Domain Controller σε ένα AD DS περιβάλλον. Σε περίπτωση που αποτύχει η εύρεση DNS, οι υπολογιστές θα προσπαθήσουν να βρουν εναλλακτικό τρόπο ένταξης στο δίκτυο κυρίως με τη χρήση του NetBIOS (NetBIOS Name Resolution) και με τεχνικές όπως η Windows Internet Name Service (WINS), το broadcast ή τα LMHosts Files. Έπειτα, μπορούμε να αποθηκεύσουμε δεδομένα του DNS στο Data Store των AD DS, μια λειτουργία που παρέχει βελτιωμένη λειτουργικότητα και ασφάλεια. Σε αντίθεση, τα ονόματα των AD DS τομέων είναι και από μόνα τους ονόματα (διευθύνσεις) DNS. Αν το AD DS δάσος μας (domain forest) περιλαμβάνει διάφορους τομείς σε ιεραρχική δομή (parent-child), η υλοποίηση του DNS μας μπορεί να αντιστοιχεί σε αυτήν των AD DS τομέων.

2.1 DNS ZONES, NAME SERVERS & RESOLVERS

Θέλοντας να αναλύσουμε κάποιους όρους του DNS τους οποίους θα χρησιμοποιήσουμε στη συνέχεια θα αναφερθούμε στις ζώνες (DNS Zones) και στους εξυπηρετητές (DNS Name Servers) και τους λύτες (DNS Resolvers).

Οι ζώνες αναφέρονται αποκλειστικά στη δομή του DNS. Οι περιοχές, ή αλλιώς τομείς (domains) χωρίζονται σε επίπεδα, όπου κάθε επίπεδο με τη σειρά του συχνά περιέχει κατώτερα επίπεδα. Για παράδειγμα, ένας τομέας πρώτου επιπέδου μπορεί να περιέχει ιεραρχικά τομείς δεύτερου επιπέδου κτλ. Η αλλαγή επιπέδου των ονομάτων χώρου είναι πολλές φορές ισοδύναμη με αλλαγή ζώνης DNS (DNS zone). Χρησιμοποιώντας την ορολογία που χρησιμοποιείται στην δενδρική δομή η ζώνη DNS είναι ένας κόμβος και ένα όνομα χώρου είναι ένα φύλλο. Όλες οι ζώνες DNS είναι και ονόματα χώρου χωρίς όμως να ισχύει και το αντίστροφο. Στην πράξη οι ζώνες DNS είναι τα φυσικά αρχεία που βρίσκονται σε εξυπηρετητές DNS και περιέχουν τις αντιστοιχίσεις ονομάτων και διευθύνσεων ή άλλων ονομάτων ως εγγραφές DNS (

DNS records ή resource records). Δηλαδή οι ζώνες DNS είναι απλές βάσεις δεδομένων και οι εγγραφές DNS είναι τα δεδομένα. Οι ζώνες DNS συνήθως σημαίνουν την αλλαγή διαχείρισης μιας περιοχής/τομέα και περιέχουν εγγραφές DNS (με κατεύθυνση από το όνομα) μόνο με το όνομα χώρου ή τομείς του. Όταν κάποιος κατοχυρώνει ένα όνομα χώρου στο σύστημα DNS στη ουσία παίρνει τον έλεγχο της ζώνης DNS αυτού του ονόματος χώρου.

Το Σύστημα DNS βασίζεται σε μια διανεμημένη βάση δεδομένων η οποία «τρέχει» στους εξυπηρετητές (Name Servers) του συστήματος και αποτελείται από ζώνες DNS οργανωμένες σε μια δενδρική δομή. Οι εξυπηρετητές DNS χωρίζονται στους αρχικούς (root) εξυπηρετητές, τους εξουσιοδοτημένους (authoritative) εξυπηρετητές, και τους αποθηκευτικούς (caching) εξυπηρετητές. Οι εξουσιοδοτημένοι εξυπηρετητές DNS χωρίζονται σε πρωτεύοντες και εναλλακτικούς (masters and slaves). Συνήθως κάποιος από τους πρωτεύοντες εξουσιοδοτημένους εξυπηρετητές ενός ονόματος χώρου είναι ο πρωταρχικός. Σε αυτόν γίνονται συνήθως οι αλλαγές.

Πελάτες των υπηρεσιών που παρέχουν οι εξυπηρετητές DNS είναι οι λύτες DNS (DNS resolvers). Οι λύτες είναι λογισμικό που χρησιμοποιείται από έναν χρήστη ή κάποιο πρόγραμμα που ζητά τις υπηρεσίες DNS. Οι λύτες διαβάζουν τα ονόματα του DNS από δεξιά προς τα αριστερά. Κάθε τελεία δείχνει την αρχή ενός υποσυνόλου και το σύνολο που περιλαμβάνει όλα τα σύνολα είναι η πιο δεξιά τελεία που ονομάζεται ρίζα και συνήθως παραλείπεται.

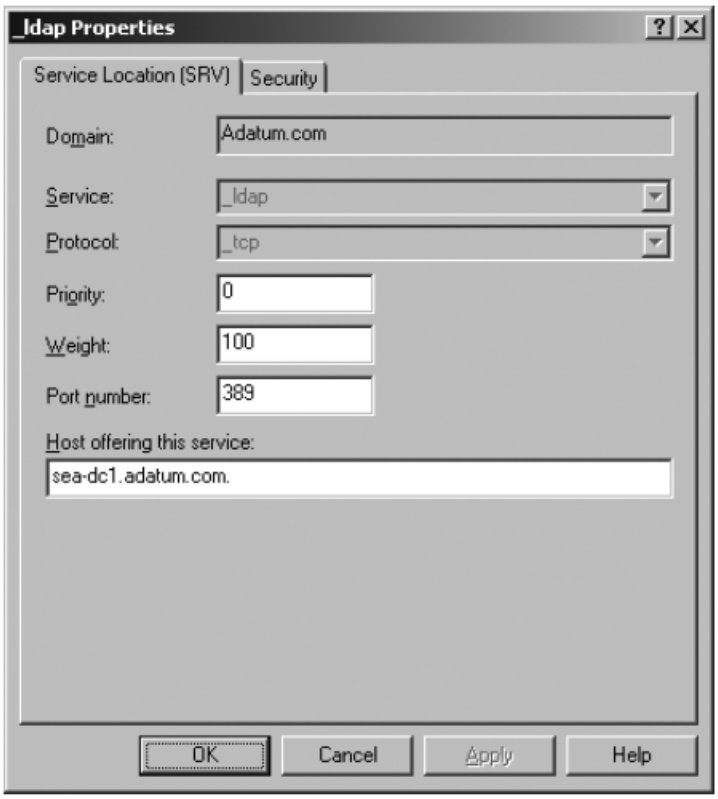
2.2 SRV RESOURCE RECORDS

Για τη διευκόλυνση του ορισμού της τοποθεσίας ενός Domain Controller σε κάποιον client, οι AD DS κάνουν χρήση των SRV resource records. Μία εγγραφή SRV χρησιμοποιείται για να προσδιορίσει υπολογιστές που παρέχουν υπηρεσίες τομέα διαμέσου ενός TCP/IP δικτύου. Η υπόδειξη των υπολογιστών αυτών στα Windows Server 2008, γίνεται μέσω καταχώρησης SRV εγγραφών στον DNS . Κάθε μία εγγραφή SRV χρησιμοποιεί προκαθορισμένο τρόπο σύνταξης. Ένα παράδειγμα μιας SRV εγγραφής παρουσιάζεται αναλυτικά παρακάτω.

“_ldap._tcp.informatics.com. 60 IN SRV 0 100 669 srv1-informatics.com”

- *_ldap* (service): σε αυτό το σημείο της εγγραφής ορίζεται η υπηρεσία που προσδιορίζει η κάθε εγγραφή. Η συγκεκριμένη εγγραφή προσδιορίζει τον server (συνήθως domain controller) που απαντά σε LDAP αιτήσεις. Οι πιθανές τιμές που μπορούν να ανατεθούν σε αυτό το τμήμα της SRV εγγραφής είναι οι _ldap , _kerberos , _kpasswd και _gc, προσδίδοντας η κάθε μία, στην εγγραφή, μία ξεχωριστή ιδιότητα.
- *_tcp* (protocol): το πρωτόκολλο που χρησιμοποιείται για αυτή την υπηρεσία. Οι τιμές που μπορεί να πάρει είναι TCP ή UDP.
- *informatics.com* (name): το όνομα τομέα στον οποίο απευθύνεται η εγγραφή.
- *60* (TTL): ο χρόνος που μπορεί να μείνει ενεργή αυτή η εγγραφή πριν διαγραφεί αυτόματα (δευτερόλεπτα)
- *IN* (class): δηλώνει την κλάση του DNS
- *SRV* (resource record): δηλώνει πως πρόκειται για SRV εγγραφή
- *0* (priority): αριθμός που προσδιορίζει την προτεραιότητα της εγγραφής για τον client. Εάν υπάρχουν πολλαπλές εγγραφές που αναφέρονται στην ίδια υπηρεσία, οι clients θα συνδεθούν στον server με την μικρότερη τιμή προτεραιότητας.
- *100* (weight): τιμή που αναφέρεται σε μηχανισμό εξισορρόπησης φορτίου (load-balance). Σε περίπτωση που πολλαπλές εγγραφές αναφέρονται στην ίδια υπηρεσία και ταυτόχρονα έχουν και τον ίδιο αριθμό προτεραιότητας, τότε οι clients μπορούν να διαλέξουν την εγγραφή με την μεγαλύτερη βαρύτητα, την οποία δηλώνει και αυτός ο αριθμός.
- *669* (port): η θύρα που χρησιμοποιείται από την υπηρεσία.
- *srv1-informatics.com* (target): Ο host που παρέχει την υπηρεσία που περιγράφεται από την εγγραφή.

Θέλοντας να συνοψίσουμε την έννοια της παραπάνω εγγραφής σε μια πρόταση θα πούμε ότι, εάν κάποιος client αναζητά κάποιον LDAP server στον τομέα informatics.com, τότε ο client θα συνδεθεί στον server srv1-informatics.com.



Λεπτομέρειες μιας SRV εγγραφής

Κατά την εγκατάσταση του DNS δημιουργούνται δύο νέα διαμερίσματα καταλόγου (Directory Partitions) στις AD DS. Αυτοί οι κατάλογοι είναι οι DomainDNSZones και ForestDNSZones. Με αυτόν τον τρόπο , οι πληροφορίες των ζωνών του DNS καταχωρούνται σε αυτούς τους καταλόγους αντί σε κάποιο text αρχείο στο δίσκο του DNS Server.

Καθένα από αυτά τα διαμερίσματα καταλόγων, περιέχει διαφορετικές πληροφορίες και έχει διαφορετική διαδικασία σχηματισμού αντιγράφου. Το DomainDNSZones partition περιέχει όλες τις εγγραφές του Domain Controller που είναι σημαντικές για τον εντοπισμό των υπηρεσιών ενός Domain Controller εντός του τομέα. Όλες οι εγγραφές που περιγράφησαν νωρίτερα καταχωρούνται στο DomainDNSZones partition. Τα δεδομένα του DomainDNSZones

partition αντιγράφονται σε όλους τους DNS Servers που τρέχουν σε κάποιον Domain Controller ενός τομέα.

Το ForestDNSZones partition περιέχει τις πληροφορίες που απαιτούνται από Domain Controllers και clients για να εντοπίσουν υπηρεσίες των Domain Controllers σε διαφορετικό τομέα του δάσους (domain forest). Το ForestDNSZones partition αντιγράφεται σε όλους τους DNS Servers που τρέχουν στους Domain Controllers ενός δάσους.

2.3 DNS & GROUP POLICY

Μια δυνατότητα που μας παρέχει το λογισμικό Windows Server είναι ότι κάνοντας χρήση των group policies μπορούμε να διαχειριστούμε τον τρόπο που οι Domain Controllers καταχωρούν τις SRV εγγραφές στον DNS. Παρεμβαίνοντας στο default Domain Controllers Policy μπορούμε να εφαρμόσουμε αυτόματα τις ρυθμίσεις σε όλους του Domain Controller μας. Αντίθετα, σε περίπτωση που θέλουμε να κάνουμε ρυθμίσεις, μόνο σε συγκεκριμένους Domain Controllers της επιλογής μας, θα προχωρήσουμε πρώτα στη δημιουργία ενός νέου αντικειμένου Group Policy και στη συνέχεια, κάνοντας χρήση κάποιου φίλτρου, θα εφαρμόσουμε τις ρυθμίσεις που ορίσαμε στο αντικείμενο στους Domain Controllers που θα έχουμε επιλέξει. Ορισμένες από τις διαθέσιμες ρυθμίσεις αναφέρονται παρακάτω (τις ρυθμίσεις αυτές μπορούμε να τις βρούμε στη διαδρομή Administrative Templates\System\Net Logon\DC Locator DNS Records).

- *Domain Controller Address Type Returned:* Καθορίζει αν ο Domain Controller θα επιστρέφει μόνο IPv4 διεύθυνση, ή IPv4 και IPv6. Από προεπιλογή επιστέφονται και οι δύο τύποι διευθύνσεων. Αν όμως απενεργοποιηθεί τότε θα επιστρέφει μόνο IPv4.
- *Dynamic Registration Of The Domain Controller Locator DNS Records:* Καθορίζει αν είναι ενεργοποιημένη η δυναμική καταχώρηση των εγγραφών στον DNS. Οι εγγραφές καταχωρούνται δυναμικά μέσω της Net Logon υπηρεσίας.
- *DC Locator DNS Records Not Register By The Domain Controllers:* Καθορίζει ποιες DNS εγγραφές δεν είναι καταχωρημένες μέσω της υπηρεσίας Net Logon.

Μπορούμε να αποκλείσουμε τους Domain Controllers από το να καταχωρούν συγκεκριμένους τύπους εγγραφών.

- *Weight Set In The Domain Controller Locator DNS SRV Records:* Καθορίζει την τιμή του πεδίου "φορτίο" σε μια εγγραφή SRV.
- *Priority Set In The DC Locator DNS SRV Records:* Καθορίζει την τιμή του πεδίου "προτεραιότητα" σε μια εγγραφή SRV.
- *TTL Set In The DC Locator DNS SRV Records:* Καθορίζει την τιμή του πεδίου "TTL" σε μια εγγραφή SRV.
- *Force Rediscovery Interval:* Καθορίζει ένα χρονικό όριο, με τη λήξη του οποίου οι clients θα αναγκαστούν να ξανά ανιχνεύσουν τους Domain Controllers. Η ρύθμιση αυτή είναι ιδιαίτερα για τις περιπτώσεις των Domain Controllers δικτύων, των οποίων οι ρυθμίσεις μεταβάλλονται συχνά. Ο προεπιλεγμένος χρόνος κατά τον οποίων πραγματοποιείται η ανίχνευση των αλλαγών των Domain Controllers είναι οι 12 ώρες.

