



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ, ΑΠΟΚΕΝΤΡΩΣΗΣ & ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ



**ΥΠΟΕΡΓΟ: «ΔΗΜΙΟΥΡΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΥΛΙΚΟΥ ΠΡΟΓΡΑΜΜΑΤΩΝ ΓΙΑ
ΤΗΝ ΑΝΑΠΤΥΞΗ ΤΟΥ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ ΤΗΣ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ
ΒΑΣΕΙ ΣΧΕΔΙΩΝ ΕΚΠΑΙΔΕΥΣΗΣ»**

ΤΙΤΛΟΣ ΠΡΟΓΡΑΜΜΑΤΟΣ:

ΔΙΑΧΕΙΡΙΣΗ WINDOWS SERVER 2008

ΕΚΠΑΙΔΕΥΤΙΚΟ ΥΛΙΚΟ

Κωδικός εκπαιδευτικού υλικού:

Κωδικός Πιστοποίησης προγράμματος:



**ΥΠΟΕΡΓΟ: «ΔΗΜΙΟΥΡΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΥΛΙΚΟΥ ΠΡΟΓΡΑΜΜΑΤΩΝ ΓΙΑ
ΤΗΝ ΑΝΑΠΤΥΞΗ ΤΟΥ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ ΤΗΣ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ
ΒΑΣΕΙ ΣΧΕΔΙΩΝ ΕΚΠΑΙΔΕΥΣΗΣ»**

ΤΙΤΛΟΣ ΠΡΟΓΡΑΜΜΑΤΟΣ:

ΔΙΑΧΕΙΡΙΣΗ WINDOWS SERVER 2008

ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ

Μέλη Ομάδας

Συντονιστής/στρια:

Τσιμάρας Δημήτριος

Συντάκτες/κτρίες:

Κολαΐτης Χρήστος

Σαλής Αναστάσιος

Σταματιάδης Ευάγγελος



ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΕΧΟΜΕΝΟ ΚΑΙ ΣΤΟΧΟΙ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ	13
1.1 Σκοπός και στόχοι	13
ΕΙΣΑΓΩΓΗ ΣΤΟ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ WINDOWS SERVER	14
2.1 Εισαγωγή	14
2.2 Εισαγωγή στο λειτουργικό σύστημα Windows Server 2008.....	14
2.2.1 Ιστορία και εκδόσεις λειτουργικού συστήματος (NT4, 2000, 2003).....	14
2.2.1.1 Windows NT 4.0	15
2.2.1.2 Windows 2000.....	15
2.2.1.3 Windows Server 2003	16
2.2.1.4 Windows Server 2008	17
2.2.2 Νέα χαρακτηριστικά της έκδοσης 2008	18
2.2.2.1 Server Core.....	18
2.2.2.2 Active Directory Roles	19
2.2.2.3 Failover Clustering	20
2.2.2.4 Windows Powershell.....	20
2.2.2.5 Self-healing NTFS	21
2.2.2.6 Hyper-V	21
2.2.2.7 Windows System Resource Manager	22
2.2.2.8 Server Manager.....	22
2.2.2.9 Άλλα Χαρακτηριστικά.....	22
2.2.2.10 Χαρακτηριστικά που απομακρύνθηκαν.....	26
2.2.3 Εκδόσεις.....	27
2.2.4 Service Packs	28
2.2.4.1 Service Pack 2.....	28
2.2.5 Windows Server 2008 R2	28
2.3 Διαφορετικές εκδόσεις του προϊόντος και απαιτήσεις υλικού ανά έκδοση 29	
2.3.1 Απαιτήσεις Συστήματος	29
2.3.2 Αδειοδότηση – Ενδεικτικές Τιμές	31
ΕΓΚΑΤΑΣΤΑΣΗ WINDOWS SERVER 2008	32
3.1 Εισαγωγή	32
3.2 Εγκατάσταση Windows Server 2008	32
3.2.1 Εγκατάσταση και ρυθμίσεις	32
3.2.2 Ενέργειες μετά την εγκατάσταση	45

3.3 Εγκατάσταση Ρόλων.....	65
3.4 Εγκατάσταση Active Directory	72
ΥΛΟΠΟΙΗΣΗ, ΔΙΑΧΕΙΡΙΣΗ, ΣΥΝΤΗΡΗΣΗ ΔΙΚΤΥΑΚΗΣ ΥΠΟΔΟΜΗΣ ..	120
4.1 Εισαγωγή	120
4.2 Εισαγωγή στα TCP/IP δίκτυα.	120
4.2.1 Διευθύνσεις IP: Δίκτυα και κεντρικοί υπολογιστές	121
4.2.2 Μάσκα υποδικτύου	122
4.2.3 Κλάσεις δικτύου	123
4.2.4 Δημιουργία υποδικτύων	124
4.2.5 Προεπιλεγμένες πύλες (Default Gateway)	126
4.2.6 Αντιμετώπιση προβλημάτων	127
4.2.6.1 Εσφαλμένη μάσκα υποδικτύου	127
4.2.6.2 Εσφαλμένη διεύθυνση IP	127
4.2.6.3 Εσφαλμένη προεπιλεγμένη πύλη	128
4.3 TCP/IP δίκτυα και OSI	128
4.4 Dynamic Host Configuration Protocol (DHCP).....	130
ΥΠΗΡΕΣΙΕΣ ΚΑΤΑΛΟΓΟΥ.....	146
5.1 Εισαγωγή στις υπηρεσίες καταλόγου και στην υπηρεσία DNS - Αρχιτεκτονική του Active Directory	146
5.1.1 Τι είναι το Active Directory;	146
5.1.2 Τι είναι το DNS;	146
5.1.3 Περιεχόμενα Καταλόγου	146
5.2 Active Directory Forests και Domains	148
5.2.1 Βασικές Έννοιες	148
5.2.2 Windows Server 2008 Domain and Forest Functional Levels	150
5.3 Ρόλοι του AD -Active Directory roles	153
5.3.1 Object Names	153
5.3.2 Global Catalog.....	153
5.3.3 Replication	154
5.3.4 Flexible Single Master	154
5.4 Active Directory Services & Server Roles	156
5.4.1 Read-Only Domain Controller	157
5.4.2 Restartable Active Directory Domain Services.	160
5.4.3 Fine-Grained Password Policies	161
5.4.4 Identity Management για UNIX	162

5.5	Εγκατάσταση της υπηρεσίας AD DS	162
	ΥΠΗΡΕΣΙΕΣ ΟΝΟΜΑΤΩΝ- ΣΧΕΔΙΑΣΜΟΣ DNS.....	164
6.1	Η κατανόηση των ονομάτων DNS	164
6.2	Σχεδιάζοντας ένα χώρο ονομάτων DNS	165
6.2.1	Δημιουργία ενός ονόματος τομέα DNS.....	165
6.2.2	Δημιουργία ονόματα υπολογιστών DNS	166
6.3	Εγκατάσταση και ρύθμιση ADDS και DNS	167
6.4	Διαχείριση της Υπηρεσίας DNS.....	174
6.4.1	DNS κονσόλα και διαμόρφωση.....	174
6.4.2	Διαχείριση DNS	178
6.5	Active Directory & DNS	183
6.6	Forwarders & Conditional Forwarders.....	185
6.7	GlobalNames Zone (GNZ)	186
	ACTIVE DIRECTORY USERS AND COMPUTERS	188
7.1	Active Directory Users and Computers console.....	188
7.1.1	Δυνατότητες του Active Directory Users and Computers	188
7.1.2	Πρόσβαση στο Active Directory Users and Computers	190
7.1.3	Επιλογές του Μενού	191
7.1.4	Τα κουμπιά πλοήγησης-button bar	191
7.1.5	To Console Tree	193
7.2	Active Directory objects	196
	Ιδιότητες κυριότερων αντικειμένων	196
7.2.1	Computer Objects:.....	196
7.2.2	Group Objects	198
7.2.3	User Objects.	201
7.3	Πραγματοποιώντας εργασίες με το Active Directory Users και Computers 203	
7.3.1	Δημιουργώντας έναν νέο χρήστη -new user.....	203
7.3.2	Δημιουργία νέας ομάδας -new group	203
7.3.3	Δημιουργία ενός νέου κοντέινερ ,υποδοχέα - organizational unit	203
7.3.4	Προσθήκη ενός χρήστη -user σε μια ομάδα –group	203
7.3.5	Αλλαγή κωδικού πρόσβασης - Change a password	204
7.3.6	Για να ξεκλειδώσουμε ένα λογαριασμό.....	204
7.3.7	Απενεργοποίηση λογαριασμού	204
7.3.8	Μετακίνηση ενός χρήστη	204

7.3.9	Περιορισμός χρόνου σύνδεσης -Restrict logon times.....	204
7.3.10	Μεταβίβαση εξουσιών Delegate authority	204
7.3.11	Άδεια στους χρήστες να χρησιμοποιούν VPN	205
7.3.12	Για μια αλλαγή σε ένα συγκεκριμένο χαρακτηριστικό ενός αντικείμενου	205
7.4	Στρατηγικές ομάδων Group strategies	205
7.4.1	GROUP SCOPE.....	205
7.4.2	Domain Local Groups.....	206
7.4.3	Global Groups	206
7.4.4	Universal Groups	206
7.4.5	Local Groups	206
7.4.6	Στρατηγικές για την παροχή δικαιωμάτων	207
	ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΣΒΑΣΗΣ ΣΕ ΠΟΡΟΥΣ	208
8.1	Εισαγωγή	208
8.2	Διαχείριση πρόσβασης σε πόρους	208
8.3	Βασικές έννοιες.....	208
8.4	Δημιουργία και Διαχείριση	210
8.4.1	Δημιουργία και διαχείριση δικαιωμάτων κοινόχρηστων φακέλων μέσω των ιδιοτήτων του φακέλου	210
8.4.2	Διαχείριση δικαιωμάτων φακέλων (NTFS permissions).....	211
8.4.3	Share and Storage management.	216
8.4.4	Διαχείριση αποθηκευτικών χώρων.....	223
8.4.5	Shadow copies of Share folders	223
8.5	Offline caching	225
8.6	Υλοποίηση και διαχείριση εκτυπώσεων	227
8.6.1	Εγκατάσταση και κοινή χρήση εκτυπωτών	227
8.6.2	Διαχείριση πρόσβασης στους εκτυπωτές.....	230
8.6.3	Προτεραιότητες εκτυπώσεων – Printer Spooler.....	232
	ΔΙΣΚΟΙ & ΑΠΟΘΗΚΕΥΣΗ ΔΕΔΟΜΕΝΩΝ.....	234
9.1	Εισαγωγή	234
9.2	Διαχείριση Δίσκων (Disks Management).....	234
9.2.1	Βασικοί Ορισμοί.....	235
9.2.2	Μετατροπές Δίσκων.....	236
9.2.3	Online, offline status	237
9.2.4	Initializing (Αρχικοποίηση).....	237

9.2.5	Μεταφορά δίσκου σε άλλο H/Y	238
9.2.6	Basic σε Dynamic	239
9.2.7	Dynamic σε Basic	240
9.2.8	Χειρισμός Χαμένου ή εκτός λειτουργίας Δυναμικού δίσκου	240
9.2.9	Shrink (Συρρίκνωση) τόμου	240
9.2.10	Χειρισμός Βασικού δίσκου	241
9.2.11	9.2.11 Χειρισμός Δυναμικού δίσκου	241
9.2.12	Simple Volume	242
9.2.13	Spanned Volume	244
9.2.13.1	Striped Volume.....	247
9.2.13.2	Mirrored Volume	250
9.2.13.3	Raid-5 Volume.....	253
9.2.13.4	Extend (επέκταση) τόμου	256
9.2.13.5	Επιπρόσθετες δυνατότητες Disk Management	258
9.2.14	Σύνδεση φακέλου (Mount point folder path) σε Drive.....	258
9.2.15	Απομακρυσμένη διαχείριση δίσκων.....	259
9.3	Διαχείριση Αποθήκευσης Δεδομένων.....	259
9.3.1	EFS File Encryption	259
9.3.2	Συμπίεση Αρχείων (File compression)	261
9.3.3	Quotas	262
9.3.3.1	Disk Quotas σε τοπική μονάδα δίσκου	263
9.3.3.2	Quotas σε φάκελο.....	266
	DISASTER RECOVERY	272
10.1	Εισαγωγή	272
10.2	Disaster Recovery.....	272
10.3	Βασικοί Ορισμοί.....	272
10.4	Windows Server Backup	273
10.4.1	Προπαρασκευαστικές εργασίες	275
10.4.2	Δημιουργία Αντιγράφων Ασφαλείας Δεδομένων (Backup)	277
10.4.3	Χρονοπρογραμματισμός Εργασιών Backup	280
10.4.4	Ανάκτηση δεδομένων από Αντίγραφο Ασφαλείας (Restore)	282
10.4.5	Windows Recovery Environment και ένα backup δημιουργημένο στο Windows Server Backup	287
10.4.6	Active directory Restore.....	288
10.4.7	Shadow copies.....	289

10.4.8	Μέθοδοι και εργαλεία disaster recovery	289
ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΔΙΑΧΕΙΡΙΣΗ		290
11.1	Εισαγωγή	290
11.2	Βασικοί Ορισμοί.....	290
11.3	Απομακρυσμένη Διαχείριση.....	290
11.3.1	Χρήση Κονσόλας Διαχείρισης της Microsoft (MMC)	290
11.3.1.1	Stand-Alone και Extension snap-ins	292
11.3.1.2	Επιλογές Κονσόλας (Console Options)	293
11.3.1.3	Χρήση Απομακρυσμένης Διαχείρισης Υπολογιστών.....	294
11.3.2	Χρήση Remote Desktop.....	296
11.3.3	Ενεργοποίηση του Remote Desktop	296
11.3.4	Απαιτήσεις και Ρυθμίσεις - Remote Desktop Connection Client	297
11.4	Remote Server Administration Tools (RSAT)	299
11.4.1	Τι είναι τα RSAT.....	299
11.4.2	Εγκατάσταση και χρήση των RSAT	300
ORGANIZATIONAL UNITS.....		303
12.1	Εισαγωγή	303
12.2	Βασικοί Ορισμοί.....	303
12.3	Ορισμός, Βασικές έννοιες, Δομή	303
12.3.1	Απόδοση / Μεταβίβαση Διαχειριστικού Ελέγχου	304
12.3.2	Ιεραρχία των OUs	304
12.3.3	Group Policy Object (GPO)	306
12.3.4	Δημιουργία OUs για την απόκρυψη αντικειμένων	306
12.4	Δημιουργία και διαχείριση OUs	306
12.4.1	Διαχείριση αντικειμένων του Active Directory	308
12.4.2	Τροποποίηση δικαιωμάτων πρόσβασης του Active Directory	309
12.4.3	Μεταβίβαση διαχειριστικού ελέγχου OUs.....	312
GROUP POLICY.....		314
13.1	Εισαγωγή	314
13.2	Βασικοί Ορισμοί.....	314
13.3	Group Policy	314
13.3.1	Ιεράρχηση εφαρμογής πολιτικών Ασφαλείας	314
13.3.1.1	Local Security Policy	314
13.3.1.2	Domain & DC policies	316
13.3.1.3	Προεπιλεγμένα εργαλεία.....	318

13.3.1.4	Group Policy Object (GPO)	320
13.3.1.5	Group Policy Management	324
13.3.1.6	Create, Link, Block Inheritance	326
13.3.1.7	Δημιουργία και διαχείριση GPOs σε Domain	328
13.3.1.8	Backup, Restore GPOs	331
13.3.1.9	Group Policy Refresh Rates	334
13.3.1.10	Παράδειγμα υλοποίησης GPO	336
	ΣΕΝΑΡΙΟ GROUP POLICY	339
14.1	Εισαγωγή	339
14.2	Σύνδεση με Remote Desktop στους client H/Y	339
14.2.1	Ενεργοποίηση Remote Desktop στον client H/Y	339
14.2.2	Εξαίρεση Remote Desktop στο Windows Firewall του client HY...340	
14.2.3	Επιλογή απομακρυσμένων χρηστών	341
14.3	Ρυθμίσεις Internet Explorer	342
14.3.1	Internet Explorer User Interface.....	343
14.3.2	Ρυθμίσεις Proxy	344
14.3.3	Αρχική Σελίδα, Αγαπημένα και Συνδέσεις.....	345
14.3.4	Προχωρημένες Ρυθμίσεις Internet Explorer	346
14.4	Περιβάλλον Χρήστη.....	347
	ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΕΓΚΑΤΑΣΤΑΣΗ ΛΟΓΙΣΜΙΚΟΥ	350
15.1	Εισαγωγή	350
15.2	Δημιουργία Υποδομής	350
15.2.1	Πακέτα Εγκατάστασης.....	352
15.2.1.1	MS Office Installation Packages.....	353
15.2.1.2	Adobe Installation Packages	355
15.3	Απομακρυσμένη Εγκατάσταση Λογισμικού.....	358
15.4	Απομακρυσμένη Απεγκατάσταση Λογισμικού	362
15.5	Απομακρυσμένη Εγκατάσταση νέας έκδοσης – Αναβάθμιση Λογισμικού 363	
15.5.1	Επιτόπια Αναβάθμιση σε νέα έκδοση (In-place Upgrade)	364
15.5.2	Αντικατάσταση με νέα έκδοση (Replace)	368
15.6	Δημοσίευση Λογισμικού (Publish Software)	369
15.6.1	Προχωρημένες Ρυθμίσεις Δημοσίευσης.....	372
15.6.2	Εγκατάσταση Δημοσιευμένου Λογισμικού (user-side).....	375
	WINDOWS DEPLOYMENT SERVICES	377

16.1	Εισαγωγή	377
16.2	Διαφορές μεταξύ WDS και RIS	377
16.2.1	Πλεονεκτήματα	378
16.2.2	Αναβάθμιση από server με RIS και Windows Server 2003 SP1 ή SP2	379
16.3	Εγκατάσταση Windows Deployment Services	381
16.3.1	Προαπαιτούμενα Στοιχεία.....	381
16.3.2	Διαδικασία Εγκατάστασης Windows Deployment Services	382
16.4	Παραμετροποίηση Windows Deployment Services	386
16.4.1	Διαδικασία Ρύθμισης Windows Deployment Services	387
16.4.2	Προσθήκη Εικόνων (Images).....	391
16.5	Ρύθμιση του boot menu	402
16.5.1	Διαδικασίες Ρύθμισης του Boot Menu	403
16.6	Δημιουργία Custom Install Images	404
16.6.1	Διαδικασίες Δημιουργίας Capture Image.....	405
16.6.2	Διαδικασίες Δημιουργίας Install Image	409
16.7	Discover Images	415
	Windows Server Update Services (WSUS).....	422
17.1	Γενικά για το WSUS	422
17.1.1	Περισσότερες πληροφορίες	422
17.1.2	WSUS Clients	422
17.1.3	Τοπολογία WSUS	422
1.	Αρχεία express εγκατάστασης (express installation files)	426
17.2	Εγκατάσταση WSUS	427
17.2.1	Πριν από την εγκατάσταση	427
17.2.2	Υλικό και λογισμικό για την εγκατάσταση του WSUS	427
17.2.3	Απαιτήσεις εγκατάστασης (software requirements) για clients	427
17.2.4	Δικαιώματα.....	427
17.2.5	Προετοιμασία εγκατάστασης του WSUS 3.0 SP2	428
17.2.6	Εγκατάσταση WSUS Server ή Administration Console	429
17.2.7	Χρήση του οδηγού εγκατάστασης WSUS 3.0 SP2	429
17.3	Παραμετροποίηση WSUS	433
17.3.1	Παραμετροποίηση δικτυακών ρυθμίσεων WSUS	433
17.3.2	Παραμετροποίηση ενημερώσεων και συγχρονισμού	439
2.	Με χρήση του οδηγού παραμετροποίησης του WSUS	439

17.3.3	Με χρήση της κονσόλας διαχείρισης του WSUS	444
17.3.4	Παραμετροποίηση ομάδων υπολογιστών	446
17.4	Έγκριση και διάθεση ενημερώσεων.....	448
17.4.1	Αυτόματη έγκριση ενημερώσεων	449
17.4.2	Έγκριση αντικαταστάτριας ενημέρωσης	451
17.4.3	Κατηγορίες ενημερώσεων WSUS.....	452
17.5	Παραμετροποίηση WSUS clients με χρήση πολιτικών σε Active Directory 453	
17.5.1	Παραμετροποίηση Automatic Updates.....	454
17.5.2	Προσδιορισμός του WSUS server με GPO.....	454
3.	Ένταξη clients σε ομάδες υπολογιστών μέσω GPO -Enable client-side targeting	455
17.5.3	Επαναπρογραμματισμός προγραμματισμένων εγκαταστάσεων - Reschedule Automatic Updates scheduled installations.....	456
17.5.4	Μη αυτόματη επανεκκίνηση για ολοκλήρωση εγκαταστάσεων - No auto-restart for scheduled Automatic Update installation options	457
	Διαδικασία αποτροπής αυτόματης επανεκκίνησης του client για προγραμματισμένες εγκαταστάσεις ενημερώσεων	458
17.5.5	Συχνότητα ελέγχου νέων ενημερώσεων - Automatic Updates detection frequency	458
17.5.6	Άμεση εγκατάσταση ενημερώσεων - Allow Automatic Update immediate installation	458
	Διαδικασία άμεσης εγκατάστασης ενημερώσεων	459
17.5.7	Καθυστέρηση επανεκκίνησης - Delay restart for scheduled installations 459	
	Διαδικασία καθυστέρησης επανεκκίνησης των clients	459
17.5.8	Επανάληψη υπενθύμισης για επανεκκίνηση - Re-prompt for restart with scheduled installations	459
17.5.9	Ειδοποιήσεις προς χρήστες που δεν έχουν δικαιώματα διαχείρισης - Allow non-administrators to receive update notifications	460
17.5.10	Να επιτρέπεται η λήψη ενημερώσεων και από τρίτους κατασκευαστές - Allow signed content from the intranet Microsoft update service location.....	461
17.5.11	Αφαίρεση συνδέσμων και πρόσβασης στο Windows Update - Remove links and access to Windows Update.....	461
17.5.12	Απαγόρευση πρόσβασης στο Windows Update - Disable access to Windows Update	461
17.6	WSUS για απομονωμένα δίκτυα.....	463
17.6.1	Επιλογές για αρχεία και γλώσσες	463

17.6.2	Μεταφορά αρχείων στον απομονωμένο server.....	464
17.6.3	Μεταφορά metadata στον απομονωμένο server.....	465
17.7	Διαχείριση αναφορών στο WSUS.....	467
17.7.1	Κατάσταση εγκατάστασης ενημέρωσης.....	468
17.7.2	Δημιουργία αναφορών	468
17.8	Χρήση των αναφορών.....	468
17.8.1	Αναφορές ενημερώσεων	468
17.8.2	Αναφορές υπολογιστών.....	469
17.8.3	Αναφορές συγχρονισμού	470
17.9	Βέλτιστες πρακτικές WSUS	471

ΠΕΡΙΕΧΟΜΕΝΟ ΚΑΙ ΣΤΟΧΟΙ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ

1.1 Σκοπός και στόχοι

Βασικός στόχος του προγράμματος Διαχείριση του Microsoft Windows Server 2008 είναι να παρουσιαστούν οι δυνατότητες και οι τρόποι διαχείρισης του λογισμικού στους επιμορφωμένους υπαλλήλους έτσι ώστε να αποκτηθεί ανάλογη εμπειρία για:

- Την εξασφάλιση, διαχείριση και διατήρηση της ακεραιότητας των δεδομένων και πληροφοριών που περιέχονται στα δίκτυα των Φορέων του Δημοσίου και στα μέσα μόνιμης αποθήκευσης.
- Τη διασφάλιση της συνεχούς και απρόσκοπτης επικοινωνίας των Δημοσίων Υπηρεσιών μεταξύ τους.
- Τη βελτιστοποίηση της αποδοτικότητας της πληροφοριακής υποδομής προς όφελος των υπαλλήλων, των πολιτών και της εξυπηρέτησης των Υπηρεσιών γενικότερα.

Οι επιθυμητές γνώσεις και δεξιότητες που θα αποκτήσουν οι επιμορφωμένοι στη Διαχείριση του Microsoft Windows Server 2008 και ιδιαίτερα από την αλληλεπίδραση στην δικτυακή εικονική προσομοίωση τυπικής διάταξης, θα τους καταστήσουν ικανούς να δημιουργούν, μέσω ρυθμίσεων δικαιωμάτων ομάδων και χρηστών του εσωτερικού δικτύου, ασφαλές περιβάλλον επεξεργασίας, αποθήκευσης και διαχείρισης δεδομένων αλλά και διασύνδεσης, των Φορέων με τον έξω κόσμο, με ελεγχόμενες διεπαφές επικοινωνίας.

ΕΙΣΑΓΩΓΗ ΣΤΟ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ WINDOWS SERVER

2.1 Εισαγωγή

Οι επιθυμητές γνώσεις και δεξιότητες που θα αποκτήσουν οι επιμορφωμένοι στην ενότητα «Εισαγωγή στο λειτουργικό σύστημα Windows Server» θα τους καταστήσουν ικανούς να:

- Γνωρίζουν την ιστορία και τις εκδόσεις του λειτουργικού συστήματος Windows Server 2008
- Γνωρίζουν τις νέες δυνατότητες της έκδοσης 2008

2.2 Εισαγωγή στο λειτουργικό σύστημα Windows Server 2008

2.2.1 Ιστορία και εκδόσεις λειτουργικού συστήματος (NT4, 2000, 2003)

Το 1983 η Microsoft ανακοίνωσε την ανάπτυξη των Windows, ένα γραφικό περιβάλλον χρήσης για τον δικό της λειτουργικό σύστημα το MS-DOS, το οποίο το διανείμετο με τους IBM-PCs και τους IBM συμβατούς υπολογιστές από το 1981. Με την πάροδο του χρόνου, το προϊόν αυτό από ένα απλό «γραφικό περιβάλλον χρήσης» που ξεκίνησε, εξελίχθηκε σε ένα μοντέρνο λειτουργικό σύστημα με δύο βασικούς άξονες-οικογένειες σχεδίασης, καθένας με τον δικό του κώδικα και το δικό του εγγενές σύστημα αρχείων.

Οι οικογένειες 3.x και 4.x περιλαμβάνουν τα MS-DOS, Windows 95, Windows 98 και τα Windows Me. Τα “Windows for Workgroups 3.11” που ήταν βασισμένα στο DOS, έκαναν την επανάσταση στην δικτύωση από τα 16 στα 32 bit και στην 32-αμπιτη πρόσβαση στον σκληρό δίσκο. Η ειδοποιός διαφορά με τα Windows 95 ήταν η μετάβαση από τον “Program Manager” στον “Explorer”, αλλά επιπρόσθετα αρκετά στοιχεία και υποσυστήματα του λειτουργικού ξαναγράφτηκαν από την αρχή και μετατράπηκαν σε κώδικα 32-bit για τα Windows 95. Στα Windows 95 έχουμε για πρώτη φορά, έστω και κάπως πρώιμα υποστήριξη του “Plug and Play”.

Η οικογένεια των Windows NT ξεκίνησε το 1993 με την έκδοση των NT 3.1. Τα μοντέρνα λειτουργικά συστήματα των Windows βασίζονται στον πυρήνα (kernel) της νεώτερης έκδοσης των Windows NT ο οποίος αρχικά δημιουργήθηκε για να χρησιμοποιηθεί στο OS/2. Τα Windows τρέχουν σε επεξεργαστές IA-32, x86-64 και σε επεξεργαστές τεχνολογίας Itanium. Οι πρώτες εκδόσεις υποστήριζαν και αρχιτεκτονικές επεξεργαστών της εποχής όπως Alpha, MIPS, Fairchild Clipper και Power PC. Είχε γίνει ακόμα και αρκετή δουλειά για υποστήριξη SPARC. Ο πυρήνας

των NT δανείστηκε πολλές από τις αρχιτεκτονικές του VMS. Με την έκδοση των NT 4.0 το 1996 το κέλυφος εργασίας (shell) άλλαξε από τον “Program Manager” στον “Explorer”. Η υποστήριξη για επεξεργαστές στις αρχικές εκδόσεις των NT περιλάμβανε τους PowerPC, MIPS και DEC Alpha, αλλά στις μεταγενέστερες εκδόσεις συγκεντρώνεται στις τεχνολογίες Itanium, 386, 486 και σήμερα στις x64.

2.2.1.1 Windows NT 4.0

Η Microsoft έδωσε τα Windows NT 4.0, με ενσωματωμένο το καινούριο γραφικό περιβάλλον χρήσης (interface) των Windows 95, πάνω από τον πυρήνα (kernel) των Windows NT. Υπήρξε ακόμα και κάποια έκδοση patch ώστε να μπορούν οι developers να εγκαταστήσουν το νέο περιβάλλον χρήστη (User Interface – UI) των Windows 95 στα Windows NT 3.51, αλλά παρουσίασε αρκετά προβλήματα (bugs).

Τα Windows NT 4.0 βγήκαν σε τέσσερις εκδόσεις:

- Windows NT 4.0 Workstation
- Windows NT 4.0 Server
- Windows NT 4.0 Server, Enterprise Edition με ενσωματωμένη υποστήριξη μέχρι 8 επεξεργαστών (8 way SMP - Symmetric Multi Processing) και clustering
- Windows NT 4.0 Terminal Server

2.2.1.2 Windows 2000

Η Microsoft, το Φεβρουάριου του 2000 έδωσε σε κυκλοφορία τα Windows 2000, τα οποία κατά την φάση ανάπτυξής τους ήταν γνωστά ως Windows NT 5.0. Χρησιμοποιήθηκαν με αρκετή επιτυχία τόσο στην αγορά των Server όσο και στην αγορά των Workstations. Ανάμεσα στα πιο σημαντικά νέα χαρακτηριστικά των Windows 2000, ήταν η σχεδόν πλήρης αντικατάσταση του “Windows Server domain model” των NT 4.0 από το “Active Directory”, το οποίο αναπτύχθηκε χρησιμοποιώντας εδραιωμένες τεχνολογίες στην βιομηχανία όπως το DNS, LDAP και το Kerberos ώστε να διασυνδέονται οι υπολογιστές μεταξύ τους.

Η υπηρεσία “Terminal Services”, η οποία ήταν προηγουμένως διαθέσιμη ως ξεχωριστή έκδοση των NT 4, επεκτάθηκε σε όλες τις εκδόσεις των Server λειτουργικών. Επιπλέον ενσωματώθηκε ένα μεγάλος αριθμός από χαρακτηριστικά δανεισμένα από τα Windows 98, όπως ο “Device Manager”, ο “Windows Media Player” και μια ανανεωμένη έκδοση της βιβλιοθήκης “Direct X” η οποία για πρώτη φορά κατέστησε δυνατή την λειτουργία πολλών μοντέρνων παιχνιδιών στον πυρήνα των NT. Τα Windows 2000 αποτέλεσαν την τελευταία έκδοση των λειτουργικών

συστημάτων βασισμένων στον πυρήνα των NT τα οποία δεν απαιτούσαν ενεργοποίηση (Product Activation) μέσα από την διαδικασία της Microsoft.

Ενώ υπήρχαν εκδόσεις αναβάθμισης σε Windows 2000 (upgrades) από τα Windows 95 και τα Windows 98, εντούτοις δεν απευθύνονταν σε οικιακούς χρήστες.

Τα Windows 2000 ήταν διαθέσιμα σε έξι εκδόσεις:

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server
- Windows 2000 Advanced Server Limited Edition
- Windows 2000 Datacenter Server Limited Edition

2.2.1.3 Windows Server 2003

Στις 25 Απριλίου του 2003, η Microsoft έδωσε σε κυκλοφορία τα “Windows Server 2003”, μια αξιοσημείωτη αναβάθμιση των “Windows 2000 Server”, ενσωματώνοντας πολλά καινούρια χαρακτηριστικά ασφαλείας, έναν νέο οδηγό (wizard) με όνομα “Manage Your Server” ο οποίος απλοποιεί την ρύθμιση του υπολογιστή για συγκεκριμένους ρόλους και βελτιωμένη απόδοση. Έχουν τον αριθμό έκδοσης NT 5.2. Μερικές υπηρεσίες που δεν κρίθηκαν απαραίτητες για περιβάλλοντα Server, έχουν απενεργοποιηθεί για λόγους σταθερότητας, όπως οι υπηρεσίες “Windows Audio” και “Themes”. Οι χρήστες πρέπει να τους ενεργοποιήσουν «χειροκίνητα» ώστε να έχουν ήχο ή το θέμα (Theme) “Luna” για να μοιάζουν με τα Windows XP. Η επιτάχυνση υλικού (hardware acceleration) για την κάρτα γραφικών, είναι επίσης απενεργοποιημένη, και οι χρήστες πρέπει να την ενεργοποιήσουν χειροκίνητα ρυθμίζοντας το επίπεδό της, αν εμπιστεύονται πάντα το πρόγραμμα οδήγησης (driver) της κάρτας γραφικών.

Τον Δεκέμβριο του 2005, η Microsoft έκδωσε τα “Windows Server 2003 R2”, τα οποία στην πραγματικότητα είναι τα “Windows Server 2003” με SP1 (Service Pack 1) μαζί με ένα πακέτο επαύξησης (add-on package). Μεταξύ των νέων χαρακτηριστικών υπάρχει ένας αριθμός από χαρακτηριστικά διαχείρισης, εξυπηρέτηση αρχείων, εκτυπώσεις, και ενοποιημένες υπηρεσίες στην επικράτεια μια εταιρίας.

Τα Windows Server 2003 διατίθεντο σε έξι εκδόσεις:

- Web Edition (32-bit)
- Standard Edition (32 και 64-bit)

- Enterprise Edition (32 και 64-bit)
- Datacenter Edition (32 και 64-bit)
- Small Business Server (SBS) (32-bit)
- Storage Server (OEM channel only)

2.2.1.4 Windows Server 2008

Τα “Windows Server 2008” που δόθηκαν σε κυκλοφορία στις 27 Φεβρουαρίου του 2008, αρχικά ήταν γνωστά ως “Windows Server Codename Longhorn”. Τα “Windows Server 2008” βασίστηκαν τόσο στις τεχνολογικές προόδους όσο και στις προόδους στον τομέα της ασφάλειας που έγιναν στα Windows Vista, και είναι σημαντικά πιο αρθρωτά (modular) σε τεχνολογία από τον προκατόχο τους τα Windows Server 2003. Στο “Professional Developers Conference (PDC) 2008” η Microsoft ανακοίνωσε τα Windows Server 2008 R2 ως παραλλαγή των Windows 7 για συστήματα Server. Τα Windows Server 2008 R2 υποστηρίζουν μόνο 64-bit συστήματα (x64 και Itanium). Επομένως μπορούμε να πούμε ότι τα Windows 2008 αποτελούν το τελευταίο λειτουργικό για Server της Microsoft με υποστήριξη σε 32-bit συστήματα.

Τα Windows Server 2008 υπάρχουν σε δέκα (10!) συνολικά εκδόσεις:

- Windows Server 2008 Standard Edition (32-bit και 64-bit)
- Windows Server 2008 Enterprise Edition (32-bit και 64-bit)
- Windows Server 2008 Datacenter Edition (32-bit και 64-bit)
- Windows HPC Server 2008
- Windows Web Server 2008 (32-bit και 64-bit)
- Windows Storage Server 2008 (32-bit και 64-bit)
- Windows Small Business Server 2008 (64-bit only)
- Windows Essential Business Server 2008 (32-bit και 64-bit)
- Windows Server 2008 για Itanium-based συστήματα
- Windows Server 2008 Foundation Server

Αναφορές:

http://en.wikipedia.org/wiki/History_of_Microsoft_Windows

<http://www.microsoft.com>

2.2.2 Νέα χαρακτηριστικά της έκδοσης 2008

Τα Windows Server 2008 έχουν βασιστεί στον ίδιο βασικό κώδικα με τα Windows Vista, γι' αυτό και μοιράζονται αρκετή από την αρχιτεκτονική και τις λειτουργίες τους. Για αυτό το λόγο και μόνο διαθέτουν τα περισσότερα χαρακτηριστικά ασφάλειας και διαχείρισης που παρουσιάστηκαν με τα Windows Vista, όπως την γραμμένη εκ νέου στοίβα δικτύωσης (με εγγενή υποστήριξη του IPV6, των ασύρματων δικτύων με σημαντικές βελτιώσεις στον τομέα της ταχύτητας και της ασφάλειας), βελτιωμένες δυνατότητες εγκατάστασης μέσα από την χρήση “images”, δυνατότητες “deployment” και ανάκτησης από καταστροφή (recovery), βελτιωμένα εργαλεία διάγνωσης, παρακολούθησης, καταγραφής συμβάντων αλλά και δημιουργίας αναφορών.

Νέα χαρακτηριστικά ασφαλείας όπως ο Bitlocker για την προστασία των δεδομένων στους δίσκους και το ASLR (Address space layout randomization) για προστασία από επιθέσεις προϊόντων malware. Το τείχος προστασίας των Windows έχει και αυτό βελτιωθεί και είναι ενεργοποιημένο. Έχουμε ακόμα τεχνολογίες .NET Framework 3.0, και ειδικά “Windows Communication Foundation”, “Microsoft Message Queuing” και “Windows Workflow Foundation”, μαζί με βελτιώσεις στον πυρήνα (kernel) του λειτουργικού, της διαχείρισης της μνήμης και του συστήματος αρχείων.

Οι επεξεργαστές και οι μνήμες έχουν μοντελοποιηθεί πλέον και αυτοί ως συσκευές τύπου “plug and play” ώστε να επιτραπούν οι εύκολες αλλαγές αυτών των συσκευών ακόμα και με το σύστημα εν λειτουργία σε κάποιες περιπτώσεις. Αυτό ακριβώς επιτρέπει του πόρους του συστήματος να διαμερισματοποιούνται δυναμικά χρησιμοποιώντας το “Dynamic Hardware Partitioning” όπου κάθε προκύπτον διαμέρισμα έχει την δική του μνήμη, τον δικό του επεξεργαστή, ακόμα και συσκευές εισόδου – εξόδου (I/O host bridge devices) ανεξάρτητες από τα άλλα διαμερίσματα.

2.2.2.1 Server Core

Τα Windows Server 2008 έχουν μια παραλλαγή της εγκατάστασης που ονομάζεται “Server Core”. Το “Server Core” είναι στην ουσία μια σημαντικά περικομμένη εγκατάσταση στην οποία απουσιάζει παντελώς το γνώριμο περιβάλλον χρήσης του “Windows Explorer”. Όλες οι ρυθμίσεις και η συντήρηση γίνονται αποκλειστικά μέσω της γραμμής εντολών (command line interface windows) ή με απομακρυσμένη σύνδεση χρησιμοποιώντας το εργαλείο “Microsoft Management Console (MMC)”. Υπάρχουν όμως, το πρόγραμμα επεξεργασίας κειμένου “Notepad” και κάποιες

ελάχιστες εφαρμογές τους πίνακα ελέγχου όπως οι ρυθμίσεις περιοχής (Regional Settings”).

Η εγκατάσταση “Server Core” δεν περιλαμβάνει τα “.NET Framework”, “Internet Explorer”, “Windows PowerShell” και καμία από όσες λειτουργίες δεν σχετίζονται με τα χαρακτηριστικά του πυρήνα του λειτουργικού (Server Core Features). Το μηχάνημα που εκτελεί τα “Server Core” μπορεί να ρυθμιστεί για αρκετούς βασικούς ρόλους όπως: Domain controller/Active Directory Domain Services, AD LDS (ADAM), DNS Server, DHCP Server, file server, print server, Windows Media Server, IIS 7 web server ακόμα και Hyper-V virtual server. Η εγκατάσταση “Server Core” μπορεί να χρησιμοποιηθεί έτσι ώστε να δημιουργηθεί μία ομάδα διασυνδεδεμένων υπολογιστών (cluster) υψηλής διαθεσιμότητας χρησιμοποιώντας το Failover Clustering ή το Network Load Balancing.

Ο Andrew Mason, ένας επικεφαλής της ομάδας ανάπτυξης των Windows Server της Microsoft, δήλωσε ότι ένα από τα αρχικά κίνητρα για την παραγωγή της παραλλαγής “Server Core” του λειτουργικού “Windows Server 2008” ήταν η ελαχιστοποίηση των σημείων επίθεσης του λειτουργικού συστήματος, και ότι περίπου το 70% των ευπαθών σημείων των Microsoft Windows των τελευταίων πέντε ετών, δεν θα επηρέαζαν καθόλου την έκδοση “Server Core”.

2.2.2.2 Active Directory Roles

Οι ρόλοι του Active Directory επεκτάθηκαν με υπηρεσίες ταυτοποίησης, πιστοποιητικών και διαχείρισης δικαιωμάτων. Μέχρι την έκδοση Windows 2003, το Active Directory, επέτρεπε στους διαχειριστές δικτύων να διαχειρίζονται κεντρικά τους διασυνδεδεμένους υπολογιστές, να ορίζουν πολιτικές για ομάδες χρηστών και να μπορούν να εγκαθιστούν κεντρικά νέες εφαρμογές σε πολλούς υπολογιστές ταυτόχρονα. Αυτός λοιπόν ο γνωστός ρόλος του “Active Directory” έχει πλέον μετονομαστεί σε “Active Directory Domain Services” ή “AD DS” συντομογραφικά.

Ένας αριθμός από νέες επιπρόσθετες υπηρεσίες παρουσιάζονται όπως το “Active Directory Federation Services” (ADFS), “Active Directory Lightweight Directory Services” (AD LDS) το πρώην δηλαδή “Active Directory Application Mode” (ADAM), το Active Directory Certificate Services (ADCS), και το Active Directory Rights Management Services (AD RMS). Οι υπηρεσίες ταυτοποίησης (Identity services) και πιστοποιητικών (Certificate services) επιτρέπουν στους διαχειριστές να διαχειριστούν τους λογαριασμούς χρηστών και τα ψηφιακά πιστοποιητικά να έχουν πρόσβαση σε συγκεκριμένα συστήματα και υπηρεσίες.