2.4 AD DS INTEGRATED ZONES

Μέχρι τώρα η χρήση του DNS ήταν απαραίτητη ώστε να γίνει ο εντοπισμός των Domain Controller του δικτύου μας. Με τη χρήση του λειτουργικού συστήματος Windows Server 2008 παρέχεται η δυνατότητα ενσωμάτωσης του DNS στις AD DS, με την καταχώρηση των ζωνών του DNS απευθείας στο Data Store. Η διαδικασία αυτή παρέχει πολλά πλεονεκτήματα στο σύστημα μας τα οποία παρατίθενται στη συνέχεια:

Αρχικά, η διαδικασία μεταφοράς των δεδομένων του DNS σε κάποιον καινούριο, αντικαθίσταται από την προεπιλεγμένη διαδικασία αντιγραφής των AD DS (AD DS replication process). Από τη στιγμή που τα δεδομένα αποθηκεύονται στο data store των AD DS τότε η κάθε απόπειρα μεταφοράς των δεδομένων του DNS αντικαθίσταται πλήρως από τη διαδικασία αντιγραφής των AD DS. Έτσι κάθε φορά που θα γίνει κάποια αλλαγή στις ζώνες του DNS θα γίνει ενημέρωση αποκλειστικά και μόνο των αλλαγών αυτών. Στη περίπτωση όμως δημιουργίας

κάποιου νέου Domain Controller στο δίκτυο μας, τα δεδομένα του DNS θα αντιγραφούν αυτόματα στο σύνολό τους.

Έπειτα, χωρίς τη χρήση των AD DS, ένας DNS μπορεί να υποστηρίξει μόνο έναν κύριο Name Server για κάθε μία από τις ζώνες. Αυτό σημαίνει ότι οι όποιες αλλαγές γίνονται πρέπει να εφαρμοστούν αρχικά στον κύριο εξυπηρετητή και στη συνέχεια να μεταφερθούν στου δευτερεύοντες. Με την χρήση των ενσωματωμένων ζωνών, ο κάθε DNS server έχει ένα αντίγραφο των πληροφοριών του τομέα έτσι ώστε οι αλλαγές να μπορούν να γίνονται οπουδήποτε στο σύστημα μας και ταυτόχρονα η πληροφορία να αντιγράφεται στο σύνολο των εξυπηρετητών του συστήματός μας.

Τέλος η χρήση των ενσωματωμένων ζωνών μπορεί να παρέχει στο σύστημά μας αυξημένη ασφάλεια. Εξαιτίας της καταχώρησης των ζωνών στο data store των AD DS, γίνεται, κάνοντας χρήση των Access Control Lists να παρέχεται επιλεκτική πρόσβαση είτε σε ολόκληρη τη ζώνη η είτε σε κάποια συγκεκριμένη εγγραφή της ζώνης.

2.5 DYNAMIC DNS & SECURE UPDATES

Στο παρελθόν μια δυσκολία στη χρήση του DNS ήταν ότι η εισαγωγή των δεδομένων των ζωνών γινόταν μη αυτοματοποιημένα. Με την πάροδο όμως του χρόνου και φτάνοντας στο σήμερα, όμως οι DNS Servers έχουν αποκτήσει τη δυνατότητα να ρυθμίζονται ώστε να δέχονται αυτόματες ενημερώσεις των εγγραφών των ζωνών τους. Αυτή η επιλογή ονομάζεται δυναμικός DNS (dynamic DNS). Οι DNS Servers στα Windows Server 2008 υποστηρίζουν τον δυναμικό DNS. Από προεπιλογή όλοι οι clients με Windows 200 ή νεότερα, ενημερώνουν αυτόματα τις εγγραφές τους στον DNS. Σε αντίθεση οι Windows Server 2008 DNS Servers δέχονται επιπλέον, τη δυναμική καταχώρηση των εγγραφών και από τους DHCP Servers. Ένας Windows Server 2008 DHCP Server μπορεί να ρυθμιστεί ώστε να ενημερώνει αυτόματα τις DNS εγγραφές για κάθε

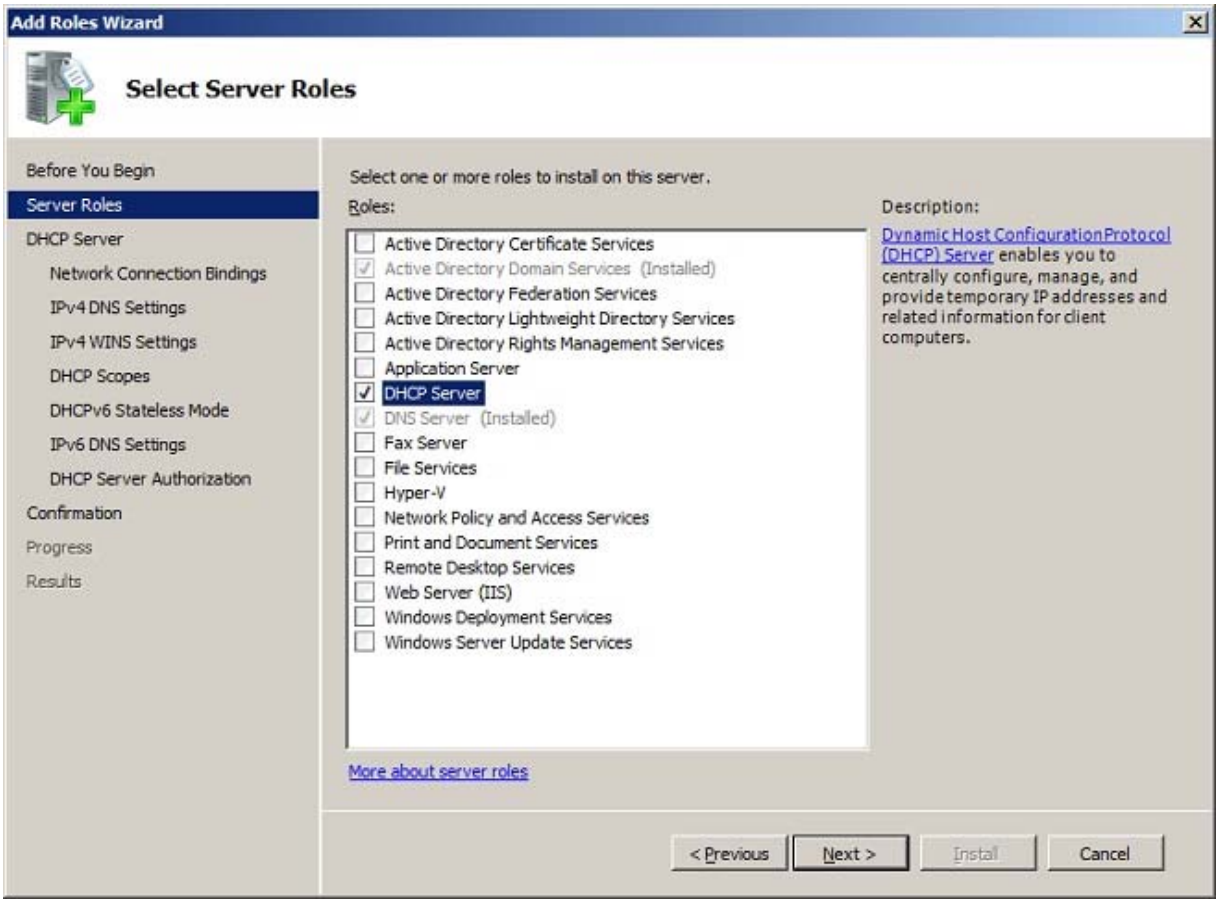
έναν από τους clients συμπεριλαμβανομένων των Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows Me και Microsoft Windows NT clients.

Ένα από τα ελαττώματα του δυναμικού DNS είναι η ασφάλεια. Χωρίς την ύπαρξη κάποιου ελέγχου σχετικά με το ποιος μπορεί να επέμβει στις εγγραφές του DNS, μπορεί θεωρητικά ο κάθε ένας να αποκτήσει πρόσβαση στο δίκτυο, να καταχωρήσει μια νέα εγγραφή DNS και να χρησιμοποιήσει την κίνηση αυτή ώστε να ανακατευθύνει την κίνηση του δικτύου. Για να αντιμετωπιστεί αυτό το πρόβλημα, προβλέφθηκαν οι ασφαλείς ενημερώσεις για τον DNS των Windows Server 2008. Οι ασφαλείς ενημερώσεις είναι διαθέσιμες μόνο στις ενσωματωμένες ζώνες των AD DS (AD DS integrated zones). Με τις ασφαλείς ενημερώσεις μπορεί ο διαχειριστής να έχει τον έλεγχο σχετικά με το ποιος έχει το δικαίωμα να προχωρήσει στην καταχώρηση ή ενημέρωση των ζωνών του DNS. Από προεπιλογή, τα μέλη του γκρουπ των πιστοποιημένων χρηστών (Authenticated Users Group) είναι αυτά που έχουν τα δικαιώματα να προχωρήσουν στην ενημέρωση των εγγραφών του DNS. Η ρύθμιση αυτή μπορεί να αλλάξει, τροποποιώντας την Access Control List (ACL) της DNS ζώνης.

ΚΕΦΑΛΑΙΟ 3. DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Ένα ακόμα στοιχείο απαραίτητο για τη ομαλή λειτουργία των AD DS είναι το πρωτόκολλο DHCP. Με τον όρο DHCP (*Dynamic Host Configuration Protocol*) αναφερόμαστε σε ένα μηχανισμό διαχείρισης πρωτοκόλλων TCP/IP . Το DHCP χρησιμοποιείται από τους υπολογιστές για την υποβολή κάποιας αίτησης παραμέτρων του Internet Protocol, όπως για παράδειγμα μια διεύθυνση IP από ένα διακομιστή δικτύου. Η λειτουργία του πρωτοκόλλου βασίζεται στο μοντέλο client - server.

Το DHCP εμφανίζεται στα Windows Server 2008 με τη λειτουργία (role) του DHCP Server. Η εγκατάστασή του (όπως και αυτή του active directory αλλά και όλων των πρόσθετων λειτουργιών των Windows Server) πραγματοποιείται μέσα από τον server manager.

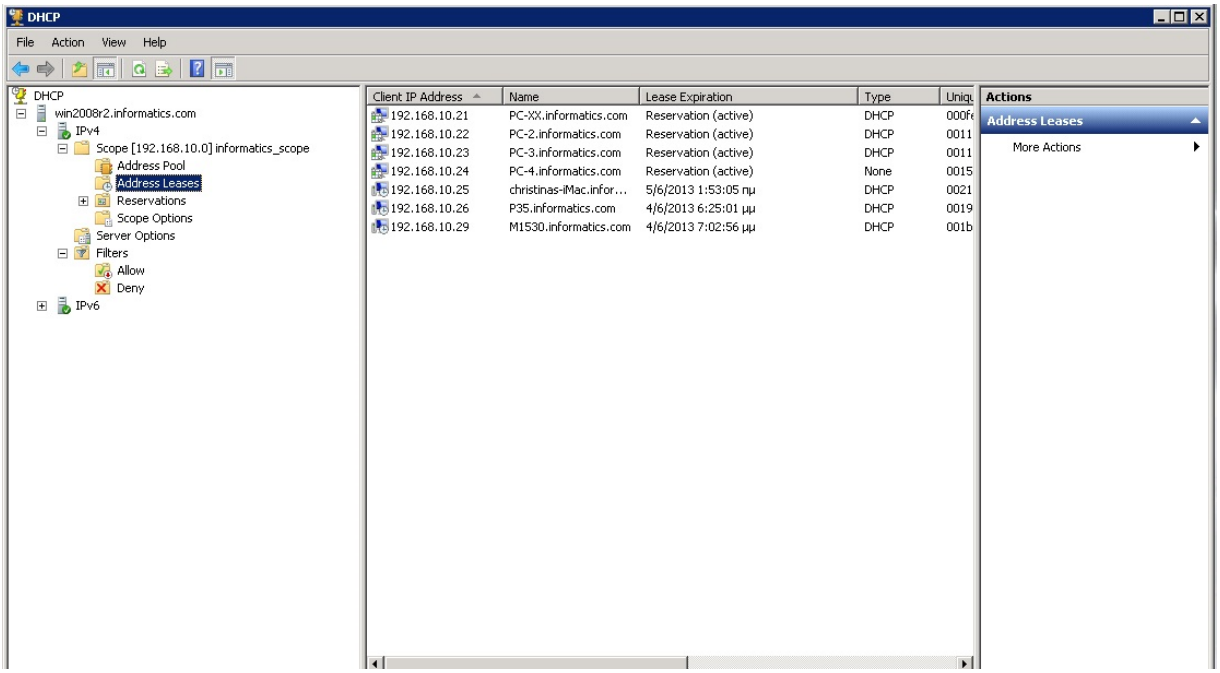


Wizard ενεργοποίησης του DHCP role

Η εγκατάσταση ενός ή και περισσοτέρων DHCP Server στο δίκτυό, μας παρέχει αυτόματα έγκυρη IP διευθυνσιοδότηση σε clients αλλά και άλλες συσκευές δικτύου των οποίων η λειτουργία βασίζεται στο TCP/IP πρωτόκολλο. Παρέχονται επίσης πρόσθετοι παράμετροι που χρειάζονται οι clients και οι συσκευές αυτές, ώστε να τους επιτραπεί να συνδεθούν σε άλλους πόρους του δικτύου όπως οι DNS Servers και οι δρομολογητές. Οι παράμετροι αυτοί ονομάζονται επιλογές DHCP (DHCP options).

Η ύπαρξη ενός DHCP Server μπορεί να παρέχει στο δίκτυο μας τις παρακάτω υπηρεσίες:

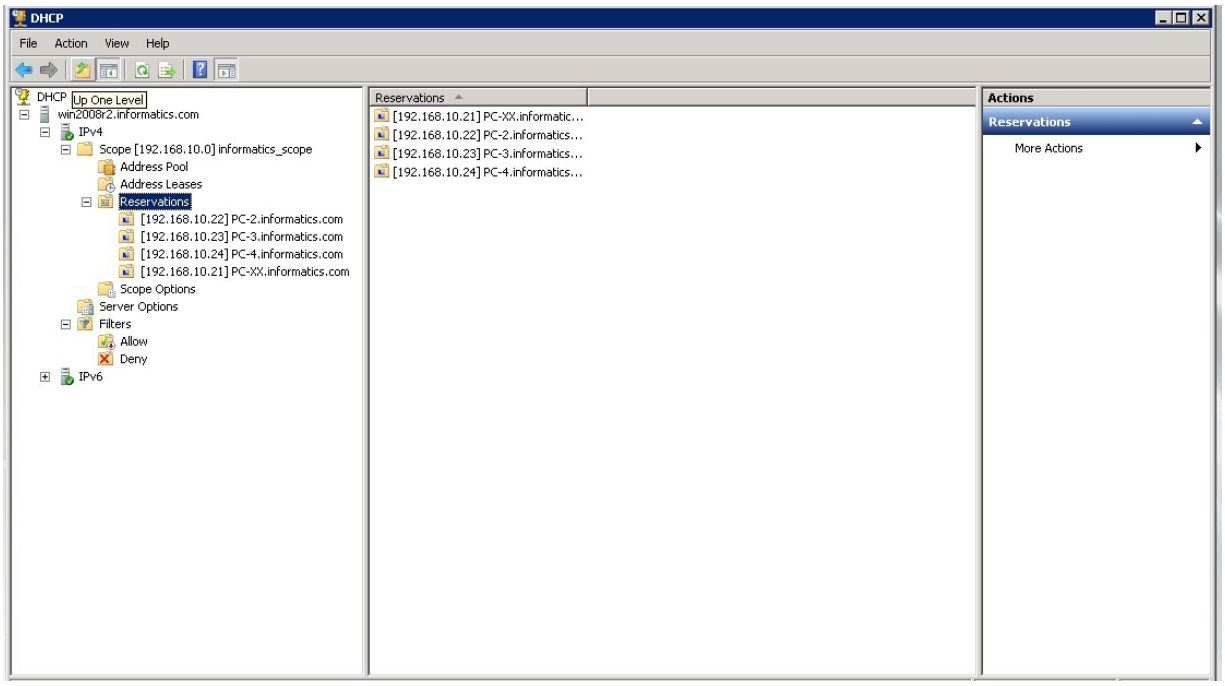
- Ενοικίαση IP διευθύνσεων σε DHCP clients (Address Leases) για συγκεκριμένο χρονικό διάστημα. Ο χρόνος της ενοικίασης ορίζεται από τον διαχειριστή. Μετά το πέρας της ενοικίασης, σε περίπτωση που ο client ζητήσει ανανέωση της διεύθυνσης, αυτή ανανεώνεται αυτόματα.