Οι υπηρεσίες “Federation management services” επιτρέπουν στις εταιρείες να διαμοιράζονται διαπιστευτήρια με έμπιστους συνεργάτες και πελάτες, επιτρέποντας για παράδειγμα ένα σύμβουλο χρησιμοποιώντας τα user name και password της εταιρίας του, να μπορεί να κάνει “log-in” στο δίκτυο ενός πελάτη του. Το “Identity Integration Feature Pack” περιλαμβάνεται ως “Active Directory Metadirectory Services”. Κάθε μία από αυτές τις υπηρεσίες αντιπροσωπεύει έναν ρόλο του server.

2.2.2.3 Failover Clustering

Τα Windows Server 2008 παρέχουν υψηλή προσβασιμότητα στις υπηρεσίες (services) και στις εφαρμογές (applications) μέσω του Failover Clustering. Οι περισσότεροι ρόλοι και χαρακτηριστικά μπορούν να προσφέρονται με ελάχιστο έως και καθόλου downtime.

Στα “Windows Server 2008” και “Windows Server 2008 R2”, ο τρόπος με τον οποίο τα “clusters” ορίζονται και παραμετροποιούνται έχει αλλάξει σημαντικά με την εισαγωγή αυτοματοποιημένου οδηγού εγκατάστασης (cluster validation wizard). Αυτός ο οδηγός είναι ένα χαρακτηριστικό ενσωματωμένο στο “failover clustering” στα “Windows Server 2008” και “Windows Server 2008 R2”. Με τον “wizard” αυτόν μπορούμε να εκτελέσουμε μια σειρά από επικεντρωμένα σενάρια ελέγχου στην ομάδα των servers που σκοπεύουμε να χρησιμοποιήσουμε ως κόμβους σε μια τοπολογία cluster. Τα σενάρια ελέγχου, ελέγχουν και πιστοποιούν το υποκείμενο υλικό και λογισμικό απευθείας και ένα προς ένα μεμονωμένα, έτσι ώστε να επιτύχουμε ακριβή αξιολόγηση του πόσο καλά η υπάρχουσα τοπολογία μπορεί να υποστηρίξει το “failover clustering”.

Σημείωση: Αυτό το χαρακτηριστικό υπάρχει διαθέσιμο μόνο στις εκδόσεις Enterprise και Datacentre των Windows Server 2008.

2.2.2.4 Windows Powershell

Τα Windows Server 2008 είναι το πρώτο λειτουργικό σύστημα Windows τα οποία έρχονται με ενσωματωμένη την τεχνολογία Windows PowerShell, η οποία αποτελεί την νέα «γραμμή εντολών» της Microsoft, με τεχνολογία κατάλληλη για scripting βασισμένο σε εργασίες (task-based scripting). Το PowerShell βασίζεται σε αντικειμενοστραφή προγραμματισμό και την έκδοση 2.0 .NET Framework της Microsoft, και περιλαμβάνει περισσότερα από 120 εργαλεία διαχείρισης συστήματος, διατηρεί συνεπή σύνταξη και συμβάσεις ονοματολογίας σε αντίθεση με την κλασσική γραμμή εντολών, και έχει ενσωματωμένες δυνατότητες για εργασία με συνήθη δεδομένα διαχείρισης όπως είναι το “Windows registry”, το “certificate store” και το

“Windows Management Instrumentation”. Η γλώσσα του PowerShell, σχεδιάστηκε ειδικά για διαχειριστές, και μπορεί να χρησιμοποιηθεί στη θέση του cmd.exe και του WindowsScriptHost.

2.2.2.5 Self-healing NTFS

Στις προηγούμενες εκδόσεις των Windows, πριν από την έκδοση Windows Vista, αν το λειτουργικό σύστημα ανίχνευε βλάβη του συστήματος αρχείων ενός διαμερίσματος NTFS, τότε μάρκαρε το διαμέρισμα (volume) ως βρώμικο (dirty). Για να διορθωθούν τα σφάλματα στον τόμο αυτό θα έπρεπε πρώτα να τεθεί εκτός λειτουργίας (off-line). Με το αυτοεπισκευαζόμενο NTFS (Self-healing NTFS), ένα NTFS worker thread ξεκινάει την λειτουργία του στο background και πραγματοποιεί μια τοπική επισκευή των δομών δεδομένων που έχουν υποστεί τη ζημιά, μη επιτρέποντας την πρόσβαση μόνο σε εκείνα τα αρχεία – φακέλους που επηρεάζονται, χωρίς να κλειδώνει εκτός ολόκληρο το διαμέρισμα του δίσκου και να απαιτείται να τεθεί εκτός λειτουργίας ο server.

Το λειτουργικό σύστημα διαθέτει και τεχνικές ανίχνευσης S.M.A.R.T. ώστε να μπορεί να ειδοποιείται εγκαίρως όταν κάποιος σκληρός δίσκος έχει αυξημένη πιθανότητα να παρουσιάσει βλάβη.

2.2.2.6 Hyper-V

Το Hyper-V είναι ένα σύστημα υλοποίησης εικονικών μηχανών το οποίο επιτρέπει να εκτελούνται ταυτόχρονα πολλαπλά διαφορετικά λειτουργικά συστήματα στην ίδια πραγματική μηχανή. Τα αρχικά του προέρχονται από τις λέξεις HyperVisor-based Virtualization system, το οποίο και αποτελεί τον βασικό πυρήνα της στρατηγικής του Virtualization της Microsoft.

Δημιουργεί εικονικούς servers στο επίπεδο του πυρήνα του λειτουργικού συστήματος. Δηλαδή μπορούμε να πούμε ότι διαμερισματοποιεί έναν φυσικό server σε πολλά μικρότερα υπολογιστικά τμήματα. Το Hyper-V εμπεριέχει την δυνατότητα να δρα ως εξυπηρετητής επόπτη εικονικοποίησης Zen (Xen virtualization hypervisor host) που επιτρέπει σε λειτουργικά συστήματα πελάτη με δυνατότητες Zen (Xen) να τρέξουν εικονικοποιημένα.

Μια δοκιμαστική (beta) έκδοση του Hyper-V διατέθηκε με κάποιες x86-x64 εκδόσεις του λειτουργικού συστήματος Windows Server 2008, πριν από την επίσημη και τελική έκδοση της Microsoft που έγινε στις 26 Ιουνίου του 2008 και είναι ελεύθερα διαθέσιμη για κατέβασμα. Υπάρχει επιπλέον και αυτοδύναμη (standalone) έκδοση του Hyper-V. Αυτή η έκδοση υποστηρίζει μόνο τις x86-x64 αρχιτεκτονικές. Ενώ οι

εκδόσεις x86 των Windows Server 2008 δεν μπορούν να εκτελέσουν τις ενσωματώσεις Hyper-V (Hyper-V intergrations) μπορούν να εκτελέσουν των κονσόλα διαχείρισης και τα εργαλεία του Hyper-V.

2.2.2.7 Windows System Resource Manager

Το Windows System Resource Manager (WSRM) έχει ενσωματωθεί στα Windows Server 2008. Παρέχει διαχείριση των πόρων και μπορεί να χρησιμοποιηθεί για να ελέγξει το ποσό των πόρων που μια διαδικασία ή ένας χρήστης μπορεί να χρησιμοποιήσει βασισμένο σε επιχειρησιακές προτεραιότητες. Μέσω μιας διαδικασίας ελέγχου βασισμένη σε κριτήρια, “Process Matching Criteria”, βάσει του ονόματος, του τύπου ή του ιδιοκτήτη μιας διεργασίας (process), εφαρμόζονται περιορισμοί στην χρήση πόρων, σε όποια-ες διεργασία-ες ικανοποιούν τα κριτήρια αυτά. Μια διεργασία μπορεί να περιοριστεί ως προς τον χρόνο επεξεργαστή (CPU time) που θα έχει, το εύρος (bandwidth) που θα καταναλώσει, τον αριθμό των επεξεργαστών που μπορεί να τρέξει. Οι περιορισμοί μπορεί να ισχύουν και επιλεκτικά μόνο για κάποιες συγκεκριμένες ημερομηνίες.

2.2.2.8 Server Manager

Ο “Server Manager” είναι ένα καινούριο εργαλείο διαχείρισης για τα Windows Server 2008, βασισμένο σε ρόλους. Είναι ένας συνδυασμός των “Manage Your Server” και του “Security Configuration Wizard” που είχαμε στα Windows Server 2003. Ο “Server Manager” είναι μια βελτιωμένη έκδοση του “Configure my Server” που ξεκινάει προκαθορισμένα στα Windows Server 2003. Εν τούτοις ο “Server Manager” δεν αποτελεί μόνο ένα σημείο εκκίνησης για την ρύθμιση νέων ρόλων αλλά σημείο συγκέντρωσης όλων των λειτουργιών που οι χρήστες θα θελήσουν να διενεργήσουν στον Server, όπως το να ρυθμίσουν μια απομακρυσμένη μέθοδο deployment, το να προσθέσουν νέους ρόλους στον Server, κλπ. και προσφέρει μια συγκεντρωτική όψη της κατάστασης του κάθε ρόλου που εκτελείται στον Server, σε μορφή που θυμίζει portal.

2.2.2.9 Άλλα Χαρακτηριστικά

Ανάμεσα σε άλλα νέα ή βελτιωμένα χαρακτηριστικά περιλαμβάνονται τα:

Βελτιώσεις στο Core OS

- Πλήρως πολύ-τμηματοποιημένο λειτουργικό σύστημα
- Βελτιωμένη εφαρμογή patches εν λειτουργία (hot patching), που επιτρέπει σε όλα τα Patches που δεν αφορούν τον πυρήνα του λειτουργικού να εφαρμόζονται χωρίς την ανάγκη για επανεκκίνηση.

- Υποστήριξη για έναρξη λειτουργία από EFI-συμβατά firmware (Extensible firmware Interface-compliant firmware) σε x86-x64 συστήματα.
- Δυναμική Κατανομή του Hardware
- Υποστήριξη για εν λειτουργία προσθήκη ή αντικατάσταση επεξεργαστών και μνημών, εφόσον πάντα υπάρχει το κατάλληλο hardware.

Βελτιώσεις στο Active Directory

- Ένας καινούριος τρόπος λειτουργίας του Active Directory, ο “Read-Only Domain Controller”, ο οποίος έχει ομάδα στόχου τα παραρτήματα εταιριών όπου ένας domain-controller συνήθως βρίσκεται σε περιβάλλον χαμηλής φυσικής ασφάλειας. Ο RODC, κρατάει ένα μη εγγράψιμο αντίγραφο του Active Directory, και ανακατευθύνει όλες τις προσπάθειες εγγραφής σε έναν «κανονικό» Domain Controller. Αναπαράγει (replicates) όλους τους λογαριασμούς εκτός από τους ευαίσθητους. Τα διαπιστευτήρια (credentials) δεν κρατούνται στην μνήμη cache, ως αρχική ρύθμιση. Επιπλέον, μόνο ο εταίρος Server αναπαραγωγής του RODC χρειάζεται να τρέχει Windows Server 2008. Επίσης, οι τοπικοί διαχειριστές μπορούν να συνδεθούν με τον υπολογιστή για την εκτέλεση εργασιών συντήρησης χωρίς να απαιτούνται δικαιώματα διαχειριστή στον τομέα (domain).
- Το επανεκκίνησιμο Active Directory, επιτρέπει στους ADDS, να σταματούν και να επανεκκινούνται από την κονσόλα διαχείρισης (Management Console) ή από την γραμμή εντολών χωρίς να απαιτείται φυσική επανεκκίνηση ολόκληρου του domain controller. Αυτό ελαττώνει πολύ τον χρόνο downtime για τις offline λειτουργίες και ελαττώνει σημαντικά τις απαιτήσεις για συντήρηση του Domain Controller με την χρήση του Server Core. Το ADDS υλοποιείται ως ένα Domain Controller Service στα Windows Server 2008.

Βελτιώσεις σχετικές με τις Πολιτικές (Policy related improvements)

- Εμπεριέχονται όλες οι βελτιώσεις της πολιτικής ομάδας (Group Policy) από τα Windows Vista. Η κονσόλα διαχείρισης Group Policy Management Console (GPMC) είναι ενσωματωμένη. Τα αντικείμενα του Group Policy, έχουν δεικτοδοτηθεί (indexed) για γρήγορη αναζήτηση και μπορούν να σχολιαστούν.

- Δικτύωση βασισμένη σε πολιτικές, με την χρήση του Network Access Protection, για βελτιωμένη διαχείριση παραρτημάτων και αυξημένη συνεργασία τελικών χρηστών. Οι πολιτικές μπορούν να δημιουργηθούν έτσι ώστε να διασφαλίσουν καλύτερη ποιότητα υπηρεσίας για συγκεκριμένες εφαρμογές ή υπηρεσίες που απαιτούν προτεραιότητα στο διαθέσιμο εύρος του δικτύου μεταξύ του πελάτη (client) και του εξυπηρετητή (server).
- Πολλαπλές ρυθμίσεις κωδικού πρόσβασης σε έναν ενιαίο τομέα (domain) – δυνατότητα για εφαρμογή διαφορετικών πολιτικών κωδικού πρόσβασης για τους λογαριασμούς των διαχειριστών με βάση τις "ομάδες" και τους "χρήστες", αντί για ένα ενιαίο σύνολο ρυθμίσεων κωδικού πρόσβασης σε ολόκληρο τον τομέα.

Βελτιώσεις στην Διαχείριση Δίσκων και στην αποθήκευση αρχείων

- Προστέθηκε η ικανότητα να αλλάζει δυναμικά το μέγεθος των διαμερισμάτων (partitions) των σκληρών δίσκων, χωρίς να σταματάει η λειτουργία του server, ακόμα και στο κύριο διαμέρισμα του συστήματος. Αυτό ισχύει βεβαίως μόνο σε spanned volumes και όχι σε striped.
- Δημιουργία αντιγράφων ασφαλείας σε επίπεδο μπλοκ δεδομένων, βασισμένο στην τεχνολογία “Shadow Copy”, με την υποστήριξη οπτικών μέσων, δικτυακά διαμοιρασμένους πόρους, ακόμα και στο περιβάλλον του “Windows Recovery Environment” ή αλλιώς WinRE.
- Επεκτάσεις του DFS (Distributed File System) όπως SYSVOL σε DFS-R, Read-only Replication Member. Υπάρχει ακόμα υποστήριξη για domain-based DFS namespaces τα οποία υπερβαίνουν τις προηγούμενες συστάσεις μεγέθους των 5000 φακέλων με στόχους εντός του namespace.
- Αρκετές βελτιώσεις στον τομέα του Failover Clustering προκειμένου να έχουμε High-availability clusters.
- Ο Internet Storage Naming Server (iSNS) δίνει τη δυνατότητα κεντρικής εγγραφής και διαγραφής, καθώς και ερωτημάτων για iSCSI σκληρούς δίσκους.

Βελτιώσεις Πρωτοκόλλων και Κρυπτογραφίας

- Υποστήριξη για 128- και 256-bit κωδικοποίησης AES, για το πρωτόκολλο ελέγχου ταυτότητας Kerberos.

- Νέο API κρυπτογραφίας (CNG) το οποίο υποστηρίζει κρυπτογραφία ελλειπτικών καμπυλών και βελτιωμένη διαχείριση πιστοποιητικών.
- Το Secure Socket Tunneling που αποτελεί ένα νέο ιδιόκτητο πρωτόκολλο της Microsoft για υλοποίηση VPN.
- Το AuthIP, που είναι μια ιδιόκτητη επέκταση της Microsoft, του IKE cryptographic protocol, που χρησιμοποιείται στα δίκτυα IPsec VPN.
- Το πρωτόκολλο Server Message Block 2.0 μέσα στην καινούρια στοίβα TCP/IP παρέχει μια σειρά από βελτιώσεις στην επικοινωνία, συμπεριλαμβανομένης της μεγαλύτερης απόδοσης στις συνδέσεις με τα κοινόχρηστα αρχεία πάνω από συνδέσεις υψηλής καθυστέρησης απόκρισης καθώς και μεγαλύτερη ασφάλεια μέσω της χρήσης της αμοιβαίας ταυτοποίησης και υπογραφής μηνυμάτων.

Βελτιώσεις λόγω των επεκτάσεων από την πλευρά του πελάτη (Windows Vista)

- Αναζητώντας σε servers με λειτουργικό Windows Server 2008 από υπολογιστές που χρησιμοποιούν Windows Vista, έχουμε ανάθεση του ερωτήματος στο διακομιστή (server), ο οποίος χρησιμοποιεί την τεχνολογία του Windows Search για την αναζήτηση και τη μεταφορά των αποτελεσμάτων πίσω στον πελάτη.
- Σε ένα δικτυακό περιβάλλον με ένα διακομιστή εκτύπωσης που τρέχει Windows Vista, οι πελάτες μπορούν να επεξεργαστούν τις εκτυπώσεις τους σε τοπικό επίπεδο και να τις καταστήσουν κατάλληλες για εκτύπωση, πριν την αποστολή τους στους εξυπηρετητές εκτύπωσης (print servers) ώστε να μειώσουν το φορτίο στον server και να αυξηθεί η διαθεσιμότητά του.
- Η διαβίβαση συμβάντων, συγκεντρώνει και προωθεί τα αρχεία καταγραφής (logs) των εγγεγραμμένων Windows Vista υπολογιστών πελάτη (client), σε κεντρική κονσόλα διαχείρισης. Η διαβίβαση των συμβάντων (event forwarding) μπορεί να επιτραπεί στους εγγεγραμμένους χρήστες από τον κεντρικό εξυπηρετητή απευθείας από την κεντρική κονσόλα διαχείρισης συμβάντων.

Διάφορες Βελτιώσεις

- Τα Windows Deployment Services αντικαθιστούν τα Automated Deployment Services (ADS) και Remote Installation Services (RIS). Τα Windows Deployment Services (WDS) υποστηρίζουν βελτιωμένη

δυνατότητα πολλαπλής διανομής κατά το deployment λειτουργικών συστημάτων μέσω εικόνων (images).

- Έχουμε τον νέο IIS-7 (Internet Information Services 7) με αυξημένη ασφάλεια, deployment με χρήση του Robocopy, βελτιωμένα διαγνωστικά εργαλεία, και δυνατότητες ανάθεσης τμημάτων της διαχείρισης.
- Υπάρχει η Windows Internal Database, μια παραλλαγή του SQL Server Express 2005, η οποία χρησιμεύει ως κοινός αποθηκευτικός χώρος για διάφορα άλλα στοιχεία, όπως το Windows System Resource Manager, τα Windows SharePoint Services και το Windows Server Update Services (WSUS). Δεν προορίζεται για χρήση από εφαρμογές τρίτων.
- Ένα προαιρετικό στοιχείο παρέχει το γραφικό περιβάλλον εργασίας χρήστη (GUI) Windows Aero, όπως στα Windows Vista, τόσο για τους τοπικούς χρήστες, καθώς και σε απομακρυσμένους χρήστες μέσω της σύνδεσης απομακρυσμένης επιφάνειας εργασίας (Remote Desktop).

2.2.2.10 Χαρακτηριστικά που απομακρύνθηκαν

- Αφαιρέθηκε από την υπηρεσία δρομολόγησης και απομακρυσμένης πρόσβασης (Routing and Remote Access service) το πρωτόκολλο δρομολόγησης Open Shortest Path First (OSPF).
- Έχουν αφαιρεθεί υπηρεσίες για υπολογιστές Macintosh, που παρείχαν κοινή χρήση αρχείων και εκτυπωτών μέσω του ξεπερασμένου πρωτοκόλλου AppleTalk. Υπηρεσίες για Macintosh καταργήθηκαν και στα Windows XP αλλά ήταν διαθέσιμες στον Windows Server 2003.
- Το παλαιό NTBackup αντικαταστάθηκε από τον Windows Server Backup, το οποίο δεν υποστηρίζει πλέον μονάδες μαγνητοταινίας. Ως αποτέλεσμα της απομάκρυνσης του NTBackup, ο Exchange Server 2007 δεν έχει διαθέσιμες όλες τις λειτουργίες δημιουργίας αντιγράφων ασφαλείας. Ωστόσο ο Exchange Server 2007 SP2 προσθέτει πίσω ένα πρόσθετο (plugin) για το Windows Server Backup και αποκαθιστά μερική από την χαμένη λειτουργικότητα. Οι εκδόσεις Windows Small Business Server και Windows Essential Business Server περιλαμβάνουν το πρόσθετο αυτό για το Exchange backup.
- Η υπηρεσία POP3 έχει αφαιρεθεί από το Internet Information Services 7.0. Η υπηρεσία SMTP (Simple Mail Transfer Protocol) δεν υπάρχει διαθέσιμη

ως ρόλος του εξυπηρετητή στον IIS 7.0. Είναι ένα χαρακτηριστικό του εξυπηρετητή που διαχειρίζεται μέσω του IIS 6.0.

- Το NNTP (Network News Transfer Protocol) δεν αποτελεί πλέον τμήμα του Internet Information Services 7.0.
- Το πρόσθετο “Post Office Protocol component” ξεπεράστηκε και δεν διατίθεται ως τμήμα του λειτουργικού συστήματος Windows.

2.2.3 Εκδόσεις

Οι περισσότερες εκδόσεις του Windows Server 2008 είναι διαθέσιμες σε x86-64 (64-bit) και x86 (32-bit) εκδόσεις. Τα Windows Server 2008 για συστήματα βασισμένα σε Itanium υποστηρίζουν IA-64 επεξεργαστές. Η έκδοση IA-64 είναι βελτιστοποιημένη για σενάρια μεγάλου φόρτου εργασίας, όπως είναι οι διακομιστές βάσεων δεδομένων (database servers) και εφαρμογές ειδικών απαιτήσεων μεγάλων οργανισμών ή εταιριών (Line of Business - LOB applications).

Ως εκ τούτου, δεν είναι βελτιστοποιημένη για χρήση ως διακομιστής αρχείων ή διακομιστής πολυμέσων. Η Microsoft ανακοίνωσε ότι τα Windows Server 2008 είναι το τελευταίο 32-bit λειτουργικό σύστημα Windows για Server. Τα Windows Server 2008 είναι διαθέσιμα στις εκδόσεις που αναφέρονται παρακάτω, κατά αντιστοιχία με τα Windows Server 2003.

- Windows Server 2008 Standard (x86 and x86-64)
- Windows Server 2008 Enterprise (x86 and x86-64)
- Windows Server 2008 Datacenter (x86 and x86-64)
- Windows HPC Server 2008 (Codename "Socrates") (αντικατέστησε το Windows Compute Cluster Server 2003)
- Windows Web Server 2008 (x86 και x86-64)
- Windows Storage Server 2008 (Codename "Magni") (x86 και x86-64)
- Windows Small Business Server 2008 (Codename "Cougar") (x86-64) για μικρές επιχειρήσεις
- Windows Essential Business Server 2008 (Codename "Centro") (x86-64) για μεσαίου μεγέθους επιχειρήσεις
- Windows Server 2008 για συστήματα βασισμένα σε επεξεργαστές Itanium
- Windows Server 2008 Foundation (Codename "Lima")

Η έκδοση “Server Core” είναι διαθέσιμη σε εκδόσεις Web, Standard, Enterprise και Datacenter. Δεν υπάρχει διαθέσιμη σε έκδοση για Itanium. Η έκδοση Server Core

είναι απλά μια εναλλακτική επιλογή εγκατάστασης που υποστηρίζεται από κάποιες από τις εκδόσεις και όχι μια ξεχωριστή έκδοση από μόνη της. Κάθε αρχιτεκτονική έχει ένα ξεχωριστό DVD εγκατάστασης. Τα Windows Server 2008 Standard Edition είναι διαθέσιμα στους σπουδαστές δωρεάν μέσω του προγράμματος DreamSpark της Microsoft.

2.2.4 Service Packs

Η Microsoft κατά καιρούς εκδίδει πακέτα επισκευών – service packs για τα λειτουργικά συστήματα Windows, ώστε να διορθώσει σφάλματα αλλά και να προσθέσει νέα χαρακτηριστικά.

2.2.4.1 Service Pack 2

Επειδή τα Windows Server 2008 είναι βασισμένα στον πυρήνα Windows NT 6.0 Service Pack 1, η έκδοση RTM θεωρείται να είναι το Service Pack 1. Κατά συνέπεια το πρώτο Service Pack καλείται Service Pack 2. Ανακοινώθηκε στις 24 Οκτωβρίου 2008, και περιέχει τις ίδιες αλλαγές και βελτιώσεις όπως και το Windows Vista Service Pack 2, καθώς και την τελική έκδοση του Hyper-V 1.0 και περίπου 10% ελάττωση στην κατανάλωση ισχύος.

Το πρώτο beta SP2, κυκλοφόρησε τον Οκτώβριο του 2008, ενώ η πρώτη έκδοση beta διαθέσιμη στο κοινό κυκλοφόρησε τον Δεκέμβριο του 2008 και μια έκδοση Release Candidate (RC) δόθηκε στους testers τον Ιανουάριο του 2009. Τα Windows Vista και τα Windows Server 2008, μοιράζονται ένα κοινό εκτελέσιμο αρχείο με το Service Pack, αντικατοπτρίζοντας το γεγονός ότι οι βάσεις του κώδικά τους ενοποιήθηκαν με την έκδοση του Server 2008. Στις 26 Μαΐου του 2009, το Service Pack 2 δόθηκε σε επίσημη κυκλοφορία. Τώρα πλέον γίνεται διαθέσιμο και με το Windows Update.

2.2.5 Windows Server 2008 R2

Μια δεύτερη έκδοση, τα Windows Server 2008 R2, εκδόθηκαν στις 22 Οκτωβρίου του 2009. Η έκδοση “retail” ήταν διαθέσιμη στις 14 Σεπτεμβρίου του 2009. Τα Windows Server 2008 R2, έφτασαν στην έκδοση RTM στις 22 Ιουλίου του 2009. Όπως και τα Windows 7, είναι βασισμένα στα Windows NT 6.1. Νέα χαρακτηριστικά, όπως καινούρια χαρακτηριστικά εικονικοποίησης (virtualization), καινούρια χαρακτηριστικά στο Active Directory, IIS 7.5 και υποστήριξη μέχρι και 256 επεξεργαστές. Η υποστήριξη για επεξεργαστές των 32bit (x86) έχει αφαιρεθεί. Στις 22 Ιουλίου του 2009, η Microsoft επισήμως έδωσε και τα Windows Server 2008 R2 και τα Windows 7 στην παραγωγή. Τα 2008 R2 Server, έγιναν διαθέσιμα για

κατέβασμα από τις 19 Αυγούστου του 2009 και για αγορά τύπου “retail” από τις 22 Οκτωβρίου του 2009.

2.3 Διαφορετικές εκδόσεις του προϊόντος και απαιτήσεις υλικού ανά έκδοση

2.3.1 Απαιτήσεις Συστήματος

Οι απαιτήσεις του συστήματος για τα Windows Server 2008 καταγράφονται στον ακόλουθο πίνακα:

	Ελάχιστες απαιτήσεις για Windows Server 2008	Συνιστώμενος εξοπλισμός για Windows Server 2008	Ελάχιστες απαιτήσεις για Windows Server 2008 R2	Συνιστώμενος εξοπλισμός για Windows Server 2008 R2
Επεξεργαστής	1 GHz (x86) ή 1.4 GHz (x64) ή Intel Itanium2	2 GHz ή γρηγορότερος	1.4 GHz (x64 processor) ή Intel Itanium 2	
Μνήμη	512 MB RAM (με περιορισμό στην απόδοση και σε κάποια χαρακτηριστικά)	2 GB RAM ή περισσότερη Μέγιστη (σε 32-bit συστήματα): 4 GB RAM (Standard) ή 64 GB RAM (Enterprise, Datacenter) Μέγιστη (σε 64-bit συστήματα): 8 GB (Foundation) ή 32 GB RAM (Standard) ή 2 TB RAM (Enterprise, Datacenter και Itanium-based Systems)	512 MB RAM	Μέγιστη: 8 GB (Foundation) ή 32 GB (Standard) ή 2 TB (Enterprise, Datacenter, και Itanium-Based Systems)

Κάρτα Γραφικών και οθόνη	Super VGA (800 x 600)	Super VGA (800 x 600) ή υψηλότερη ανάλυση	Super VGA (800 x 600)	Super VGA (800 x 600) ή υψηλότερη ανάλυση
Ελεύθερος χώρος στο σκληρό δίσκο	10 GB ή Ελάχιστος (32-bit systems): 20 GB ή μεγαλύτερο ς Ελάχιστος (64-bit systems): 32 GB ή περισσότερ ο Foundation: 10 GB ή περισσότερ ος. Υπολογιστέ ς με περισσότερ ο από 16 GB μνήμης RAM απαιτούν περισσότερ ο χώρο στο σκληρό δίσκο για λειτουργίες paging, αδρανοποίη σης (hibernation) , και dump files.	40 GB ή περισσότερο	32 GB ή μεγαλύτερος Foundation: 10 GB ή περισσότερος Υπολογιστές με περισσότερο από 16 GB μνήμης RAM απαιτούν περισσότερο χώρο στο σκληρό δίσκο για λειτουργίες paging, αδρανοποίησης (hibernation), και dump files.	
Οπτικά Μέσα	DVD-ROM			
Συσκευές	Οθόνη Super VGA (800 x 600) ή υψηλότερης ανάλυσης, πληκτρολόγιο και ποντίκι			

2.3.2 Αδειοδότηση – Ενδεικτικές Τιμές

Ακολουθεί η εικόνα 2.1. που περιλαμβάνει συγκριτικό πίνακα με εκδόσεις και ενδεικτικές τιμές. Επιμένουμε στο ενδεικτικές τιμές διότι τελικά δίδονται προσφορές ανάλογες με το μέγεθος του πελάτη, τη χρήση και τους προμηθευτές.

Edition	Description	Price	Max. Ram for 32-bit	Max. Ram for 64-bit	When to use
Standard	Does almost everything	\$999 w/5 CAL's	4 GB	32GB	Small to medium environments, File and Print Servers, less intensive applications
Enterprise	Does it all	\$3999 w/25 CAL's	64GB	2TB	Large environments, clustering
Datacenter	All that and a bag of chips	\$2999 PER PROCESSOR	64GB	2TB	For massive environments – includes unlimited virtualization licenses!
Web Server	Just a Web Server (IIS 7.0)	\$469	4GB	32GB	You don't need me to explain this. Really, you don't.
Itanium	For high-end web/application servers	\$2,999	N/A	2TB	When you need to run super powered databases or high end applications. Only has Application Server Role.

Εικ.2.1. – Πίνακας με ενδεικτικές τιμές αδειών

ΕΓΚΑΤΑΣΤΑΣΗ WINDOWS SERVER 2008

3.1 Εισαγωγή

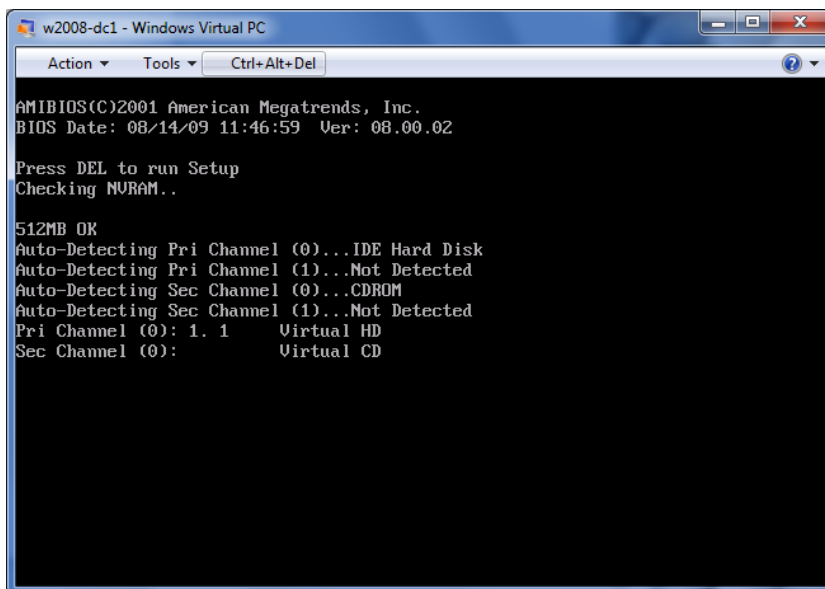
Οι επιθυμητές γνώσεις και δεξιότητες που θα αποκτήσουν οι επιμορφωμένοι στην ενότητα «Εγκατάσταση Windows Server 2008» θα τους καταστήσουν ικανούς να:

- Εγκαθιστούν το λειτουργικό σύστημα Server 2008 λαμβάνοντας υπόψη τις απαιτήσεις υλικού.
- Καθορίσουν τους ρόλους ενός Windows Server 2008 και να τους συνδυάζουν σε διαφορετικά σενάρια ανάπτυξης.

3.2 Εγκατάσταση Windows Server 2008

3.2.1 Εγκατάσταση και ρυθμίσεις

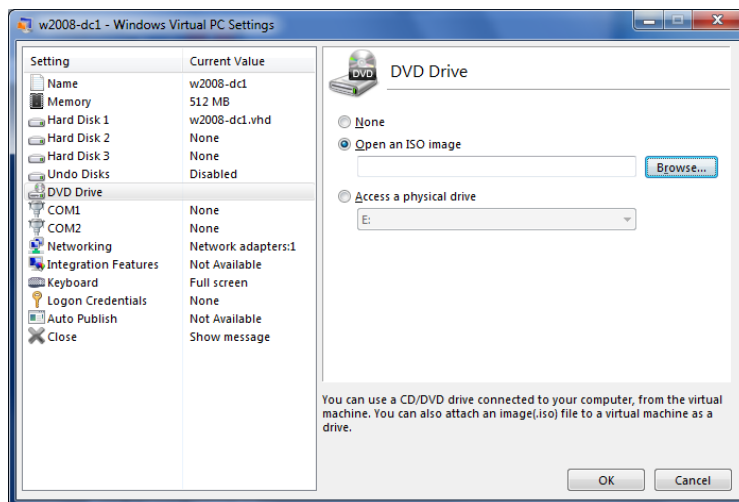
Προκειμένου να εγκαταστήσουμε τα Windows Server 2008, ξεκινάμε το μηχάνημα με φορτωμένο το DVD της εγκατάστασης στην μονάδα οπτικής ανάγνωσης (Εικ.3.1). Σε περίπτωση φυσικού μηχανήματος (server) τότε υποχρεωτικά ξεκινάμε την εγκατάσταση από τα διαθέσιμα DVD του κατασκευαστή, τα οποία φορτώνουν έναν οδηγό εγκατάστασης συνήθως βασισμένο σε κάποιο Linux, ο οποίος και πραγματοποιεί δομημένα όλες τις βασικές ρυθμίσεις που χρειάζεται ο Server, αλλά κυρίως φορτώνει στην μνήμη όλους τους οδηγούς υλικού που απαιτούνται προκειμένου να γίνει η εγκατάσταση και να μην παρουσιαστούν προβλήματα. Σε περίπτωση που δεν έχουμε διαθέσιμο το DVD αυτό το αναζητούμε στο διαδίκτυο. Αν και πάλι δεν το βρούμε τότε προχωράμε στην διαδικασία όπως ακριβώς περιγράφεται ακολούθως.



Εικ.3.1

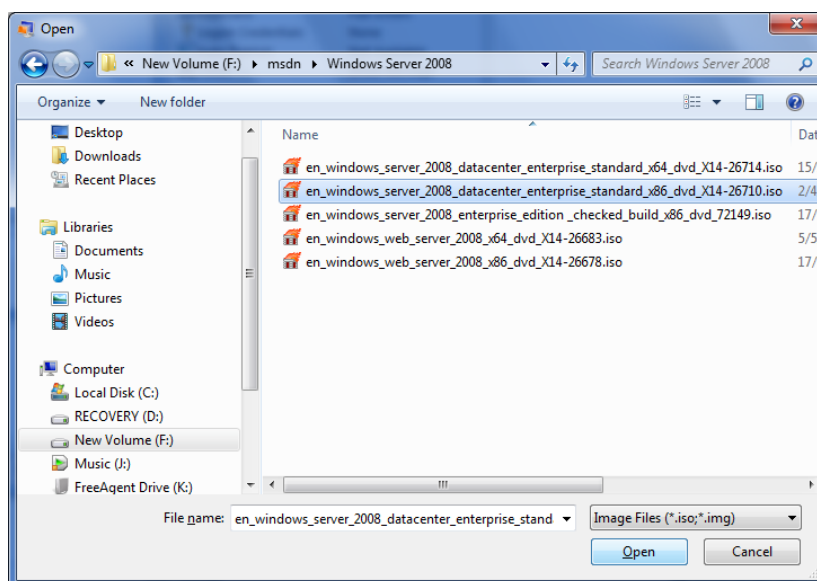
Στην περίπτωση του Virtual PC πρέπει να κάνουμε Mount το μέρος στον δίσκο που έχουμε την εικόνα του φυσικού μέσου εγκατάστασης, συνήθως σε ένα αρχείο της μορφής ISO, ή σε κάποιο φυσικό οπτικό μέσο και να κάνουμε τις απαραίτητες ρυθμίσεις στην εικονική μηχανή.

Εδώ πατώντας “Browse” επιλέγουμε να δώσουμε το path που έχουμε το ISO με τα αρχεία της εγκατάστασης. Εναλλακτικά πατώντας “Access a physical drive” δίνουμε πρόσβαση στην εικονική μηχανή σε κάποιο φυσικό οπτικό μέσο. (Εικ.3.2)



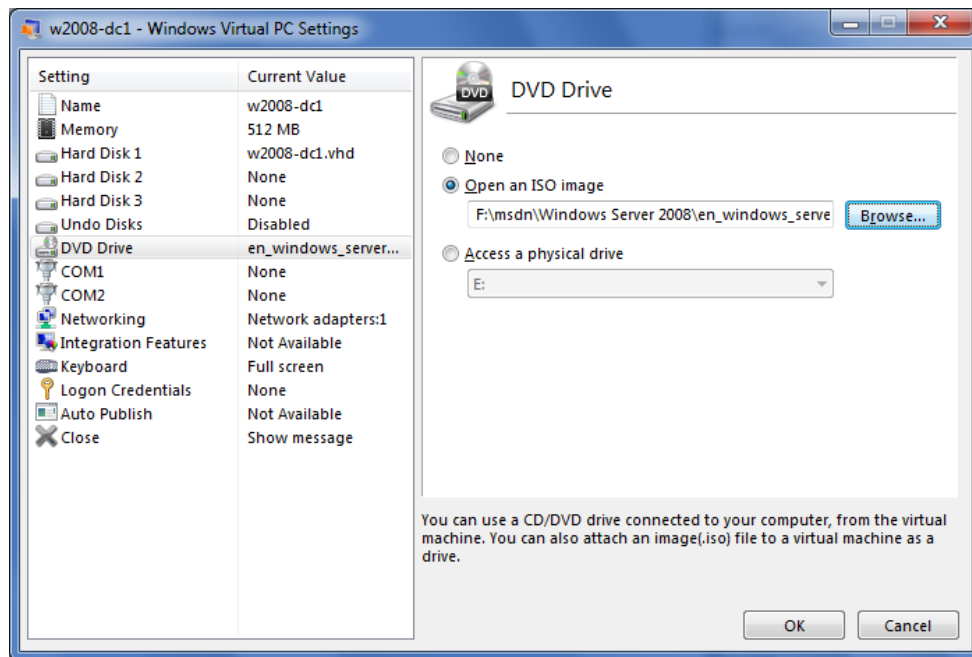
Εικ.3.2

Εμείς εδώ επιλέγουμε από το Path την εικόνα που ανταποκρίνεται στις εγκαταστάσεις που θα κάνουμε για το εργαστήριο. Έτσι διαλέγουμε π.χ. την εικόνα της εγκατάστασης της έκδοσης 2008 datacenter enterprise (Εικ.3.3), ή όποια άλλη επιθυμούμε.



Εικ.3.3

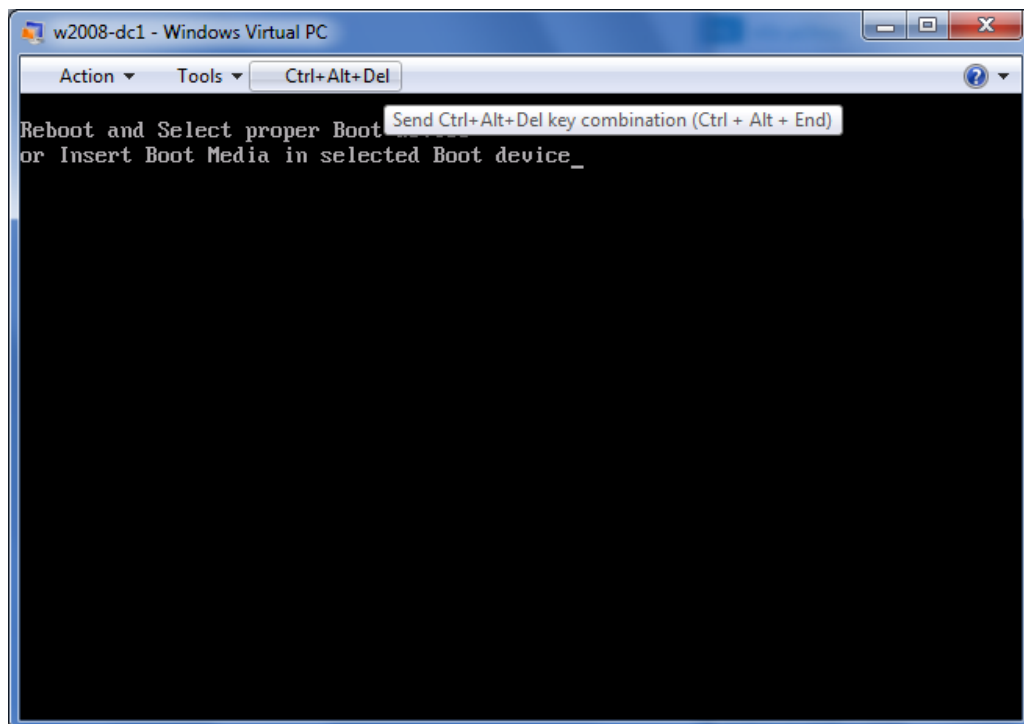
Και πατώντας “ok” ολοκληρώνουμε την επιλογή μας (Εικ.3.4).