Address leases

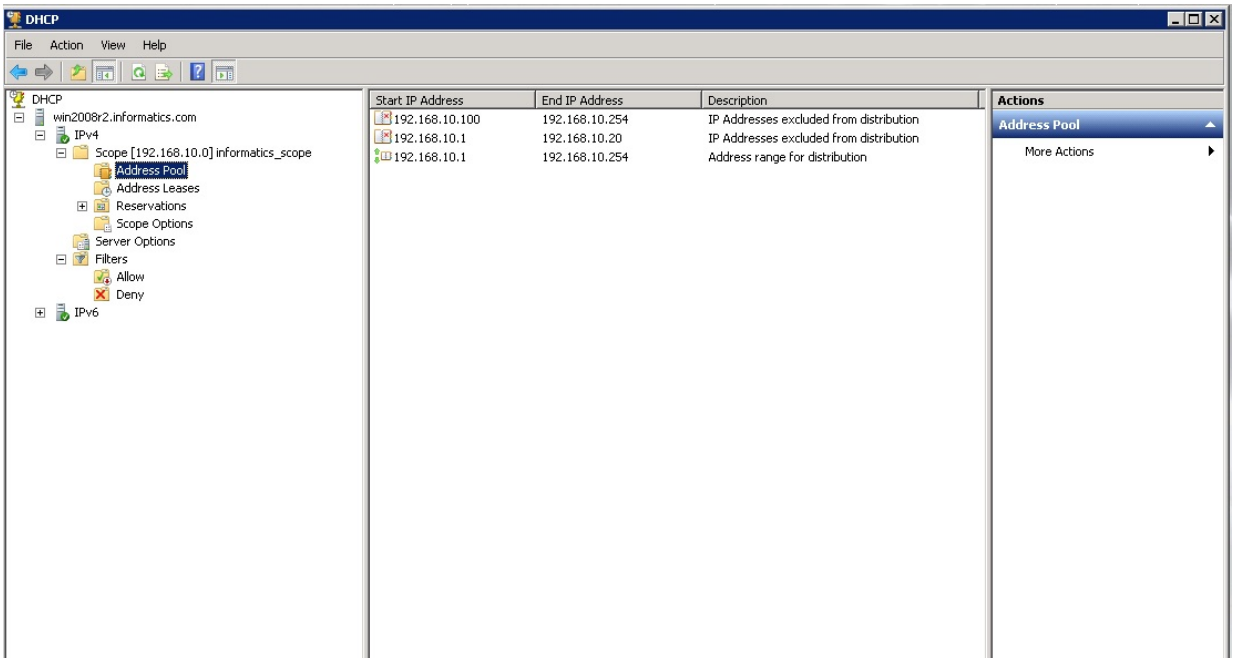
- Αυτόματη ενημέρωση όλων των clients για κάθε μία αλλαγή που μπορεί να πραγματοποιηθεί στις ρυθμίσεις του DHCP Server.

- Δέσμευση ενός εύρους, ή μεμονωμένων IP διευθύνσεων (Reservations), για συγκεκριμένους υπολογιστές ή άλλες συσκευές ώστε να έχουν πάντα την ίδια IP διεύθυνση και να λαμβάνουν συνεχώς τις πιο ενημερωμένες επιλογές DHCP.



Reservations

- Εξαίρεση εύρους η μεμονωμένων IP διευθύνσεων από τη διανομή του DHCP Server (IP Addresses Excluded from distribution), ώστε να χρησιμοποιηθούν για στατική ρύθμιση δρομολογητών, Servers ή όποιων άλλων συσκευών απαιτούν στατικές IP διευθύνσεις.



Address pool

- Παροχή DHCP υπηρεσιών σε πολλά υποδίκτυα με την προϋπόθεση ότι οι δρομολογητές μεταξύ του DHCP Server και του υποδικτύου, είναι ρυθμισμένοι να προωθούν DHCP μηνύματα.
- Δυνατότητα ρύθμισης του DHCP Server ώστε να εφαρμόζει υπηρεσίες καταχώρησης ονομάτων DNS στους DHCP clients.

3.1 MULTICAST ADDRESS DYNAMIC CLIENT ALLOCATION PROTOCOL (MADCAP) SERVER

Στα Windows Server 2008 παρέχεται η δυνατότητα στον DHCP Server να λειτουργεί και ως MADCAP Server. Όταν ο DHCP λειτουργεί ως MADCAP server, έχει τη δυνατότητα να εκχωρήσει δυναμικά, πολλαπλά εκπεμπόμενες (multicast) IP διευθύνσεις , σε πελάτες που θέλουν να εισέλθουν στο group αυτών που λαμβάνουν τις πληροφορίες που αποστέλλονται μέσω των πολλαπλά εκπεμπόμενων μηνυμάτων. Η πολλαπλή εκπομπή μηνυμάτων είναι χρήσιμη για τη

μετάδοση πληροφοριών, όπως ήχος ή video σε ένα διαδίκτυο, από έναν αποστολέα σε πολλούς παραλήπτες (point-to-multipoint delivery). Οι client παραλήπτες έχουν επιλεγεί από το μενού επιλογών του DHCP Server. Ορίζεται έτσι ένα ξεχωριστό τμήμα (scope) -μπορεί ακόμα και υποδίκτυο ή υποδίκτυα- στο οποίο μπορούν να εφαρμοστούν οι ρυθμίσεις που επιθυμούμε.

Το πλεονέκτημα αυτής της μεθόδου είναι ότι για την εκπομπή των μηνυμάτων γίνεται χρήση ενός και μόνο πακέτου χωρίς να δημιουργείται καμία επιβάρυνση για τη διατήρηση λίστα παραληπτών. Σε αντίθεση με τη λειτουργία του broadcast, η πολλαπλή εκπομπή (multicast) δεν επεμβαίνει στους clients που δεν ανήκουν στο κομμάτι αυτό των παραληπτών. Οι δρομολογητές μπορούν να εφαρμόσουν τη λειτουργία της πολλαπλής εκπομπής και να προωθήσουν τα πακέτα σε όλα τα δίκτυα στα οποία υπάρχει τουλάχιστον ένας διαθέσιμος παραλήπτης.

Τέλος να σημειωθεί πως ο MADCAP Server υποστηρίζεται μόνο στο IPv4.

3.2 ΑΛΛΑΓΕΣ DHCP SERVER ΣΤΑ WINDOWS SERVER 2008 R2

Η Microsoft με τον Windows Server 2008 R2 DHCP Server έχει επενδύσει στα θέματα ασφάλειας, αξιοπιστίας και χρηστικότητάς του. Παρακάτω παρουσιάζονται κάποιες από τις σημαντικότερες αλλαγές που περιέχονται στην καινούρια έκδοση:

- Υποστηρίζει μηχανισμό ελέγχου εισόδου στο δίκτυο βασισμένο στη mac διεύθυνση (MAC address based network access control mechanism). Με αυτόν τον τόπο ο DHCP διαχειριστής θα μπορεί να επιτρέπει η να απορρίπτει την μίσθωση των IP διευθύνσεων.
- Υποστηρίζει την πρόληψη των προβλημάτων που προκύπτουν με την κατάληψη δεσμευμένων ονομάτων, εξαιτίας της εισόδου στο δίκτυο υπολογιστών χωρίς λειτουργικό σύστημα Windows. Ο μηχανισμός αυτός ονομάζεται προστασία ονόματος (Name Protection feature). Κάνοντας χρήση αυτού του μηχανισμού αποτρέπεται σε υπολογιστές χωρίς Windows λειτουργικό, η καταχώρηση ονόματος που υπάρχει ήδη καταχωρημένο στον DNS Server από κάποιον άλλο υπολογιστή.

- Υποστηρίζει καταγραφή ενεργειών του DHCP Server σε log αρχείο (DHCP Server Activity Logging), επιτρέποντας έτσι στους Administrators του συστήματος να παρακολουθούν τις αλλαγές των ρυθμίσεων των DHCP Servers. Οι διαχειριστές μπορούν να χρησιμοποιήσουν αυτή την ιδιότητα για θέματα ασφαλείας και παρακολούθησης της κίνησης του δικτύου.
- Υποστηρίζει την Option 16 (user class) του DHCP Server. Με αυτή την επιλογή ο client μπορεί να ταυτοποιήσει τον τύπο του χρήστη που αυτός αντιπροσωπεύει. Η υλοποίηση γίνεται από τη πλευρά και του DHCP Server αλλά και του client.
- Υποστηρίζει την Option 32 (information refresh time) του DHCP Server. Με αυτήν την επιλογή θέτεται ένα ανώτερο όριο στον χρόνο αναμονής ενός client πριν προχωρήσει στην ανανέωση των πληροφοριών που ανακτώνται από τον DHCP Server. Η υλοποίηση γίνεται από τη πλευρά και του DHCP Server αλλά και του client

3.3 MICROSOFT NETWORK ACCESS PROTECTION (NAP)

Μια ακόμα πολύτιμη υπηρεσία που περιλαμβάνεται στα Windows Server 2008 είναι αυτή της προστασίας πρόσβασης στο δίκτυο (Network Access Protection –NAP). Η NAP είναι μια policy-based management υπηρεσία η οποία επιτρέπει στον διαχειριστή του δικτύου να ελέγχει την πρόσβαση σε πόρους του δικτύου.

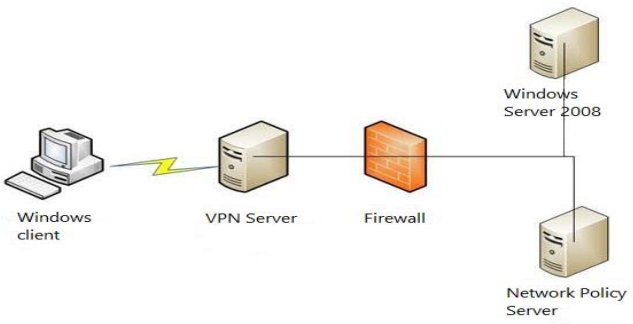
Ένα τερματικό, μέλος του δικτύου μας, το οποίο είτε δεν διαθέτει κάποια προστασία από κακόβουλο λογισμικό (malware, spyware, ιούς κτλ), είτε δεν είναι ενημερωμένο με τα τελευταία update patches του λογισμικού του συστήματος ή περιέχει ένα όχι σωστά ρυθμισμένο firewall, μπορεί να αποτελέσει σημαντικό κίνδυνο για το δίκτυο στο οποίο είναι μέλος. Με τη λειτουργία του NAP εξασφαλίζεται ότι όλες οι παραπάνω προαπαιτήσεις, αλλά και άλλες πολλές, ικανοποιούνται και μόνο έτσι ο υπολογιστής θα είναι σε θέση να αποκτήσει πρόσβαση στο

δίκτυο. Τυχόν συσκευές που δεν ικανοποιούν τις οριζόμενες από τον διαχειριστή προδιαγραφές, τους απαγορεύεται η είσοδος ή ακόμα μπλοκάρονται οριστικά από τυχόν μελλοντική απόπειρα εισόδου.

Η όλη λειτουργία του NAP έχει δομηθεί γύρω από έναν Network Policy Server (NPS) ο οποίος αντικατέστησε τον προκάτοχό του, Internet Authentication Server (IAS) στα Windows Server 2003. Ο NPS είναι ένας εξυπηρετητής συμβατός με το πρωτόκολλο RADIUS (Remote Authentication Dial-In User Service) και έχει σχεδιαστεί για να παρέχει επαλήθευση ταυτότητας και αδειοδότηση σε απομακρυσμένους clients ενώ ενεργεί ως Server «αξιολόγησης της υγείας» των clients για τη λειτουργία του NAP.

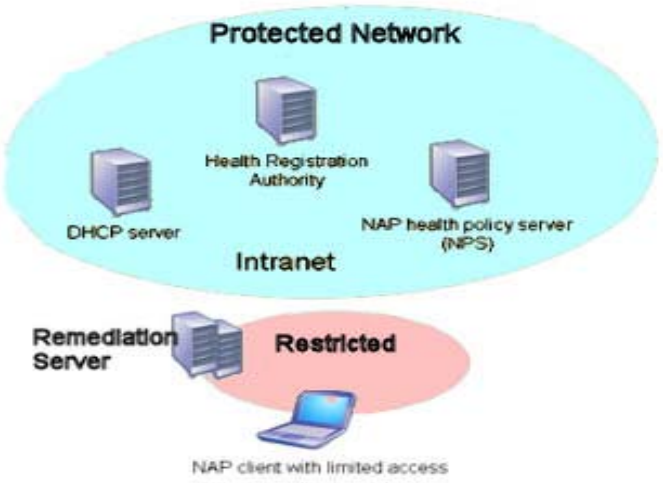
Η επικύρωση η όχι των κανόνων που έχουν οριστεί, πραγματοποιείται από κάποιον client του δικτύου μας ο οποίος είναι συμβατός με το πρωτόκολλο RADIUS και ικανός να επικοινωνήσει με τον NPS.

Η διαδικασία που ακολουθείται για να εισέλθει κάποιος υπολογιστής στο δίκτυο μέσω της λειτουργίας NAP είναι η ακόλουθη: Κατά τα διάρκεια της εισόδου (login), ένας NAP client αποστέλλει τα δεδομένα τα οποία περιγράφουν την κατάσταση του συστήματος σε κάποια αρμόδια συσκευή, όπως ένα switch, ένας VPN Server ή ένας DHCP Server. Η συσκευή αυτή με τη σειρά της αναφέρει την κατάσταση της υγείας του τερματικού, στον NPS των Windows Server 2008 ο οποίος αξιολογεί τα αποσταλμένα δεδομένα σε σχέση με τις απαιτήσεις που έχουν οριστεί από τον διαχειριστή του συστήματος.



Διαδικασία NAP

Εάν η κατάσταση του NAP client συμφωνεί με τις απαιτήσεις του NPS τότε αυτόματα του επιτρέπεται η είσοδος στο σύστημα. Σε αντίθετη περίπτωση που δεν συμφωνεί με τις απαιτήσεις του διαχειριστή, είτε αποτρέπεται η είσοδος στο δίκτυο είτε εισέρχεται σε ένα «εφεδρικό» δίκτυο με περιορισμένη πρόσβαση, μέχρις ότου η κατάσταση της υγείας του να διορθωθεί από τον χρήστη μέσω ενός επονομαζόμενου server αποκατάστασης (remediation server) ο οποίος περιέχει τις απαραίτητες ρυθμίσεις ασφαλείας, τα απαραίτητα patches, ψηφιακές υπογραφές ή άλλο απαραίτητο υλικό. Όταν η υγεία του client αναβαθμιστεί και είναι ποια συμβατή με τις απαιτήσεις του συστήματος αποστέλνεται μια καινούρια αίτηση ελέγχου και ακολουθείται εκ νέου η παραπάνω διαδικασία.



ΚΕΦΑΛΑΙΟ 4. HYPER-V

Με τον όρο Hyper-V αναφερόμαστε σε μια τεχνολογία δημιουργίας πολλαπλών εικονικών λειτουργικών συστημάτων τα οποία τρέχουν μέσα σε ένα κύριο (λειτουργικό σύστημα). Πρόκειται για μια τεχνολογία ανεπτυγμένη αποκλειστικά από Microsoft η οποία παρουσιάστηκε για πρώτη φορά τον Ιούνιο του 2008 και από τότε αποτελεί μία από τις ενσωματωμένες τεχνολογίες της έκδοσης των Windows Server 2008. Η ίδια λειτουργία επιτυγχάνεται μεν και σήμερα με 3rd party λογισμικό όπως το Oracle VirtualBox και το VMWare, στη συγκεκριμένη όμως περίπτωση αναφερόμαστε σε λειτουργία ενσωματωμένη στο λειτουργικό μας σύστημα.

Το Hyper-V δίνει στους οργανισμούς τη δυνατότητα στους οργανισμούς να αξιοποιήσουν στο μέγιστο τις δυνατότητες των υπολογιστικών τους συστημάτων μέσω ενοποίησης περισσότερων ρόλων εξυπηρετητών, οι οποίοι λειτουργούν σε μια μόνο φυσική μηχανή, ως ξεχωριστές εικονικές μηχανές. Επιπλέον μέσω του Hyper-V επιτυγχάνεται η αποτελεσματική παράλληλη λειτουργία διαφορετικών λειτουργικών συστημάτων, σε έναν μόνο server, κάνοντας χρήση ενός η περισσοτέρων φυσικών επεξεργαστών. Κάποια από τα οφέλη που επιτυγχάνονται από τα παραπάνω χαρακτηριστικά στους οργανισμούς είναι η μείωση του κόστους, η σωστή αξιοποίηση του υλικού, η βελτίωση της διαθεσιμότητας εξυπηρετητών και εφαρμογών καθώς και η δυνατότητα κλιμακούμενης αξιοποίησης του υλικού.

Το Hyper-V υποστηρίζει μια σειρά από «φιλοξενούμενα» λειτουργικά συστήματα (guest OS), δηλαδή λειτουργικά που μπορούν να φιλοξενηθούν σε εικονικές μηχανές. Τα λειτουργικά αυτά είναι τα εξής:

- Windows Server 2000 (όλες οι εκδόσεις)
- Windows Server 2003 (όλες οι εκδόσεις)
- Windows Server 2008 (όλες οι εκδόσεις)
- SUSE Linux Enterprise Server 10
- Windows XP Professional SP3
- Windows Vista SP2 x32, x64 (Business, Enterprise, Ultimate, N & KN)
- Windows 7 SP1 x32, x64 (Enterprise, Professional, Ultimate, N & KN)

Εκτός από την απαίτηση των φιλοξενούμενων λειτουργικών να είναι ένα από τα παραπάνω το Hyper-V απαιτεί επεξεργαστές που έχουν ενσωματωμένες δυνατότητες για την υποστήριξη του virtualization (Hardware Assisted Virtualization). Οι επεξεργαστές αυτοί είναι υποχρεωτικά αρχιτεκτονικής 64bits της Intel και της AMD με τεχνολογίες γνωστές ως Intel VT και AMD-V.

4.1 HYPER-V ARCHITECTURE

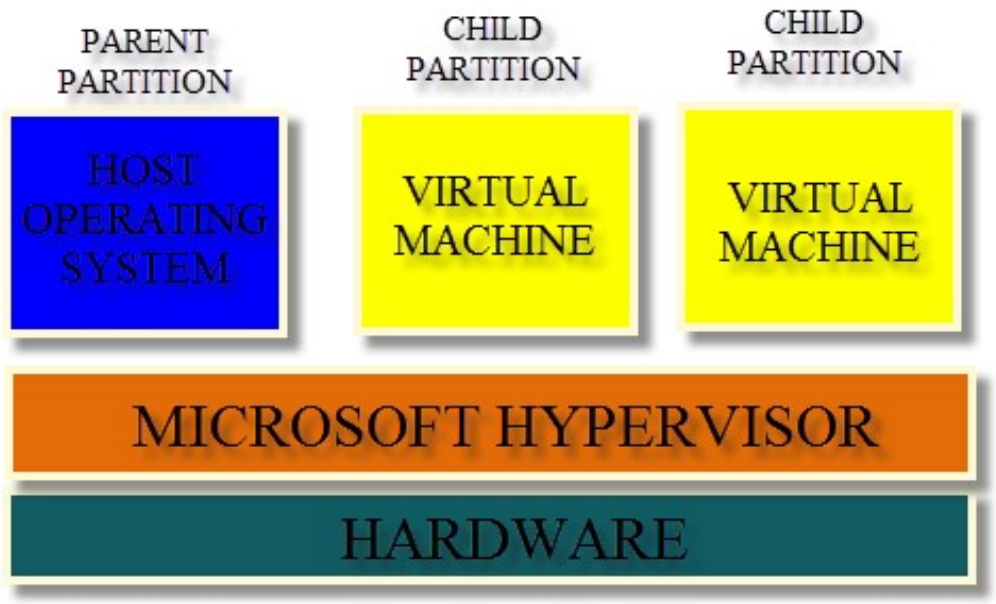
Το βασικό στοιχείο αυτής της τεχνολογίας είναι ο ορισμός του hypervisor. Με τον όρο hypervisor περιγράφουμε εκείνο το software επίπεδο το οποίο μας επιτρέπει να δημιουργήσουμε virtual machines οι οποίες χρησιμοποιούν όλες τους ίδιους πόρους του φυσικού server.

Οι hypervisors γενικότερα χωρίζονται σε δυο κατηγορίες: σε εκείνους που λειτουργούν πάνω από το επίπεδο του λειτουργικού συστήματος και εκείνους που λειτουργούν κάτω ακόμα και από το επίπεδο του λειτουργικού και αλληλοεπιδρούν άμεσα με το hardware τους μηχανήματος όπως CPU, RAM και κάρτα δικτύου.

Το πρώτο είδος ονομάζεται Type 1 hypervisors και μπορεί να τους συναντήσουμε και ως bare metal hypervisors. Αυτό το είδος των hypervisors τρέχει σε επίπεδο hardware (πιο κάτω ακόμα και από το επίπεδο του λειτουργικού) προσφέροντας καλύτερη απόδοση και ασφάλεια. Ουσιαστικά τα δικαιώματα του Type 1 hypervisor είναι περισσότερα ακόμα και από αυτά του ίδιου του λειτουργικό που τρέχει στο μηχάνημα. Κρίνοντας από τα παραπάνω συμπεραίνουμε ότι το λειτουργικό σύστημα τρέχει ένα επίπεδο πιο πάνω από το hypervisor αλλά στο ίδιο επίπεδο με τα virtual machines. Έτσι το host λειτουργικό σύστημα μετατρέπεται και αυτό σε ένα ειδικό virtual machine το οποίο περιέχει το virtualization stack και το οποίο είναι υπεύθυνο για την διαχείριση των virtual machines.

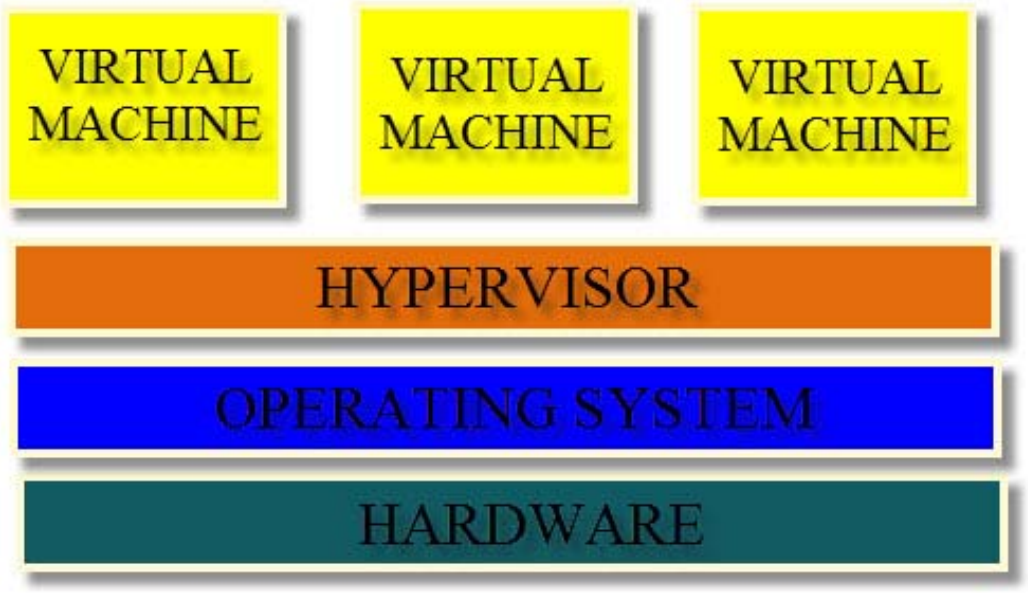
Αφού κάνουμε reboot το μηχάνημα μας, κατά την Boot διαδικασία, το winload.exe θα φορτώσει τον hvboot.sys driver ο οποίος είναι υπεύθυνος για τον αν οι επεξεργαστές στο

σύστημα υποστηρίζουν virtualization ή όχι. Σαν τελευταίο βήμα, το hypervisor image file φορτώνεται και είμαστε έτοιμοι να δημιουργήσουμε virtual machines. Το host λειτουργικό σύστημα και τα virtual machines ονομάζονται partitions επειδή τρέχουν στο ίδιο επίπεδο. Πιο συγκεκριμένα, το host λειτουργικό ονομάζεται parent partition ενώ τα virtual machines ονομάζονται child partitions. Στην Type 1 κατηγορία των hypervisors ανήκει το Microsoft Hyper-V.



Στους Type 2 hypervisors ή hosted hypervisors όπως αλλιώς ονομάζονται, βρίσκουμε εκείνους τους hypervisor οι οποίοι τρέχουν ένα επίπεδο πιο πάνω από το λειτουργικό σύστημα όπως ακριβώς σαν μια εγκαταστημένη εφαρμογή ή απλό πρόγραμμα. Σε αυτή την κατηγορία, τα virtual machines τρέχουν επάνω στο Hypervisor που με την σειρά του τρέχει επάνω στο λειτουργικό σύστημα. Κάτω από αυτή την λογική, καταλαβαίνουμε ότι ο hypervisor αυτής της κατηγορίας δεν έχει άμεση πρόσβαση στο hardware και κατά συνέπεια αυξάνεται η πίεση στον hypervisor. Σε αυτό το πλεονέκτημα, έρχεται να προστεθεί και το γεγονός ότι οι type 2 hypervisors τρέχουν σαν Windows service. Εάν σταματήσει το service όλη η virtualization

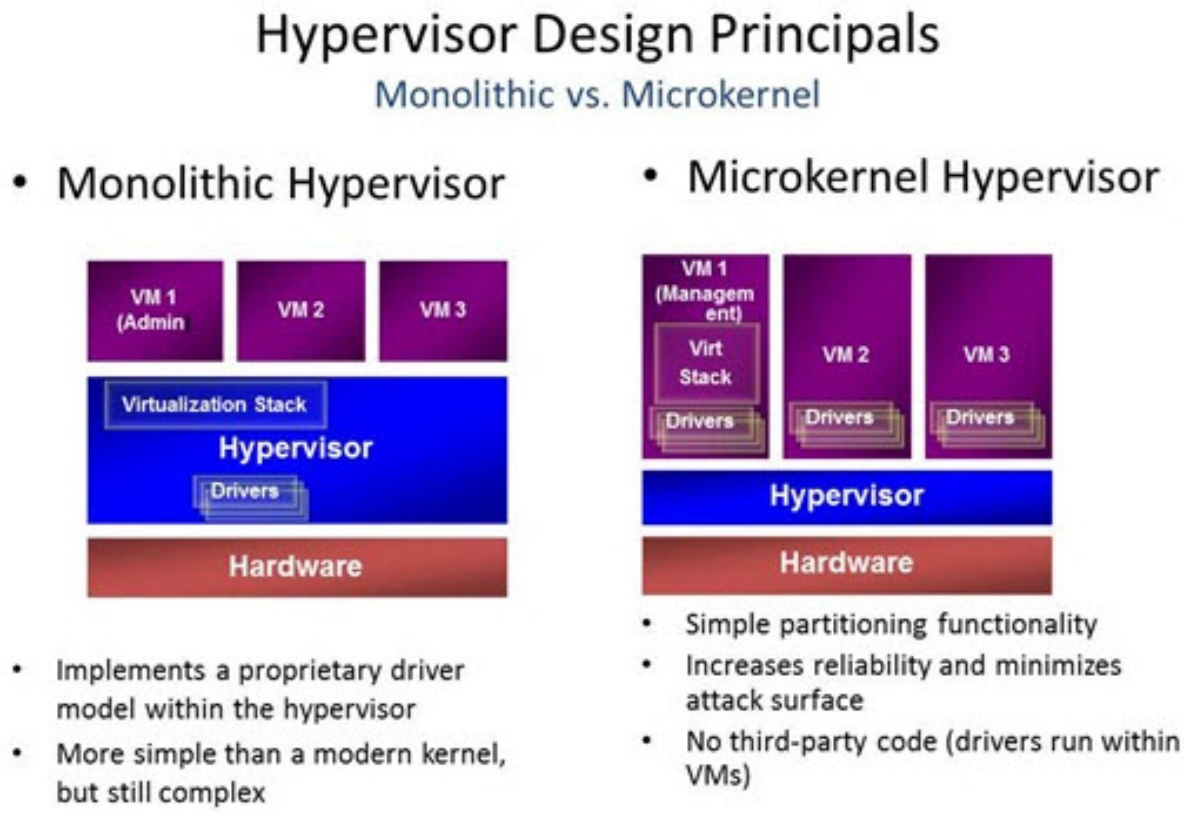
πλατφόρμα δεν θα είναι διαθέσιμη. Σε αυτή την κατηγορία ανήκουν τα Microsoft Virtual Server και Virtual PC.