Εικ.3.4

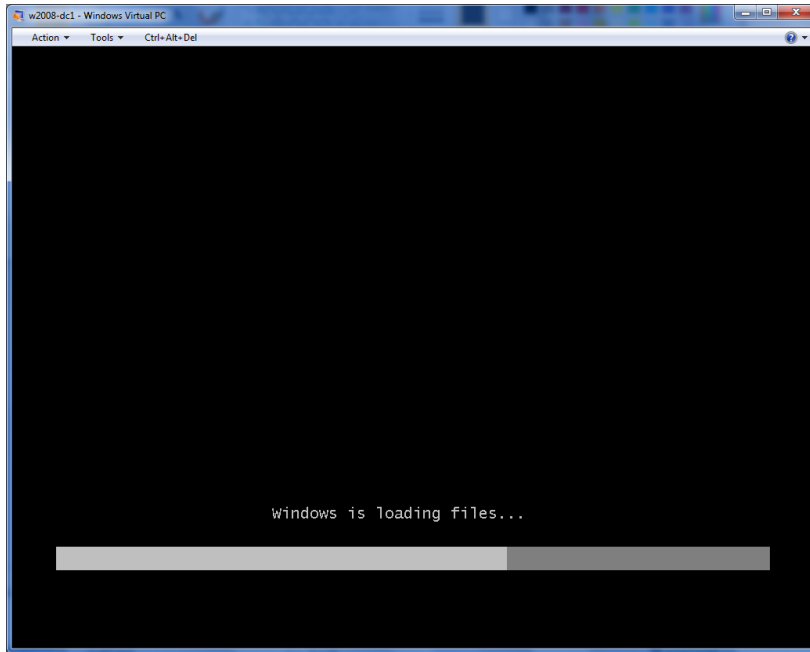
Σε περίπτωση που δεν έχουμε ήδη βάλει από την αρχή την εικόνα τότε θα πρέπει να κάνουμε ένα “reset” πατώντας τα πλήκτρα “Ctrl+Alt+Del” στην εικονική μηχανή.

Αυτό γίνεται πατώντας το κατάλληλο κουμπί όπως φαίνεται στην Εικ.3.5.



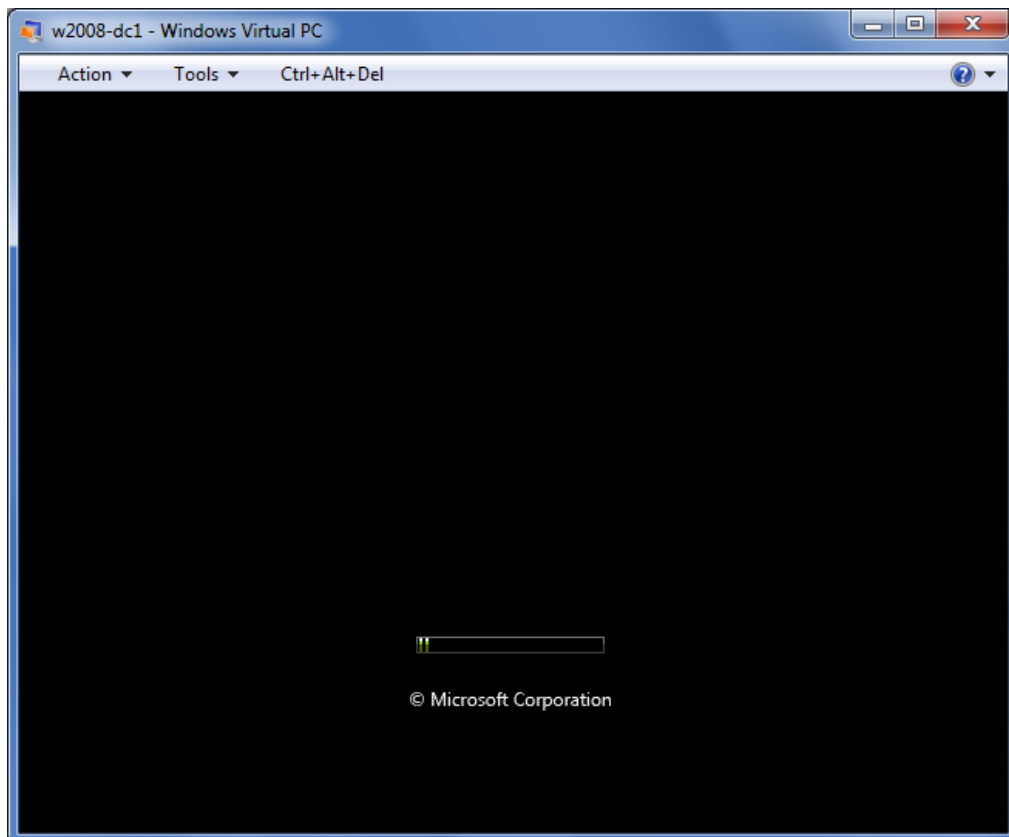
Εικ.3.5

Το σύστημα κάνει reset και ξεκινάει πάλι από την αρχή. Αυτή τη φορά βρίσκει το dvd με τα αρχεία που χρειάζεται και η εγκατάσταση των Windows ξεκινάει.



Εικ..3.6

Τα Windows φορτώνουν το νέο εξ ολοκλήρου γραφικό περιβάλλον εγκατάστασης



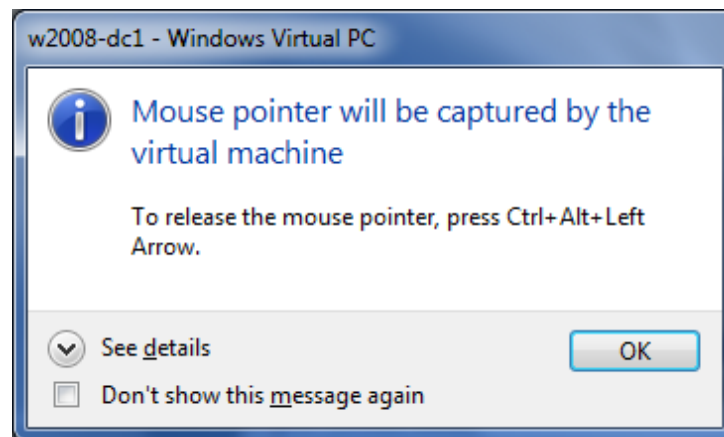
Εικ..3.7

Η πρώτη επιλογή είναι η γλώσσα του λειτουργικού και οι ρυθμίσεις της περιοχής για την ώρα και τους αριθμούς, καθώς και για το πληκτρολόγιο.



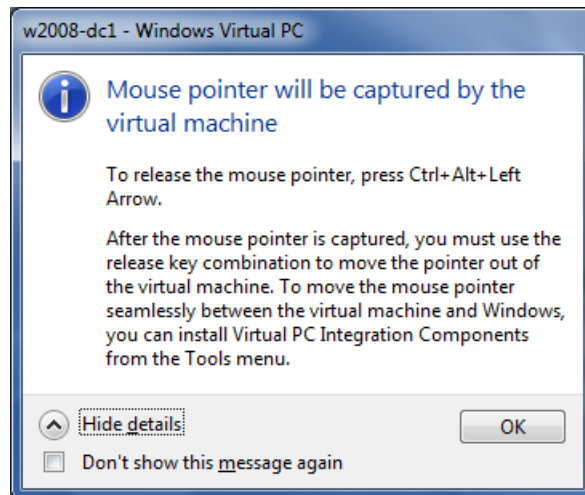
Εικ.3.8

Εδώ με το που πάμε να χρησιμοποιήσουμε το ποντίκι για να κάνουμε τις επιλογές στην εικονική μηχανή εμφανίζεται το ακόλουθο μήνυμα Εικ.3.9, το οποίο μας ενημερώνει ότι το mouse θα δεσμευτεί για χρήση εντός virtual-pc και για να αποδεσμευτεί θα πρέπει να πατήσουμε το “Ctrl + Alt + Left Arrow” ώστε να επανέλθει για χρήση στον υπολογιστή μας.



Εικ.3.9

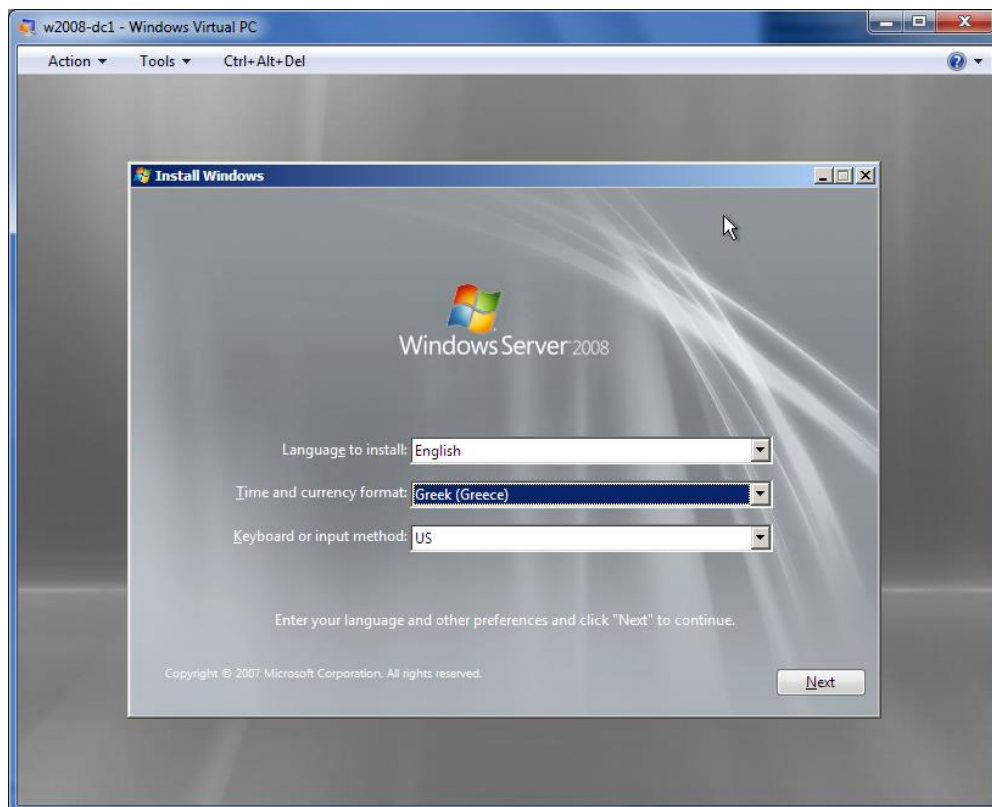
Πατώντας για λεπτομέρειες στο “See details” παίρνουμε περισσότερες λεπτομέρειες για την χρήση του Mouse καθώς και την συμβουλή για εγκατάσταση του Virtual PC Integration Components το οποίο μας επιτρέπει να μετακινούμε ελεύθερα το mouse αλλά και αρχεία μεταξύ του PC μας και του virtual PC βλέποντάς το ως άλλο παράθυρο ανοικτό χωρίς να έχουμε δέσμευση του Mouse με κάποιον τρόπο (Εικ.3.10)



Εικ.3.10

Καλό είναι μετά την ολοκλήρωση της εγκατάστασης, να εγκαταστήσουμε τα Virtual PC Integration Components, έτσι ώστε να μπορούμε να εκτελούμε εύκολα λειτουργίες αντιγραφής και επικόλλησης από το PC στο εικονικό και να μην δεσμεύεται το Mouse, αλλά να συμπεριφέρεται το Virtual PC σαν ένα απλό παράθυρο Windows.

Στη συνέχεια επιλέγουμε στην μεσαία επιλογή “Greek(Greece)” όπως στην ακόλουθη εικόνα (Εικ.3.11) και πατάμε next



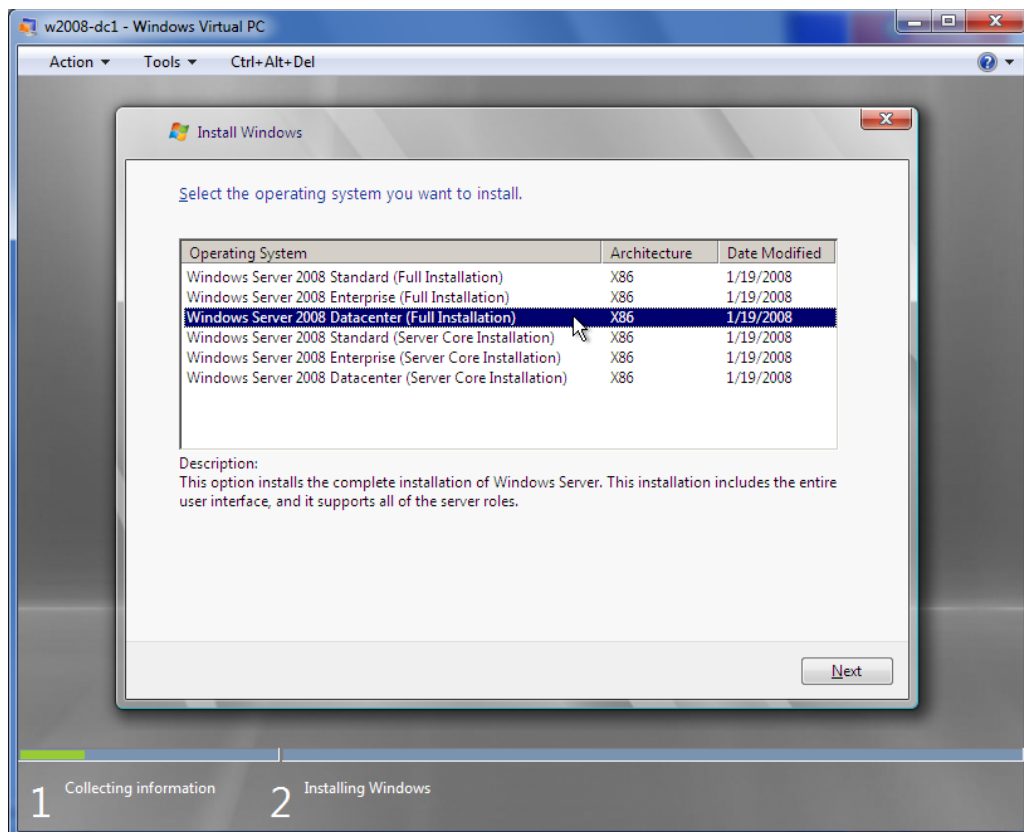
Εικ.3.11

Πατώντας το πλήκτρο “Install now” προχωράμε στην διαδικασία της εγκατάστασης.



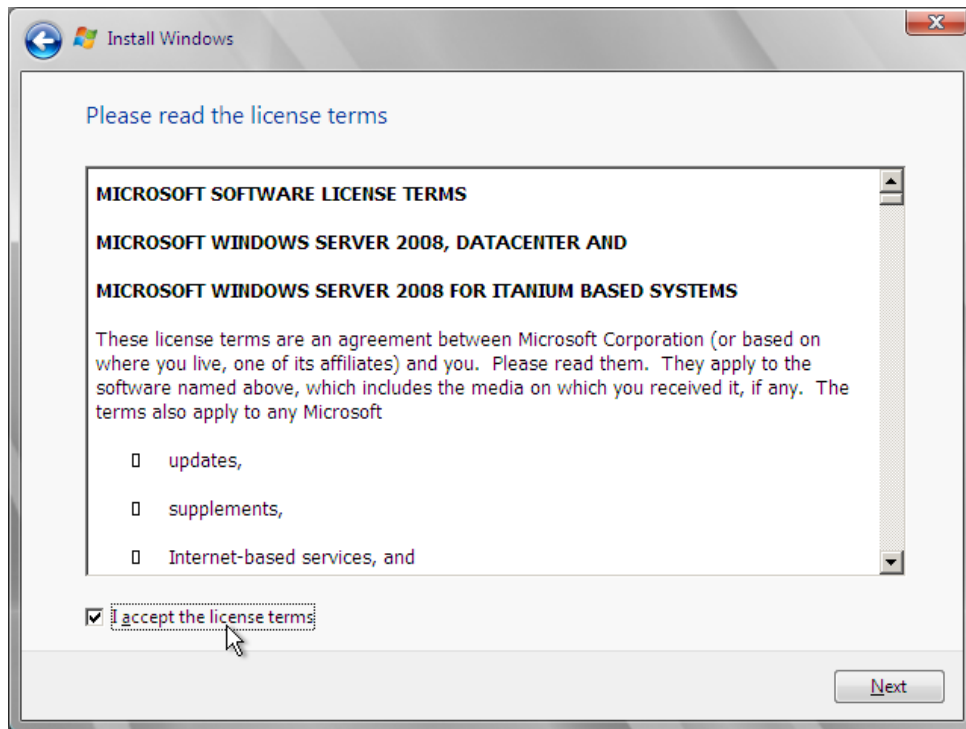
Εικ.3.12

Εδώ επιλέγουμε μια από τις διαθέσιμες εκδόσεις λειτουργικού, και συγκεκριμένα την “Windows Server 2008 Datacenter (Full Installation)” όπως στην Εικ.3.13.



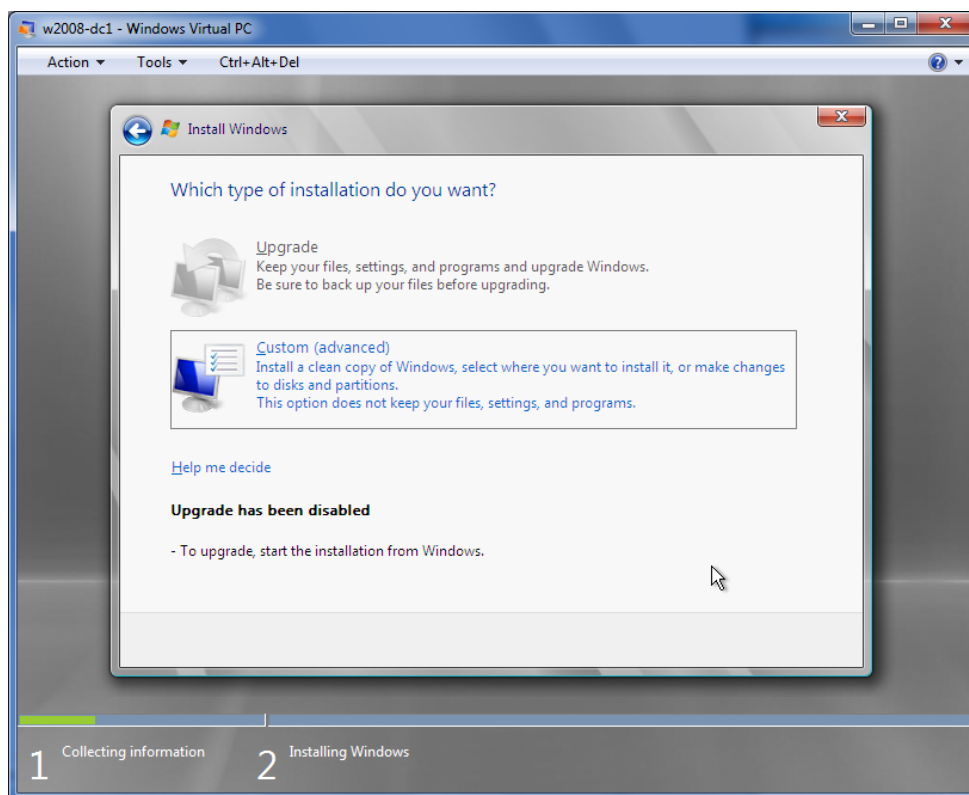
Εικ.3.13

Κάνουμε υποχρεωτικά αποδοχή των όρων χρήσης Εικ.3.14.



Εικ.3.14

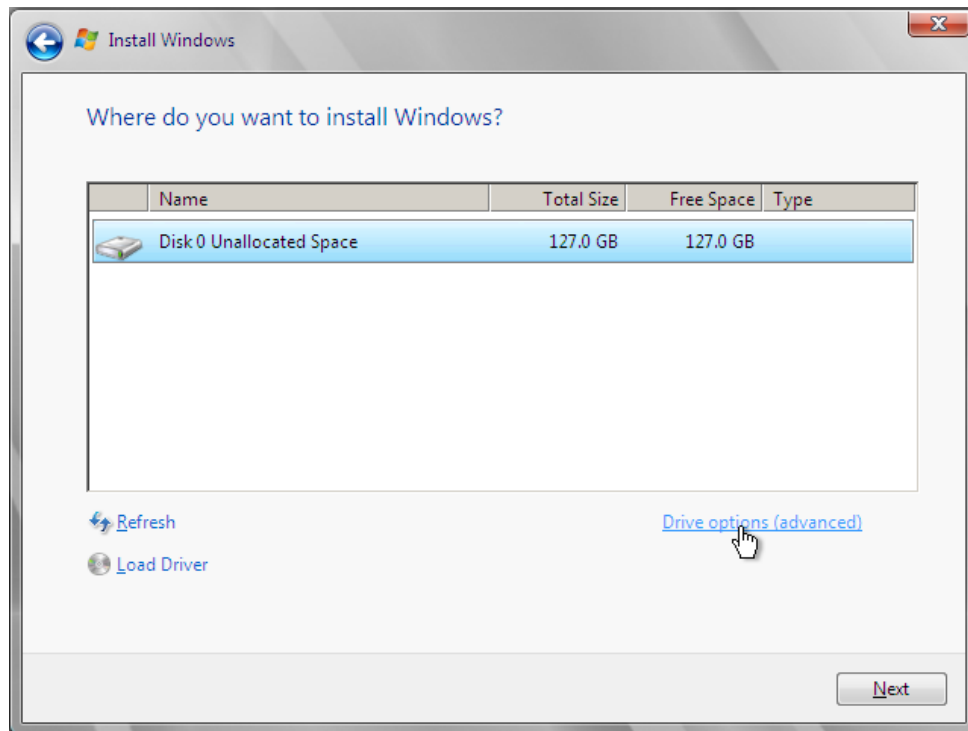
Για νέα εγκατάσταση σε «καινούριο» υπολογιστή όπως στην περίπτωση μας επιλέγουμε το Custom (advanced) όπως στην Εικ.3.15.



Εικ.3.15

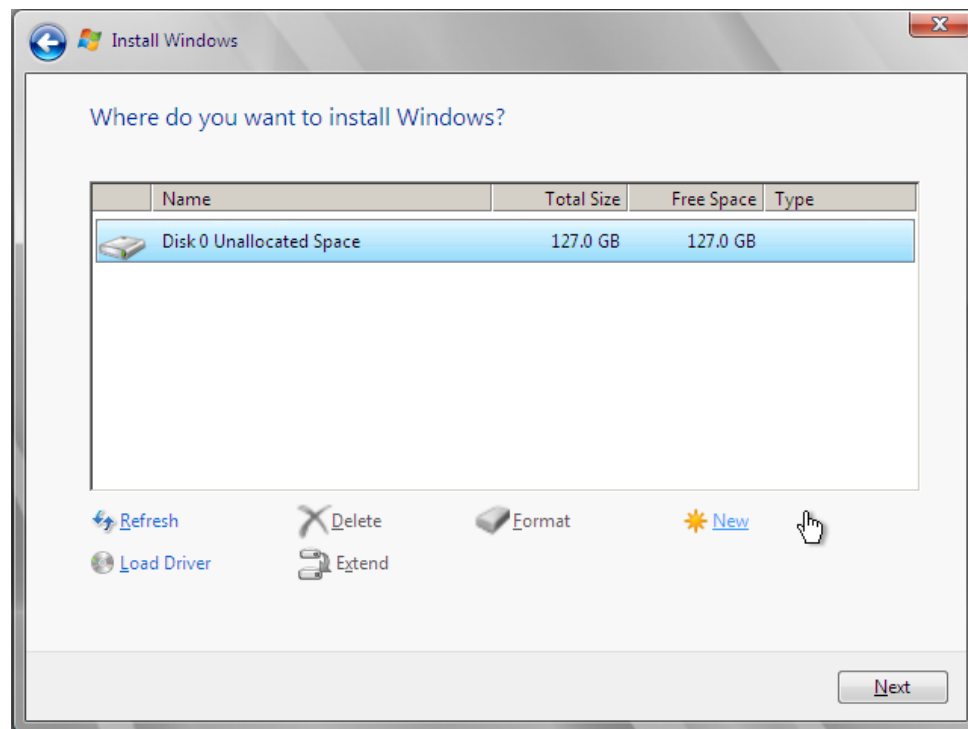
Επιλέγουμε το διαμέρισμα του δίσκου που θα γίνει η εγκατάσταση, και από το “Drive

options” μπορούμε να κάνουμε κάποιες πιο προχωρημένες λειτουργίες αν επιθυμούμε κάτι τέτοιο Εικ.3.16.



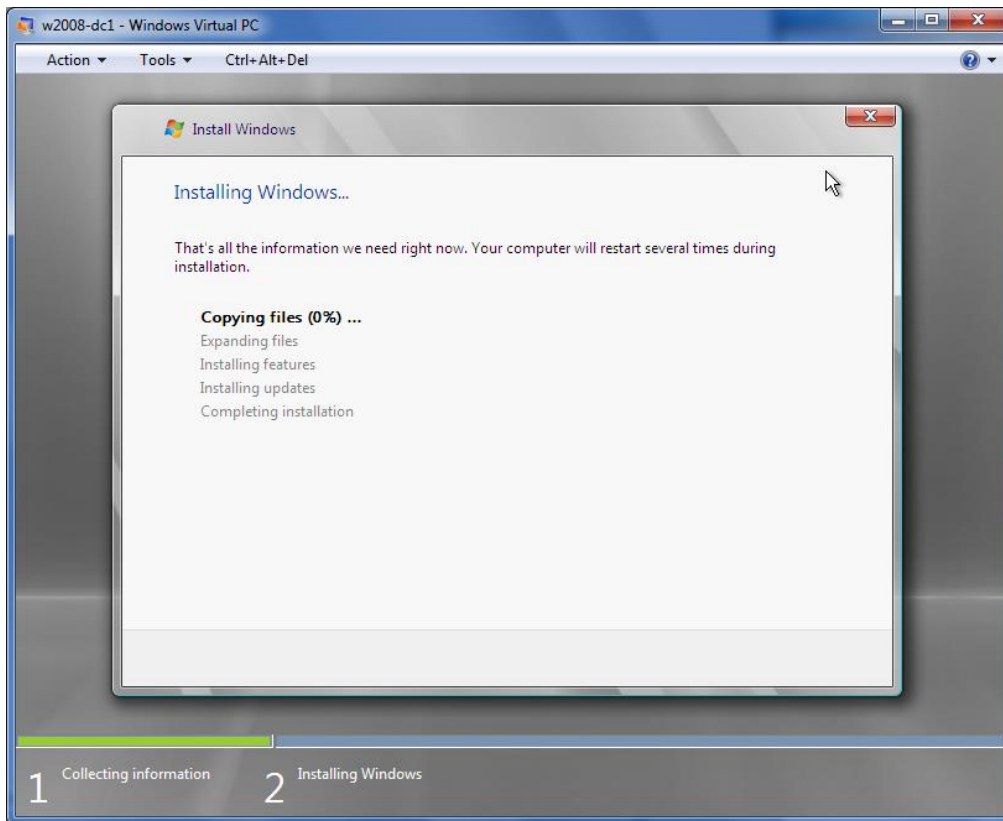
Εικ..3.16

Πατάμε στην επιλογή “New” (Εικ.3.17) και αφήνουμε τα Windows να προχωρήσουν στην εγκατάσταση μέχρι την ολοκλήρωση της διαδικασίας.



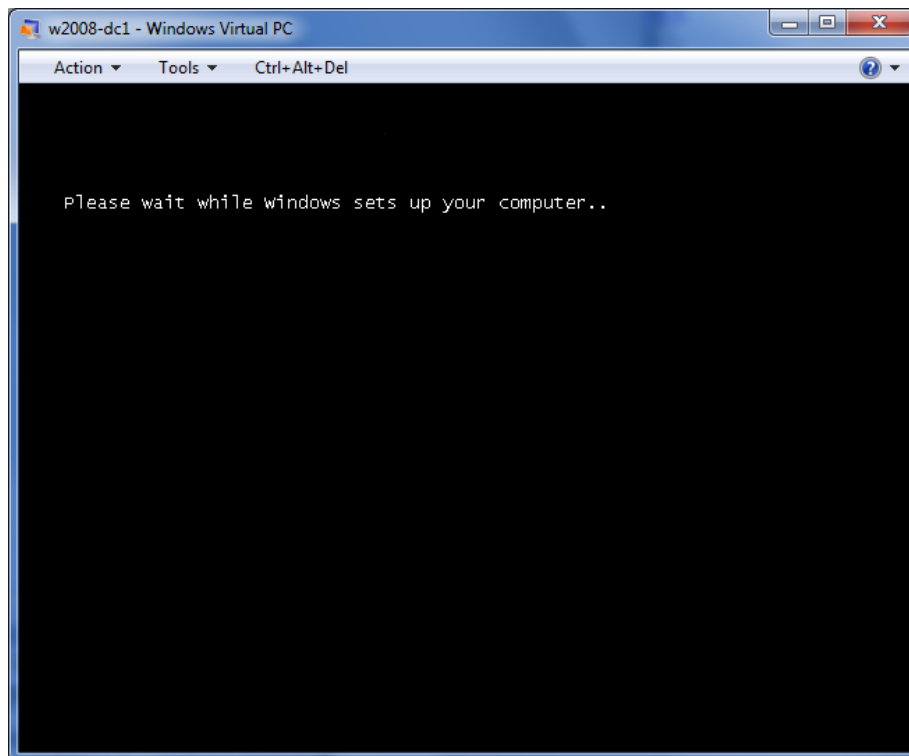
Εικ..3.17

Στη συνέχεια παρακολουθούμε την πρόοδο της διαδικασίας της εγκατάστασης.



Εικ..3.18

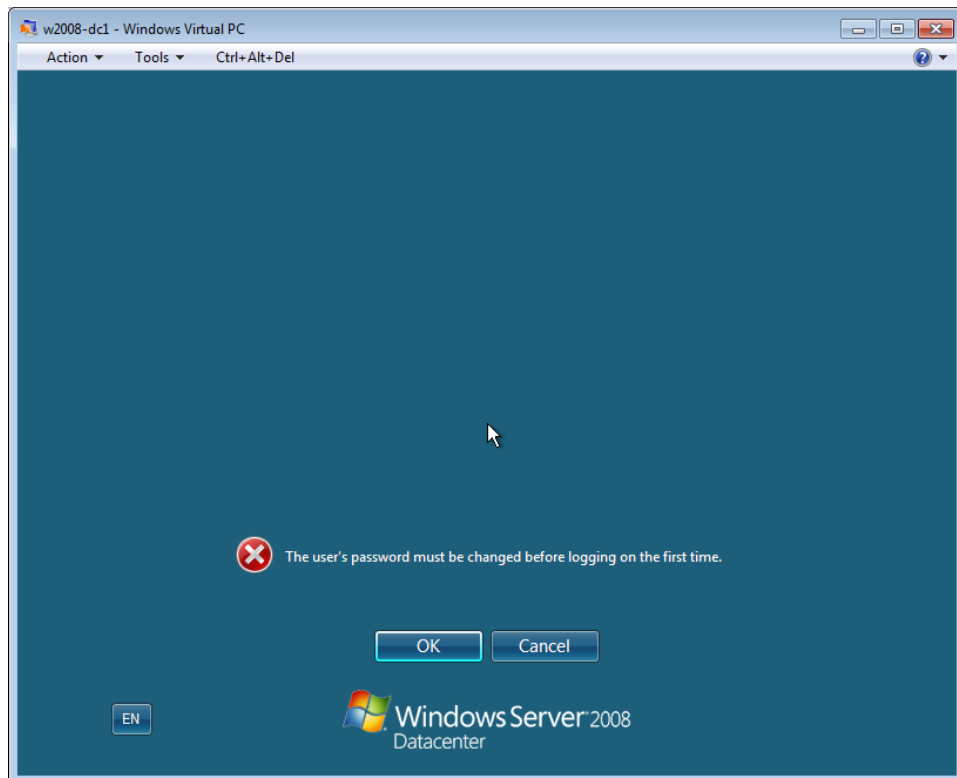
Γίνεται επανεκκίνηση του υπολογιστή και εμφανίζεται η ακόλουθη οθόνη.



Εικ..3.19

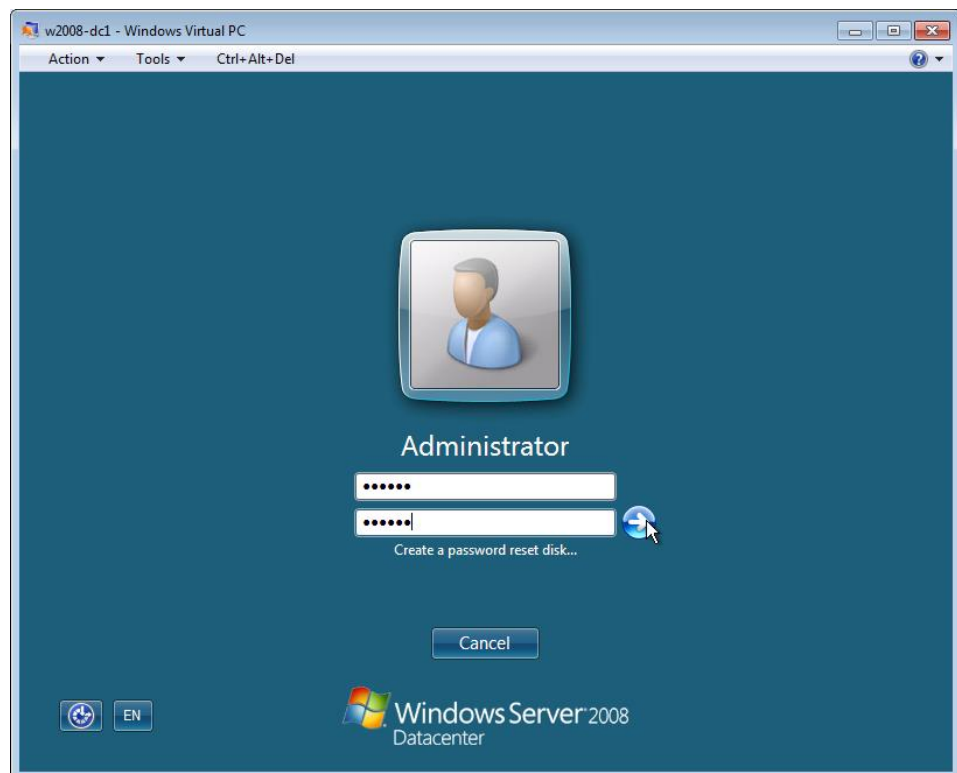
Με την ολοκλήρωση του φορτώματος και την πραγματοποίηση όλων των ρυθμίσεων-

αρχικοποιήσεων θα εμφανιστεί η ακόλουθη εικόνα στην οποία καλούμαστε να δώσουμε κωδικό στον administrator (διαχειριστή).



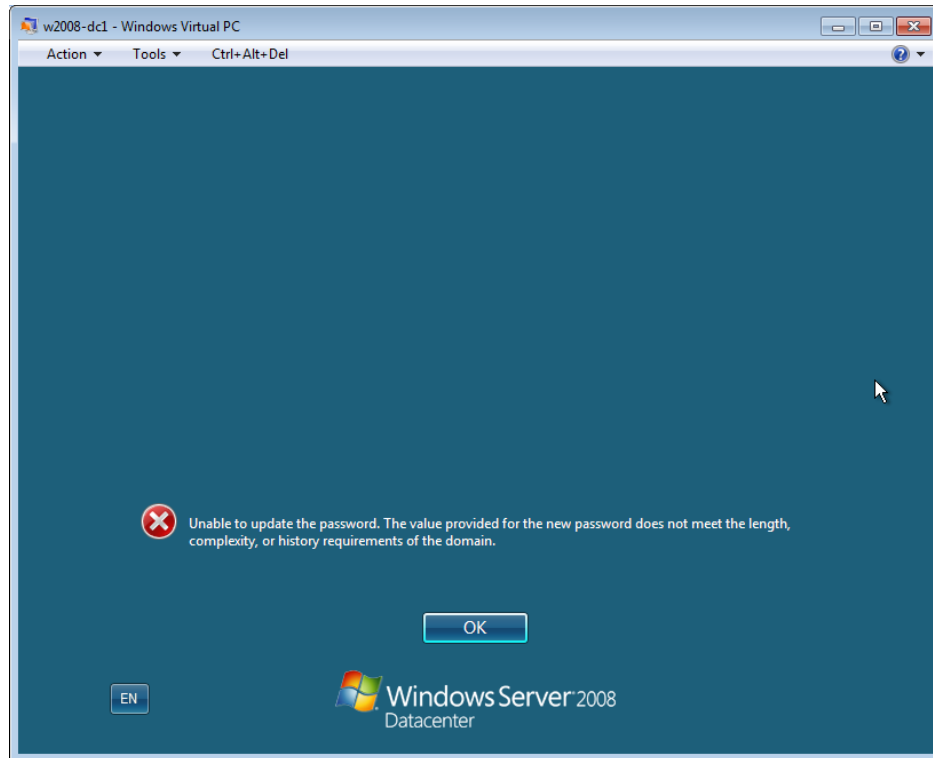
Εικ..3.20

Δίνουμε κωδικό προσέχοντας φυσικά να τον θυμόμαστε.



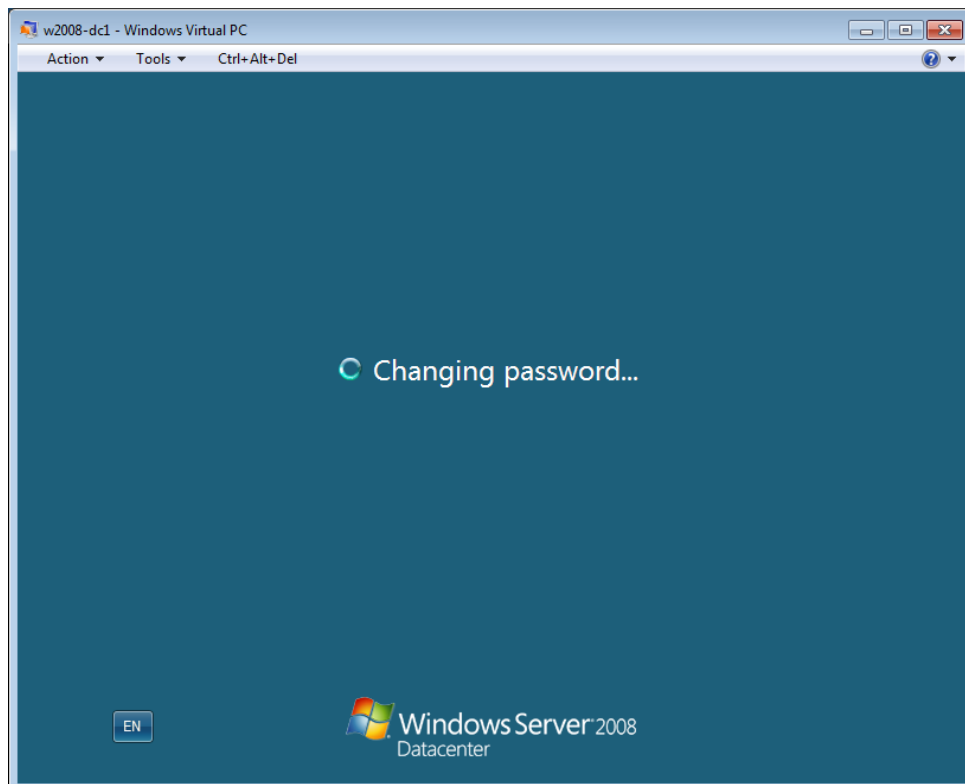
Εικ..3.21

Σε περίπτωση που ο κωδικός δεν είναι ικανοποιεί τα κριτήρια ασφάλειας του συστήματος, τότε καλούμαστε να δώσουμε άλλον ασφαλέστερο.



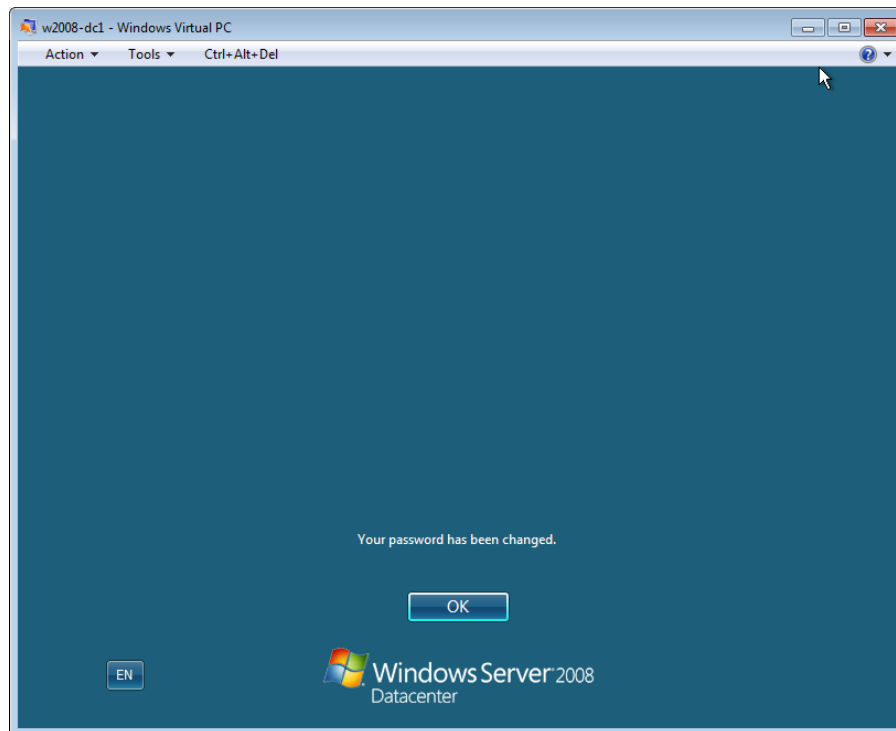
Εικ..3.22

Συνιστούμε την χρήση μεγάλων **pass-phrases** και όχι μικρών κωδικών σε μέγεθος.