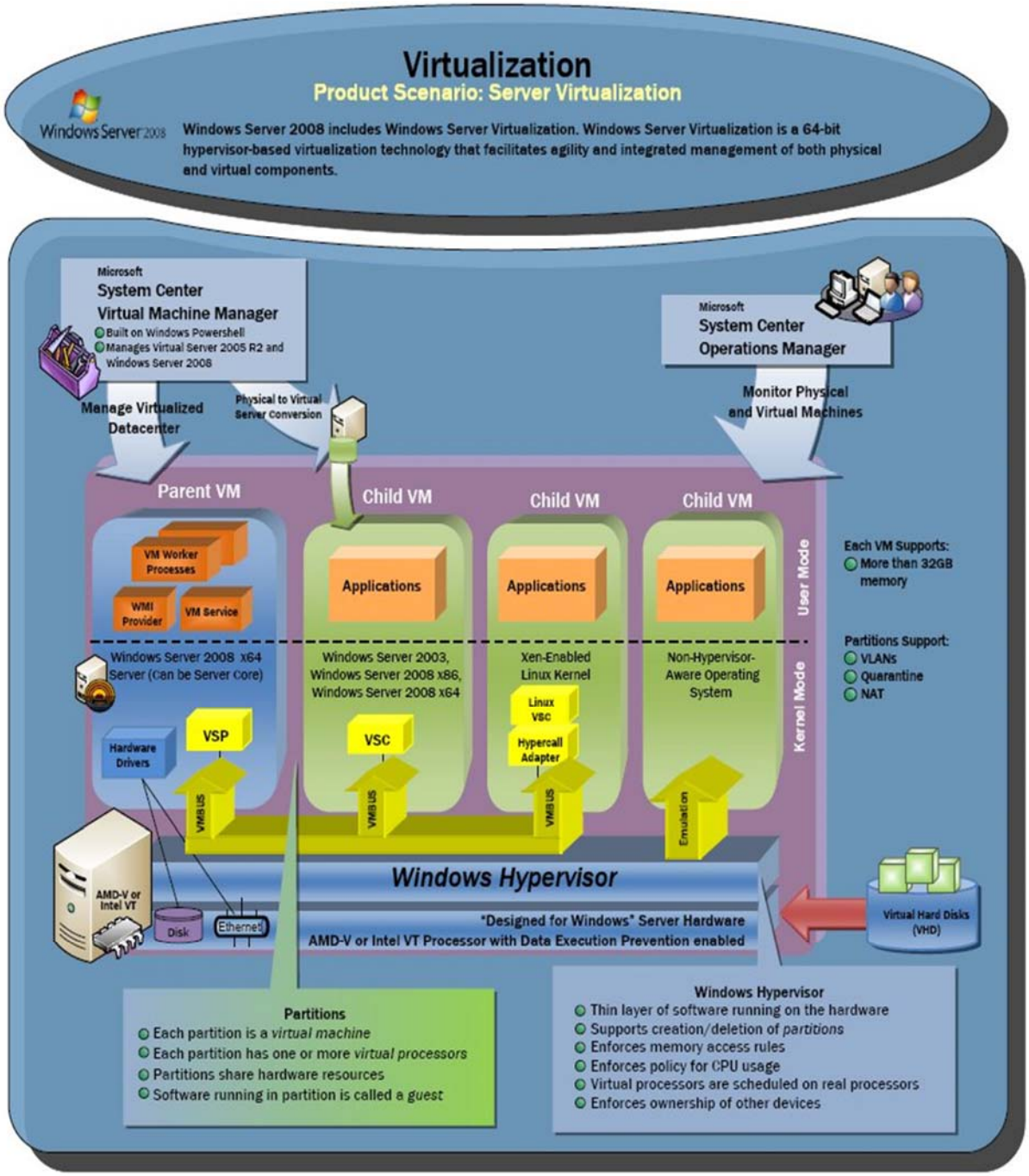
Εκτός όμως από τις δύο κύριες κατηγορίες που αναφέραμε παραπάνω θα πρέπει να αναφέρουμε και τις δύο υποκατηγορίες του Type 1 hypervisor οι οποίες βασικά αντιπροσωπεύουν την πραγματική λειτουργία της γενικότερης έννοιας του virtualization. Η πρώτη κατηγορία είναι οι ονομαζόμενοι monolithic hypervisors ενώ η δεύτερη ονομάζεται microkernel hypervisors.

Οι monolithic hypervisors, ως Type 1 hypervisors που είναι, γνωρίζουμε πως επικοινωνούν άμεσα με το hardware. Μια λειτουργία που προσθέτουν είναι ότι στο επίπεδο που λειτουργούν έχουν και όλους τους οδηγούς συσκευών (device drivers) για τα λειτουργικά συστήματα που θα φορτωθούν στα virtual machines. Το πλεονέκτημα τους λοιπόν είναι ότι λόγω της άμεσης επικοινωνίας τους με το hardware, έχουν ήδη εκείνοι τους drivers που χρειάζονται με συνέπεια να μην χρειάζονται κανένα parent λειτουργικό σύστημα. Παρόλα αυτά όμως παρουσιάζουν και κάποια αρκετά σημαντικά μειονεκτήματα. Το πρώτο είναι ότι δεν αναπτύσσουν όλοι οι

κατασκευαστές hardware, drivers για αυτό το είδος των Hypervisors καθώς επίσης, επειδή drivers και hypervisor μιλάνε απευθείας στο hardware υπάρχει πάντα η πιθανότητα να παρουσιαστούνε προβλήματα από κακόβουλα προγράμματα και ιούς.



Η δεύτερη κατηγορία (microkernel hypervisors) είναι εκεί στην οποία ανήκει η Hyper-V τεχνολογία της Microsoft. Ο microkernel hypervisor απαιτεί οι device drivers για το hardware να εγκατασταθούν στο λειτουργικό σύστημα το οποίο τρέχει στο parent partition του hypervisor. Αυτό σημαίνει ότι δεν είναι απαραίτητο να εγκαθιστούμε drivers για κάθε λειτουργικό σύστημα, αλλά όταν κάποιο guest operating system θέλει να αποκτήσει πρόσβαση στο φυσικό hardware του συστήματος αυτό το πετυχαίνει δια μέσω του parent partition.



Κατά τη διαδικασία εγκατάστασης του Hyper-V ρόλου, δημιουργείται και το parent partition και το parent partition hypervisor πηγαίνει κάτω από το επίπεδο του λειτουργικού

συστήματος. Συνεπώς τα Windows Server 2012 τρέχουν πάνω στο parent partition. Σαν αποτέλεσμα αυτής της διαδικασίας έχουμε το γεγονός ότι το parent partition είναι ο εγκέφαλος όλης της διαχείρισης του Hyper-V ή όπως αλλιώς ονομάζεται Hyper-V virtual stack management και οτιδήποτε άλλο virtual περιβάλλον δημιουργήσουμε θα εγκατασταθεί σαν child partition. Έτσι κάθε φορά που ξεκινάμε τον Hyper-V server, το parent partition είναι αυτό που δημιουργείται πρώτο και είναι εκείνο που παραπέμπει τα child partitions στον hypervisor.

ΚΕΦΑΛΑΙΟ 5. NETWORK BOOT SERVICES ::

Στην προσπάθεια να αξιοποιήσουμε στον μέγιστο βαθμό τις δυνατότητες που μας παρέχει ένα δίκτυο υπολογιστών, προχωρήσαμε στη δημιουργία μιας τόσο βοηθητικής, όσο και αναγκαίας υπηρεσίας, η οποία μπορεί να παρέχει στους διαχειριστές του συστήματος επιπλέον δυνατότητες και εργαλεία, τα οποία εμφανίζονται κατά την εκκίνηση του υπολογιστή (boot services) και σκοπό έχουν την εποπτεία και στη διαχείριση των υπολογιστών – μελών του δικτύου. Για τη δημιουργία αυτής της υπηρεσίας προχωρήσαμε σε συνδυασμό διαφόρων τεχνολογιών, κάποιες από τις οποίες παρέχονται από τα Windows Server 2008 και άλλες από ανεξάρτητες εφαρμογές. Στη συνέχεια αυτού του κεφαλαίου θα παρουσιαστούν όλες οι τεχνολογίες που χρησιμοποιήθηκαν καθώς και το τελικό αποτέλεσμα.

5.1 TRIVIAL FILE TRANSFER PROTOCOL (TFTP)

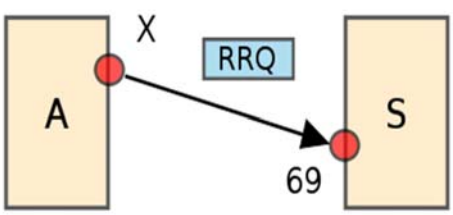
Το TFTP είναι ένα, απλό στον σχεδιασμό του, πρωτόκολλο μεταφοράς αρχείων. Η πιο συχνή χρήση του παρουσιάζεται σε περιπτώσεις λήψης ή αποστολής δεδομένων, από ή προς κάποιον απομακρυσμένο server. Για τη μεταφορά των δεδομένων κάνει χρήση του User Datagram Protocol (UDP). Συγκρίνοντας το με το File Transfer Protocol (FTP) θα παρατηρήσουμε ότι παρέχει μηδενικό επίπεδο ασφάλειας και ελέγχου των μεταφερόμενων δεδομένων και γι’ αυτό η χρήση του περιορίζεται σχεδόν αποκλειστικά στη μεταφορά δεδομένων σε επίπεδο τοπικού δικτύου. Ο πολύ απλός σχεδιασμός του το καθιστά σχεδόν επικίνδυνο για εφαρμογή σε επίπεδο διαδικτύου.

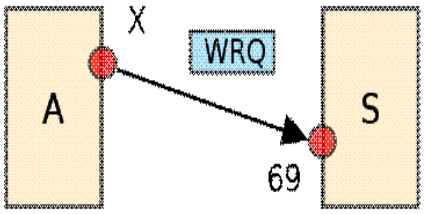
Το TFTP μπορεί να φανεί πολύ χρήσιμο σε περιπτώσεις υπολογιστών ή συσκευών που επιχειρούν να εκκινήσουν χωρίς να έχουν σκληρό δίσκο, λόγω του ότι μπορεί να υλοποιηθεί κάνοντας χρήση ελάχιστου χώρου στη μνήμη. Αυτό το χαρακτηριστικό το κατατάσσει σε ένα από

τα αναγκαία συστατικά για την υλοποίηση του Preboot eXecution Enviroment (PXE) το οποίο και θα παρουσιάσουμε αναλυτικά στη συνέχεια.

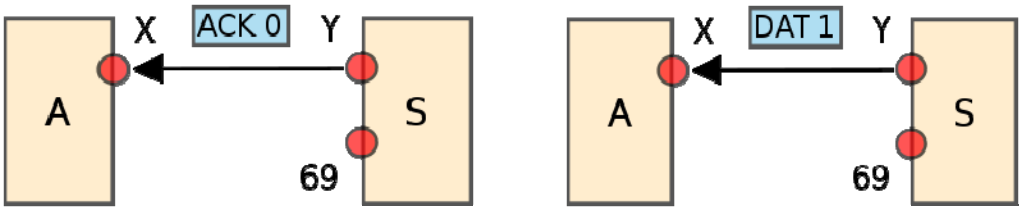
Η μεταφορά των δεδομένων μέσω του TFTP συνήθως πραγματοποιείται μέσω της θύρας 69. Παρόλα αυτά, οι πόρτες μεταφοράς των δεδομένων μπορούν να επιλεγούν από τον αποστολέα και τον παραλήπτη κατά την αρχικοποίηση της σύνδεσής τους. Στη συνέχεια παρουσιάζεται η διαδικασία αποστολής ενός πακέτου μέσω του TFTP πρωτοκόλλου μεταξύ ενός host A και ενός host B:

- Ο host A αποστέλλει διαμέσου της πόρτας 69, ένα πακέτο RRQ (Read ReQuest) ή WRQ (Write ReQuest) στον host S, το οποίο περιέχει το όνομα του αρχείου και τρόπο μεταφοράς του.

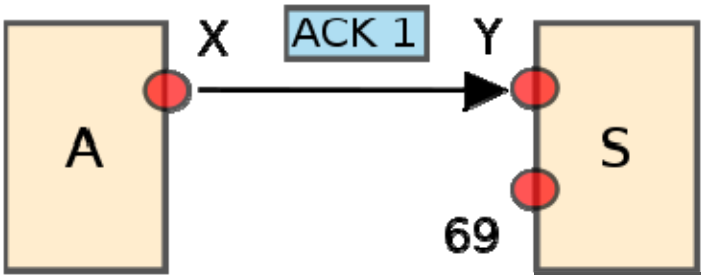




- Ο host S, αν το πακέτο που έχει αποσταλεί είναι WRQ, απαντάει με ένα πακέτο ACK (ACKnowledgement), αλλιώς αν το πακέτο είναι RRQ απαντάει αυτόματα με ένα DATA πακέτο.

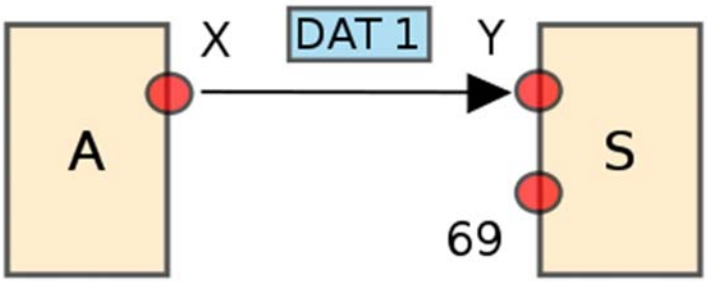


ο Ο host «πομπός» (ανάλογα με τη φύση του αρχικού πακέτου RRQ ή WRQ αλλάζει η ιδιότητα του κάθε host) αποστέλλει αριθμημένα πακέτα DATA στον host «παραλήπτη», μεγέθους 512 bytes.



ο Το τελευταίο πακέτο DATA πρέπει να έχει μέγεθος μικρότερο από 512 bytes, ώστε έτσι να υποδηλώνει ότι είναι και το τελευταίο. Εάν το συνολικό μέγεθος του αποσταλμένου μηνύματος είναι πολλαπλάσιο των 512 bytes, τότε για να δηλωθεί το τέλος του πακέτου αποστέλλεται ένα τελευταίο μπλοκ μηδενικού μεγέθους DATA (0 bytes).

ο Ο παραλήπτης απαντάει σε κάθε DATA πακέτο με ένα ACK, ενώ ο αποστολέας απαντάει σε κάθε ACK που λαμβάνει, αποστέλλοντας το επόμενο στη σειρά DATA πακέτο.