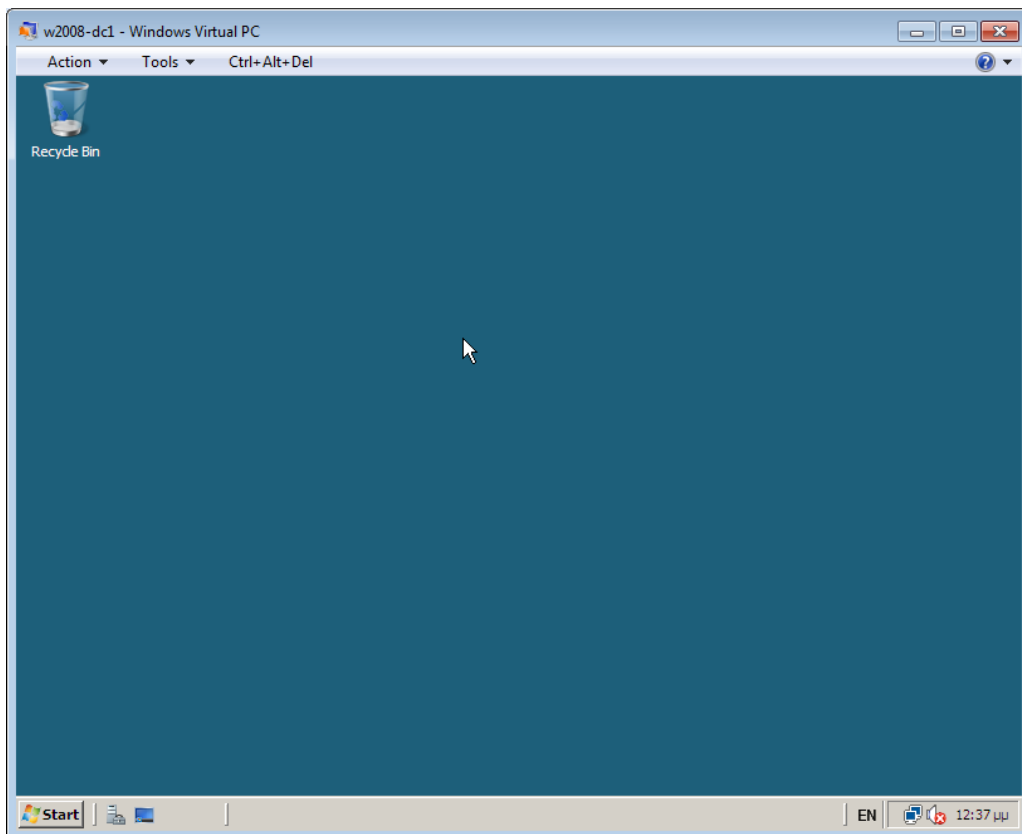
Εικ..3.23

Όταν ολοκληρωθεί η διαδικασία αλλαγής του κωδικού τα Windows μας ενημερώνουν με σχετικό μήνυμα όπως στην Εικ.3.24.



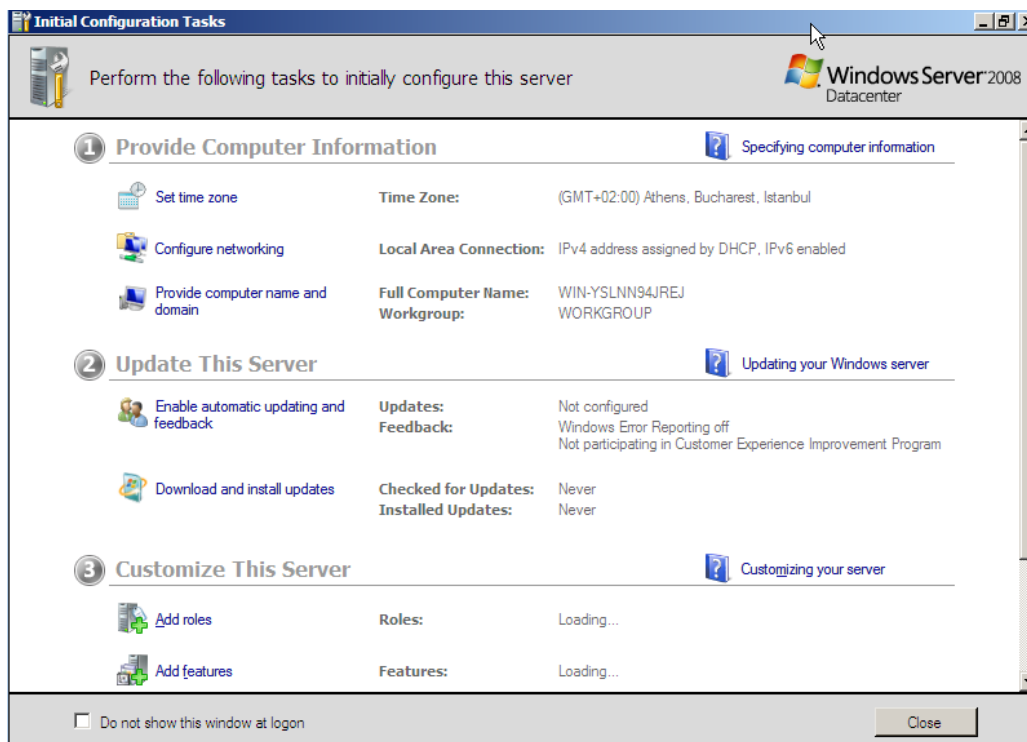
Εικ..3.24

Η εγκατάσταση έχει ολοκληρωθεί και εμφανίζεται αρχικά η επιφάνεια εργασίας.



Εικ..3.25

Την οποία και διαδέχεται ο οδηγός αρχικών ρυθμίσεων (ICT) του Server μας.



Εικ..3.26

3.2.2 Ενέργειες μετά την εγκατάσταση

Κάπως έτσι ολοκληρώθηκε η εγκατάσταση του λειτουργικού. Τώρα θα πρέπει να κάνουμε ρυθμίσεις στον server και να αναθέσουμε ρόλους. **Καλό είναι, για οικονομία χρόνου, να κλείσουμε το μηχάνημα (shutdown) και να κάνουμε αντιγραφή και μετονομασία όλων το αρχείων του server. Θα χρειαστεί να προβούμε και σε ρυθμίσεις στο Virtual PC έτσι ώστε να μπορέσουν οι δύο ίδιοι Servers που θα προκύψουν από την αντιγραφή να μπορούν να βρουν τους σωστούς σκληρούς τους δίσκους, δηλαδή τους εικονικούς δίσκους που τους αντιστοιχούν και να τεθούν σε λειτουργία.**

Αυτό γίνεται μόνο σε εικονικό περιβάλλον και μόνο για οικονομία χρόνου έτσι ώστε να μην χρειάζεται να στήσουμε εκ νέου και το δεύτερο μηχάνημα μιας και θα κάνουμε ακριβώς τα ίδια βήματα.

Εδώ σταματάμε για λίγο και σχεδιάζουμε σε χαρτί το σενάριο που θα τρέξουμε. Θέλουμε να δημιουργήσουμε δύο Domain Controllers, και αφού ρυθμίσουμε τα δικτυακά των Servers, να εγκαταστήσουμε το Active Directory. Στη συνέχεια θα σηκώσουμε έναν DHCP server, ώστε να μοιράζει αυτόματα διευθύνσεις IP στους πελάτες του δικτύου μας.

Ένας domain controller συνήθως έχει μόνο τους ακόλουθους δύο ρόλους οι οποίοι

είναι και υποχρεωτικοί προκειμένου να είναι domain controller:

- Active Directory Domain Services
- DNS (και μάλιστα σε A.D. Integrated Mode)

Στην δική μας περίπτωση τα αρχεία ρυθμίσεων των δύο μηχανημάτων που θα προκύψουν με την αντιγραφή είναι τα:

1. Labs2008-srv1.vmcx
2. Labs2008-srv2.vmcx

Με ανάλογα ονόματα στους σκληρούς τους δίσκους.

Αφού ξεκινήσω και τα δύο μηχανήματα προσέχω να τους δώσω τα εξής ονόματα:

1. w2008-dc1
2. w2008-dc2

Αυτό γίνεται έτσι ώστε να έχουμε όσο το δυνατόν πιο περιγραφικά ονόματα μηχανών και να είναι σύμφωνα με τις οδηγίες μας.

Πρόκειται να δημιουργήσουμε και να ρυθμίσουμε ένα domain το οποίο θα έχει όνομα `inep.local` και σε αυτό το domain θα κάνουμε όλες τις δοκιμές μας έτσι ώστε να ελέγξουμε τα βασικά του χαρακτηριστικά.

Το πρώτο μηχανήμα θα γίνει ο πρώτος domain controller και θα έχει αρχικά τις ακόλουθες ρυθμίσεις στην κάρτα δικτύου:

- 1) IP Address: 192.168.10.2
- 2) Subnet Mask: 255.255.255.0
- 3) Gateway: 192.168.10.1
- 4) DNS: 192.168.10.1 (έστω ότι το παρέχει ο router)

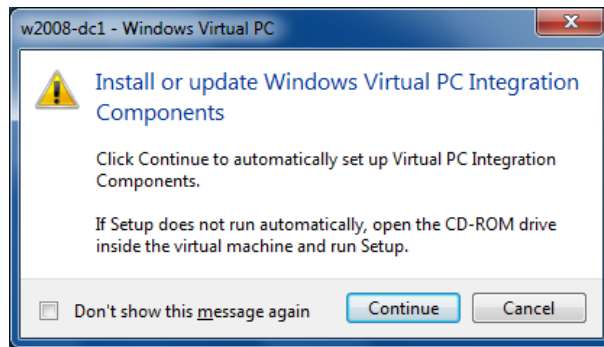
Αφού στηθεί το πρώτο μηχανήμα, το δεύτερο μηχανήμα θα γίνει ο δεύτερος domain controller και θα έχει αρχικά τις ακόλουθες ρυθμίσεις στην κάρτα δικτύου:

- 1) IP Address: 192.168.10.3
- 2) Subnet Mask: 255.255.255.0
- 3) Gateway: 192.168.10.1
- 4) DNS: 192.168.10.1 (έστω ότι το παρέχει ο router)

Αφού ρυθμιστούν και οι δύο domain controllers, θα ελέγξουμε την λειτουργία τους.

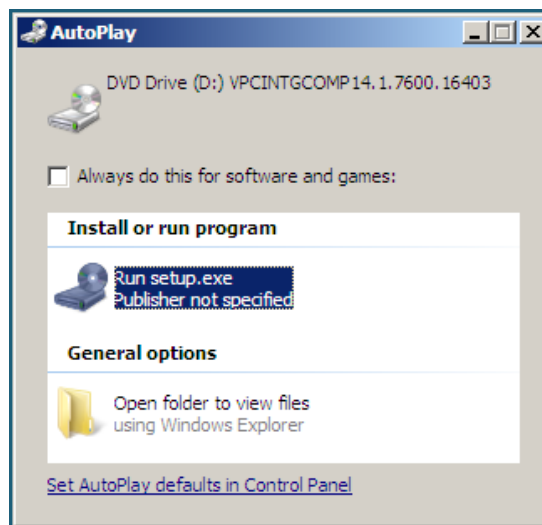
Προκειμένου όλη η διαδικασία να γίνει εύκολη θα ξεκινήσουμε με την εγκατάσταση στον πρώτο server των Windows Virtual PC Integration Components, πατώντας την κατάλληλη επιλογή από την μπάρα, αφού έχει ξεκινήσει το μηχανήμα.

Αρχικά εμφανίζεται η ακόλουθη ενημερωτική οθόνη Εικ.3.27:



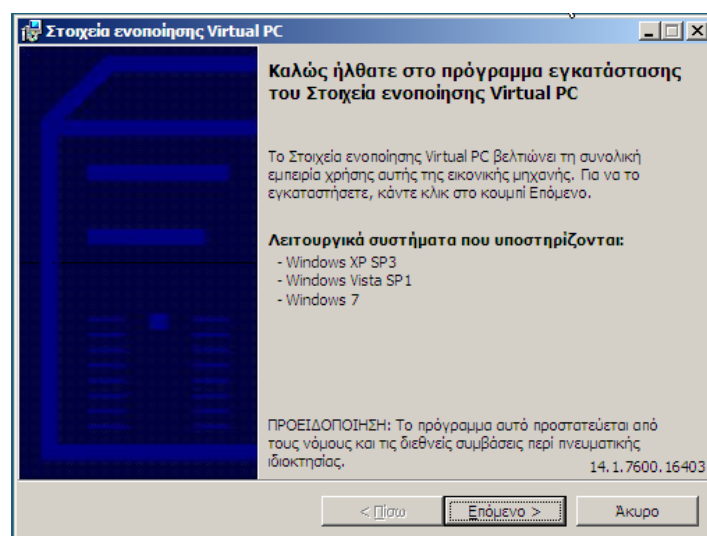
Εικ..3.27

Πατάμε φυσικά “Continue” ώστε να προχωρήσει η εγκατάσταση.
Επιλέγουμε το “Run setup.exe”



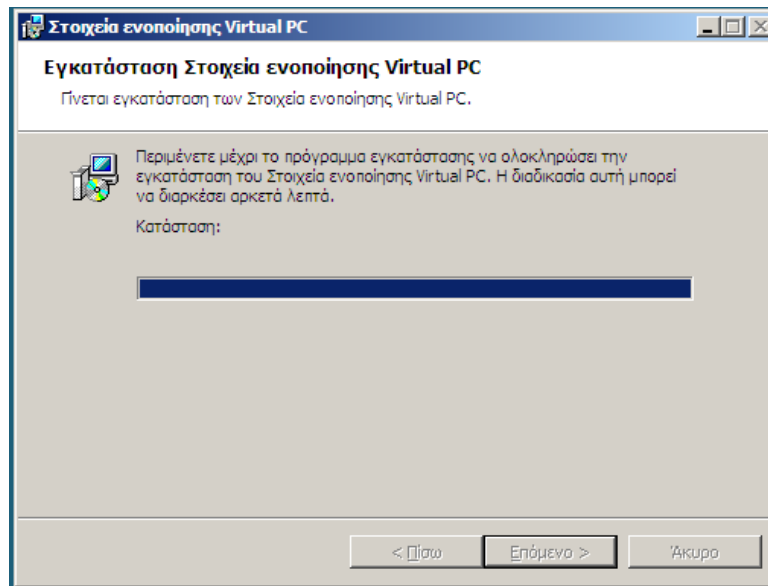
Εικ..3.28

και μετά πατάω το επόμενο.



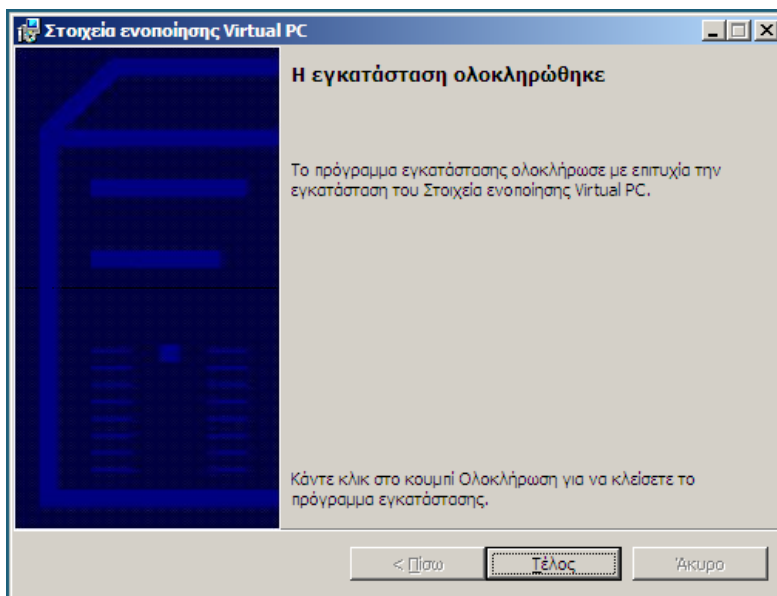
Εικ..3.29

Η εγκατάσταση συνεχίζει κανονικά όπως στην Εικ.3.30.



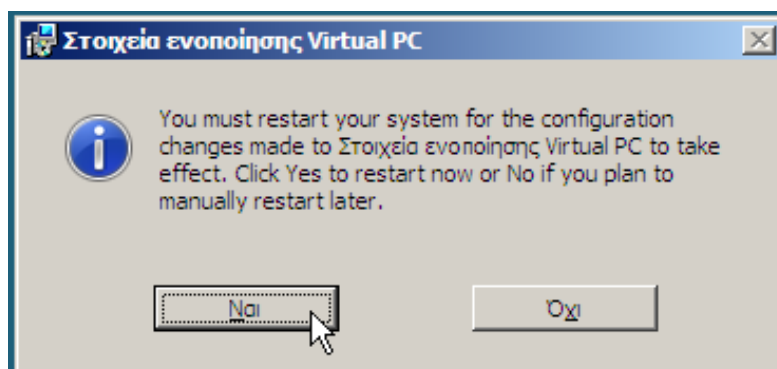
Εικ..3.30

Και με το πλήκτρο «Τέλος» ολοκληρώνουμε την εγκατάσταση.



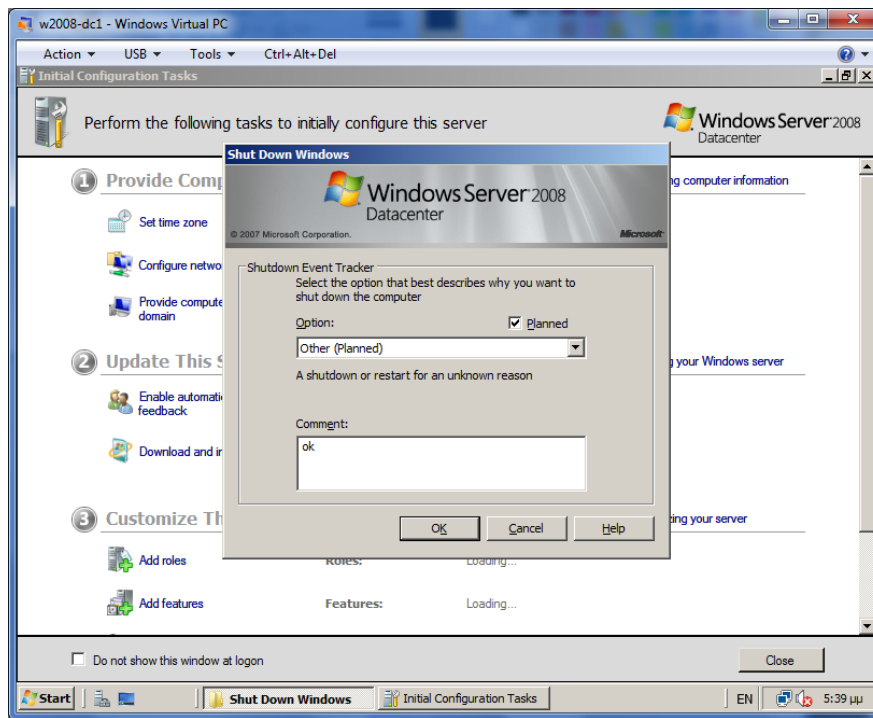
Εικ..3.31

Πατάμε το πλήκτρο «Ναι» (Εικ.3.32) προκειμένου να γίνει η επανεκκίνηση.



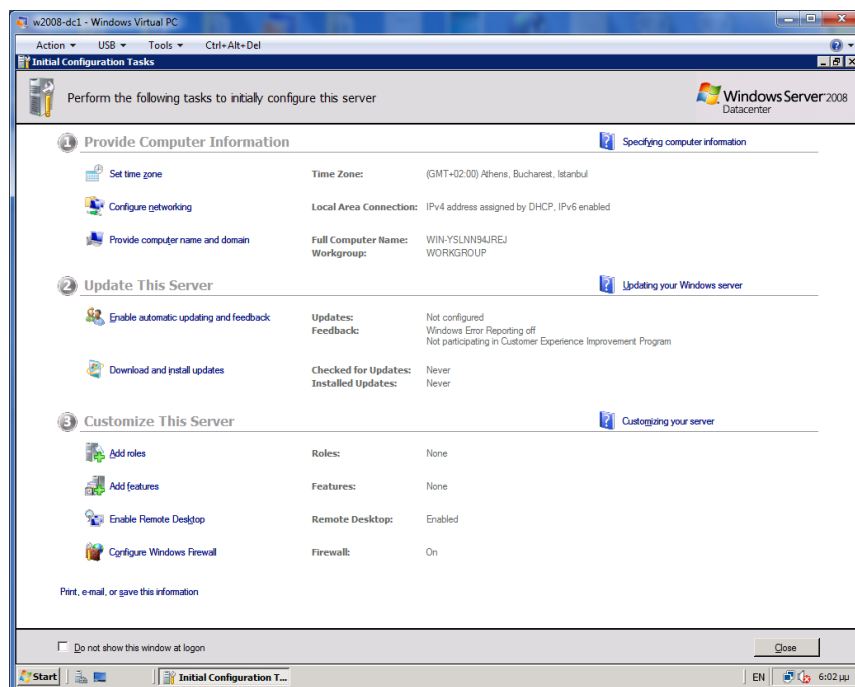
Εικ..3.32

Ο server ξεκινάει την διαδικασία της επανεκκίνησης και εμφανίζει ένα παράθυρο προκειμένου να συμπληρώσουμε στοιχεία για την επανεκκίνηση. Καλό είναι να δίνουμε τα στοιχεία αυτά όσο πιο περιγραφικά γίνεται.



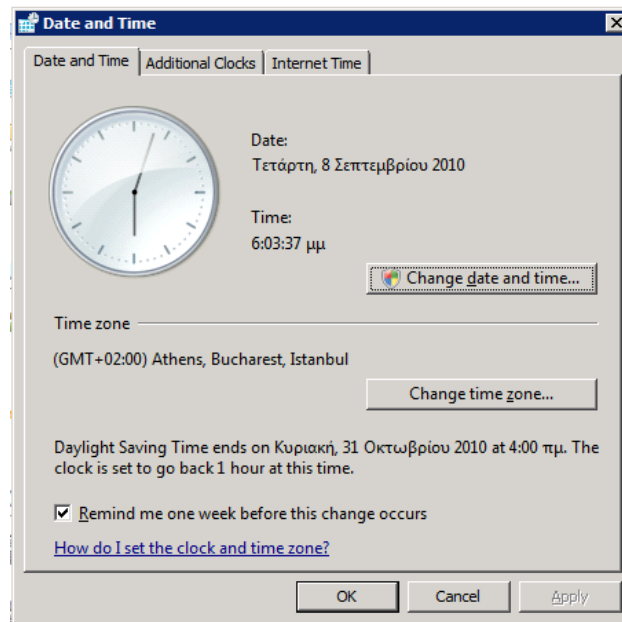
Εικ..3.33

Μετά την επανεκκίνηση και το Login εμφανίζεται η ακόλουθη οθόνη που είναι ένας οδηγός προκειμένου να μας βοηθήσει να κάνουμε τις αρχικές ρυθμίσεις στον server με τρόπο συστηματικό και οργανωμένο.



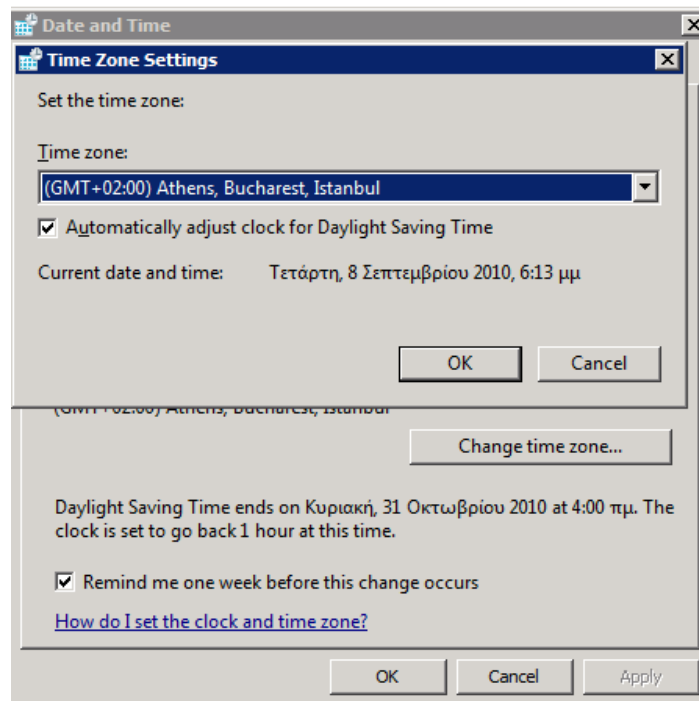
Εικ..3.34

Ξεκινάμε με τις ρυθμίσεις της ώρας, όπου πρέπει να είμαστε πολύ προσεκτικοί έτσι ώστε να επιλέξουμε τα σωστά στοιχεία περιοχής και ώρας, και στους δύο servers, αλλιώς η λειτουργία του δεύτερου DC μπορεί να παρουσιάσει σφάλματα.



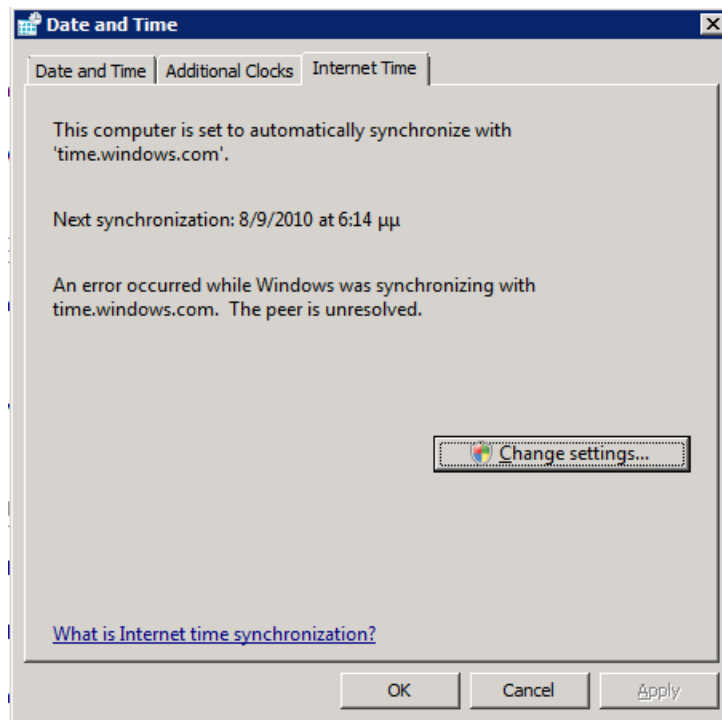
Εικ..3.35

Επιλέγουμε την σωστή ζώνη ώρας (Εικ.3.36) ώστε να έχουμε σωστές αυτόματες ενημερώσεις. Αν δεν υπάρχει η ονομασία της περιοχής μας τότε επιλέγουμε κάποια άλλη περιοχή που είναι στην ίδια ζώνη ώρας με εμάς. Η Ελλάδα έχει **GMT+02:00**.



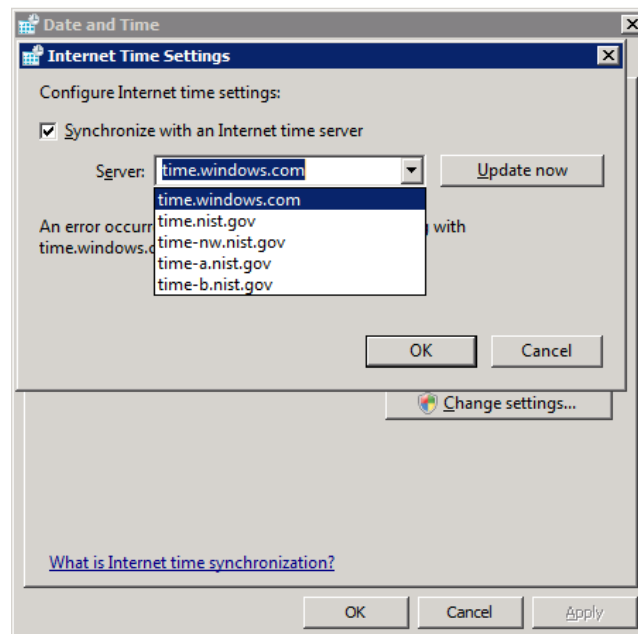
Εικ..3.36

Και μετά από το μενού “Internet Time” (Εικ.3.37) πατάμε το Change Settings,



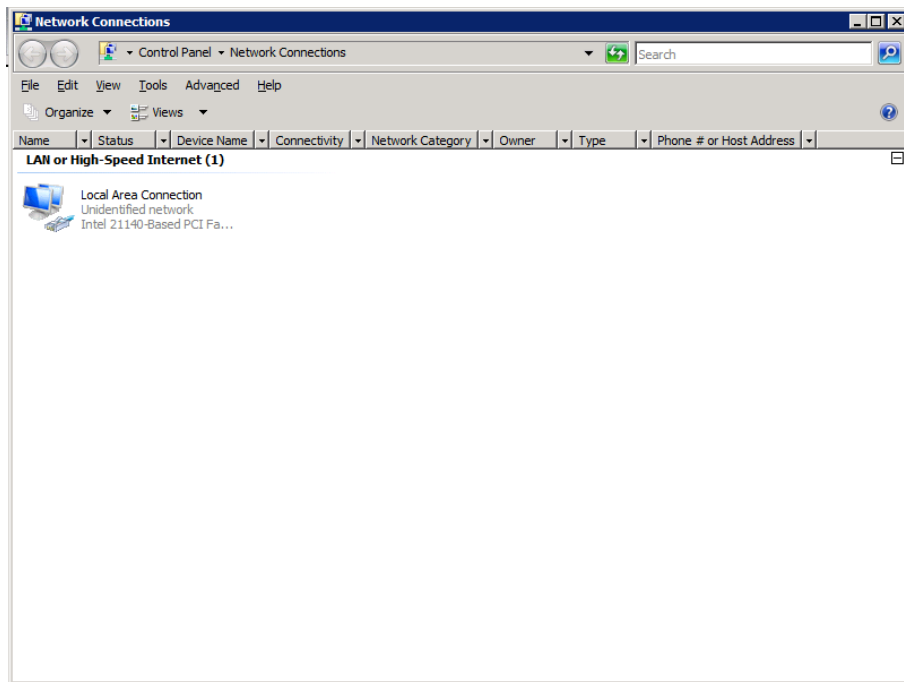
Εικ..3.37

και ορίζουμε έναν διαδικτυακό “time server” προκειμένου να έχουμε κοινή βάση αναφοράς μεταξύ των πιθανών απομακρυσμένων σημείων του δικτύου μας. Μπορούμε να αφήσουμε τον time-server της Microsoft, ή να επιλέξουμε κάποιον άλλο ή ακόμα να ορίσουμε με IP έναν δικό μας time-server (π.χ. τον router). **Η ύπαρξη κοινής βάσης ώρας είναι πάρα πολύ σημαντική για την σωστή λειτουργία ενός δικτύου.**



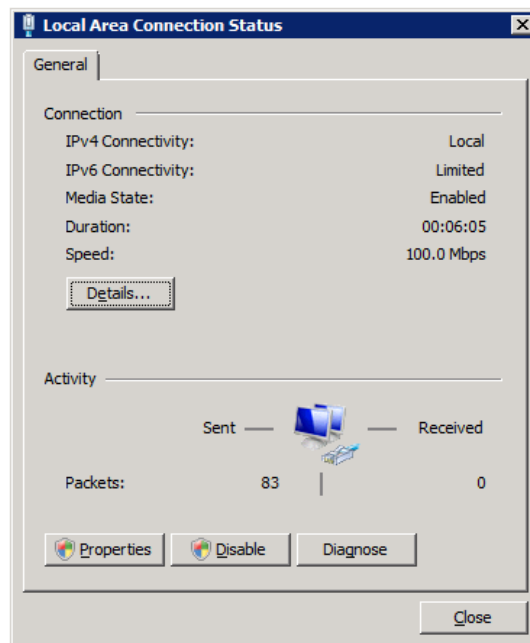
Εικ..3.38

Μετά πάμε να ρυθμίσουμε τις δικτυακές παραμέτρους του server μας. Από το “control panel” και στην συνέχεια στο “Network Connections”,



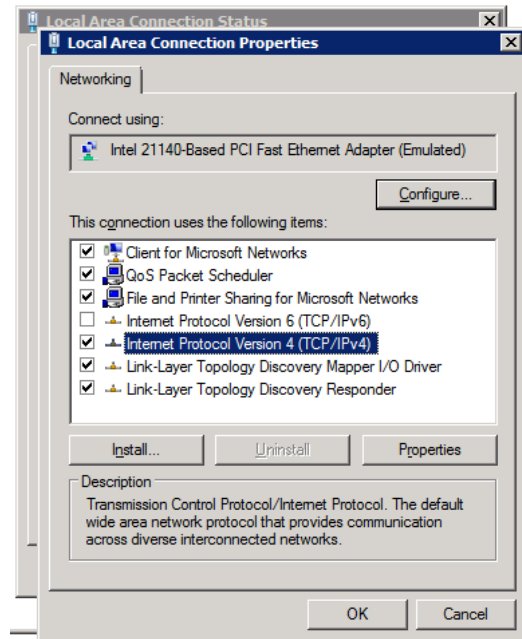
Εικ..3.39

Πάμε στο “local area connection”



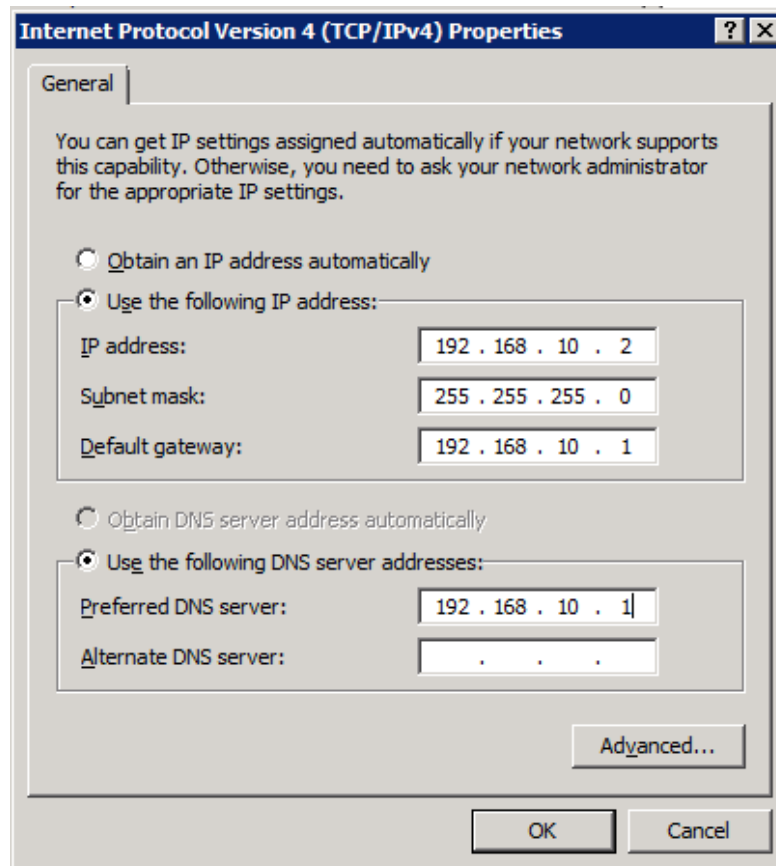
Εικ..3.40

Και στο “properties” πάμε και από-επιλέγουμε το TCP/IPv6, διότι δεν υλοποιούμε στην παρούσα άσκηση TCP/IPv6 δίκτυα. Επιλέγουμε το TCP/IPv4 και πατάμε το “properties”.



Εικ.3.41

Στην καρτέλα αυτή (Εικ.3.42) δίνουμε τις δικτυακές ρυθμίσεις του πρώτου domain controller, όπως τις αποτυπώσαμε στο χαρτί.



Εικ.3.42

IP address: 192.168.10.2

Subnet mask: 255.255.255.0

Default Gateway: 192.168.10.1

Preferred DNS Server: 192.168.10.1

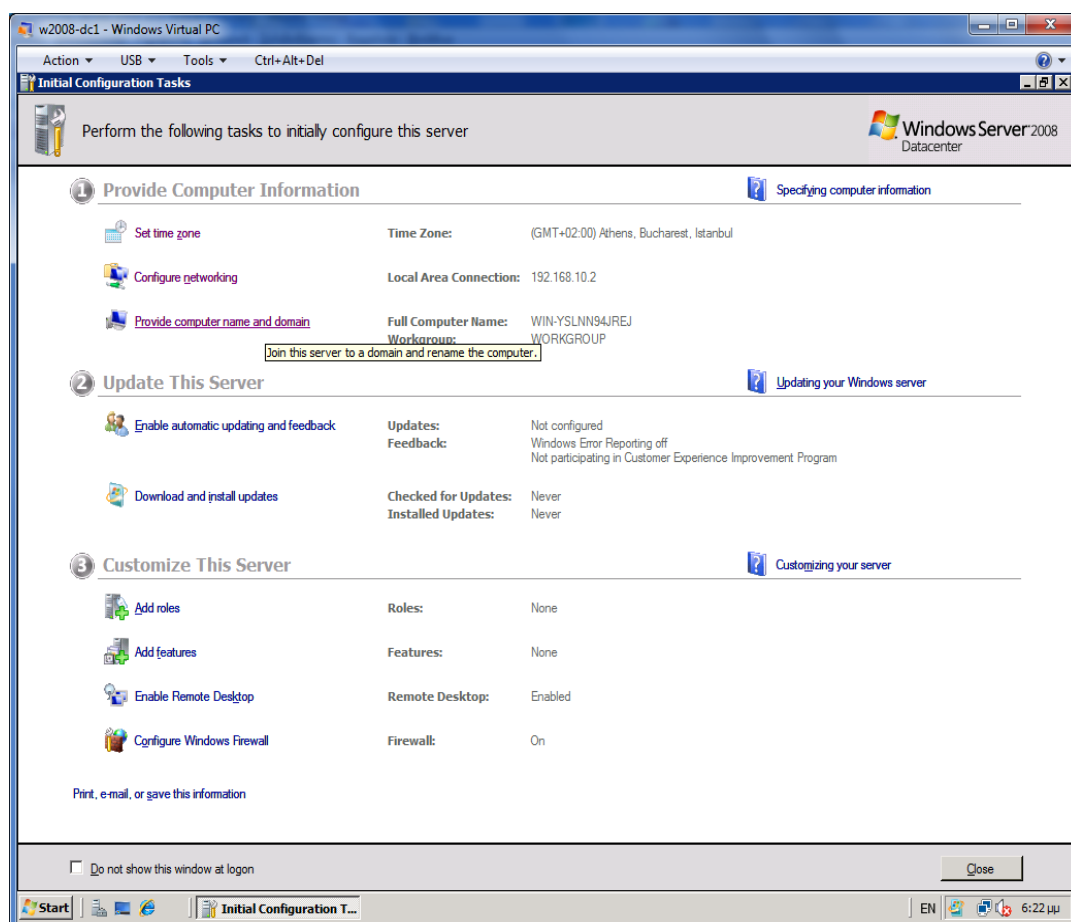
Ο preferred DNS παίρνει διεύθυνση ίδια με το Gateway, δηλαδή την διεύθυνση του router, θεωρώντας ότι το router μας, μας δίνει την υπηρεσία DNS, που είναι ένα συνηθισμένο σενάριο.

Στον Alternate DNS δεν βάζουμε προς το παρόν τίποτα, αργότερα όμως πρόκειται να το συμπληρώσουμε.

Προσέχουμε ιδιαίτερα τις ρυθμίσεις που δώσαμε διότι θα επανέλθουμε ξανά σε αυτό το σημείο αργότερα.

Στη συνέχεια ρυθμίζουμε τις υπόλοιπες επιλογές που είναι διαθέσιμες:

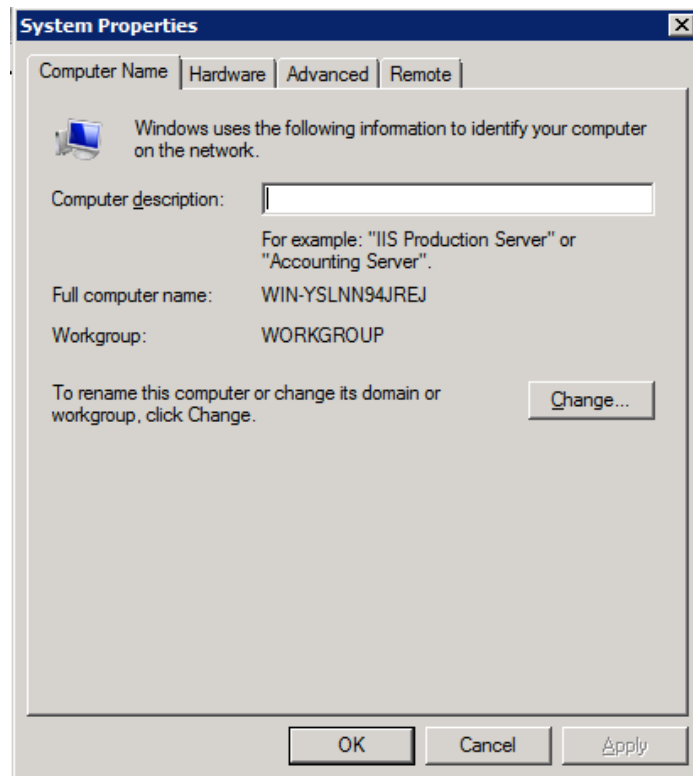
Πάμε τώρα από τον αρχικό οδηγό στην επιλογή “Provide computer name and domain” προκειμένου να δώσουμε το όνομα στον πρώτο “domain controller”.