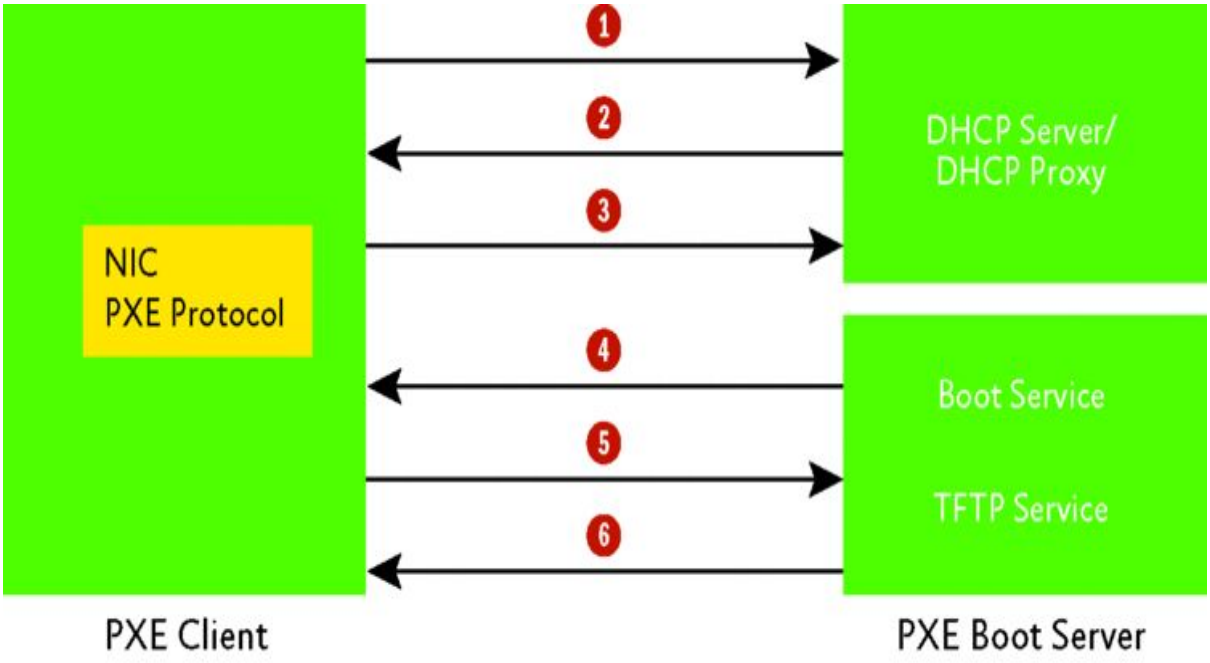


- Σε περίπτωση που κάποιο ACK δεν παραληφθεί, τότε ένας αναμεταδότης αποστέλλει ξανά το DATA πακέτο.

5.2 PREBOOT EXECUTION ENVIROMENT (PXE)

Με τον όρο PXE (Preboot eXecution Enviroment) αναφερόμαστε σε ένα περιβάλλον για την εκκίνηση υπολογιστών μέσω δικτύου ανεξάρτητα από αποθηκευτικά μέσα και εγκατεστημένα λειτουργικά συστήματα. Το PXE (συχνά συναντάται και ως Pre-Execution Enviroment –προφέρεται και ‘pixie’) αναπτύχθηκε ως τμήμα του Wired For Managemet Framework της Intel το 1999 . Κάνει χρήση διαφόρων πρωτόκολλων δικτύου, όπως Internet Protocol (IPv4), User Datagram Protocol (UDP), Dynamic Host Configuration Protocol (DHCP) και Trivial File Transfer Protocol (TFTP), καθώς επίσης και εννοιών όπως του Globally Unique Identifier (GUID), Universal Unique Identifier (UUID) και Universal Network Device Interface.

Το PXE προέρχεται από το πρωτόκολλο DHCP και είναι εφαρμοσμένο και τυπικά στις κάρτες δικτύου των υπολογιστών. Παρακάτω φαίνεται ο τρόπος λειτουργίας του:



Λειτουργία PXE

- Αρχικά ο PXE client αποστέλλει ένα πακέτο broadcast DHCPDISCOVER στη θύρα 67/UDP.

- Ο DHCP server στη συνέχεια απαντάει μ' ένα πακέτο DHCPOFFER το οποίο περιέχει μια διεύθυνση IP, στον client στη θύρα 68/UDP.

- Ο client στέλνει ένα DHCPREQUEST στον DHCP server για τη διαδρομή του αρχείου εκκίνησης.

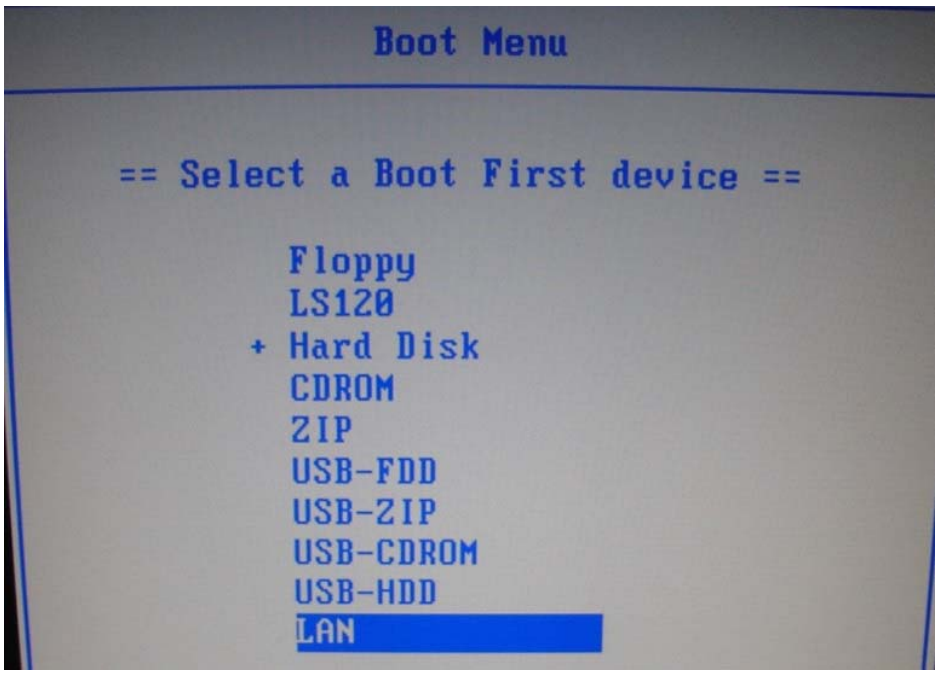
- Ο Boot Server απαντάει μ' ένα DHCPACK όπου περιέχει το όνομα του NBP (Network Boot Program) αρχείου. (Στη δική μας περίπτωση το NBP είναι το PXELINUX του οποίου η λειτουργία θα αναλυθεί στη συνέχεια)

- Ο client στη συνέχεια ζητά το αρχείο NBP από τον Boot Server

- Το αρχείο κατεβαίνει από τον TFTP Server και εκτελείται στον client.

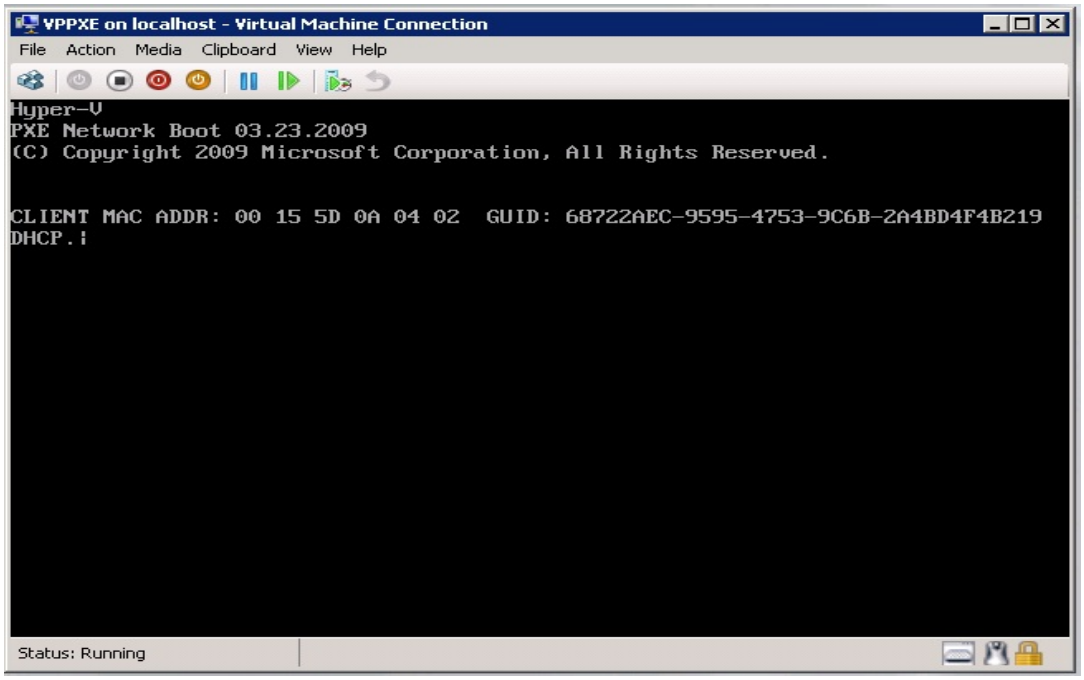
Για την υλοποίηση της παραπάνω διαδικασίας αλλά και της γενικότερης εκτέλεσης της λειτουργίας του PXE περιβάλλοντος, προαπαιτείται να οριστεί στο boot menu του BIOS του εκάστοτε τερματικού, η επιλογή εκκίνησης του υπολογιστή μέσω δικτύου (network boot). Σε περίπτωση που δεν υπάρχει η συγκεκριμένη επιλογή εκκίνησης (πράγμα που συναντάται σπάνια και σε αρκετά παλιά μηχανήματα) δεν μπορεί να εκτελεστεί τίποτα από τα προαναφερμένα. Παρακάτω παρουσιάζεται μέσω screenshots στην πράξη η όλη διαδικασία υλοποίησης του PXE περιβάλλοντος. Η υλοποίησή του έχει γίνει σε εικονικό τερματικό μέσω της υπηρεσίας Hyper-V.

Αρχικά γίνεται η επιλογή της εκκίνησης μέσω δικτύου (LAN) στο boot menu του συστήματος μας

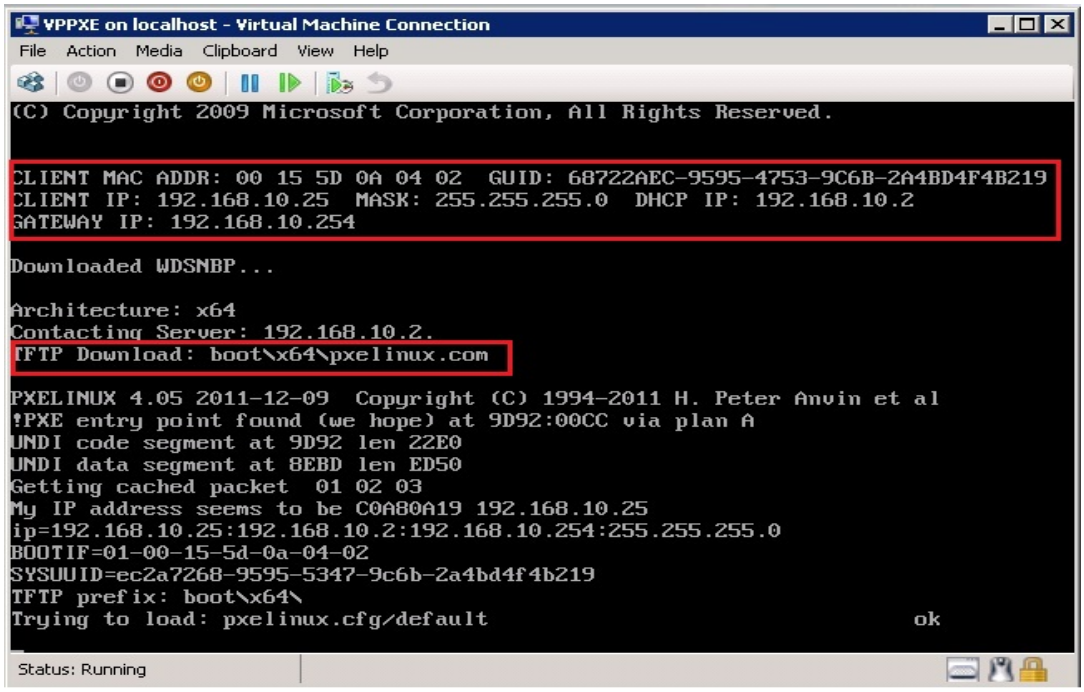


Bios boot menu

..το τερματικό μας δείχνει να αναγνωρίζει την ύπαρξη του PXE περιβάλλοντος στο σύστημα το οποίο πάει να εισέλθει.

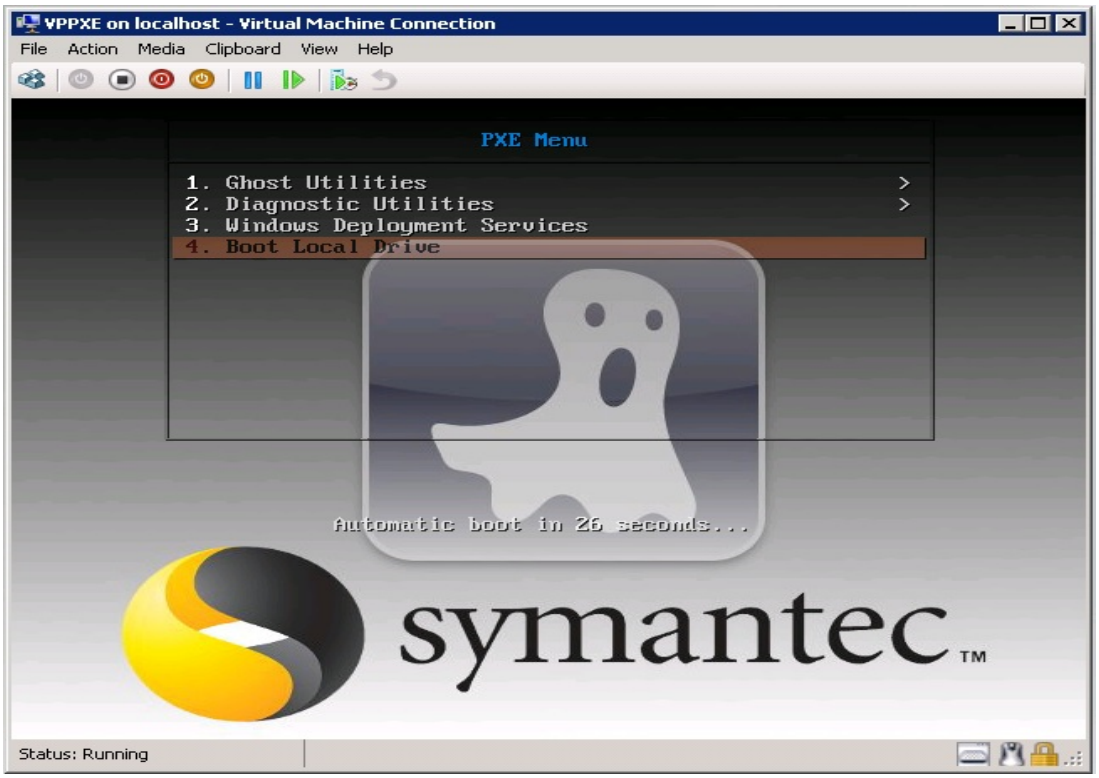


Στη συνέχεια φαίνεται χαρακτηριστικά το αποτέλεσμα των 6 βημάτων που περιγράψαμε παραπάνω.



- **CLIENT MAC ADDR**: Η φυσική διεύθυνση του client.
- **GUID**: Αριθμητικό προσδιοριστικό. Κάθε υπολογιστής που εκκινεί κατ αυτόν τον τρόπο έχει έναν τέτοιο μοναδικό αριθμό.
- **CLIENT IP**: Η διεύθυνση IP του client.
- **MASK**: Η μάσκα υποδικτύου του client.
- **DHCP IP**: Η διεύθυνση IP του DHCP server.
- **GATEWAY IP**: Η διεύθυνση IP του router.
- **TFTP Download**: Το αρχείο που κατεβαίνει από τον TFTP server και εκτελείται στον client.

Αφού εκτελεστεί επιτυχώς όλη η παραπάνω διαδικασία, και κατέβει και «τρέξει» το αρχείο PXELINUX, τότε εμφανίζεται στην οθόνη το μενού που θα έχουμε δημιουργήσει..



Το συγκεκριμένο PXE menu που έχουμε υλοποιήσει, περιέχει 4 επιλογές. Το μενού είναι πλήρως παραμετροποιήσιμο και οι επιλογές είναι ενδεικτικές. Ο ακριβής κώδικας του μενού παρατίθεται στο παράρτημα στο τέλος της εργασίας.

5.3 NETWORK BOOT PROGRAM (BOOT LOADER), PXELINUX

Θέλοντας να εξηγήσουμε τη λειτουργία του Network Boot Program PXELINUX στο οποία αναφερθήκαμε προηγουμένως θα κάνουμε πρώτα μια συνοπτική αναφορά στην έννοια του bootstrap loader ή bootstrap ή boot loader.

Όταν κάποιος υπολογιστής σβήνει, το λογισμικό, συμπεριλαμβανομένων του λειτουργικού συστήματος, των εφαρμογών και των δεδομένων, αποθηκεύεται σε μέσα όπως σκληροί δίσκοι, DVD ROMs και USB flash drives. Όταν στη συνέχεια χρειαστεί να εκκινήσει ξανά, ο υπολογιστής ουσιαστικά δεν έχει κάποιο λογισμικό τοποθετημένο στη μνήμη RAM του. Η εκκίνηση γίνεται μέσω της μνήμης ROM στην οποία και βρίσκεται μόνιμα αποθηκεμένο ένα μικρό πρόγραμμα μαζί με κάποια απαραίτητα αρχεία που χρειάζονται στον υπολογιστή ώστε να μπορεί να προσπελάσει τα δεδομένα που βρίσκονται στις μονάδες που αναφέραμε προηγουμένως

Το μικρό αυτό πρόγραμμα το οποίο είναι και η αιτία να ξεκινήσει όλη η διαδικασία εκκίνησης του υπολογιστή μας ονομάζεται boot loader. Η μοναδική αρμοδιότητα του προγράμματος αυτού είναι να φορτώνει άλλα αρχεία και προγράμματα απαραίτητα για την εκκίνηση του λειτουργικού στη μνήμη RAM.

Στη δικά μας περίπτωση ο boot loader που χρησιμοποιείται είναι ο PXELINUX. Ο PXELINUX είναι προσαρμοσμένη έκδοση του SYSLINUX boot loader ώστε να πραγματοποιεί εκκίνηση Linux λειτουργικών συστημάτων από έναν δικτυακό server κάνοντας χρήση δικτυακής ROM που

ταιριάζει με τα χαρακτηριστικά του Intel PXE περιβάλλοντος. Αξίζει να τονιστεί πως ο PXELINUX boot loader ΔΕΝ είναι κάποιο πρόγραμμα το οποίο μπορεί να τοποθετηθεί στην PROM της κάρτας δικτύου.

Για να μπορέσει να πραγματοποιηθεί η εκτέλεση το PXELINUX boot loader, θα πρέπει να δημιουργήσουμε αρχικά στον TFTP Server μας τον κατάλογο "*/tftpboot*" και να αντιγράψουμε εκεί το αρχείο *pxelinux.0* (από τη διανομή SYSLINUX) καθώς και τυχόν *kernel* ή *initrd* image αρχεία θέλουμε να εκκινήσουνε. Τέλος δημιουργούμε τον κατάλογο *"/tftpboot/pxelinux.cfg"* όπου και δηλώνεται και ως τοποθεσία του configuration αρχείου.

Επειδή μερικές φορές θα χρειαστεί να εκκινήσουν από τον ίδιον Server περισσότερα από ένα συστήματα, το configuration αρχείο εξαρτάται από την IP του μηχανήματος εκκίνησης. Ο PXELINUX θα ψάξει για το config αρχείο στον boot server με τον παρακάτω τρόπο.

- Πρώτα θα ψάξει για το config αρχείο χρησιμοποιώντας τον τύπο του υλικού (ARP type) και της mac διεύθυνσής του, ακολουθώντας σύνταξη με πεζά δεκαεξαδικά, χωρισμένα μεταξύ του με παύλα. Για παράδειγμα, για ένα Ethernet (ARP type 1) με mac διεύθυνση AA:BB:CC:DD:11:22, θα ψάξει για το όνομα αρχείου 01-aa-bb-cc-dd-11-22

- Στη συνέχεια θα ψάξει για το config αρχείο χρησιμοποιώντας τη δικιά του IP αλλά με κεφαλαίους δεκαεξαδικούς χαρακτήρες. Για παράδειγμα η διεύθυνση 192.0.2.91 θα μετατραπεί σε C000025B. Εάν αυτή η διεύθυνση δε βρεθεί κάθε φορά θα αφαιρεί ένα δεκαεξαδικό από το τέλος και θα επιχειρεί ξανά. Όταν θα αφαιρέσει και το τελευταίο ψηφίο τότε τη θέση του θα πάρει το αρχείο "default" (με πεζά) το οποίο και θα αναζητήσει.

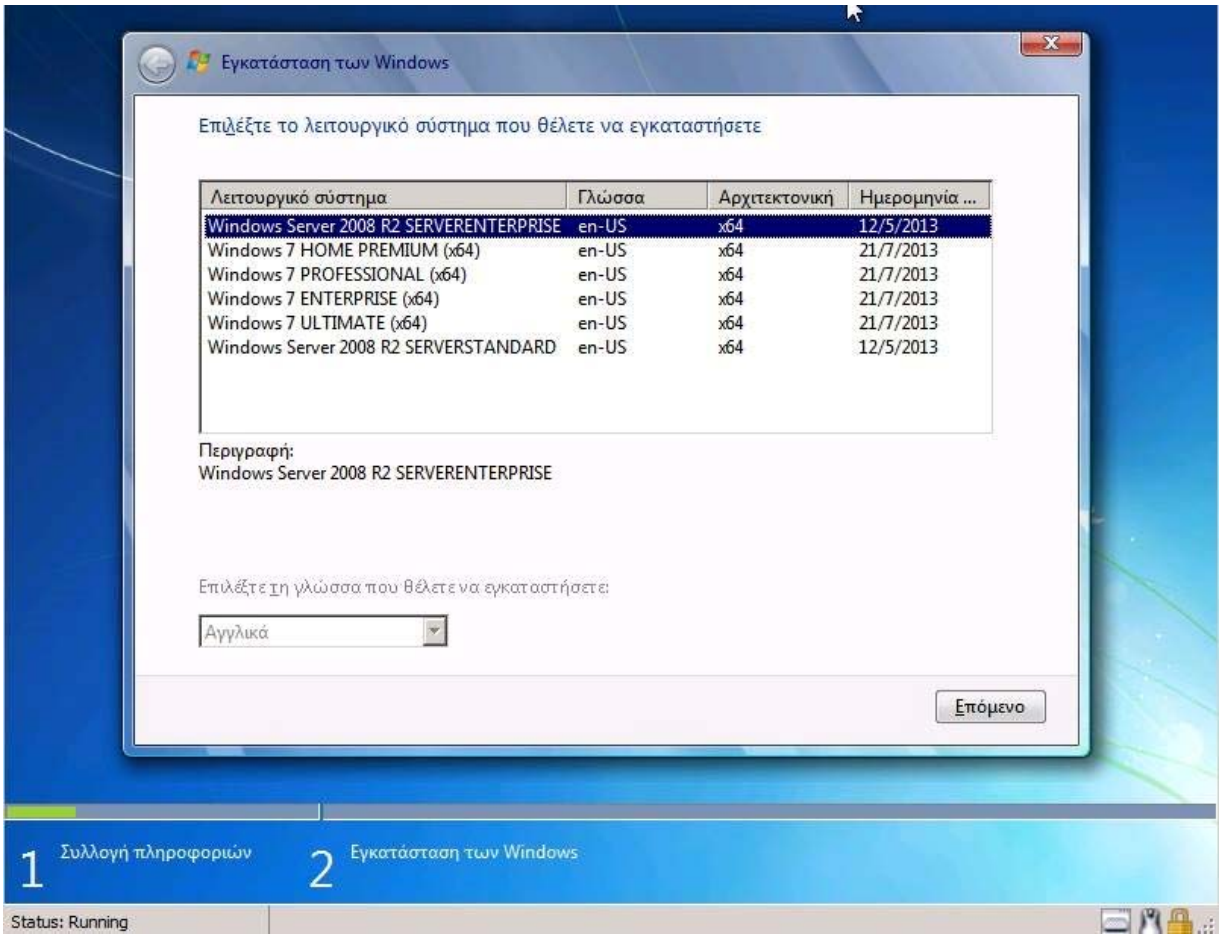
Για παράδειγμα, αν η ονομασία του αρχείου είναι /mybootdir/pxelinux.0, η Ethernet MAC ADDRESS είναι AA:BB:CC:DD:11:22 και η διεύθυνση 192.0.2.91 τότε τα αρχεία που θα δοκιμαστούν θα είναι τα παρακάτω.

/mybootdir/pxelinux.cfg/01-88-99-aa-bb-cc-dd
/mybootdir/pxelinux.cfg/C000025B
/mybootdir/pxelinux.cfg/C000025
/mybootdir/pxelinux.cfg/C00002
/mybootdir/pxelinux.cfg/C0000
/mybootdir/pxelinux.cfg/C000
/mybootdir/pxelinux.cfg/C00
/mybootdir/pxelinux.cfg/C0
/mybootdir/pxelinux.cfg/C
/mybootdir/pxelinux.cfg/default

5.4 WINDOWS DEPLOYMENT SERVICES (WDS)

Η Τρίτη επιλογή του custom pxe menu που έχουμε δημιουργήσει φέρει την ονομασία Windows Deployment Services. Με τον όρο αυτόν αναφερόμαστε σε μια server τεχνολογία ανεπτυγμένη από την Microsoft που μας παρέχει τη δυνατότητα εγκατάσταση λειτουργικού συστήματος windows αποκλειστικά μέσω δικτύου. Το WDS θεωρείται διάδοχος της παλαιότερης υπηρεσίας της Microsoft, Remote Installation Services (RIS). Σκοπός του WDS είναι η απομακρυσμένη εγκατάσταση των λειτουργικών Windows 7, Windows 8, Windows Server 2008 και Windows Server 2012, καθώς και διαφόρων άλλων λειτουργικών συστημάτων, αφού σε αντίθεση με τον προκάτοχό του RIS, τα WDS χρησιμοποιούν τη λειτουργία του disk imaging και συγκεκριμένα το Windows Imaging Format (.wim). Τα WDS συμπεριλαμβάνονται ως role του λειτουργικού Windows Server 2008 και στις 2 εκδόσεις (32 & 64 bit), ενώ αποτελούσε ένα προαιρετικά διαθέσιμο προς εγκατάσταση component στην έκδοση Windows Server 2003 Service Pack 2.

Τα WDS λειτουργούν σε συνεργασία σε συνεργασία με το Preboot eXecution Enviroment (PXE) μια έκδοση «μικρογραφία» των Windows –γνωστή ως Windows PE- ικανή για εργασίες εγκατάστασης και συντήρησης. Τα WDS ουσιαστικά λειτουργούν ως αποθηκευτικός χώρος, τόσο για τις PXE εικόνες εκκίνησης μέσω δικτύου (network boot images), όσο και για τα ίδια τα λειτουργικά συστήματα που θα εγκατασταθούν στον υπολογιστή. Όταν είναι διαθέσιμες περισσότερες από μία εικόνες διαθέσιμες προς εγκατάσταση, τότε η εκκίνηση του PXE μέσω των WDS θα εμφανίσει στην οθόνη του χρήστη ένα μενού εκκίνησης ώστε να επιλέξει την εικόνα που επιθυμεί να φορτώσει.



Διαθέσιμα λειτουργικά συστήματα

5.4 WINDOWS PE & WINDOWS AUTOMATED INSTALLATION KIT (WAIK)

Για την απλοποίηση της διαδικασίας της δημιουργίας και της εφαρμογής των image αρχείων μπορούμε να δημιουργήσουμε παραμετροποιημένα μέσω script, Windows PE image αρχεία. Η δημιουργία αυτών των αρχείων γίνεται με χρήση του Windows Automated Installation Kit, όπου σε συνδυασμό με το .wim αρχείο των Windows προστίθενται στον κατάλογο αποθήκευσης των image αρχείων του WDS Server. Τα δημιουργημένα Windows PE image αρχεία μπορούν να είναι είτε 32 είτε 64 bit.

Μια δυσκολία που παρουσιάζεται είναι η ανάγκη να συμπεριληφθούν οι οδηγοί (drivers) του δικτύου καθώς και των ελεγκτών μονάδας δίσκου, στο Windows PE boot image αρχείο. Η διαδικασία πρόσθεσης των οδηγών μπορεί να αυτοματοποιηθεί χρησιμοποιώντας την κονσόλα του WDS Server.

- Αρχικά επιλέγουμε το .wim αρχείο, το οποίο μπορεί να είναι είτε ένα καινούριο που το έχουμε δημιουργήσει από ένα αυθεντικό DVD των Windows (32 ή 64 bit), είτε ένα παλαιότερα ρυθμισμένο .wim αρχείο.
- Επιλέγουμε τους οδηγούς που επιθυμούμε να προσθέσουμε στο .wim αρχείο.
- Τα WDS τοποθετούν το .wim αρχείο σε κάποιο εικονικό κατάλογο, προσθέτουν σε αυτόν τους νέους οδηγούς και στη συνέχεια δημιουργούν εκ νέου το νέο .wim αρχείο.
- Το αναβαθμισμένο .wim αρχείο προτίθεται στον τομέα των boot image αρχείων του χώρου των WDS.

Η διαδικασία αυτή μπορεί να επαναληφθεί σε περίπτωση που χρειαστεί να δημιουργηθεί κάποιο νέο Wndows PE boot αρχείο για κάποιον νέο υπολογιστή που απαιτεί καινούριους οδηγούς.