Εικ.3.43

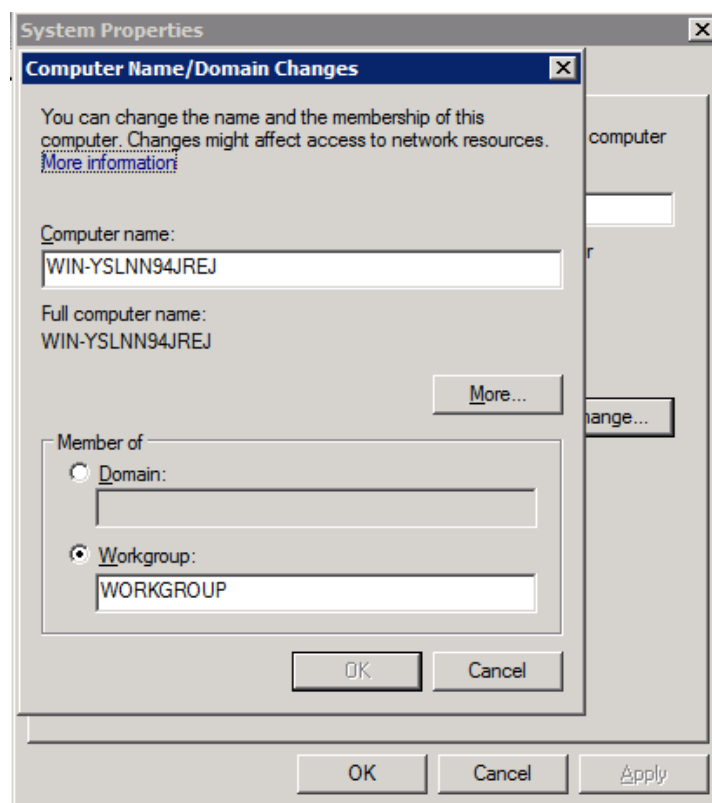
Και στο “system properties” στο tab “computer name” πατάμε στο “Change” βλέπε

Εικ.3.44



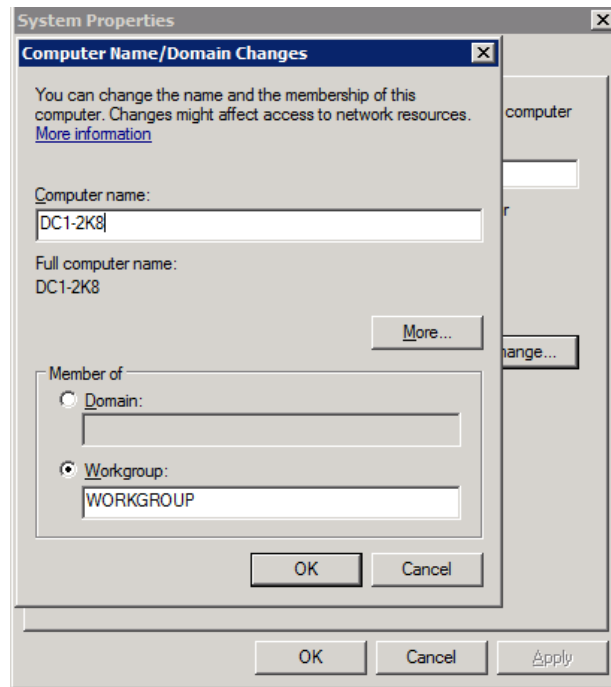
Εικ..3.44

Και αλλάζουμε το συμπληρωμένο όνομα με αυτό που θέλουμε (Εικ.3.45).



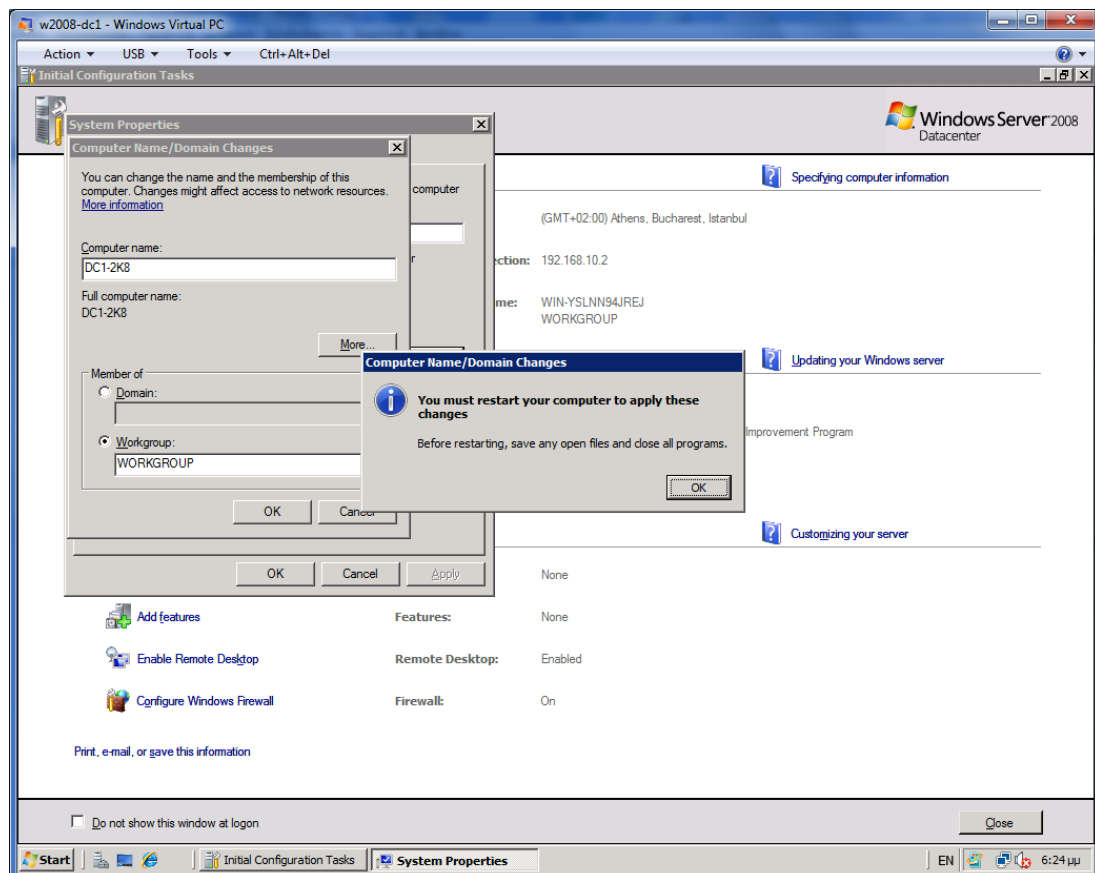
Εικ..3.45

δηλαδή το **DC1-2K8** χωρίς να πειράζουμε την τιμή του “Workgroup”



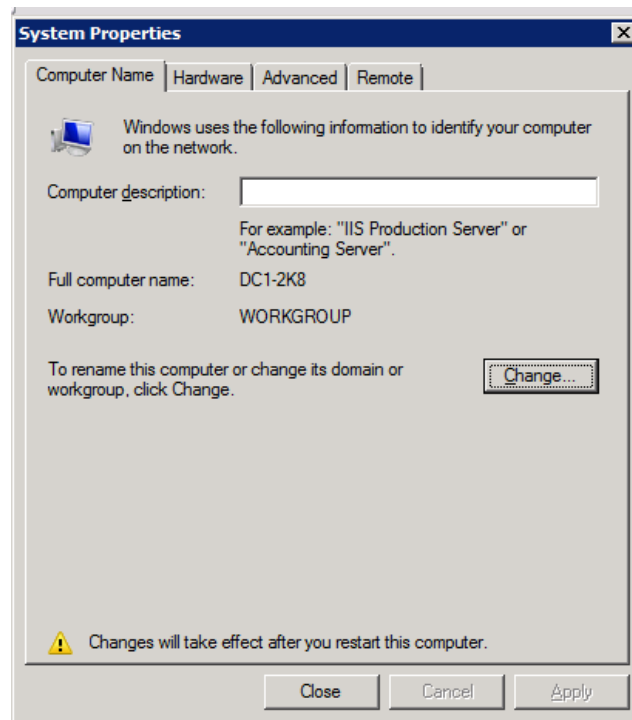
Εικ..3.46

Πατώντας το “ok” ο υπολογιστής θα μας ζητήσει να εκτελέσουμε επανεκκίνηση, πράγμα το οποίο και θα κάνουμε (Εικ.3.47).



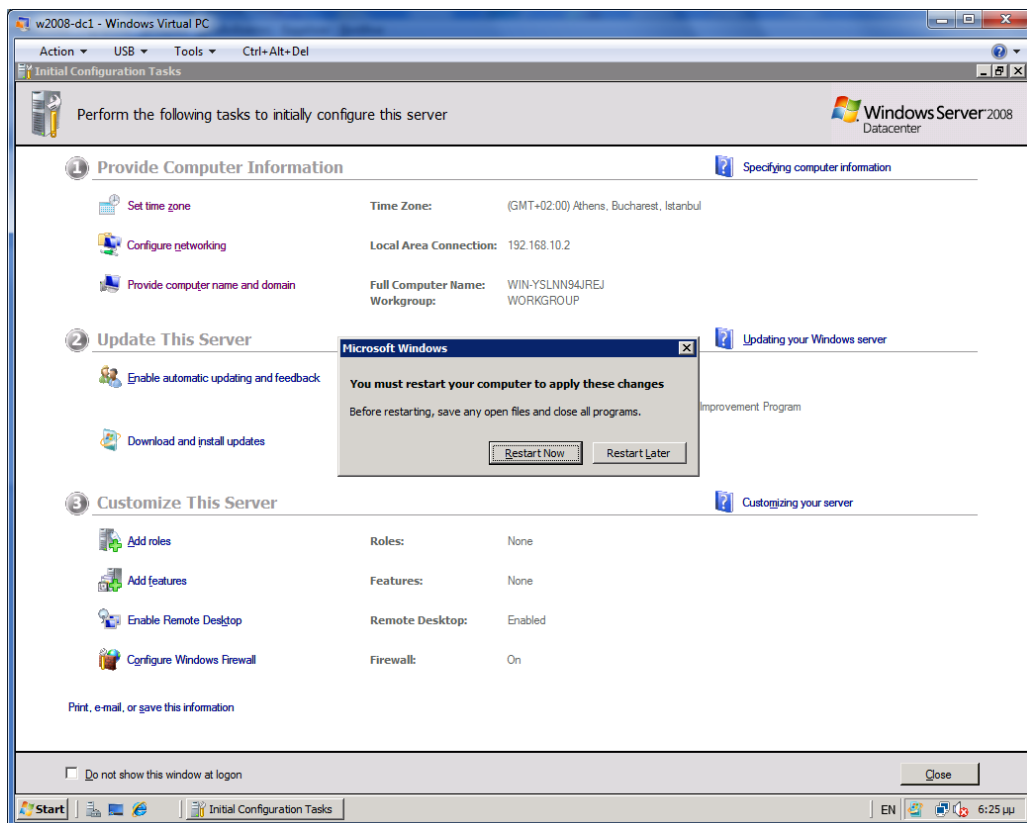
Εικ..3.47

Πατάμε “ok” και παρατηρούμε το προειδοποιητικό θαυμαστικό.



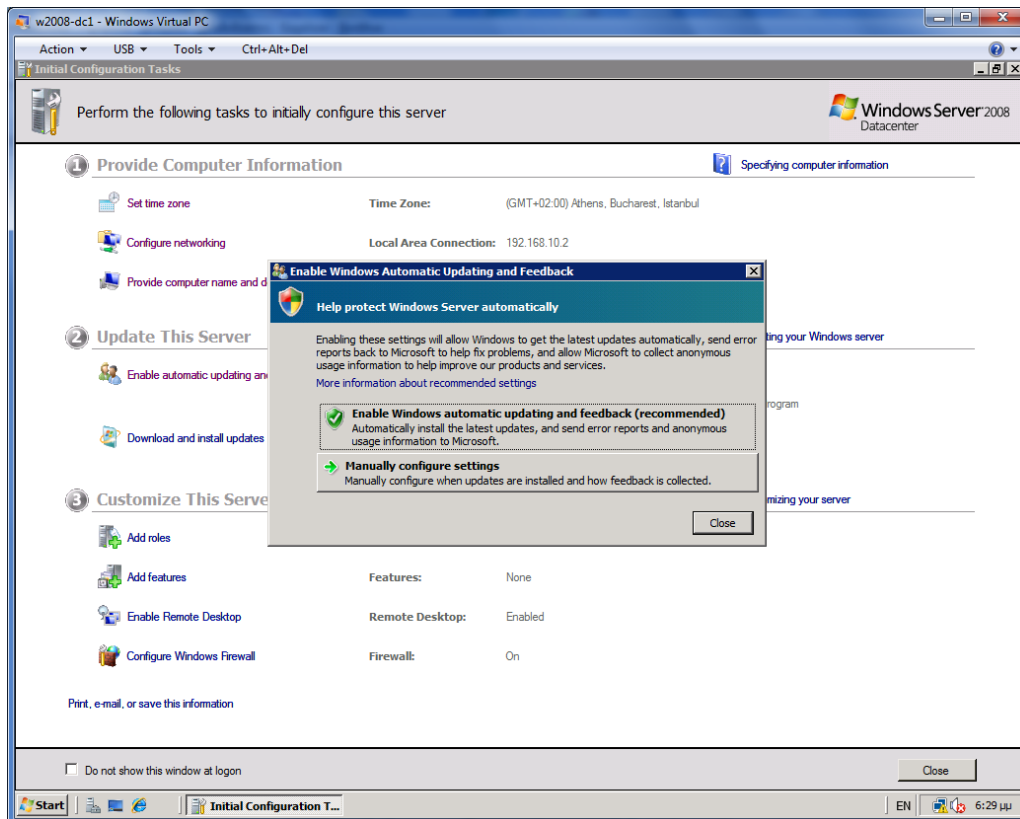
Εικ..3.48

Πατώντας και πάλι “ok” και μετά “Restart Now” γίνεται επανεκκίνηση του server.



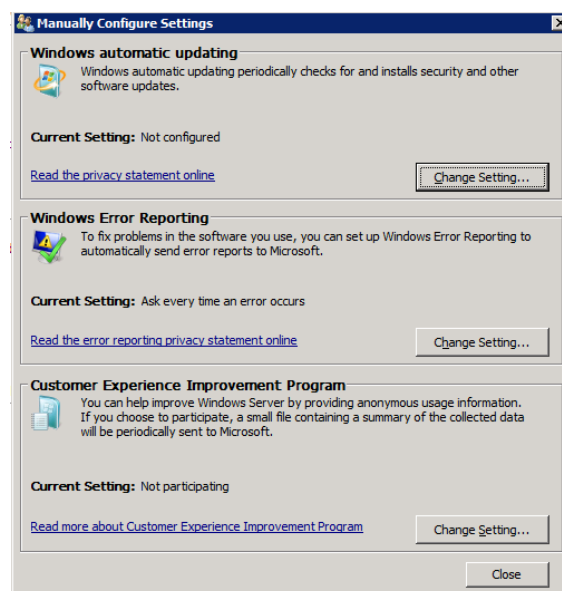
Εικ..3.49

Μετά την επανεκκίνηση συνεχίζουμε τα βήματα του οδηγού και ρυθμίζουμε το “Enable automatic updating and feedback”



Εικ.3.50

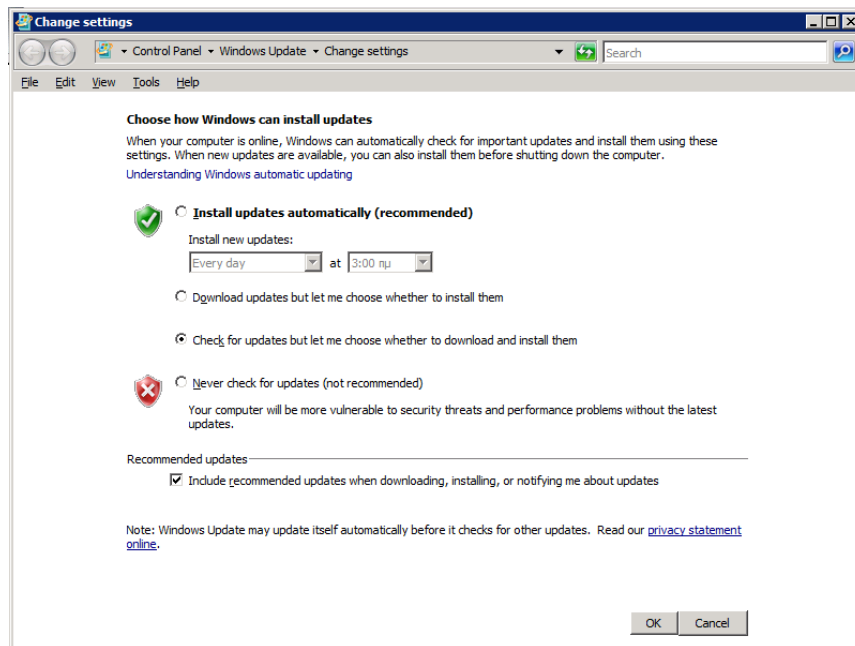
Στο σημείο αυτό συνιστούμε την επιλογή το “Manually configure settings” προκειμένου να παραμετροποιήσουμε την συμπεριφορά του server.



Εικ.3.51

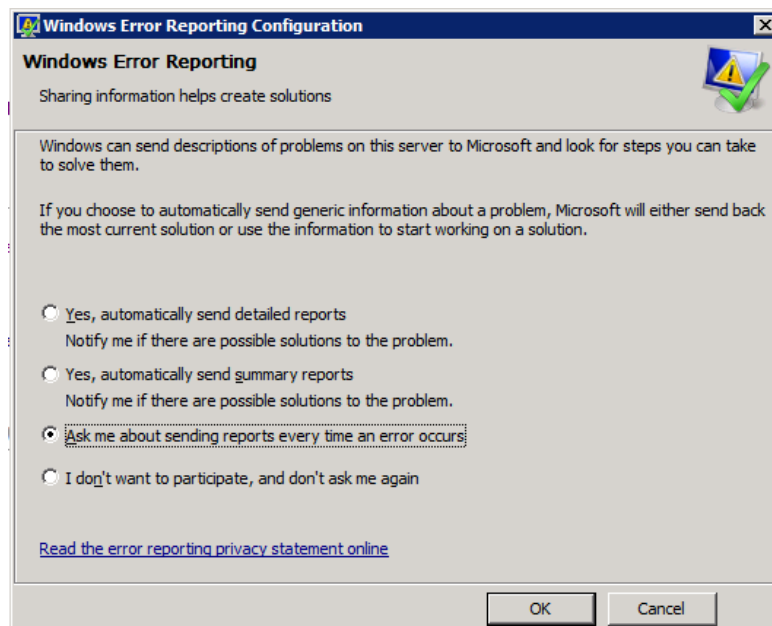
Από το μενού “Manually Configure Settings” με την σειρά ξεκινάμε από πάνω προς τα κάτω και ρυθμίζουμε κατά το δοκούν τις επιλογές. Αρχίζουμε από το “Windows automatic updating” και επιλέγουμε το “Check for updates but let me choose whether

to download and install them” έτσι ώστε να ελέγχουμε πλήρως τα updates που θα κατεβούν και να εκτελούμε μόνο τα απαραίτητα ώστε να μην γεμίζουμε τον δίσκο με περιττά δεδομένα από updates που δεν θα εγκαταστήσουμε. Δεν ξεχνάμε να επιλέξουμε το “Recommended Updates” διότι μας ενδιαφέρει να ειδοποιούμαστε και για τις συνιστώμενες ενημερώσεις από την Microsoft.



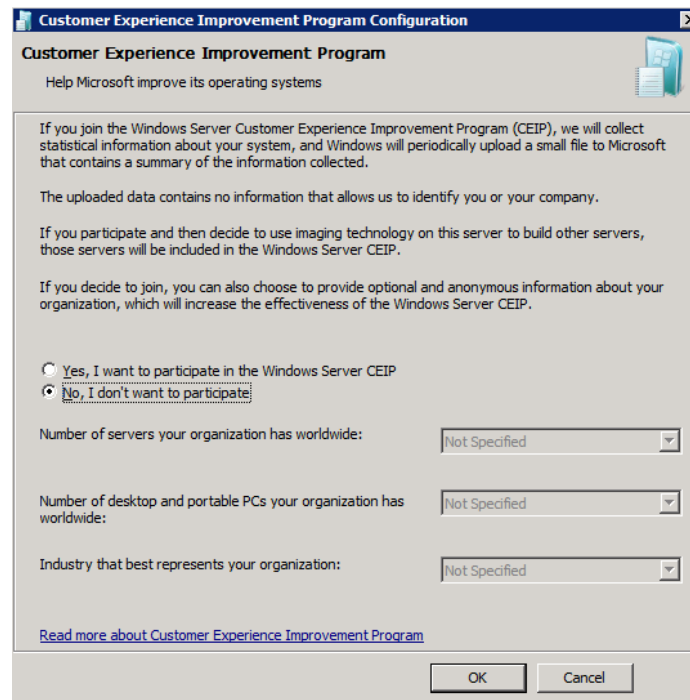
Εικ..3.52

Στην συνέχεια επιλέγουμε το “Windows Error Reporting” και επιλέγουμε να ερωτούμαστε πριν την αποστολή αναφορών στην Microsoft (Εικ.3.53).



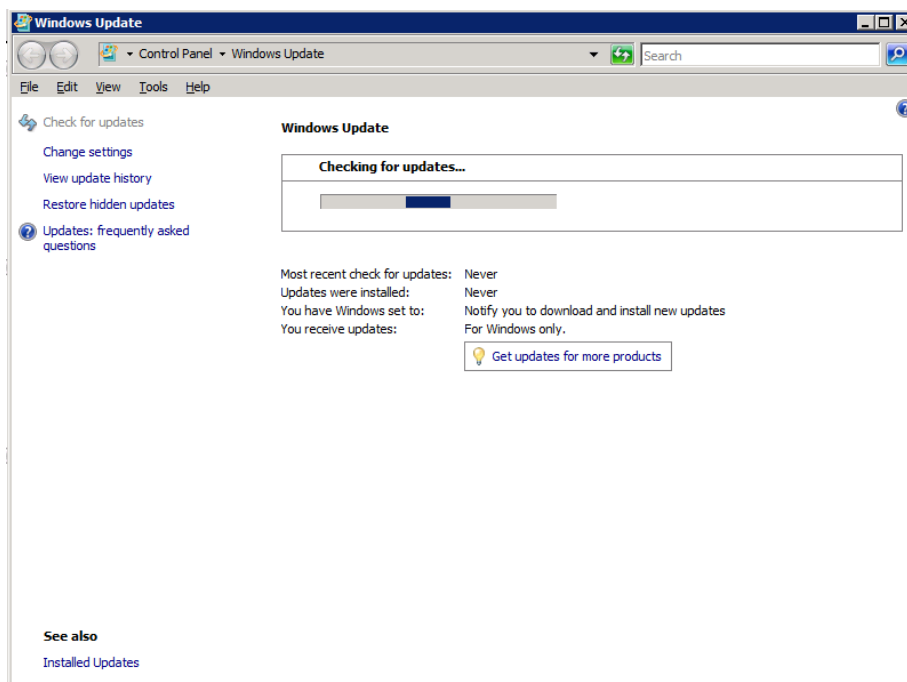
Εικ..3.53

Πατάμε “OK” και στη συνέχεια πάμε στην τρίτη επιλογή. Επειδή δεν μας ενδιαφέρει να συμμετάσχουμε στον CEIP αποστέλλοντας πληροφορίες στην Microsoft, επιλέγουμε το “No, I don’t want to participate” και μετά το “OK”.



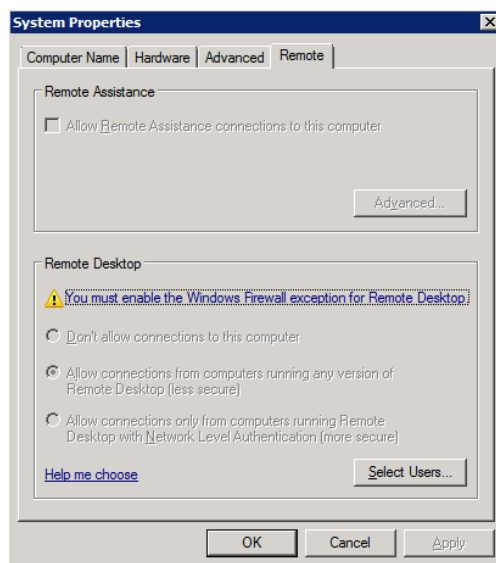
Εικ.3.54

Στη συνέχεια από το μενού “Initial Configuration Tasks” κατεβάζουμε όλα τα διαθέσιμα updates, πριν προχωρήσουμε παρακάτω και εγκαταστήσουμε ρόλους ή χαρακτηριστικά, πατώντας το “Download and Install Updates”.



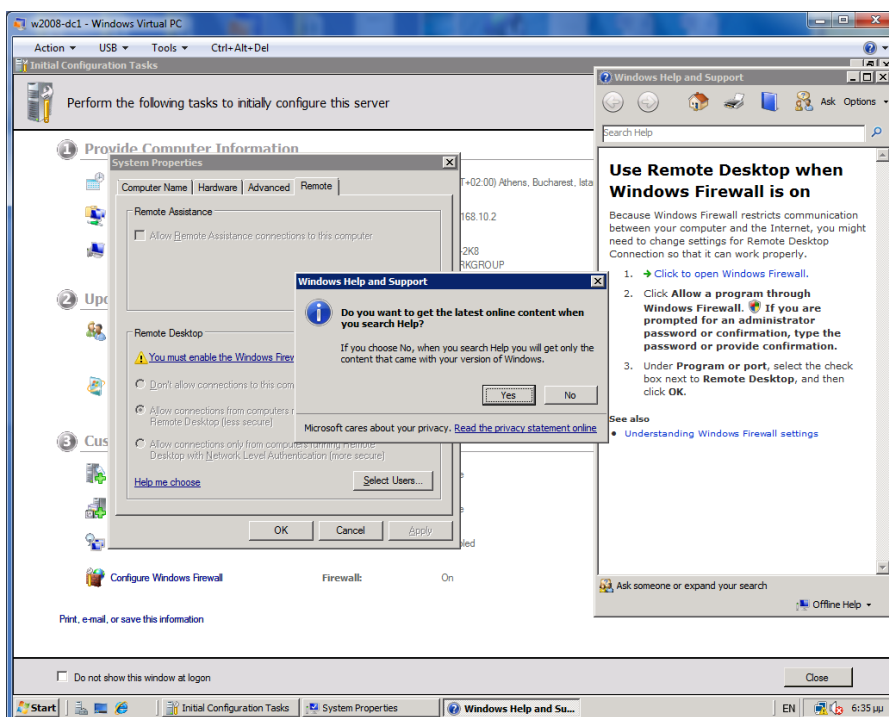
Εικ.3.55

Αφού γίνουν **όλα** τα updates, και οι πιθανές επανεκκινήσεις του Server, ρυθμίζουμε τις επιλογές για απομακρυσμένη πρόσβαση (Εικ.3.56).



Εικ.3.56

Εδώ θα έρθουμε αντιμέτωποι με μια προειδοποίηση η οποία μας λέει ότι θα πρέπει να ανοίξουμε μια εξαίρεση στο τείχος προστασίας των Windows έτσι ώστε να επιτραπεί η σύνδεση στον Server μέσω του προγράμματος απομακρυσμένης πρόσβασης (RDP protocol, TCP port 3389).

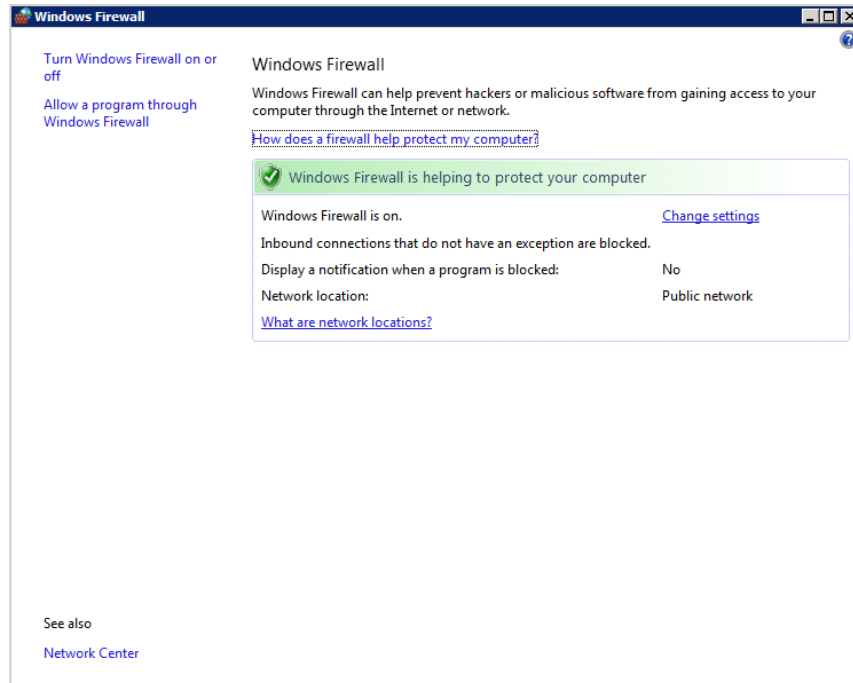


Εικ.3.57

Πατώντας πάνω στην ειδοποίηση μας εμφανίζεται ένας βοηθός προκειμένου να κάνουμε εύκολα τις απαραίτητες ρυθμίσεις. Πατάμε στο “Yes” προκειμένου να

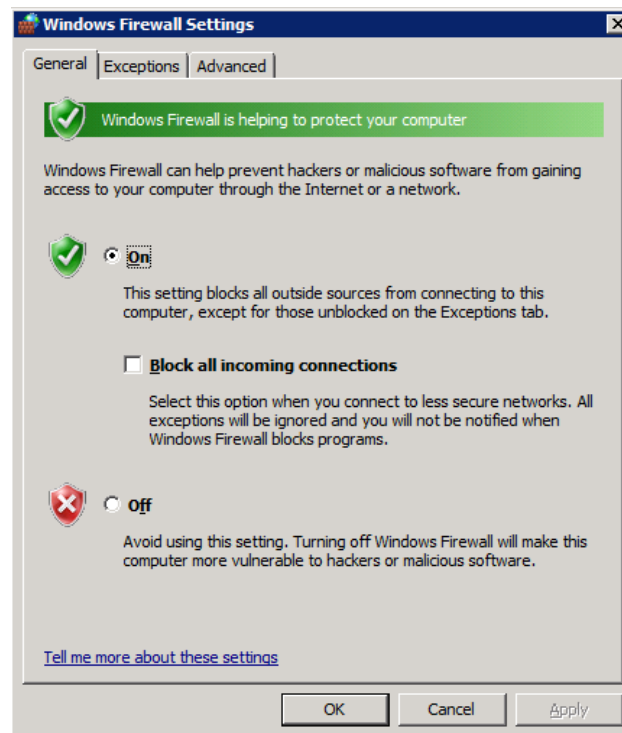
μπορούμε να αναζητήσουμε και στο διαδίκτυο όταν ζητούμε βοήθεια από τα Windows.

Στη συνέχεια, πατάμε στο 1. Έτσι ώστε να μας εμφανίσει τις ρυθμίσεις του τείχους προστασίας των Windows.



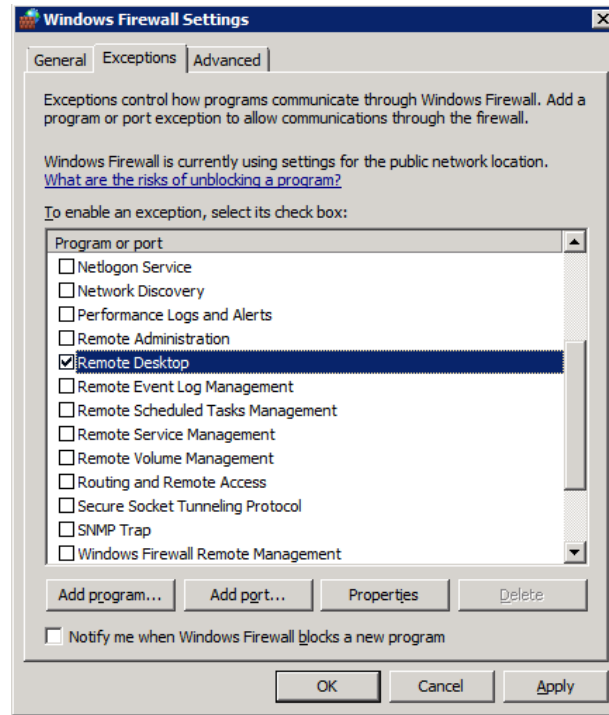
Εικ..3.58

Πατώντας στο “Change Settings” έχουμε την ακόλουθη εικόνα:



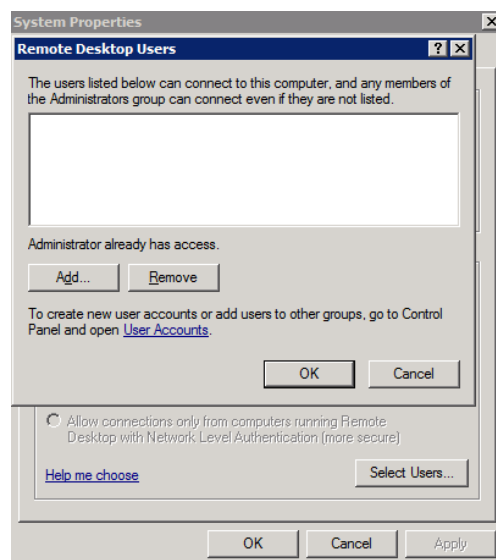
Εικ..3.59

Εν συνεχεία από την καρτέλα “Exceptions” επιλέγουμε την έτοιμη εξαίρεση για το Remote Desktop. Πολλές φορές πάντως, σε ένα Domain είναι συνηθισμένη λανθασμένη τακτική να απενεργοποιείται εντελώς το firewall, παρόλο που κάτι τέτοιο δεν συνιστάται σε καμία περίπτωση.



Εικ..3.60

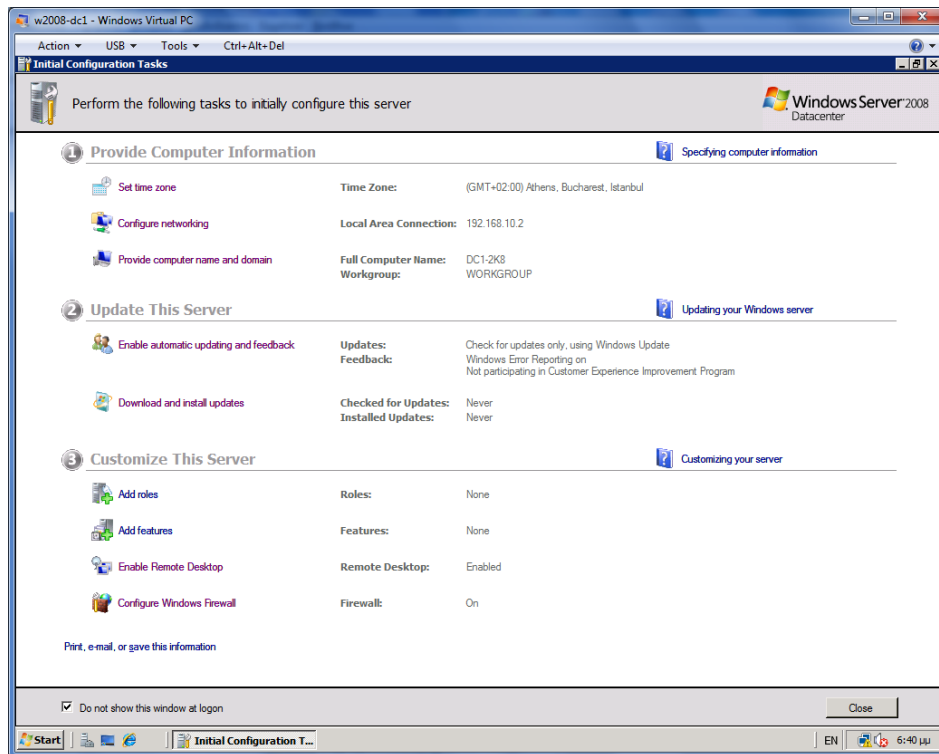
Στη συνέχεια επιλέγουμε τους χρήστες της υπηρεσίας “remote desktop”. Παρατηρούμε ότι ο διαχειριστής (administrator) έχει ήδη πρόσβαση.



Εικ..3.61

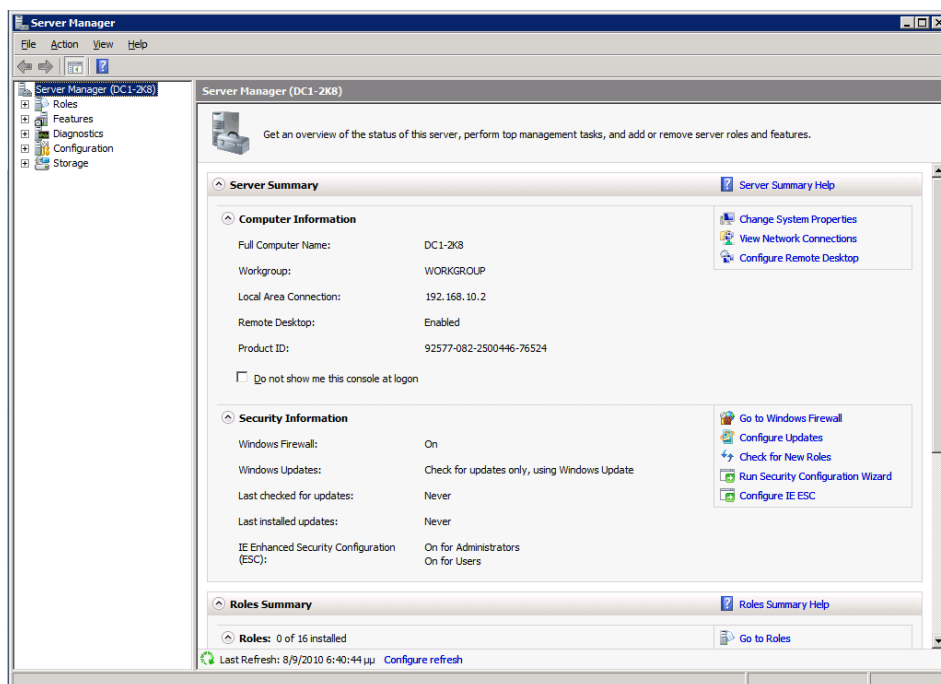
Τέλος αφού έχουμε κάνει τις βασικές ρυθμίσεις στον Server μας, επιλέγουμε το check-mark που υπάρχει κάτω αριστερά (**Do not show this windows at logon**) έτσι

ώστε να σταματήσει να εμφανίζεται συνέχεια αυτή η οθόνη (η οθόνη του ICT) με το ξεκίνημα του υπολογιστή.



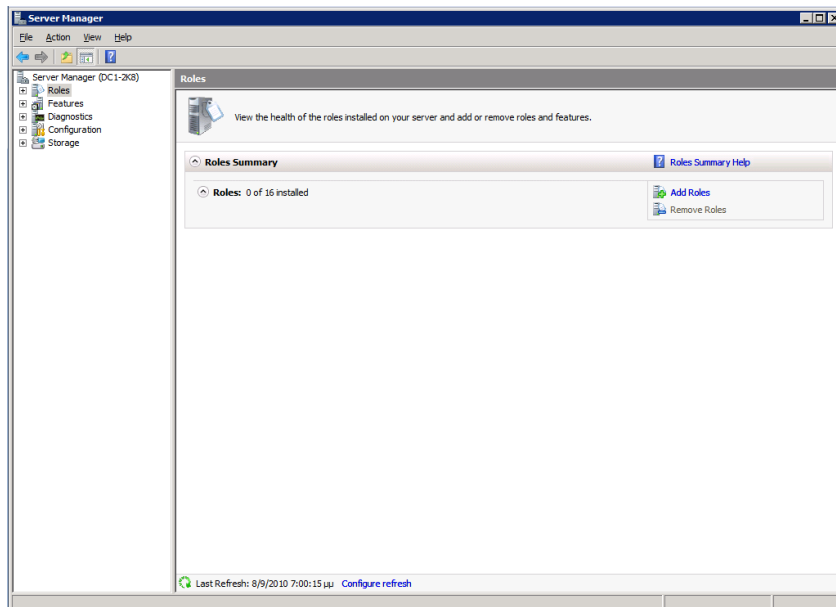
Εικ..3.62

Εν συνεχεία ανοίγει αυτομάτως ο server manager (Εικ.3.63), ένα συγκεντρωτικό εργαλείο των βασικών λειτουργιών και ρυθμίσεων του server, το οποίο είναι αρκετά βολικό για την διαχείριση του server μας, και που καλό είναι να το χρησιμοποιούμε.



Εικ..3.63

Στο αριστερό τμήμα του παραθύρου βλέπουμε με την σειρά: «Ρόλους», «Χαρακτηριστικά», «Διαγνωστικά», «Ρυθμίσεις» και «Αποθήκευση». Εμείς θέλουμε να προσθέσουμε τον «ρόλο» του Active Directory Domain Services και θα το κάνουμε από αυτό το μενού.

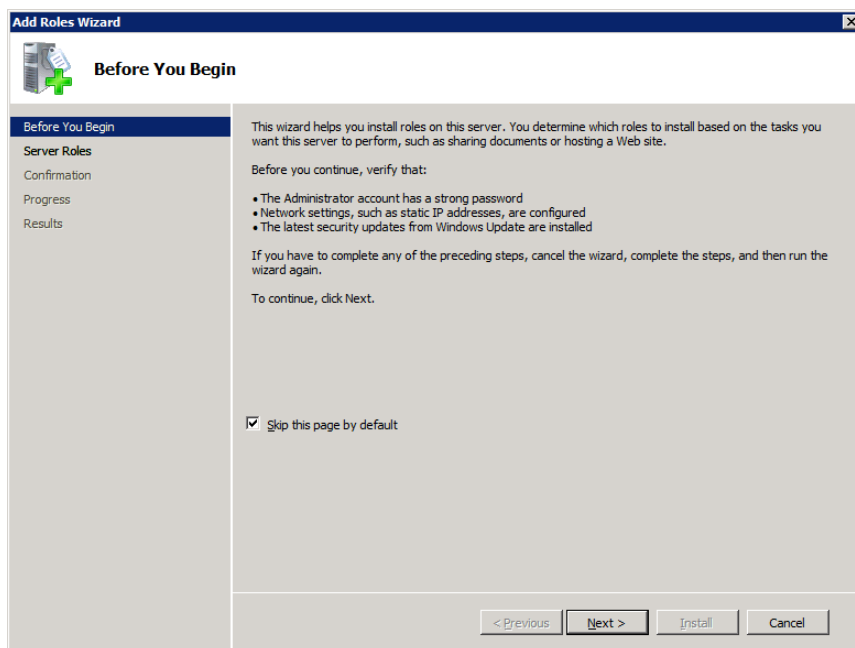


Εικ..3.64

Επιλέγοντας το “Roles” βλέπουμε ότι αρχικά δεν είναι κανένας ρόλος εγκατεστημένος.

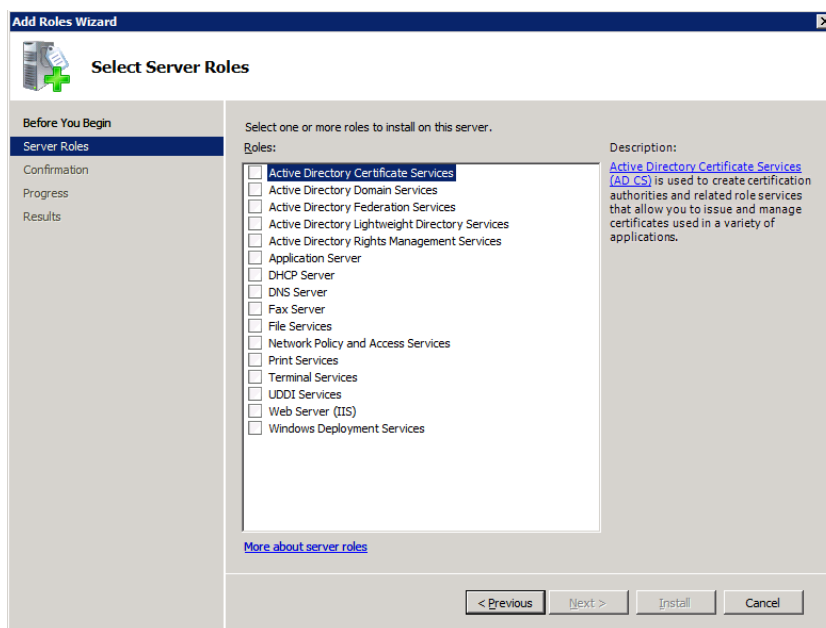
3.3 Εγκατάσταση Ρόλων

Πατώντας στο κουμπί “add roles” ξεκινάει ο ακόλουθος wizard προσθήκης ρόλων:



Εικ..3.65

Η πρώτη σελίδα είναι εντελώς πληροφοριακή και συμβουλευτική. Διαβάζοντάς την διαπιστώνουμε ότι τα τρία βήματα που λέει τα έχουμε ήδη εκτελέσει άρα προχωράμε παρακάτω πατώντας το Next.



Εικ..3.66

Πατώντας πάνω σε κάθε έναν από τους διαθέσιμους ρόλους, δεξιά μας δίνεται μια σύντομη περιγραφή με την δυνατότητα λήψης αναλυτικής βοήθειας. Με μια ματιά μπορούμε να δούμε βασικούς ρόλους όπως DNS, DHCP, ADDS, File Services, Print Services, Web Server, κ.λπ.

Συνοπτικά έχουμε διαθέσιμα τα ακόλουθα:

Όνομα Ρόλου	Περιγραφή
Active Directory Certificate Services	Ο ρόλος (AD CS) παρέχει προσαρμόσιμες υπηρεσίες για την έκδοση και διαχείριση ψηφιακών πιστοποιητικών σε συστήματα λογισμικού ασφαλείας που χρησιμοποιούν τις τεχνολογίες δημοσίου κλειδιού. Μπορείτε να χρησιμοποιήσετε τον ρόλο αυτό έτσι ώστε να δημιουργήσετε μία ή και περισσότερες αρχές πιστοποίησης (CA: Certification Authorities) ώστε να παραλάβετε αιτήματα πιστοποιητικών, να πιστοποιείτε τις πληροφορίες εντός των αιτημάτων και την ταυτότητα του αιτούντος, να εκδίδετε πιστοποιητικά, να ανακαλείτε πιστοποιητικά και να δημοσιεύετε τα δεδομένα ανάκλησης των πιστοποιητικών.

	Οι εφαρμογές που υποστηρίζονται από τον ρόλο ADCS είναι οι: Secure/Multipurpose Internet Mail Extensions (S/MIME), secure wireless networks, virtual private networks (VPN), IP security (IPSec), Encrypting File System (EFS), smart card logon, Secure Socket Layer/Transport Layer Security (SSL/TLS), και τέλος οι Ψηφιακές Υπογραφές.
Active Directory Domain Services	Ο ρόλος Active Directory Domain Services (AD DS) αποθηκεύει πληροφορίες σχετικά με χρήστες, υπολογιστές, και άλλες δικτυακές συσκευές. Ο ρόλος αυτός βοηθάει τους administrators να διαχειρίζονται με ασφάλεια όλους τους πόρους, διευκολύνει των διαμοιρασμό των πόρων και την συνεργασία μεταξύ των χρηστών. Ο ρόλος αυτός απαιτείται να εγκατασταθεί στο δίκτυο προκειμένου να εγκαταστήσουμε εφαρμογές που βασίζονται στο Active Directory όπως είναι ο Microsoft Exchange Server, και για την εφαρμογή άλλων τεχνολογιών Windows Server όπως είναι η Group Policy.
Active Directory Federation Services	Ο ρόλος Active Directory Federation Services (AD FS) παρέχει τεχνολογίες Web single-sign-on (SSO) έτσι ώστε να αυθεντικοποιεί έναν χρήστη σε πολλαπλές Web εφαρμογές χρησιμοποιώντας μόνο έναν λογαριασμό χρήστη. Ο AD FS το πετυχαίνει μέσω τις ασφαλούς διακίνησης ή και διαμοιρασμού, ταυτοτήτων χρηστών και δικαιώματα, σε μορφές ψηφιακών αιτημάτων, μεταξύ συνεργαζόμενων οργανισμών
Active Directory Lightweight Directory Services	Οι οργανισμοί που έχουν εφαρμογές που απαιτούν την ύπαρξη ενός καταλόγου (directory) για την αποθήκευση δεδομένων εφαρμογής, μπορούν να χρησιμοποιήσουν τον ρόλο Active Directory Lightweight Directory Services (AD LDS) ως τον αποθηκευτικό τους χώρο. Ο ρόλος AD LDS τρέχει και ως non-operating-system service. Για αυτό ο AD LDS δεν απαιτεί την εγκατάστασή του πάνω σε έναν

	<p>διαχειριστή τομέα (domain controller). Επειδή εκτελείται ως non-operating-system service επιτρέπεται να εκτελούνται ταυτόχρονα, στον ίδιο Server, πολλαπλές υλοποιήσεις (instances) του AD LDS, και κάθε ένα instance μπορεί να ρυθμιστεί ανεξάρτητα έτσι ώστε να εξυπηρετεί πολλαπλές εφαρμογές.</p>
Active Directory Rights Management Services (AD RMS)	<p>Ο ρόλος Active Directory Rights Management Services είναι μια τεχνολογία προστασίας της πληροφορίας που δουλεύει πολύ με όλες τις συνεργαζόμενες AD RMS - enabled εφαρμογές προκειμένου να βοηθήσει στην προστασία της ψηφιακής πληροφορίας από μη εξουσιοδοτημένη χρήση. Οι κάτοχοι της πληροφορίας μπορούν να καθορίσουν ακριβώς πως ένας παραλήπτης θα μπορεί να χρησιμοποιήσει την πληροφορία, π.χ. ποιος θα μπορεί να ανοίξει, αλλάξει, τυπώσει, προωθήσει, ή τι άλλες δράσεις θα μπορεί να εκτελέσει με την πληροφορία αυτή. Οι οργανισμοί μπορούν να δημιουργήσουν δικά τους προφίλ χρήσης όπως "Confidential – Read-Only" που μπορούν να εφαρμοστούν κατευθείαν στην πληροφορία όπως σε οικονομικές αναφορές, σε προδιαγραφές προϊόντων, δεδομένα πελατών, και μηνύματα ηλεκτρονικού ταχυδρομείου.</p>
Application Server	<p>Ο ρόλος του Application Server παρέχει μια πλήρη λύση για hosting και διαχείριση κατανεμημένων εφαρμογών υψηλής απόδοσης. Ολοκληρωμένες πληροφορίες όπως το .NET Framework, Web Server Support, Message Queuing, COM+, Windows Communication Foundation, και υποστήριξη Failover Clustering, βελτιώνουν την παραγωγικότητα σε όλο το εύρος ζωής της εφαρμογής, από τον σχεδιασμό και την ανάπτυξη μέχρι την εφαρμογή και την λειτουργία σε παραγωγικό περιβάλλον</p>
Dynamic Host Configuration	<p>Ο ρόλος του Dynamic Host Configuration Protocol (DHCP) δίνει τη δυνατότητα στους servers να αναθέτουν ή να</p>

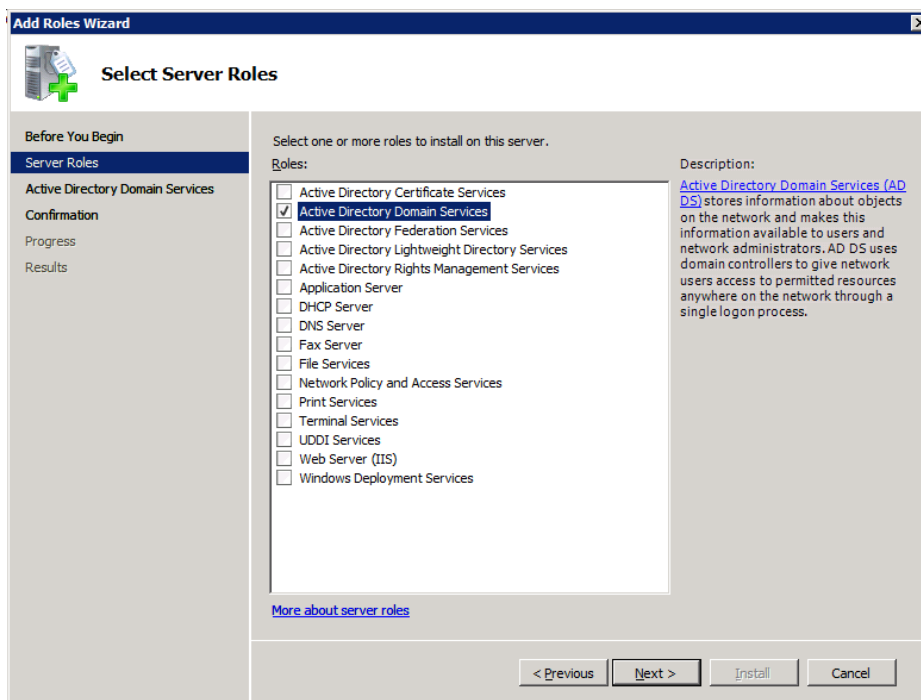
Protocol Server	<p>αναθέτουν για κάποια πεπερασμένη χρονική διάρκεια, διευθύνσεις IP σε υπολογιστές και άλλες δικτυακές συσκευές που είναι ενεργοποιημένες ως πελάτες DHCP. Εγκαθιστώντας DHCP servers στο δίκτυο αυτομάτως παρέχει στους υπολογιστές και σε άλλες δικτυακές συσκευές βασισμένες στο TCP/IP, έγκυρες διευθύνσεις IP και πρόσθετες παραμέτρους που πιθανόν να χρειάζονται αυτές οι συσκευές. Αυτές οι παράμετροι είναι γνωστές και ως DHCP options (παράμετροι DHCP), και τους επιτρέπουν να συνδέονται σε άλλους δικτυακούς πόρους όπως DNS servers, WINS servers, και routers.</p>
DNS Server	<p>Ο ρόλος Domain Name System (DNS) παρέχει μια τυποποιημένη διαδικασία συσχέτισμού ονομάτων με διευθύνσεις IP. Αυτός επιτρέπει στους χρήστες να αναφέρονται σε άλλους δικτυακούς πόρους χρησιμοποιώντας ονόματα που είναι εύκολο να θυμούνται αντί για σειρές από αριθμούς. Οι υπηρεσίες DNS των Windows, μπορούν να ενσωματωθούν με τις υπηρεσίες DHCP, εξαφανίζοντας την ανάγκη να δημιουργεί κάποιος εγγραφές DNS για κάθε συσκευή που θα προστίθεται στο δίκτυο.</p>
Fax Server	<p>Ο ρόλος του Fax Server στέλνει και λαμβάνει fax, και επιτρέπει την διαχείριση των fax με δημιουργία jobs, ρυθμίσεις, αναφορών και συσκευών fax στον Server ή δικτυακών.</p>
File Services	<p>Ο ρόλος File Services παρέχει τεχνολογίες για διαχείριση storage (αποθηκευτικών μέσων), αντιγραφή αρχείων, κατανομημένη διαχείριση χώρου ονομάτων, γρήγορη αναζήτηση αρχείων, και βελτιωμένη πρόσβαση σε αρχεία που βρίσκονται σε υπολογιστικά συστήματα βασισμένα σε UNIX.</p>
Hyper-V™	<p>Ο ρόλος Hyper-V παρέχει όλες τις υπηρεσίες που μπορείτε να χρησιμοποιήσετε για να δημιουργήσετε και να</p>

	<p>διαχειριστείτε εικονικά υπολογιστικά περιβάλλοντα και τους πόρους τους. Οι εικονικοί υπολογιστές μπορούν να λειτουργήσουν σε ένα απομονωμένο περιβάλλον λειτουργίας. Αυτό σου δίνει τη δυνατότητα να τρέχει πολλαπλά λειτουργικά συστήματα ταυτοχρόνως στον ίδιο server. Μπορείτε να χρησιμοποιήσετε ένα εικονικοποιημένο υπολογιστικό περιβάλλον για να βελτιώσετε την απόδοση των υπολογιστικών πόρων χρησιμοποιώντας περισσότερο και ποιο αποτελεσματικά το υλικό που διαθέτετε (hardware).</p>
Network Policy and Access Services	<p>Ο ρόλος Network Policy and Access Services παρέχει πολλές διαφορετικές μεθόδους για να δώσει στους χρήστες τοπική και απομακρυσμένη δικτυακή συνδεσιμότητα, για να συνδεθούν τμήματα δικτύων και να επιτραπεί στους δικτυακούς διαχειριστές (network administrators) να διαχειρίζονται κεντρικά πολιτικές δικτυακής πρόσβασης και πολιτικές υγείας πελάτη. Με την χρήση των Network Access Services, μπορείτε να υλοποιήσετε VPN servers, dial-up servers, routers, και 802.11-protected wireless access. Μπορείτε ακόμα να υλοποιήσετε RADIUS servers και proxies, και χρησιμοποιώντας το «Connection Manager Administration Kit» να δημιουργήσετε προφίλ απομακρυσμένης πρόσβασης ώστε να επιτρέψετε στους υπολογιστές των πελατών να συνδέονται στο δίκτυο.</p>
Print and Document Services	<p>Ο ρόλος Print and Document Services σας επιτρέπει να συγκεντρώσετε τις εκτυπώσεις των print server και των δικτυακών εκτυπωτών. Με αυτό το ρόλο, μπορείτε να παραλάβετε ψηφιοποιημένα έγγραφα από δικτυακούς scanners και να δρομολογήσετε τα έγγραφα σε κάποιο κοινόχρηστο δικτυακό πόρο, όπως σε ένα Windows SharePoint Services site, ή σε κάποιες διευθύνσεις e-mail.</p>
Remote Desktop Services	<p>Ο ρόλος “Remote Desktop Services” παρέχει τεχνολογίες που επιτρέπουν στους χρήστες να έχουν πρόσβαση σε</p>

	<p>προγράμματα που είναι εγκατεστημένα σε έναν remote desktop server, ή να έχουν πρόσβαση στην ίδια την επιφάνεια εργασίας των Windows, σχεδόν από οποιαδήποτε υπολογιστική συσκευή. Οι χρήστες μπορούν να συνδεόνται σε κάποιον remote desktop server για να εκτελούν προγράμματα και για να χρησιμοποιήσουν τους δικτυακούς πόρους του server αυτού.</p>
Web Server (IIS)	<p>Ο ρόλος Web Server (IIS) στα Windows Server 2008 R2 σας επιτρέπει τον διαμοιρασμό πληροφοριών με χρήστες στο διαδίκτυο και το τοπικό δίκτυο. Ο Windows Server 2008 R2 παρέχει τον IIS 7.5, που αποτελεί μια ενοποιημένη Web πλατφόρμα που έχει τον IIS, το ASP.NET, και το Windows Communication Foundation.</p>
Windows Deployment Services	<p>Ο ρόλος “Windows Deployment Services” μπορεί να χρησιμοποιηθεί για απομακρυσμένη εγκατάσταση και παραμετροποίηση των λειτουργικών συστημάτων Windows, σε υπολογιστές που έχουν Pre-boot Execution Environment (PXE) boot ROMs. Το κόστος διαχείρισης μειώνετε μέσω της χρήσης της WdsMgmt Microsoft Management Console (MMC) snap-in που διαχειρίζεται όλα τα θέματα και τις παραμέτρους του “Windows Deployment Services”. Ο ρόλος “Windows Deployment Services” παρέχει στους τελικούς χρήστες μια εμπειρία παρόμοια με το γνώριμο Windows Setup.</p>
Windows Server Update Services	<p>Ο ρόλος “Windows Server Update Services” επιτρέπει στους διαχειριστές δικτύου να καθορίζουν ποια Microsoft updates θα εγκατασταθούν, να δημιουργούν ομάδες υπολογιστών για τις διαφορετικές ομάδες από updates, και να παίρνουν αναφορές για την πρόοδο της εγκατάστασης των updates (ενημερώσεων) καθώς και πληροφορίες για τις ίδιες τις ενημερώσεις.</p>

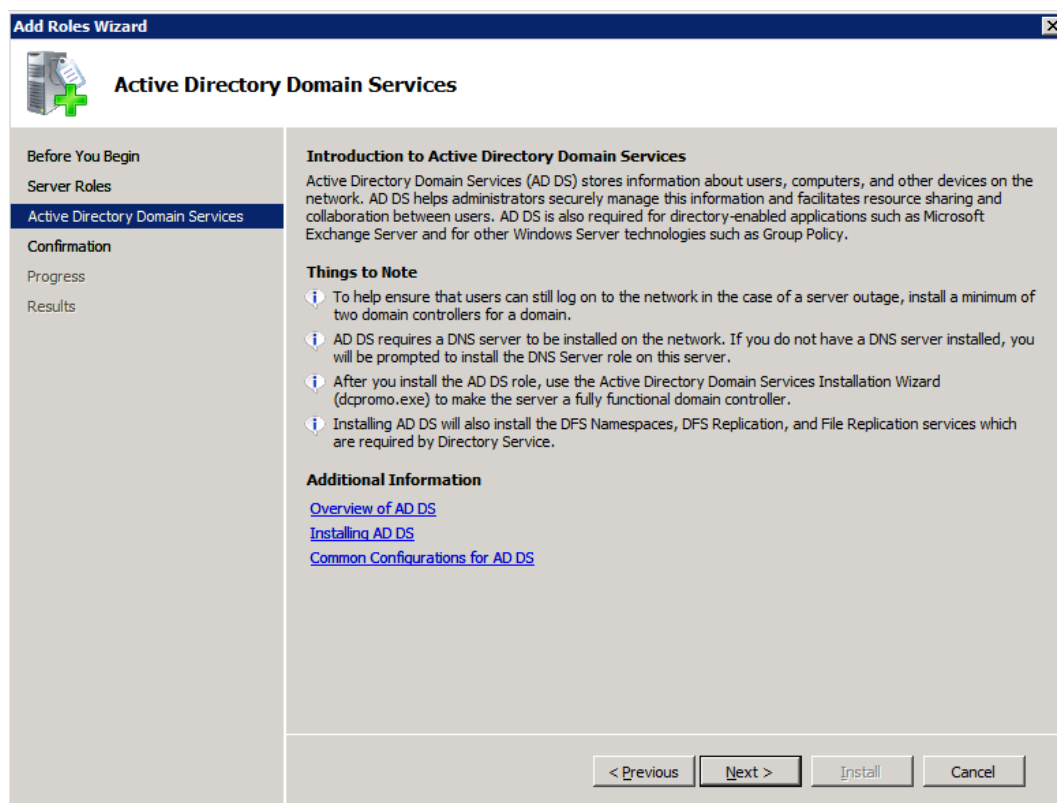
3.4 Εγκατάσταση Active Directory

Εμείς επιλέγουμε τον ρόλο Active Directory Domain Services όπως στην Εικ.3.67.



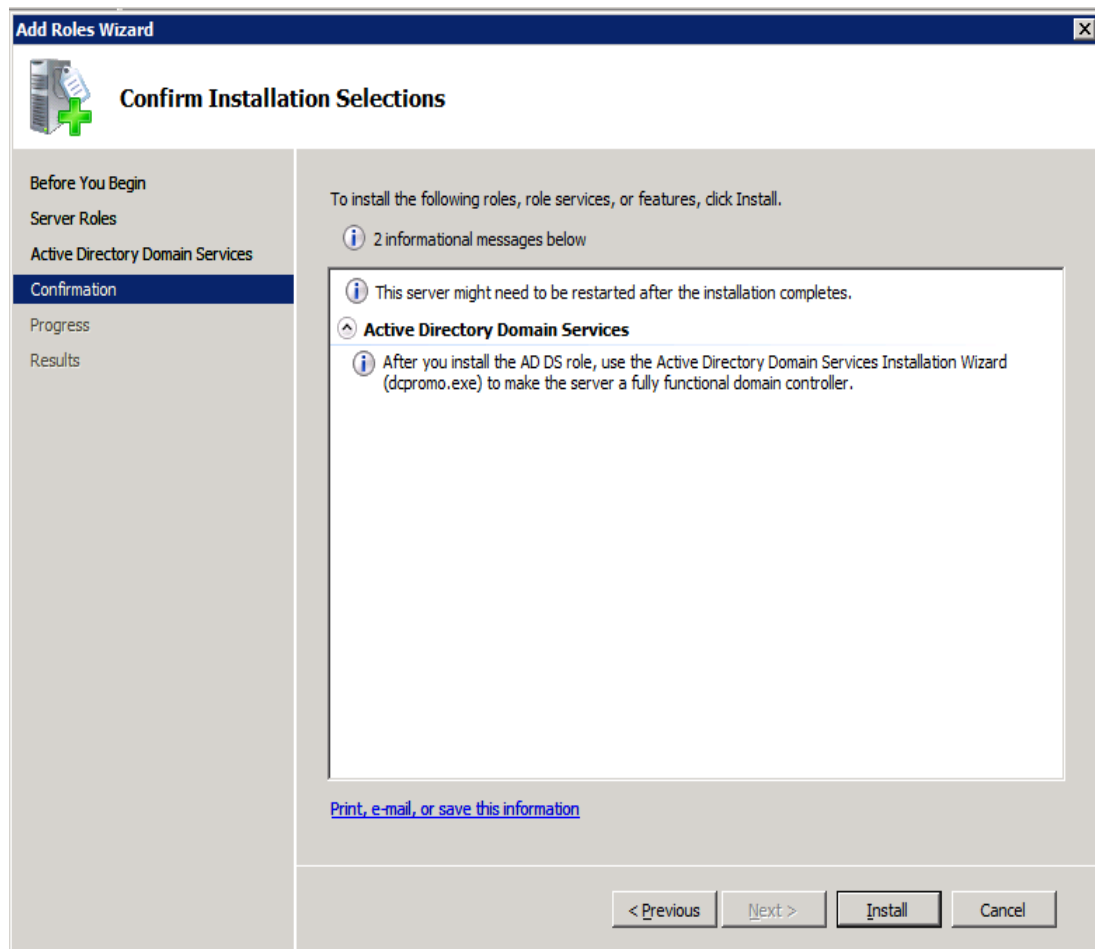
Εικ..3.67

Πατάμε το “Next” και διαβάζουμε τις συστάσεις της Microsoft για τον συγκεκριμένο ρόλο.



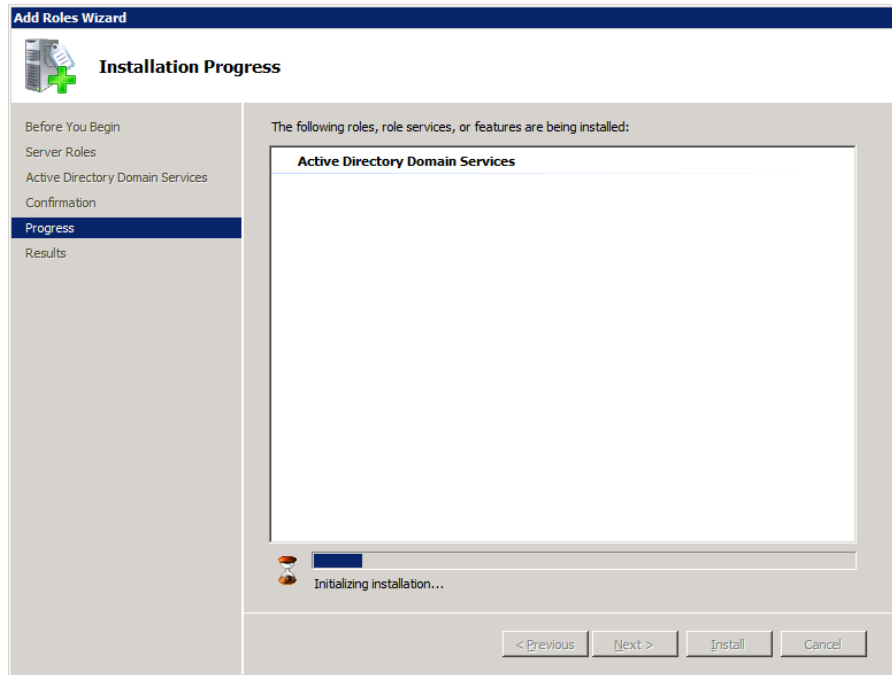
Εικ..3.68

Βασικότετη σύσταση είναι η ύπαρξη τουλάχιστον δύο domain controllers σε κάθε domain έτσι ώστε να εξασφαλίσουμε λειτουργία του domain ακόμα και σε πιθανή βλάβη του ενός από τους δύο. Βλέπουμε ακόμα ότι το ADDS βασίζεται στην υπηρεσία DNS, οπότε ο ρόλος θα εγκατασταθεί αυτόματα. Στην ουσία το ADDS δεν λειτουργεί χωρίς DNS, και σε περίπτωση που έχουμε βλάβη στο DNS θα έχουμε βλάβη και στο ADDS. Μετά την εγκατάσταση του ρόλου ADDS βλέπουμε ότι ξεκινάει αυτόματα η εκτέλεση του Active Directory Domain Services Installation Wizard το γνωστό σε όλους μας **“dcpromo.exe”** προκειμένου να γίνει ο server μας ένας πλήρως λειτουργικός domain controller. Πατάμε και πάλι Next (Εικ.3.68). Στην επιβεβαίωση της εγκατάστασης του ρόλου διαβάζουμε τα δύο ενημερωτικά μηνύματα που μας συνοψίζουν τις εργασίες που θα εκτελεστούν.



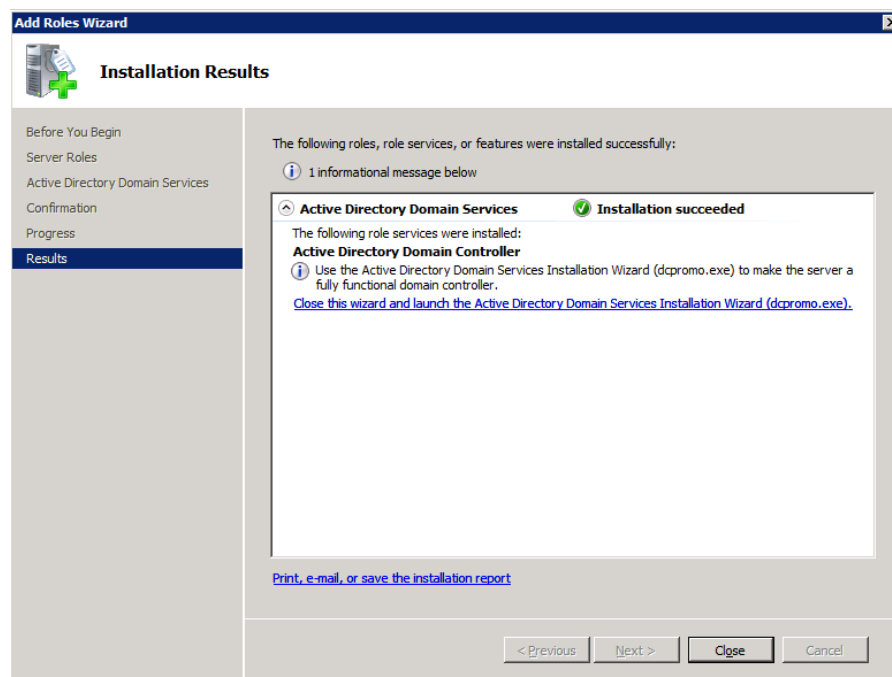
Εικ..3.69

Αναμένουμε επανεκκινήσεις του server και στο τέλος του wizard την ερώτηση για την εκκίνηση ενός δεύτερου wizard προκειμένου να τρέξει το dcpromo.exe. Πατώντας “Install” ξεκινάει η εγκατάσταση:



Εικ..3.70

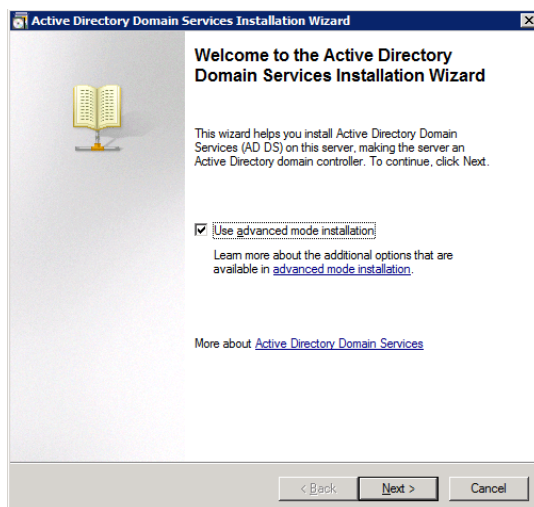
Η εγκατάσταση ολοκληρώνεται μετά από κάποιο χρόνο χωρίς άλλες ερωτήσεις ή ρυθμίσεις.



Εικ..3.71

Εδώ έχουμε δύο επιλογές: Η πρώτη είναι να πατήσουμε τα μπλε γράμματα και να τρέξει αυτοματοποιημένα το dcpromo.exe ή να πατήσουμε το “close” και να βγούμε από τον wizard και να εκτελέσουμε το dcpromo.exe από command line. Αυτή την

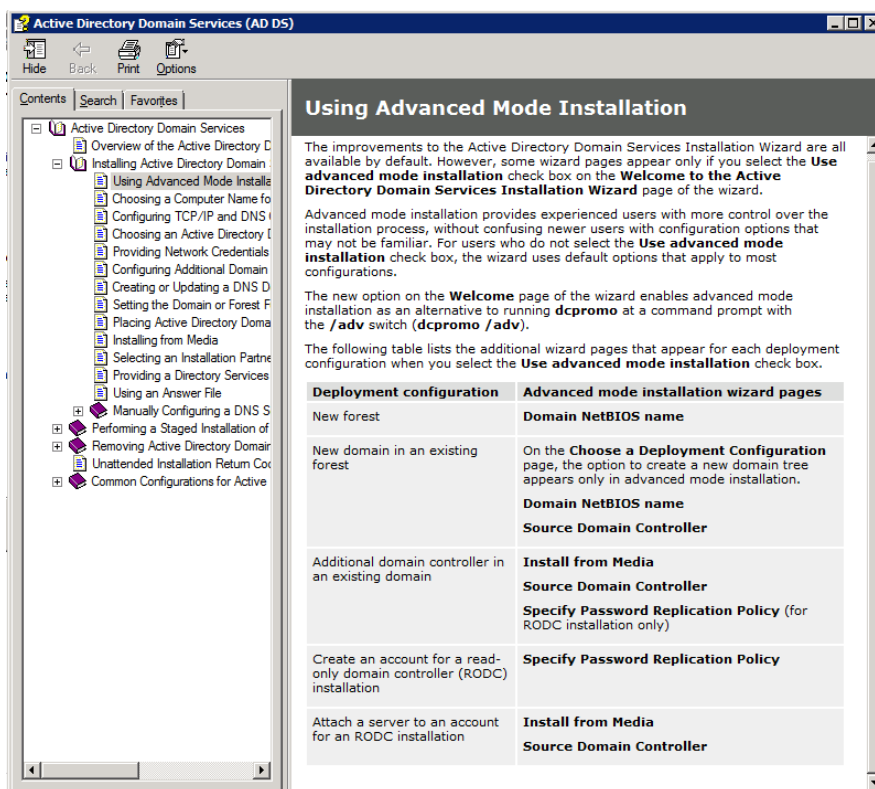
φορά θα πατήσουμε στα μπλε γράμματα: “Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe)”



Εικ.3.72

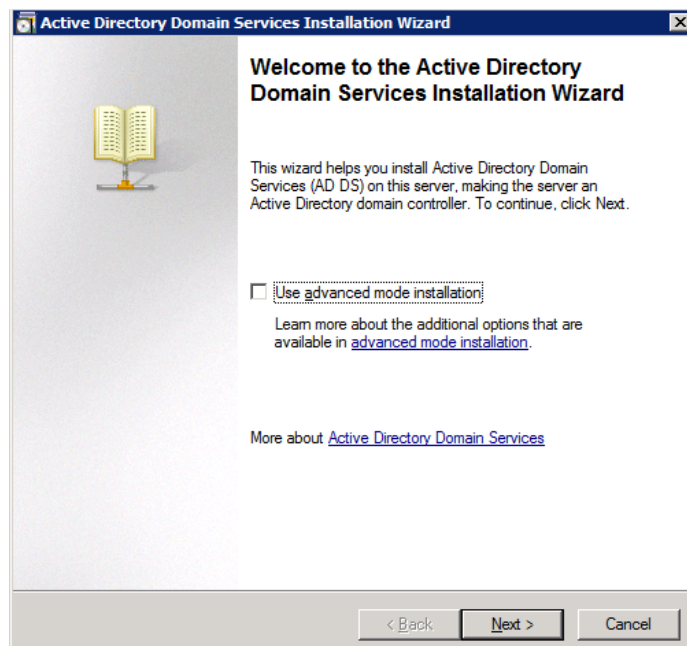
Πατώντας πάνω στο “advanced mode installation” παίρνουμε τις ακόλουθες πληροφορίες σχετικά με το προχωρημένο είδος της εγκατάστασης.

Η βοήθεια έρχεται σε πολλά επίπεδα και είναι αρκετά αναλυτική. Έχοντας τσεκαρισμένο το advanced στην ουσία είναι σαν να εκτελούμε το “dcpromo.exe /adv” από την γραμμή εντολών. Αν οι επιλογές που θέλουμε δεν είναι στο advanced, κλείνουμε την βοήθεια και επιστρέφουμε στην αρχική οθόνη επιλογής.



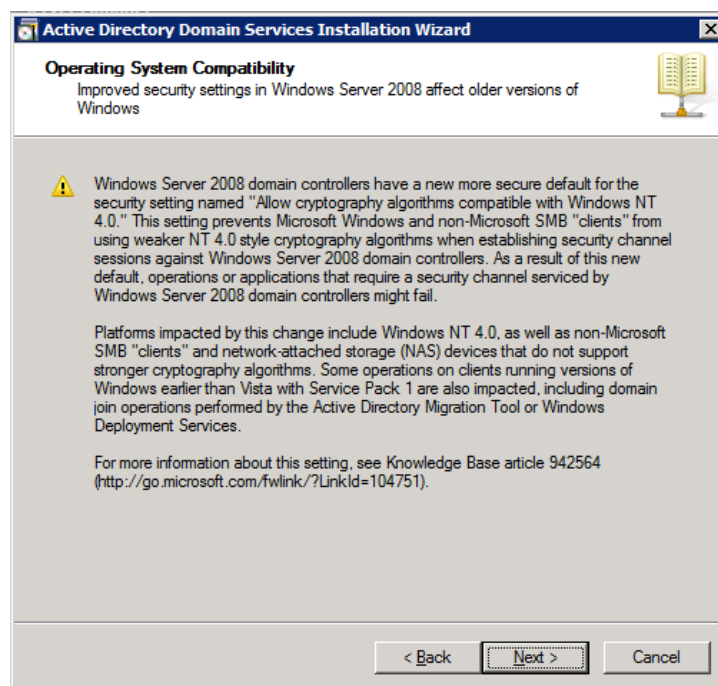
Εικ.3.73

Εμείς θα από-επιλέξουμε το “use advanced mode installation” ώστε να εκτελέσουμε μια τυπική εγκατάσταση του Active Directory.



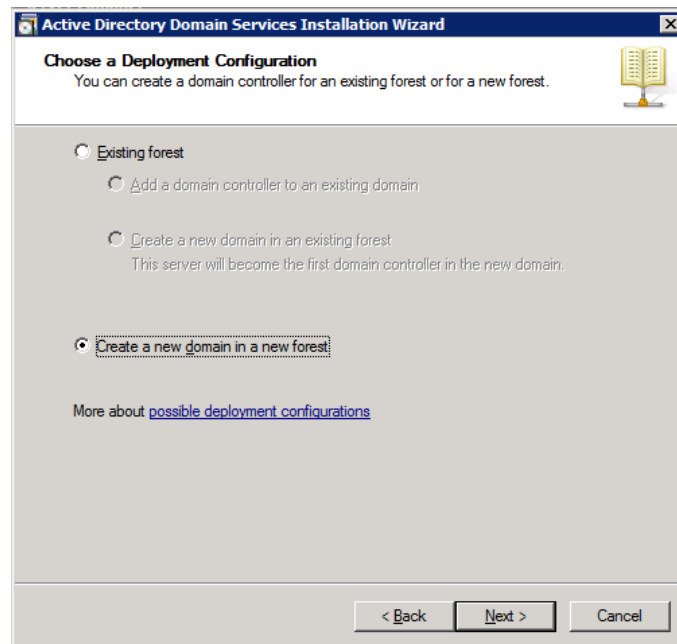
Εικ.3.74

Μετά βλέπουμε μια οθόνη προειδοποίησης (Εικ.3.75) που αφορά κυρίως την ύπαρξη servers με λειτουργικό NT 4.0 στο domain μας, αλλά και άλλα λειτουργικά Non-Microsoft, και κάποιες λειτουργίες σε πελάτες (clients) παλαιότερους από Vista με Service Pack 2. Εμείς δεν ανήκουμε σε κάποια τέτοια περίπτωση οπότε και προσπερνάμε την προειδοποίηση πατώντας το “Next”.



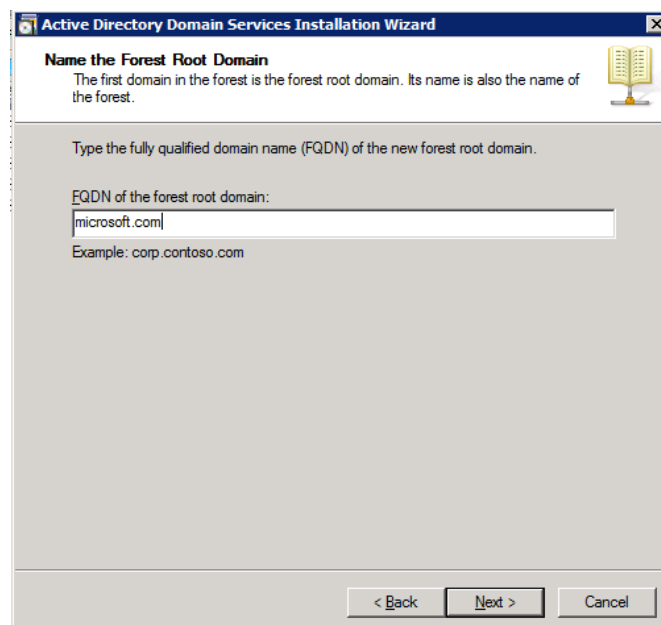
Εικ.3.75

Θέλουμε να δημιουργήσουμε ένα νέο “forest” και μέσα σε αυτό ένα νέο domain, οπότε επιλέγουμε την επιλογή “Create a new domain in a new forest”.



Εικ..3.76

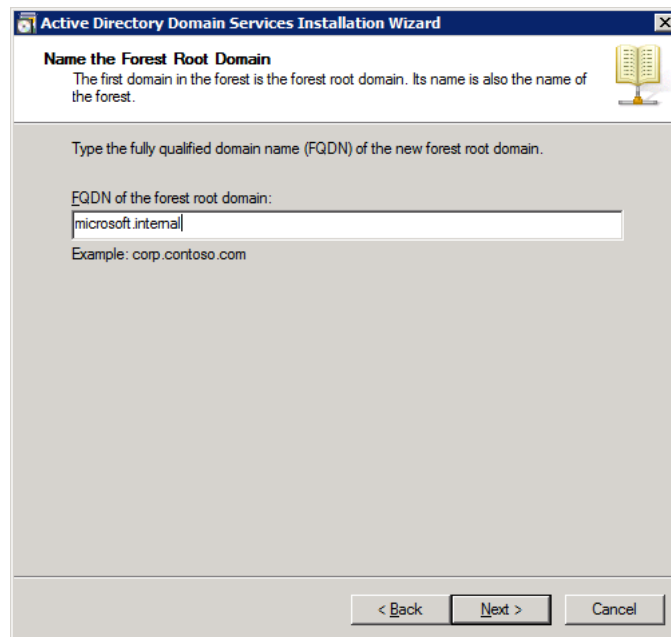
Εδώ πρέπει να γράψουμε το Fully Qualified Domain Name (FQDN) του forest root domain. Αν έχουμε αγοράσει κάποιο domain τότε το βάζουμε εδώ και περιμένουμε να περάσουμε τον έλεγχο. Για παράδειγμα θα μπορούσαμε να βάζαμε “microsoft.com” αν μας ανήκε το domain αυτό.