ΚΕΦΑΛΑΙΟ 6. LINUX MAIL SERVER

Μια ακόμα υπηρεσία την οποία χρειάστηκε να συμπεριλάβουμε είναι αυτή του mail Server. Κρίνοντας από τον σκοπό της υλοποίησης της όλης εργασίας να γίνει αποκλειστικά και μόνο με υπηρεσίες που παρέχονται δωρεαν (freeware), έγινε η επιλογή της πλατφόρμας του iredmail.

6.1 IREDMAIL

Με τον όρο iredmail αναφερόμαστε σε μία ανοιχτού κώδικα, μηδενικού κόστους, ολοκληρωμένη λύση mail Server. Πρόκειται για mail Server πλατφόρμα ανεπτυγμένη για το λειτουργικό σύστημα Linux που ως ιδιαίτερο χαρακτηριστικό της έχει την δυνατότητα σύνδεσής της με το LDAP πρωτόκολλο και το Active Directory.

Τα πλεονεκτήματα χρήσης του iredmail έχουν να κάνουν με το μηδενικό κόστος απόκτησης της πλατφόρμας (μπορεί ο καθένας να κατεβάσει το πλήρες πακέτο της υπηρεσίας από το site http://www.iredmail.org οπού παρέχονται και οι απαραίτητες οδηγίες υποστήριξης που μπορεί να χρειαστούν), την πολύ γρήγορη και εύκολη εγκατάσταση της υπηρεσίας, τα ανοιχτού κώδικα (open source) συστατικά του στοιχεία, την δυνατότητα να υλοποιηθεί σε εικονικές μηχανές και βασικότερο από όλα καθώς είναι ένα στοιχείο που το διαφοροποιεί απο τις αντίστοιχές υπηρεσίες, η δυνατότητα επικοινωνίας με το LDAP και το Active Directory.

Οι διανομές στις οποίες μπορουμε να εγκαταστήσουμε την πλατφόρμα του iredmail είναι οι εξής:

- Red Hat, CentOS
- Debian
- Ubuntu
- OpenBSD
- FreeBSD

Για την υλοποίηση του iredmail mail server έγινε χρήση της Hyper-V υπηρεσίας και εικονικού τερματικού στο οποίο είχε γίνει εγκατάσταση διανομής του λειτουργικού συστήματος linux. Στη συνέχεια παραθέτουμε έναν πίνακα με τα συστατικά στοιχεία του iredmail καθώς και τους ρόλους τους στην υλοποίηση του mail Server

Συστατικό Στοιχείο	**Ρόλος**
Postfix	MTA (SMTP)
Dovecot	POP3, IMAP
Apache	Web Server
OpenLDAP, MySql	Αποθήκευση Λογαριασμών
Amavisd	Antivirus, Antispam
Roundcube	Webmail
Awstats	Αναλυτής αρχείων log (Apache και Postfix)
phpMyAdmin, iRedAdmin	Web-Based Διαχείριση

ΒΙΒΛΙΟΓΡΑΦΙΑ

Stan Riemer, Conan Kezema, Mike Mulcare, Byron Wright ,"*Windows Server 2008 Active Directory Resource Kit*" , Microsoft Press. John Price, Brad Price, "*Mastering Active Directory for Windows Server 2008*", Sybex. Mark Minasi, Darril Gibson, Aidan Finn, Wendy Henry, Byron Hynes, *"Mastering Windows Server 2008 R2",* Sybex. Dan Holme, "*Windows Administration*", Wiley. Jeremy Moskowitz, "*Group Policy: Fundamentals, Security, and Troubleshooting*", Sybex. Mich Tulloch *"Understanding Virtualization Solutions",* Microsoft Press. William R. Stanek *"Windows Server 2008 Inside Out*", Microsoft Press. Darril Gibson *"Windows Server 2008 Administrator",* Microsoft Press. Charlie Russel, Craig Zacker, *"Introducing Windows Server 2008 R2",* Microsoft Press. Robert Larson, Janique Carbon *"Hyper-V Resource Kit",* Microsoft Press. Microsoft Technet – How the Data Store Works, http://technet.microsoft.com/en-us/library/cc772829(v=ws.10).aspx. Microsoft Technet-"*Active Directory and Directory Domain Services Port Requirements"*, http://technet.microsoft.com/en-us/library/dd772723(v=ws.10).aspx. Microsoft Technet-"*Group Policy for Begginers"* http://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx. Microsoft Technet – "*Roaming User Profiles"*, http://technet.microsoft.com/en-US/windows/ff629668.aspx?ITPID=sprblog. Microsoft Technet-"*Roaming Profiles",* http://technet.microsoft.com/en-US/windows/ff629665.aspx?ITPID=sprblog. Group Policy Central-*"Best Practices",* http://www.grouppolicy.biz/best-practices/ . Microsoft Technet-"DHCP Server Role: Configuring a DHCP Server", http://technet.microsoft.com/el-GR/library/cc756865(v=ws.10).aspx. Microsoft Technet-*"Manage Virtual Machines Remotely With Hyper-V Manager and Windows 7"*, http://technet.microsoft.com/en-us/library/ee256062(v=ws.10).aspx. Microsoft Technet-*"The Desktop Files - Network Booting Windows"*, http://technet.microsoft.com/el-gr/magazine/2008.07.desktopfiles(en-us).aspx. Wikipedia-"*Preboot Execution Enviroment*", http://en.wikipedia.org/wiki/Preboot_Execution_Environment. Symantec-"*Switches : Alphabetical List Of Switches*", http://www.symantec.com/business/support/index?page=content&id=TECH130961. Syslinux-"*PXELINUX*", http://www.syslinux.org/wiki/index.php/PXELINUX. Syslinux-*"Comboot/menu",* http://www.syslinux.org/wiki/index.php/Comboot/menu.c32. Ubuntu-*"Active Directory Wind Bind – ..How To"*, https://help.ubuntu.com/community/ActiveDirectoryWinbindHowto. Red Hat-*"*Integrating Red Hat Enterprise Linux 6 with Active Directory", http://people.redhat.com/mskinner/rhug/q3.2013/ready_rhel_ad/refarch_rhel6_to_ad.pdf. Microsoft Technet-*"Authenticating LinuxClients With Active Directory",* http://technet.microsoft.com/el-gr/magazine/2008.12.linux(en-us).aspx Samba-*"Set Up A Samba AD Member Server",* https://wiki.samba.org/index.php/Samba_%26_Active_Directory. Red Hat-"*Using Pluggable Authentication Modules (PAM)",* https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Managing_Smart_Cards/Pluggable_Authentication_Modules.html. Technoblogical-*"Windows Server 2008",* http://www.technoblogical.com/windows-server-2008/. PCTechStream-Video Tutorials, http://www.pctechstream.com/tutorials.html. ITFreeTraining-*"Active Directory Course"*, http://itfreetraining.com/70-640/index-70-640/.

ΠΑΡΑΡΤΗΜΑ

ΚΩΔΙΚΑΣ ΑΛΛΑΓΗΣ ΟΝΟΜΑΤΟΣ ΤΕΡΜΑΤΙΚΟΥ

```
@echo off
set name="PC-"
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\runonce /v boot2 /t REG_SZ /d %TEMP%\boot2.cmd
IPCONFIG |FIND "IPv4" > %TEMP%.\TEMP.DAT
FOR /F "tokens=2 delims=:" %%a in (%TEMP%.\TEMP.DAT) do set IP=%%a
del %TEMP%.\TEMP.DAT
set IP=%IP:~1%
echo %IP% > %TEMP%.\TEMP.DAT

FOR /F "tokens=4 delims=." %%b in (%TEMP%.\TEMP.DAT) do set field=%%b
del %TEMP%.\TEMP.DAT
echo %field% > %TEMP%.\PCNUM.DAT
set /a num=%field%-20

netdom RENAMECOMPUTER %COMPUTERNAME% /newname:%name%%num% /force /reboot:5
```

ΚΩΔΙΚΑΣ ΕΙΣΟΔΟΥ ΥΠΟΛΟΓΙΣΤΗ ΣΤΟ DOMAIN

```
$user = "INFORMATICS\user1"
$domain="INFORMATICS"
$pass = ConvertTo-SecureString "user010101" -AsPlainText -Force
$DomainCred = New-Object System.Management.Automation.PSCredential $user, $pass
Try
  {
  Add-Computer -DomainName $domain -credential $DomainCred -OUPath ("OU=TESTCLASS, OU=DESKTOPS,OU=COMPUTERS,OU=IT,DC=INFORMATICS,DC=COM") -PassThru -ErrorAction Stop
  }
Catch
  {
  Add-Computer -DomainName $domain -credential $DomainCred -Passthru
  }
```

ΚΩΔΙΚΑΣ ΜΕΝΟΥ ΕΠΙΛΟΓΩΝ ΠΟΥ ΕΜΦΑΝΙΖΕΤΑΙ ΣΤΗΝ ΠΡΩΤΗ ΟΘΟΝΗ ΜΕΤΑ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΤΟΥ IMAGE ΑΡΧΕΙΟΥ

```
@ECHO OFF

CLS
:MENU
CLS

ECHO ============= Boot Options =============
ECHO.
ECHO 1.  Set computer name and join Domain
ECHO 2.  Copy Applications
ECHO 3.  Create new image
ECHO.
ECHO ==========PRESS 'Q' TO QUIT=============
ECHO.

SET INPUT=
SET /P INPUT=Please select a number:

IF /I '%INPUT%'=='1' GOTO Selection1
IF /I '%INPUT%'=='2' GOTO Selection2
IF /I '%INPUT%'=='3' GOTO Selection3
IF /I '%INPUT%'=='Q' GOTO Quit

CLS

ECHO ============INVALID INPUT============
ECHO Please select a number from the Main
echo Menu [1-3] or select 'Q' to quit.
ECHO ======PRESS ANY KEY TO CONTINUE======

PAUSE > NUL
GOTO MENU

:Selection1
CALL SetComputerName.cmd
GOTO MENU

:Selection2
CALL CopyApps.cmd
```

```
GOTO MENU

:Selection3
EXIT
GOTO MENU

:Quit
CLS

ECHO ======PRESS ANY KEY TO CONTINUE======

PAUSE>NUL
EXIT
```

ΚΩΔΙΚΑΣ ΑΝΤΙΓΡΑΦΗΣ ΤΩΝ PORTABLE ΕΦΑΡΜΟΓΩΝ

```
@echo off

:set variables
set appath="D:\Applications"

:create folder
md %appath%

:map network drive
net use X: \\WIN2008R2\applications$

:copy files
xcopy X:\*.* %appath% /y

:delete netowrk drive
net use /delete * /y
```

ΚΩΔΙΚΑΣ ΔΗΜΙΟΥΡΓΙΑΣ 'PXE MENU'

```
DEFAULT vesamenu.c32
MENU BACKGROUND pxelinux.cfg/ghost2.jpg
MENU COLOR BORDER 37;44 #80ffffff #00000000 STD
menu color hotsel       1;7;37;40  #FF000000    #FFB80000 all
menu color sel          7;37;40  #FF000000  #FFB80000 all
PROMPT 0
```

```
NOESCAPE 0
ALLOWOPTIONS 0
TIMEOUT 300

  MENU TITLE   PXE Menu - INFORMATION TECHNOLOGY DEPARTMENT

        MENU BEGIN

              MENU LABEL ^1. Ghost Utilities
              MENU PASSWD $4$LpMtTgdM$tsl/sGWX34yp8o0WhDfwmAgtq74$
              MENU TITLE Ghost Utilities

              LABEL Ghost_Client_UNDI
              MENU LABEL ^1. Symantec Ghost UNDI 11.5
              kernel memdisk
              append keeppxe initrd=imz/ghost.imz

              LABEL Ghost_Client_UNDI_WINPE
              MENU LABEL ^2. Symantec Ghost WINPE
              kernel memdisk
              append iso initrd=utils/ghostboot.iso

              LABEL Restore_System_Partition
              MENU LABEL ^3. Restore Client System Partition
              kernel memdisk
              append keeppxe initrd=imz/restore_image.imz

              LABEL Create_Client_Partitions
              MENU LABEL ^4. Create Client Partitions
              kernel memdisk
              append keeppxe initrd=imz/restore_disk.imz

              LABEL Create_Client_Image
              MENU LABEL ^5. Create Client Image
              kernel memdisk
              append keeppxe initrd=imz/create_image.imz


              LABEL Create_Client_Partitions+Restore_System_Partition
              MENU LABEL ^6. Create Client Partitions + Restore System Partition
              kernel memdisk
              append keeppxe initrd=imz/rstr_disk+crt_img.imz

          MENU SEPARATOR
```

```
        LABEL return

        MENU INDENT 5
        MENU LABEL ^Esc - Return to Main Menu
        MENU EXIT

MENU END



MENU BEGIN

        MENU LABEL ^2. Diagnostic Utilities
        MENU PASSWD $4$LpMtTgdM$tsl/sGWX34yp8o0WhDfwmAgtq74$
        MENU TITLE Utilities


        LABEL WD_Disk_Diagnostics
        MENU LABEL ^1. WD Lifeguard
        kernel memdisk
        append keeppxe initrd=utils/wd.imz

        LABEL SEA_TOOLS
        MENU LABEL ^2. Seatools
        kernel memdisk
        append iso initrd=utils/seatools.iso


        LABEL Memory_Test
        MENU LABEL ^3. Memory Test
        kernel memdisk
        append iso initrd=utils/Memtest86.iso

        MENU SEPARATOR

        LABEL return

        MENU INDENT 5
        MENU LABEL ^Esc - Return to Main Menu
        MENU EXIT

MENU END
```

```
        LABEL WDS
        MENU LABEL ^3. Windows Deployment Services
        MENU PASSWD $4$LpMtTgdM$tsl/sGWX34yp8o0WhDfwmAgtq74$
        KERNEL pxeboot.0

MENU BEGIN

        MENU LABEL ^4. Install Linux Distributions
        MENU PASSWD $4$LpMtTgdM$tsl/sGWX34yp8o0WhDfwmAgtq74$
        MENU TITLE Linux Distributions


        label ubuntu-expert
        menu label ^1. Ubuntu Expert install x86
        kernel /linux/ubuntu/linux
        append priority=low vga=normal initrd=/linux/ubuntu/initrd.gz --

        label ubuntu-expert x64
        menu label ^2. Ubuntu Expert install x64
        kernel /linux/ubuntu/linux-amd64
        append priority=low vga=normal initrd=/linux/ubuntu/initrd-amd64.gz --

        label debian-expert
        menu label ^3. Debian Expert install x86
        kernel /Linux/Debian/linux
        append priority=low vga=normal initrd=/Linux/Debian/initrd.gz --

        label debian-expert x64
        menu label ^4. Debian Expert install x64
        kernel /Linux/Debian/linux-amd64
        append priority=low vga=normal initrd=/Linux/Debian/initrd-amd64.gz --

        MENU SEPARATOR

        LABEL return

        MENU INDENT 5
        MENU LABEL ^Esc - Return to Main Menu
        MENU EXIT

MENU END

        LABEL Local_Drive
```

```
MENU DEFAULT
MENU LABEL ^5. Boot Local Drive
localboot 0
```