Εικ..3.77

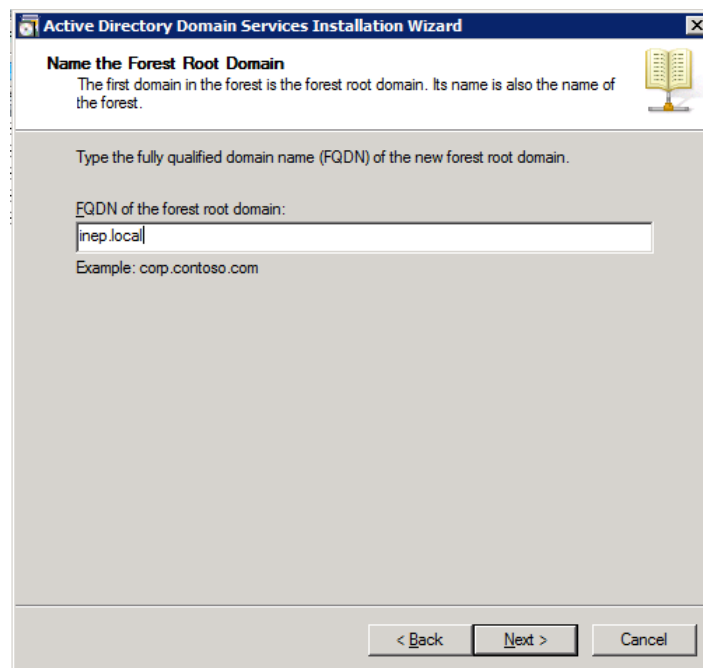
Επειδή προφανώς δεν μας ανήκει, θα μπορούσαμε να δημιουργούσαμε ένα domain με ότι όνομα θέλουμε χρησιμοποιώντας καταλήξεις της μορφής “.local” ή “.internal”.

Έτσι ενώ το όνομα “microsoft.com” είναι μη αποδεκτό για προφανείς λόγους, το όνομα domain “microsoft.internal” είναι μια εντελώς αποδεκτή επιλογή.



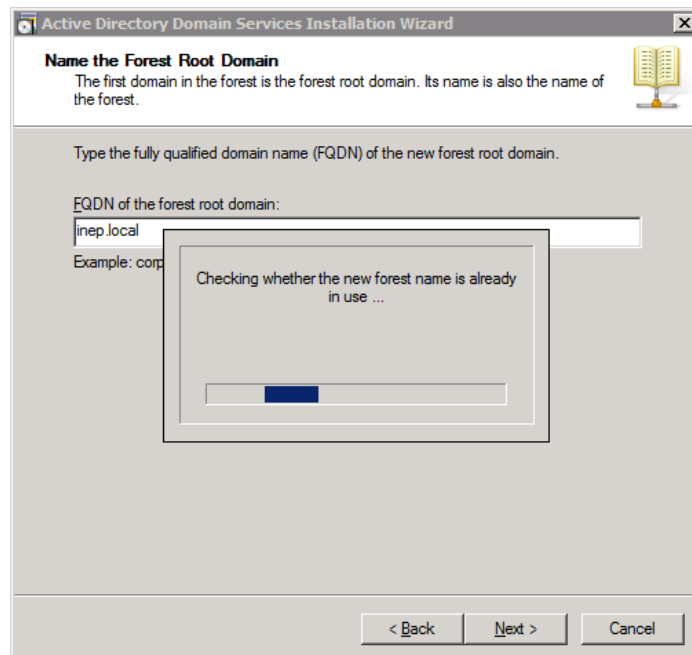
Εικ.3.78

Εμείς στην περίπτωση μας θα δημιουργήσουμε το “inep.local” οπότε και το δίνουμε ως επιλογή στο σημείο αυτό και πατάμε “Next” όπως στην Εικ.3.79.



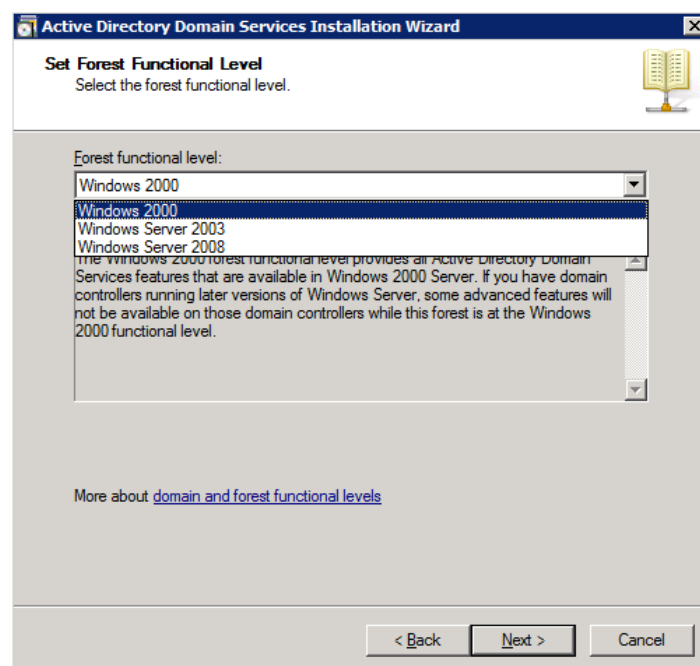
Εικ.3.79

Γίνεται ο τυπικός έλεγχος για πιθανή χρήση του domain name που δώσαμε. Δεν έχει και πολύ νόημα αν το domain είναι της μορφής “.local” ή “.internal” ή κάτι άλλο το οποίο δεν αντιστοιχεί σε πραγματική κατάληξη domain.



Εικ..3.80

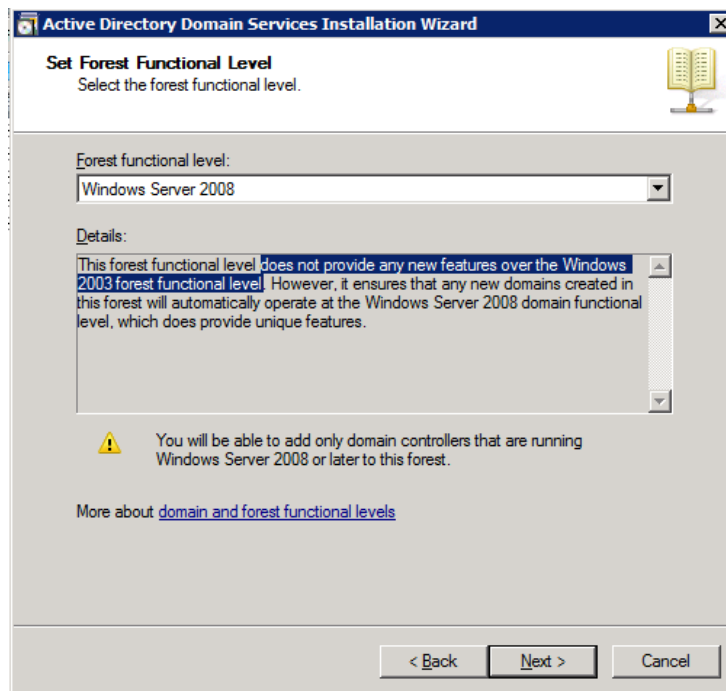
Στη συνέχεια επιλέγουμε το functional level του forest μας. Αυτό γίνεται βάσει των εγκατεστημένων μηχανημάτων που έχουμε διαθέσιμα. Συνιστάται η χρήση του functional level σε επίπεδο “Windows Server 2008”.



Εικ..3.81

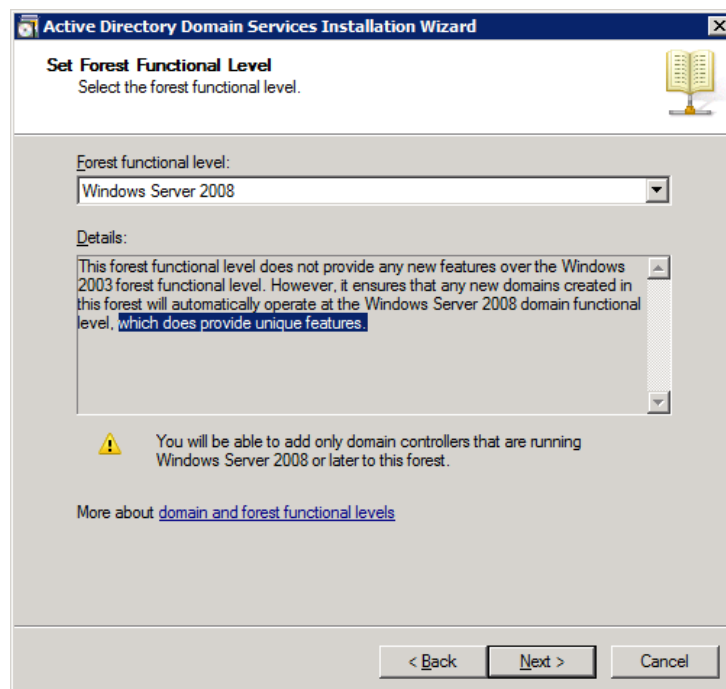
Επιλέγοντας το συνιστώμενο “Windows Server 2008” διαβάζουμε την προειδοποίηση της Microsoft. Λίγο διαφορετική αλλά καταλαβαίνουμε ότι είναι και η επιθυμητή. Προσοχή χρειάζεται μόνο στο σημείο με το θαυμαστικό που λέει ότι δεν θα μπορούμε να χρησιμοποιήσουμε domain controllers που τρέχουν σε Windows Server 2003. Σε

κάποιες περιπτώσεις migration επιλέγουμε το level 2003, και αφού ολοκληρωθεί η διαδικασία κάνουμε raise το επίπεδο του domain μας σε 2008. Πατάμε “Next” για να συνεχίσουμε:



Εικ..3.82

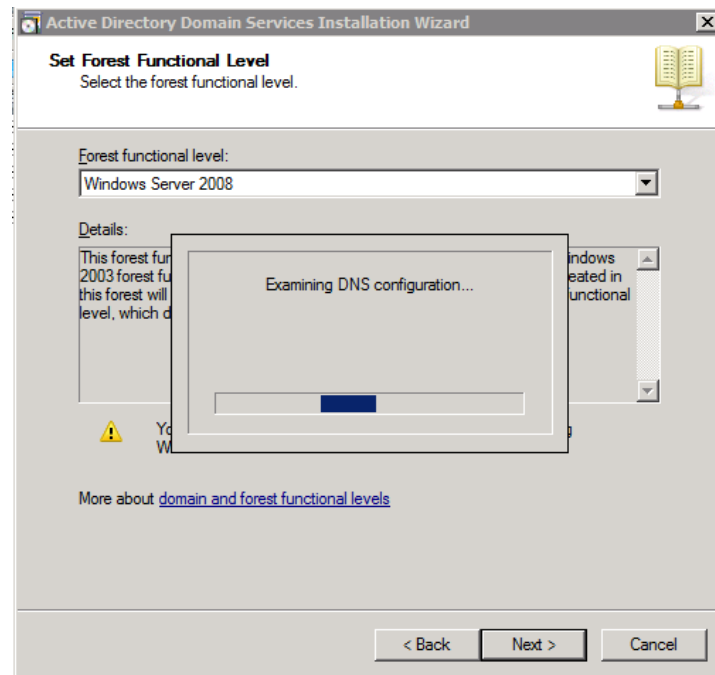
Πατάμε “Next” και προχωράμε στην εγκατάσταση σε επίπεδο “Windows 2008”.



Εικ..3.83

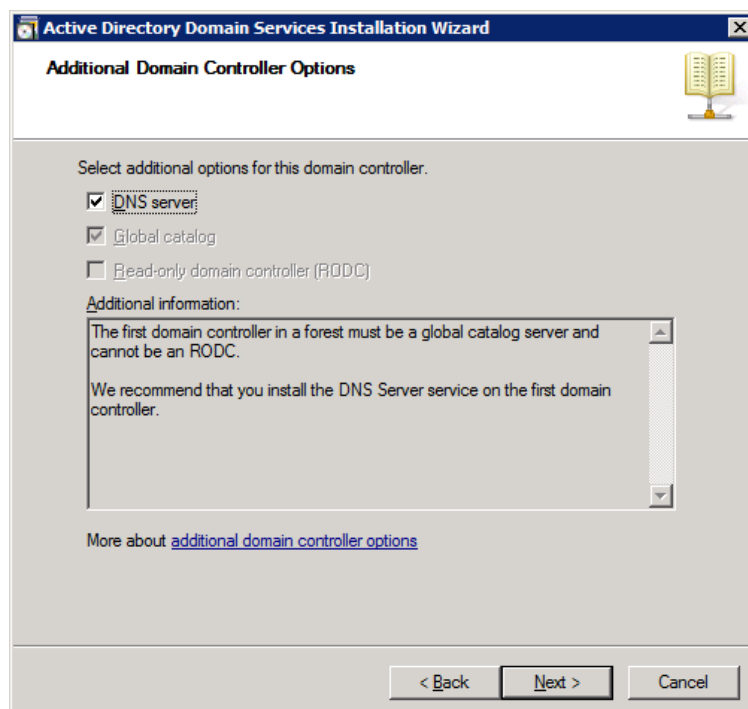
Εξετάζονται οι ρυθμίσεις για το DNS ώστε να διασφαλίσει ότι είναι σωστά ρυθμισμένο και λειτουργεί. Σε περίπτωση που δεν υπάρχει ήδη άλλος DNS τότε θα

πρέπει να εγκατασταθεί στον ίδιο τον domain controller το οποίο αποτελεί και best practice.



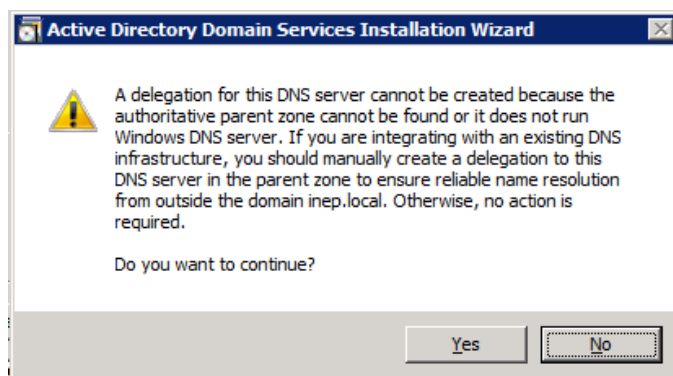
Εικ..3.84

Στην περίπτωση μας δεν έχουμε άλλον DNS Server, οπότε επιλέγουμε να εγκατασταθεί και να ρυθμιστεί ο DNS στον Server μας. Παρατηρούμε ότι επειδή στήνουμε τον πρώτο domain controller στο domain μας, ο server αυτός θα είναι υποχρεωτικά και Global Catalog.



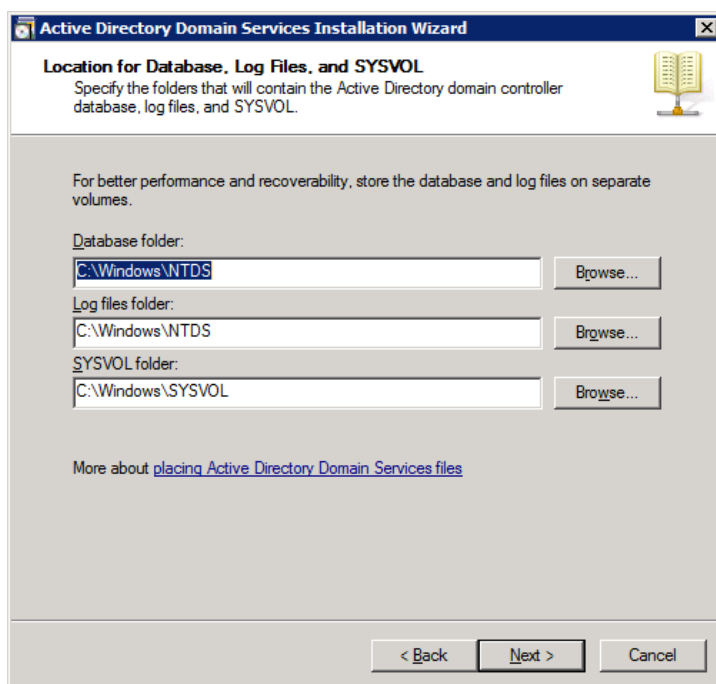
Εικ..3.85

Πατώντας Next, παίρνουμε άλλη μια προειδοποίηση που αγνοούμε με ασφάλεια.



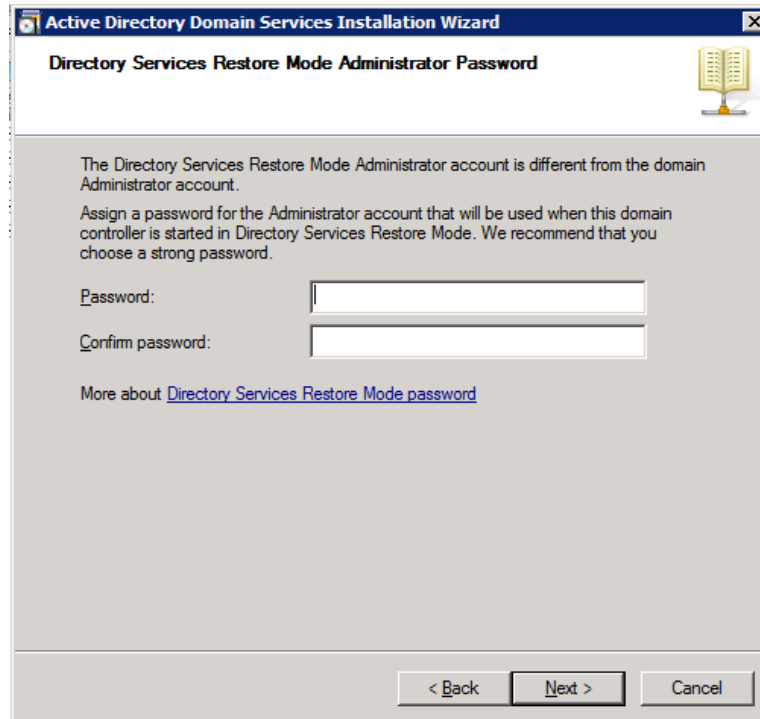
Εικ..3.86

Πατάμε “Yes” και συνεχίζουμε με τον “wizard” μας. Εδώ ζητάει να ρυθμίσουμε τους φακέλους με το Database, τα Log-Files και το SYSVOL. Καλή πρακτική σε servers με πολλούς πραγματικούς δίσκους, είναι να βρίσκονται σε διαφορετικό σύστημα δίσκων, και όχι απλά σε διαφορετικό partition, από την εγκατάσταση του λειτουργικού έτσι ώστε να δουλεύουν πιο γρήγορα. Εμείς θα τις αφήσουμε τις ρυθμίσεις αυτές ως έχουν.



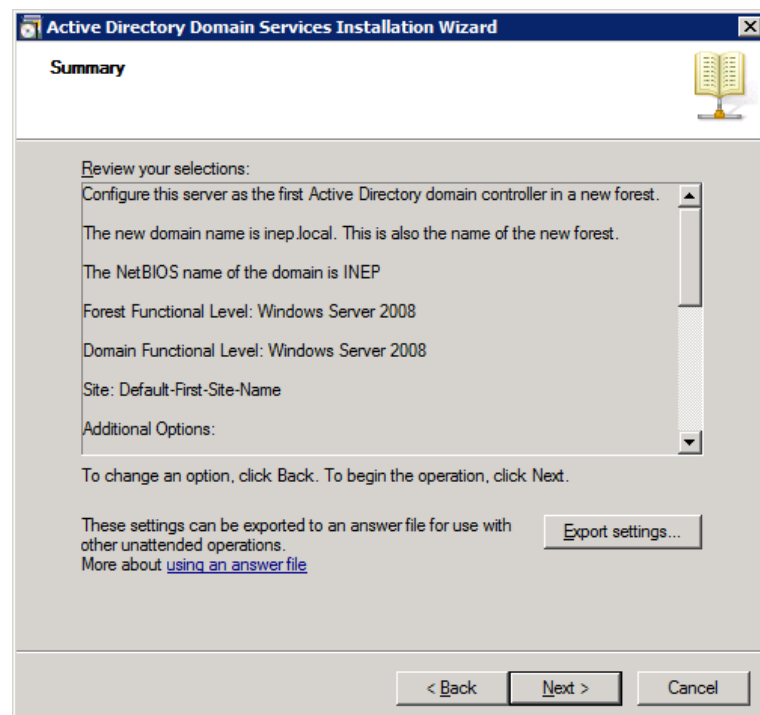
Εικ..3.87

Εδώ πρέπει να δηλώσουμε έναν **βασικότατο κωδικό ασφαλείας** ο οποίος ίσως να μην χρειαστεί και ποτέ, αλλά αν χρειαστεί και δεν τον έχουμε θα έχουμε καταστρέψει όλο το domain. Δίνουμε έναν κωδικό για το Restore Mode τον οποίο και τον σημειώνουμε κάπου φροντίζοντας να μην τον χάσουμε ή τον ξεχάσουμε. Ο κωδικός αυτός **δεν** αλλάζει στη συνέχεια.



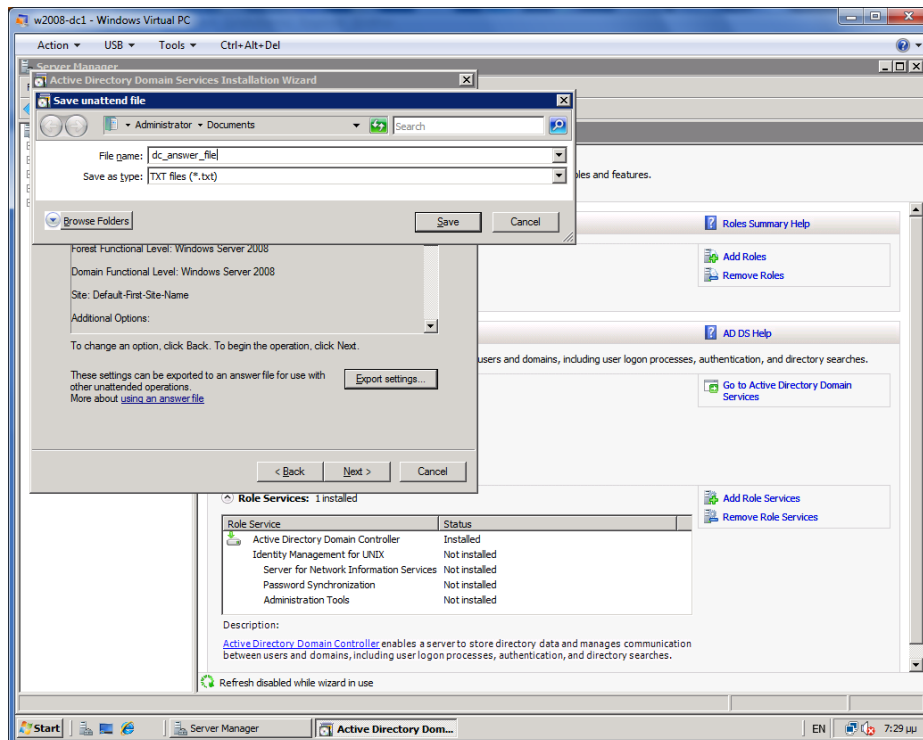
Εικ..3.88

Εδώ έχουμε μια σύνοψη όλων των εργασιών που θα εκτελεστούν, την οποία και καλό είναι να την κάνουμε export ώστε να την έχουμε.



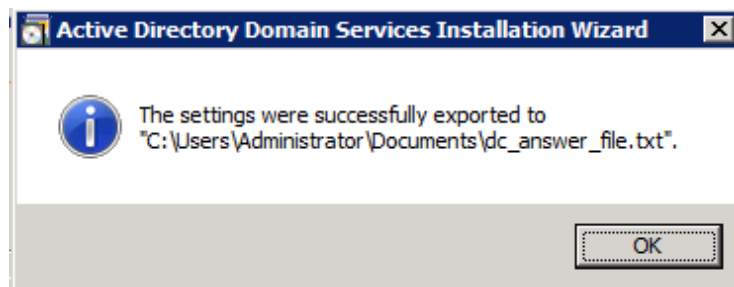
Εικ..3.89

Πατώντας “export settings” αποθηκεύουμε με την ονομασία “dc_answer_file.txt” ένα αρχείο κειμένου τις εργασίες που θα εκτελεστούν.



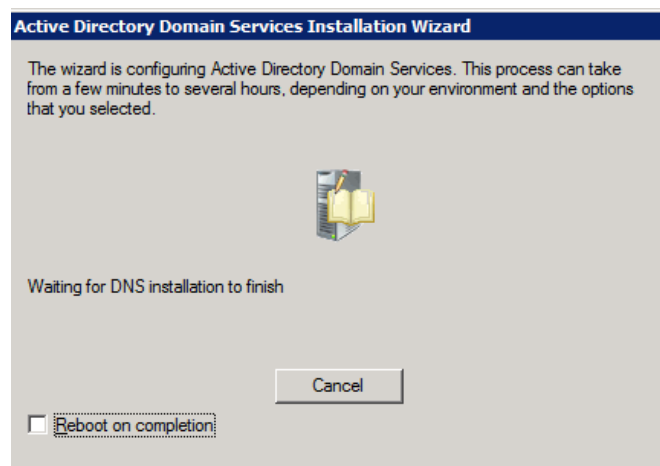
Εικ..3.90

Μόλις λάβουμε το ακόλουθο μήνυμα επιβεβαίωσης:



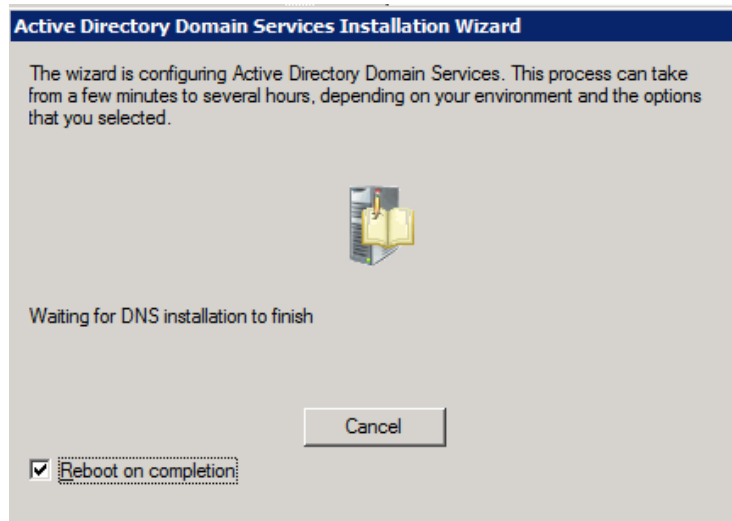
Εικ..3.91

Πατάμε “ok” για να κλείσουμε το παράθυρο αυτό και μετά πατάμε “Next” για να προχωρήσουμε στην εγκατάσταση.



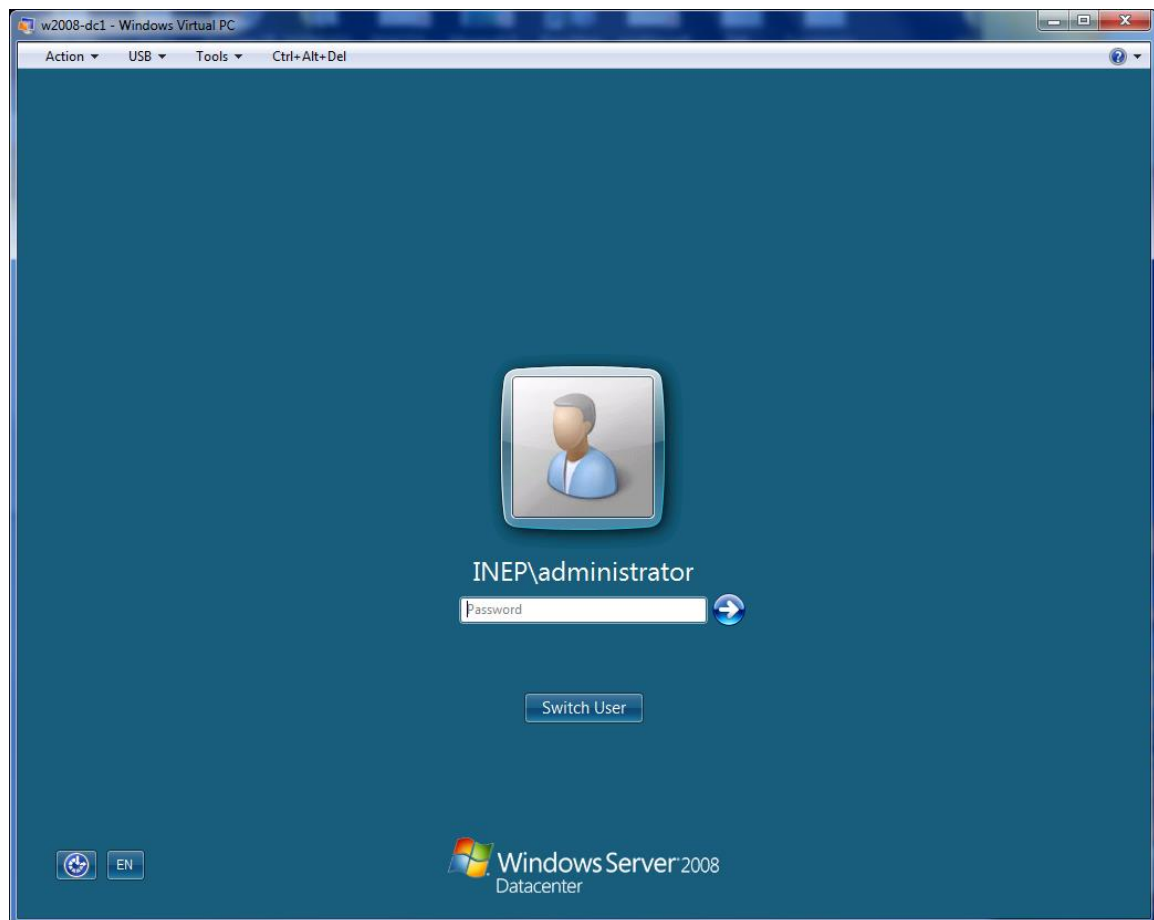
Εικ..3.92

Όσο περιμένουμε την εγκατάσταση του DNS να ολοκληρωθεί, επιλέγουμε το “Reboot on completion” έτσι ώστε να γίνει αυτόματα επανεκκίνηση του server με την ολοκλήρωση των ρυθμίσεων.



Εικ..3.93

Ο server κάποια στιγμή κάνει επανεκκίνηση και μετά την ολοκλήρωση του φορτώματος εμφανίζει την ακόλουθη οθόνη:



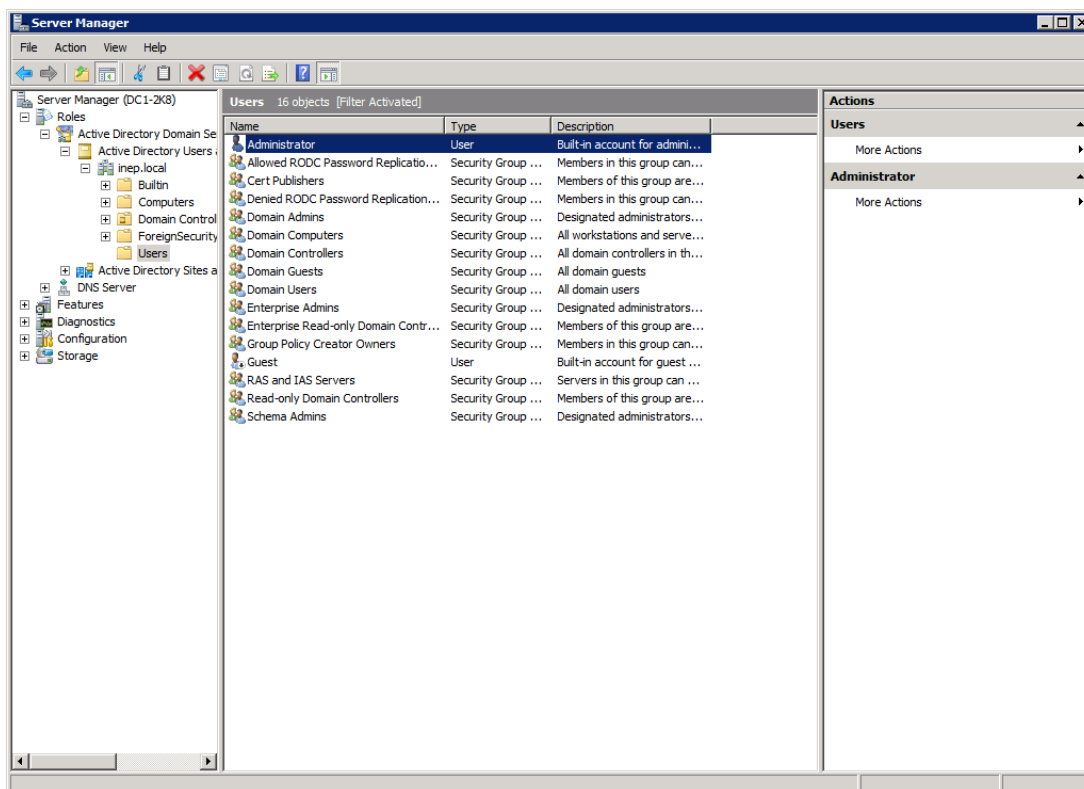
Εικ..3.94

Βλέπουμε ότι το όνομα για Login έχει γίνει **“INEP\administrator”** το οποίο είναι ισοδύναμο με το **“administrator@INEP”** και αναφέρεται πλέον στον διαχειριστή (administrator) του domain. Ο τοπικός διαχειριστής του Server έχει «γίνει» πλέον διαχειριστής του domain. **Προσοχή: Στον domain controller ΔΕΝ υπάρχουν τοπικοί χρήστες...**

Γράφουμε τον κωδικό του τοπικού administrator ο οποίος τώρα θα ισχύει για τον administrator του domain και είτε πατάμε Enter είτε κάνουμε κλικ στο βελάκι που δείχνει δεξιά. Ο κωδικός επαληθεύεται και κάνουμε login στον server.

Ανοίγει αυτόματα ο **“Server Manager”** και από τις επιλογές που υπάρχουν στο αριστερό τμήμα της οθόνη κάνουμε ανάπτυξη των **“Roles”**, και του **“Active Directory Domain Services”** που είναι και ο ρόλος που εγκαταστήσαμε. Εν συνεχεία αναπτύσσουμε το **“Active Directory Users and Computers”** όπου από κάτω βλέπουμε την ύπαρξη του domain μας όπως ακριβώς το ονομάσαμε, δηλαδή **“inep.local”**.

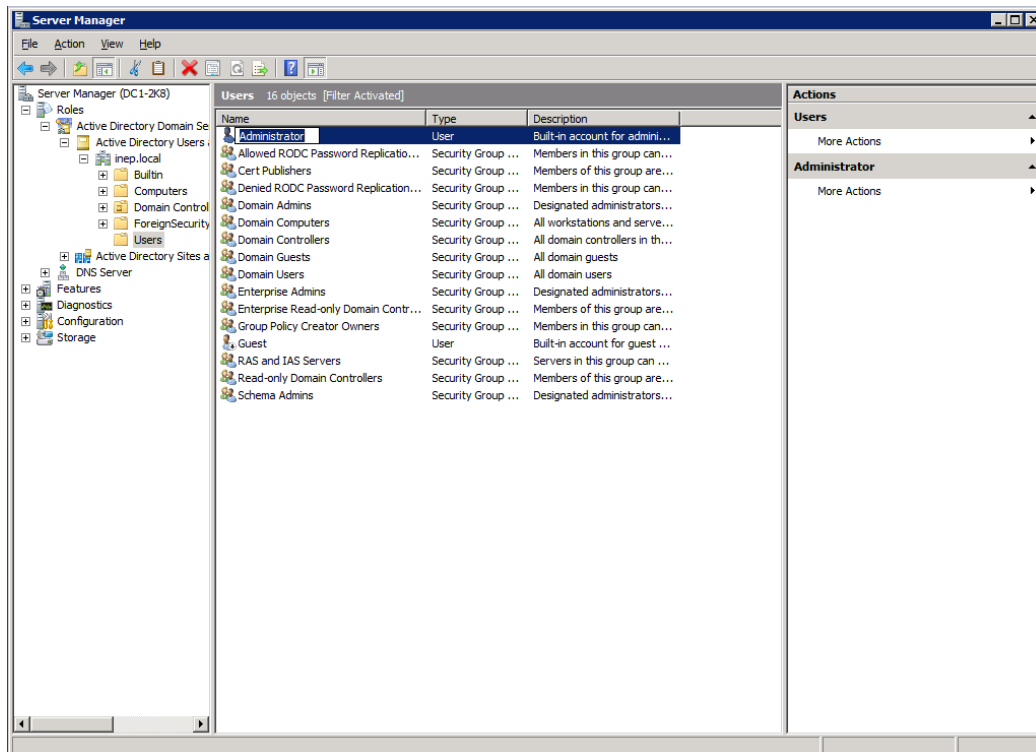
Παρατηρούμε ότι υπάρχουν πέντε βασικά containers τα: **Builtin**, **Computers**, **Domain Controllers**, **ForeignSecurity Principles** και το **Users**. Πατάμε μέσα στο **Users**, όπου βλέπουμε τους προκαθορισμένους λογαριασμούς χρηστών (default accounts).



Εικ.3.95

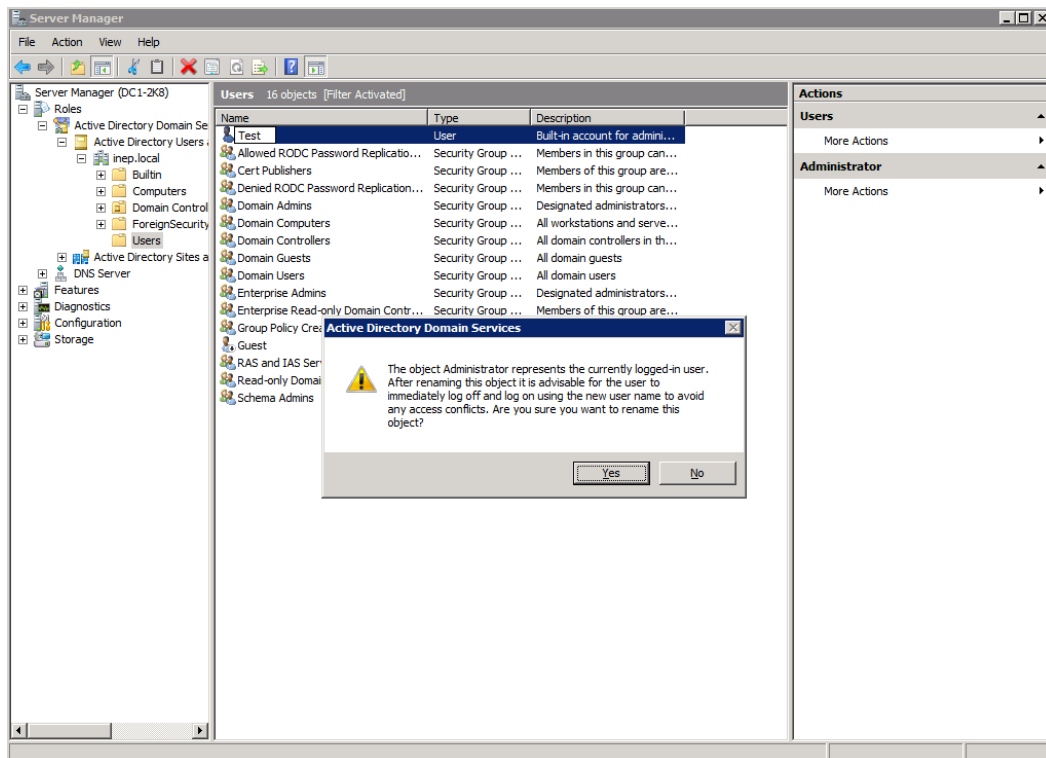
Για λόγους ασφαλείας κάνουμε δεξί κλικ πάνω στον πρώτο λογαριασμό που υπάρχει πρώτος στην λίστα που δεν είναι άλλος από τον λογαριασμό του διαχειριστή

(administrator) του domain, και επιλέγουμε Rename.



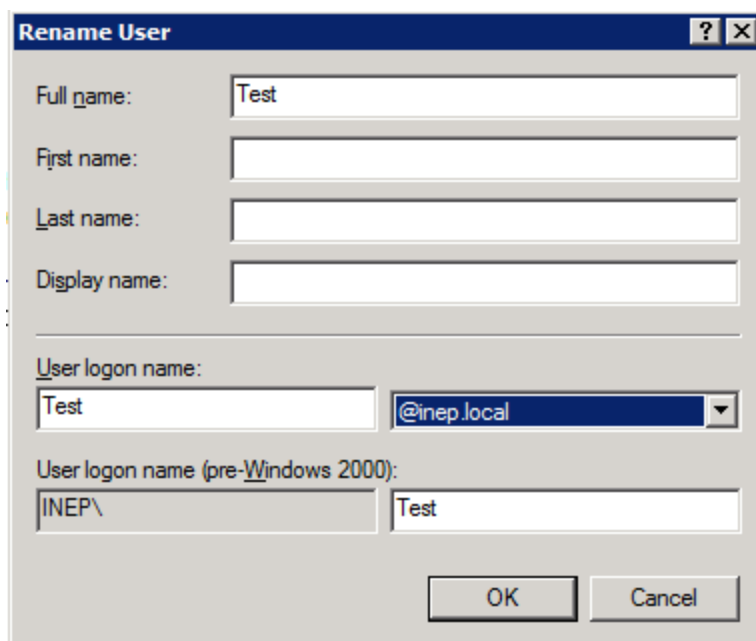
Εικ.3.96

Δίνουμε ένα όνομα διαφορετικό, με στόχο να μην προδίδει τα ιδιαίτερα δικαιώματα που έχει ο συγκεκριμένος λογαριασμός και να αποπροσανατολίζει τους επίδοξους εισβολείς. Ας ονομάσουμε λοιπόν τον λογαριασμό Test.



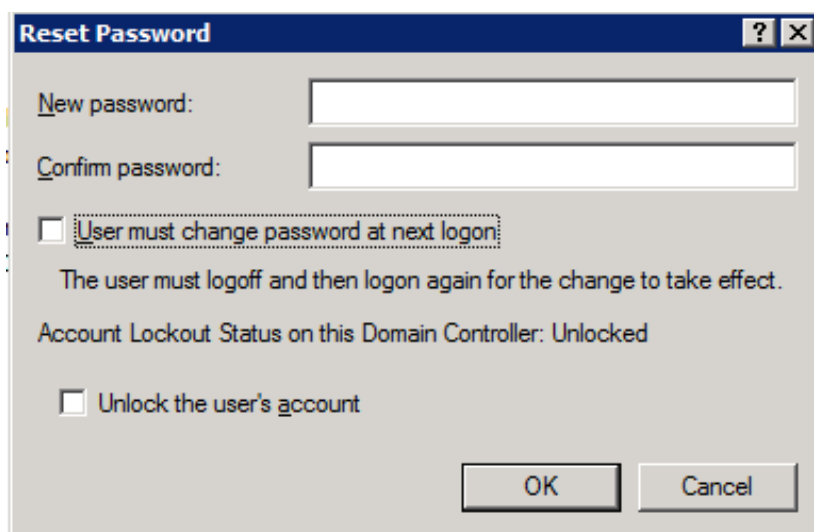
Εικ.3.97

Πατάμε yes, στην ειδοποίηση και συμπληρώνουμε όλα τα στοιχεία στο ακόλουθο παράθυρο, χωρίς να παραλείψουμε τα δύο “User logon name” και την επιλογή του domain “@inep.local”



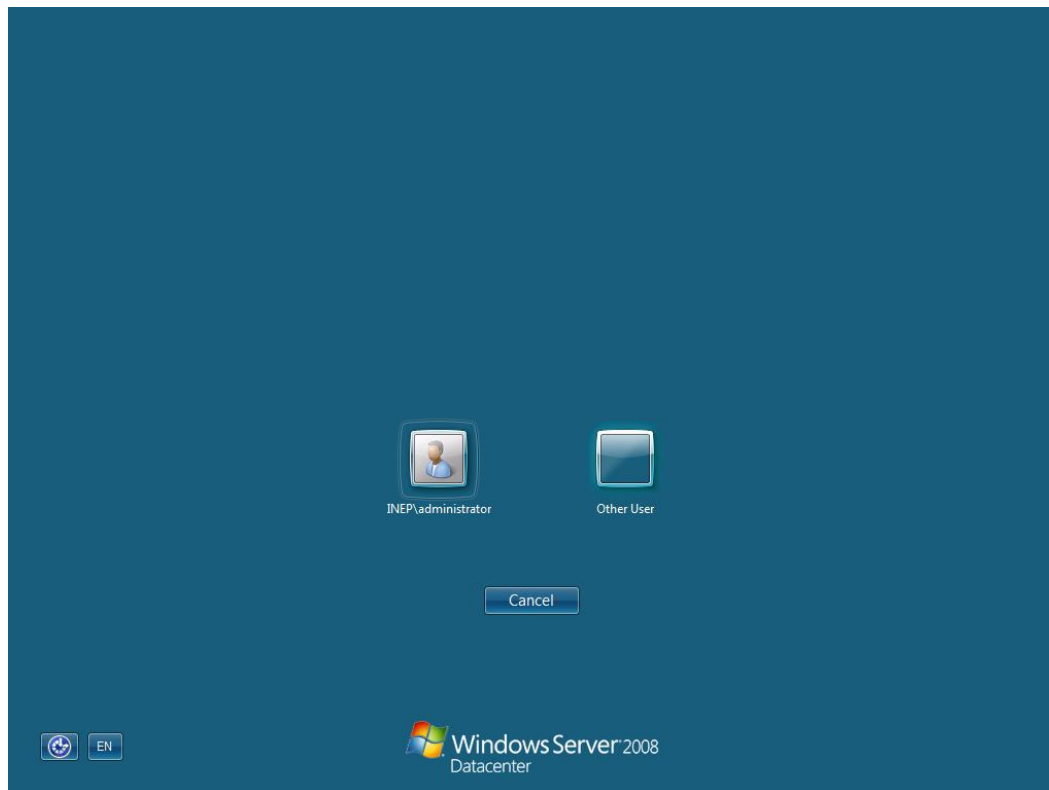
Εικ.3.98

Μετά με δεξί κλικ πάνω στον user Test, του αλλάζουμε τον κωδικό επιλέγοντας “Reset Password”. Παρατηρούμε ότι μπορούμε να αλλάξουμε κωδικό σε έναν χρήστη και να τον εξαναγκάσουμε να δηλώσει καινούριο κωδικό μόλις κάνει logon την αμέσως επόμενη φορά επιλέγοντας το “User must change password at next logon”, ή να ξεκλειδώσουμε κάποιον κλειδωμένο λογαριασμό χρήστη από το “Unlock the user’s account”



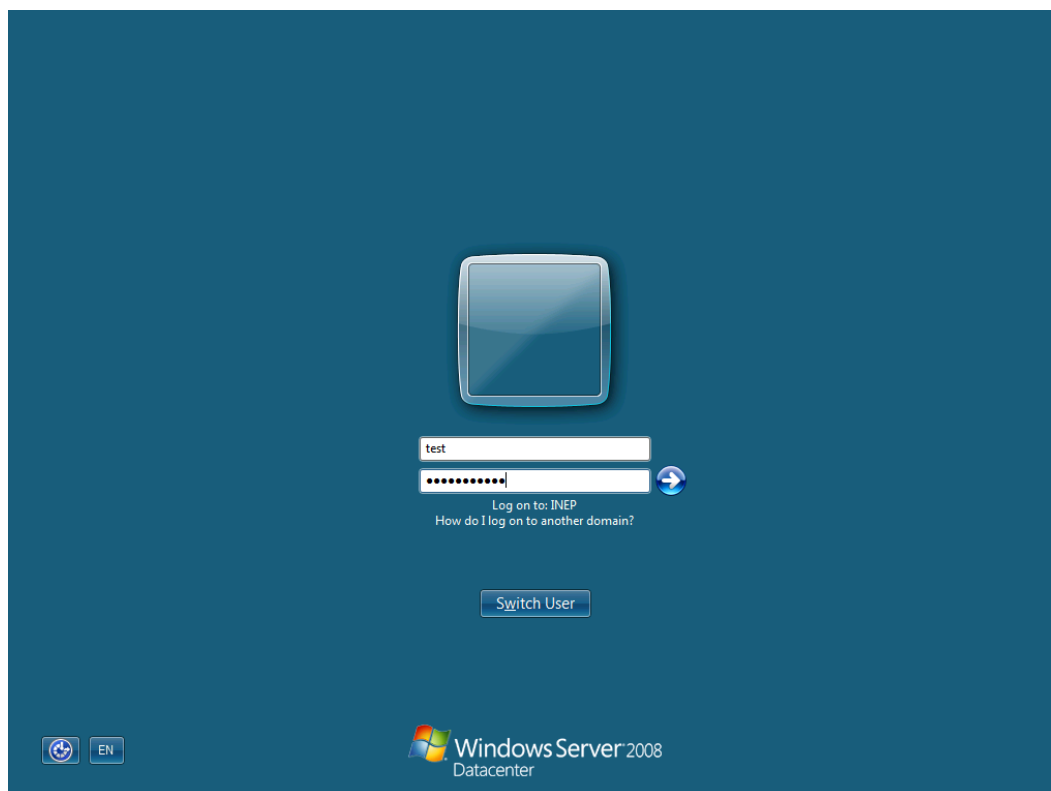
Εικ.3.99

Στην συνέχεια κλείνουμε όλα τα ενεργά παράθυρα και κάνουμε logout:



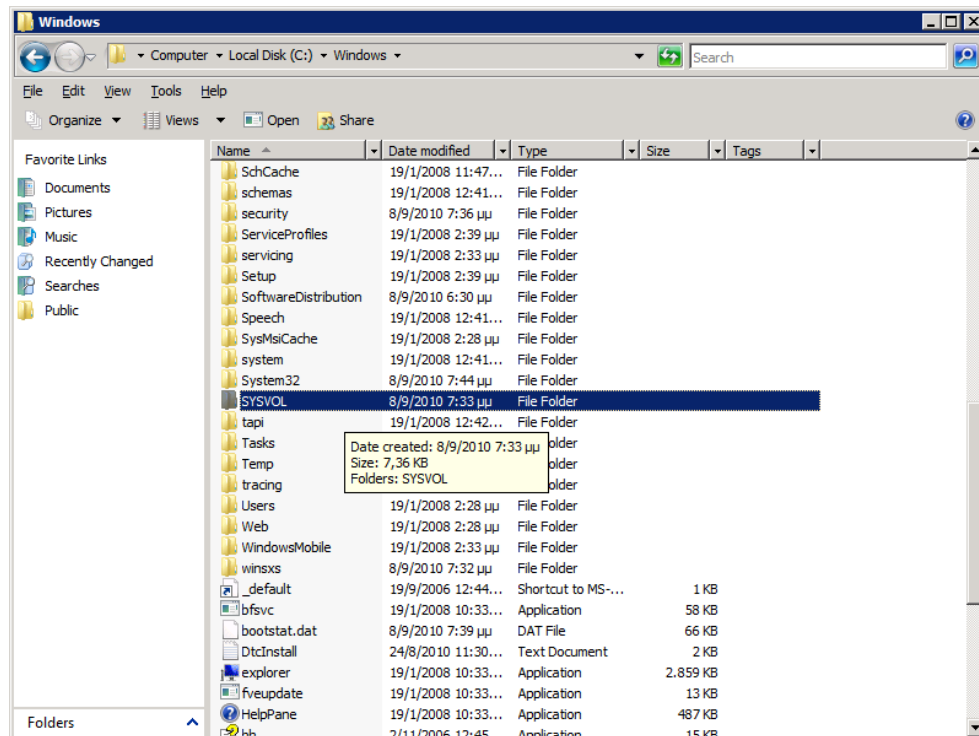
Εικ..3.100

Το account INEP\administrator δεν υπάρχει πλέον, οπότε επιλέγουμε το “Other User” και κάνουμε Logon ως test με τον καινούριο κωδικό που θέσαμε.



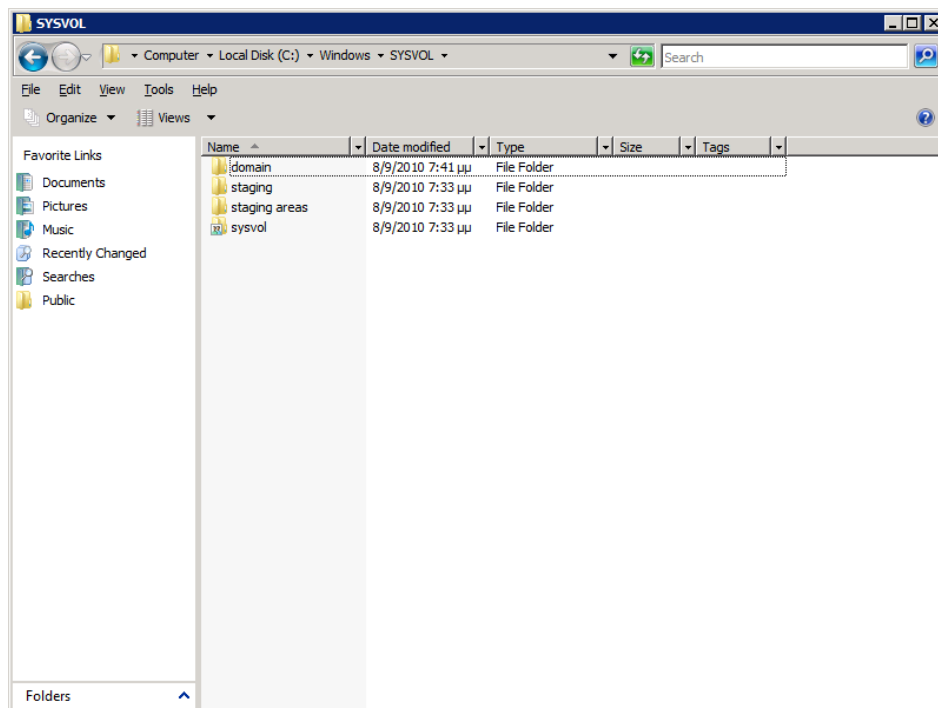
Εικ..3.101

Στη συνέχεια θα ελέγξουμε για την ύπαρξη των βασικών φακέλων του Active Directory. Πηγαίνουμε στον φάκελο C:\Windows\ όπου πρέπει να υπάρχει ο φάκελος SYSVOL.



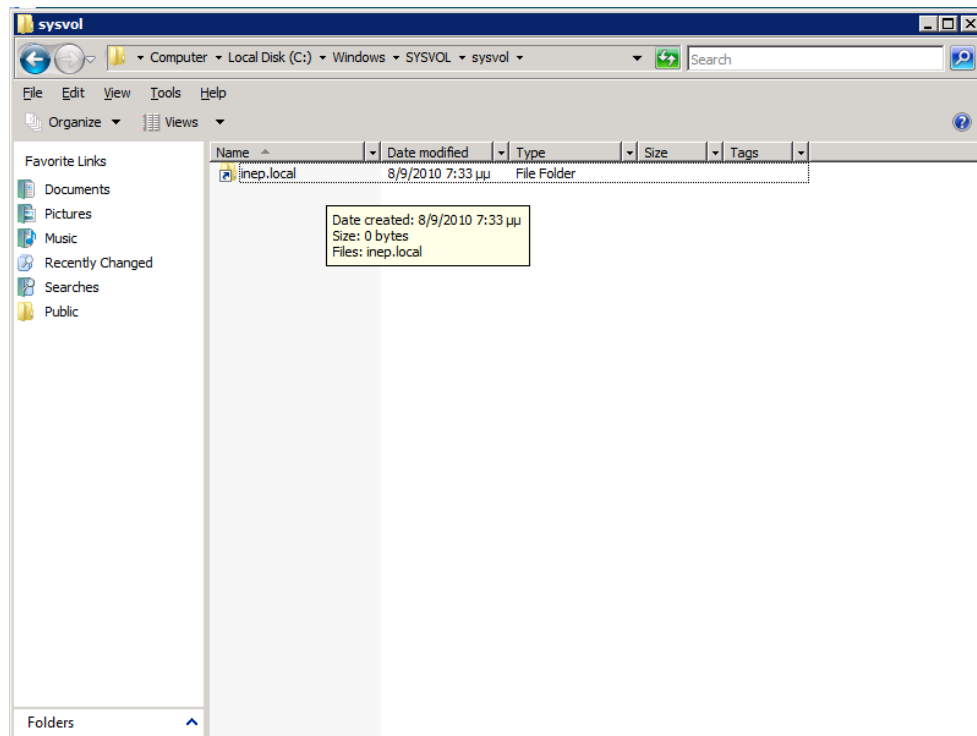
Εικ..3.102

Μέσα στον φάκελο αυτό θα υπάρχει ένας διαμοιραζόμενος φάκελος με όνομα sysvol και άλλοι τρεις φάκελοι με ονόματα: domain, staging και staging areas.



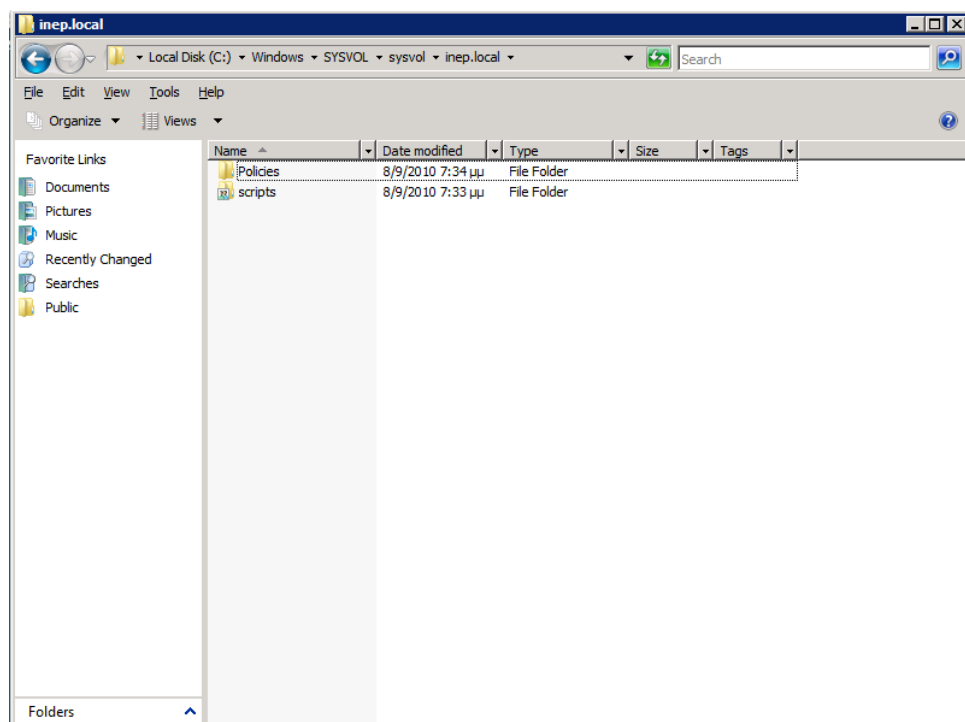
Εικ..3.103

Μέσα στον διαμοιραζόμενο φάκελο sysvol θα έχουμε μια «συντόμευση» στο “inet.local” που είναι το όνομα του domain μας.



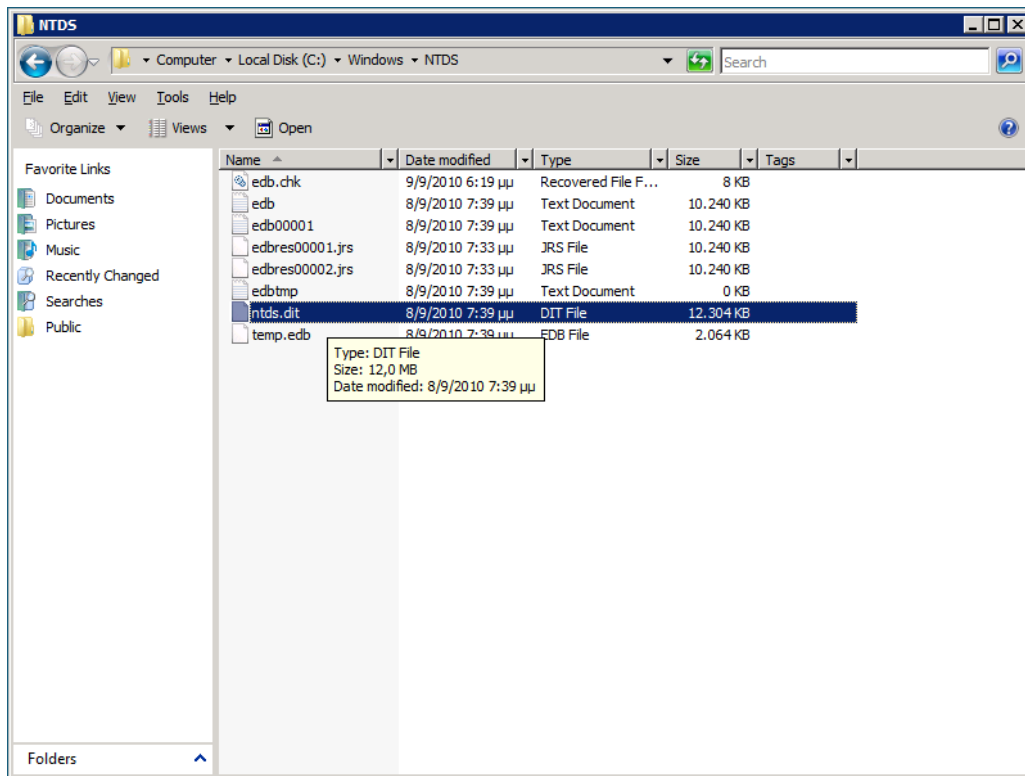
Εικ.3.104

Πατώντας μέσα στην συντόμευση περιμένω να δω έναν φάκελο με τις πολιτικές που έχει όνομα: Policies και έναν διαμοιραζόμενο φάκελο με όνομα scripts ο οποίος θα περιέχει τα διάφορα scripts που θα εκτελούνται μέσω πολιτικών (Εικ.3.105).



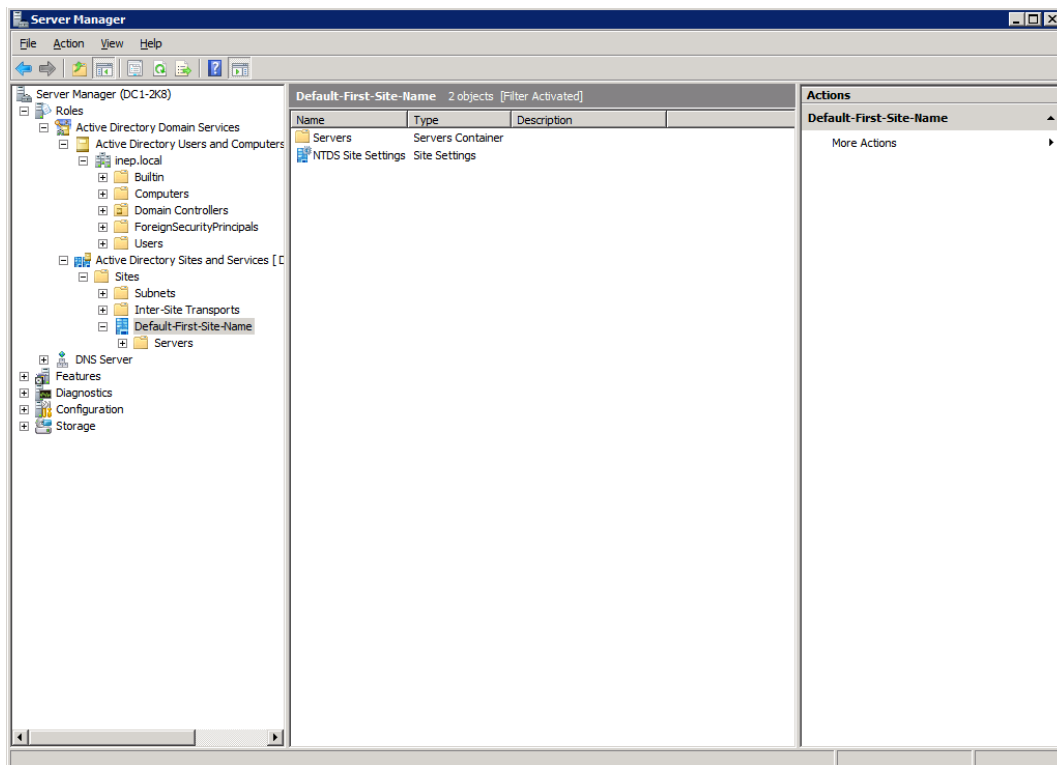
Εικ.3.105

Επίσης μέσα στον φάκελο Windows θα πρέπει να υπάρχει και ο φάκελο με όνομα NTDS ο οποίος θα περιέχει και το αρχείο της βάσης δεδομένων του AD το “**ntds.dit**”



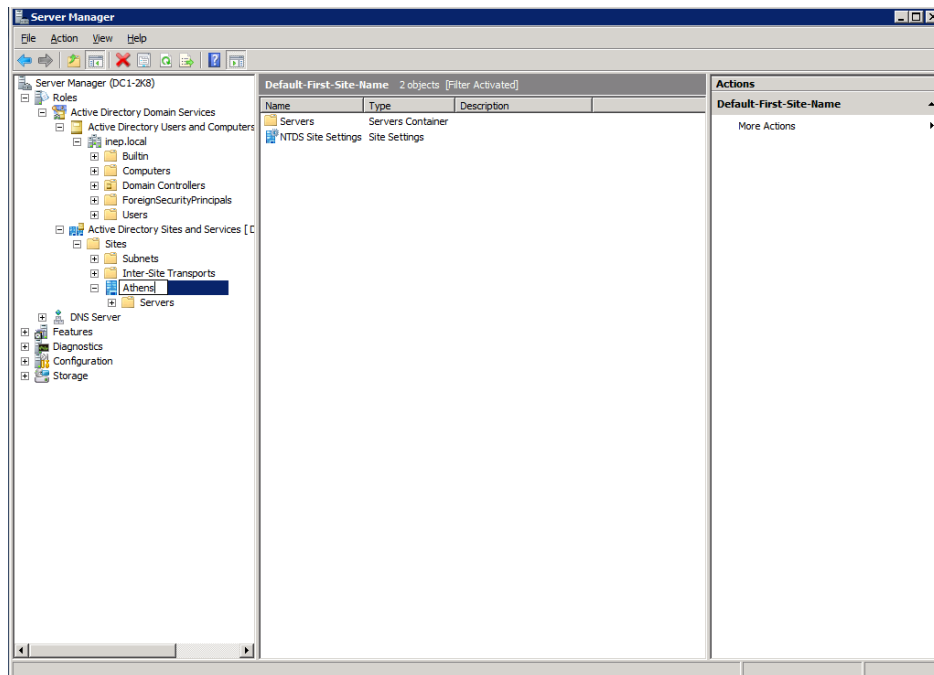
Εικ..3.106

Από τον “Server Manager” ανοίγω το Active Directory Sites and Services (ADSS),



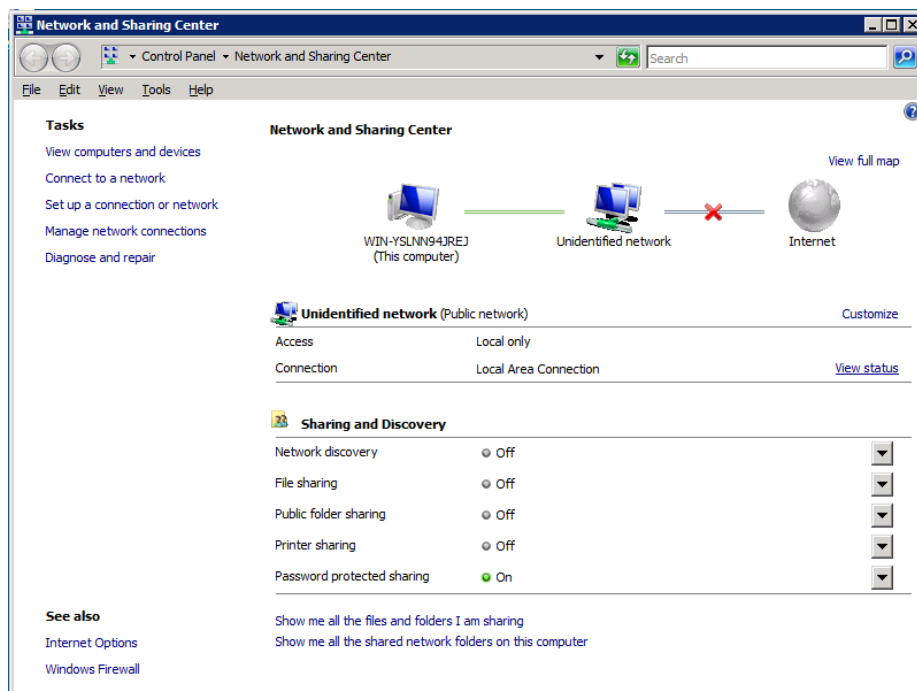
Εικ..3.107

κάνω expand το Sites και πατάω δεξί κλικ πάνω στο “Default-First-Site-Name”, και το μετονομάζω σε “Athens”.



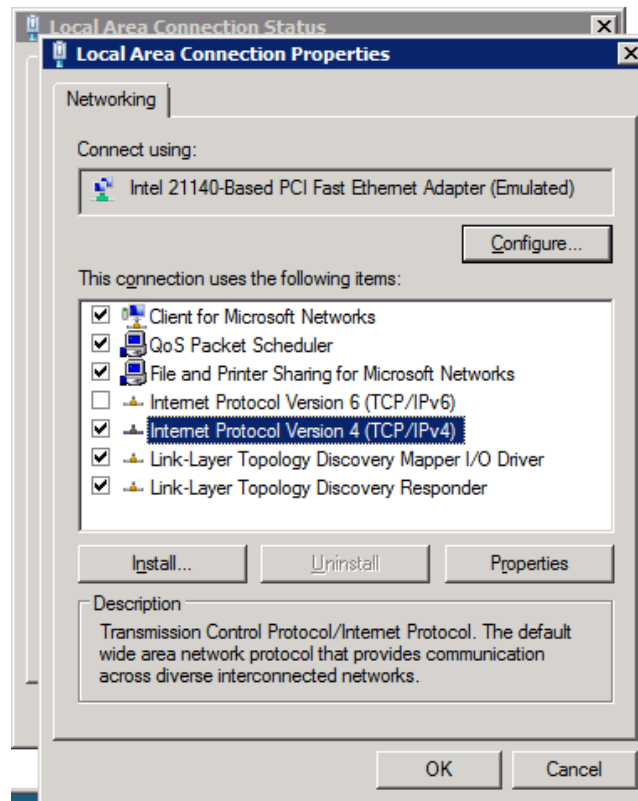
Εικ..3.108

Ανοίγω τώρα τον δεύτερο Server που θα γίνει ο δεύτερος domain controller, και με δεξί κλικ πάνω στην ένδειξη του δικτύου δίπλα από την ώρα, επιλέγω το Network and Sharing Center.



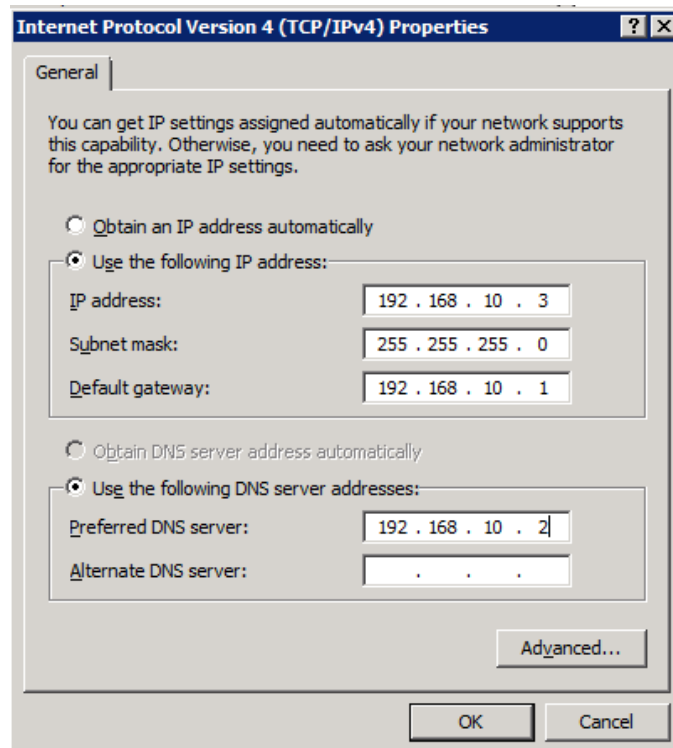
Εικ..3.109

Επιλέγουμε View status και μετά properties:



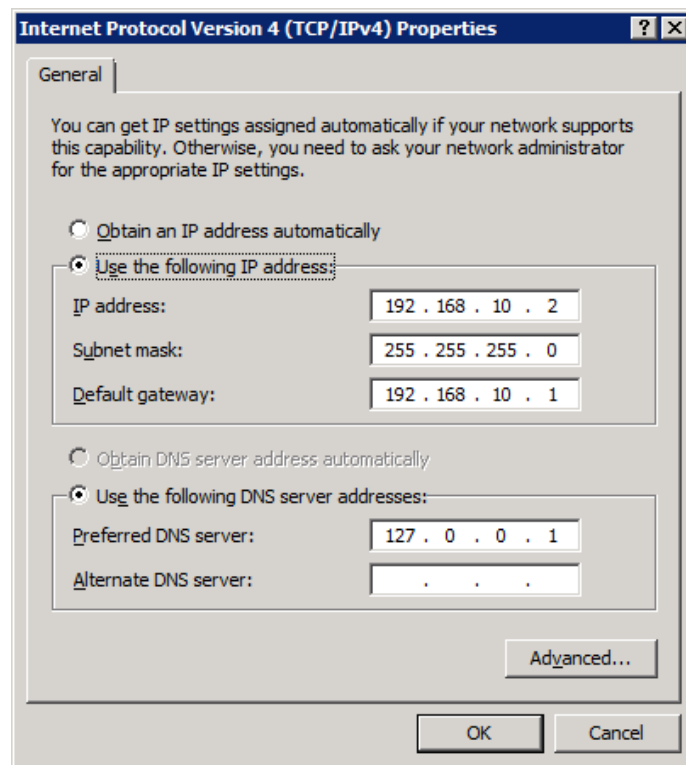
Εικ..3.110

Επιλέγουμε το IPv4 και πατάμε Properties. Τώρα συμπληρώνουμε τις δικτυακές ρυθμίσεις του δεύτερου Domain Controller. Προσοχή μεγάλη θέλει ώστε να ρυθμίσουμε ως Preferred DNS server τον πρώτο DC!



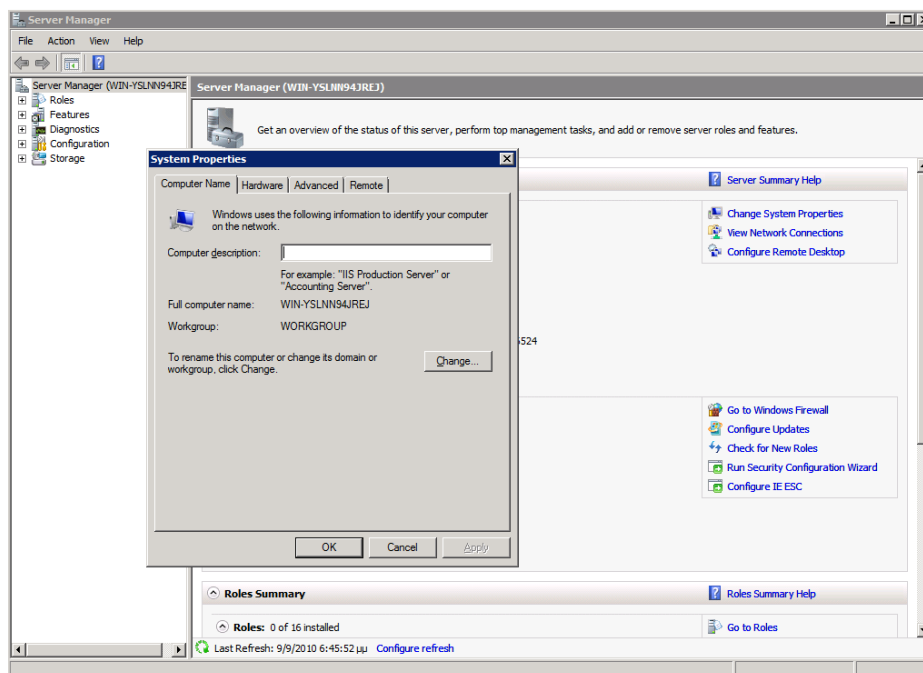
Εικ..3.111

Ας θυμηθούμε λίγο τις αντίστοιχες ρυθμίσεις στον άλλο server δηλαδή τον πρώτο DC, που έχει πλέον για Preferred DNS τον εαυτό του, μετά από την εγκατάσταση!, και όχι τον router που είχαμε ρυθμίσει εμείς.



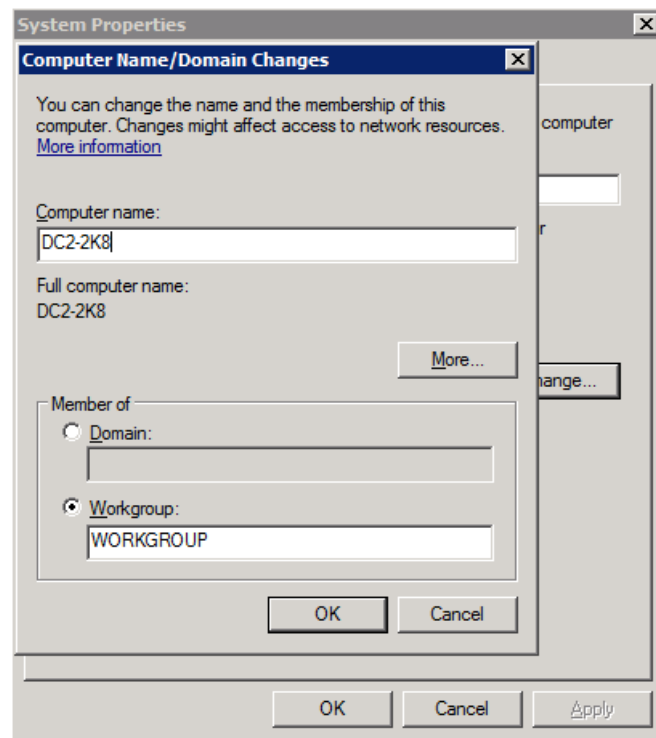
Εικ..3.112

Στη συνέχεια από το System Properties του 2ου DC, πάμε να αλλάξουμε το όνομά του:



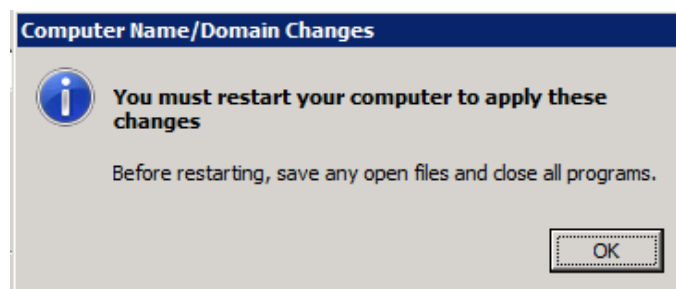
Εικ..3.113

Θα πατήσουμε στο “Change” και θα δώσουμε “DC2-2K8” για όνομα του δεύτερου DC.



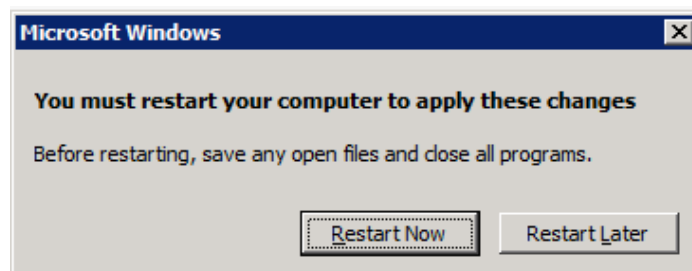
Εικ..3.114

Θα πατήσουμε “ok” στην ακόλουθη ειδοποίηση, και άλλες δύο φορές “ok” έτσι ώστε να φύγουμε από το “Computer Name” και το “System Properties”.



Εικ..3.115

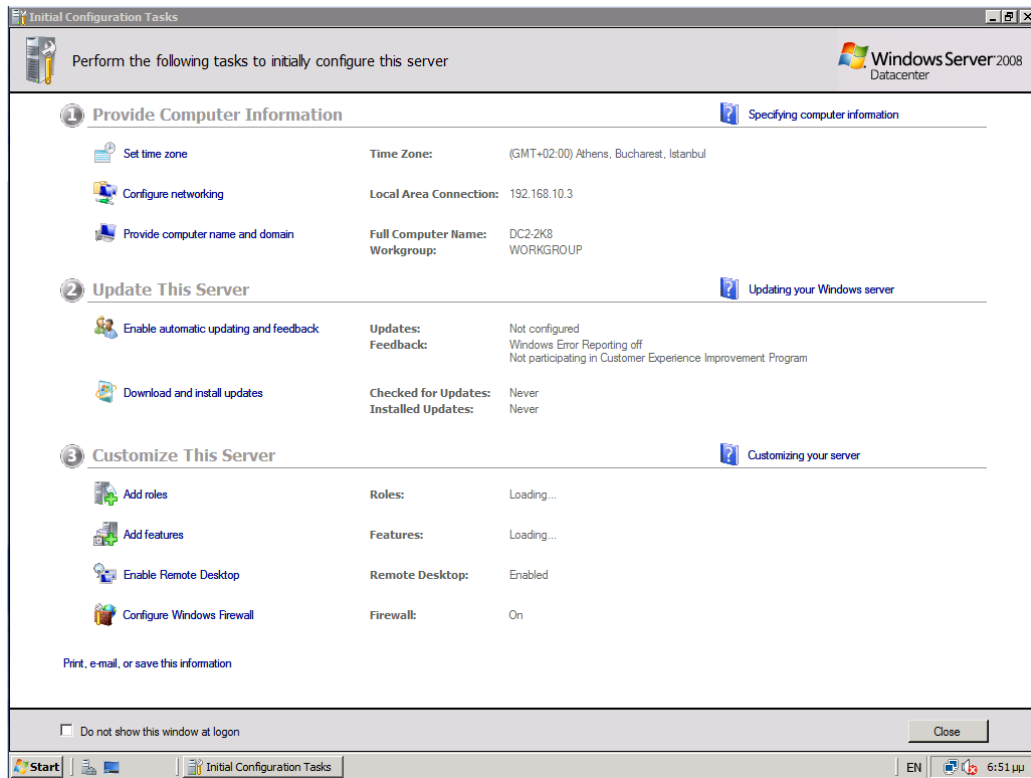
Στη συνέχεια πατάμε “Restart Now” προκειμένου να γίνει άμεσα επανεκκίνηση του server.



Εικ..3.116

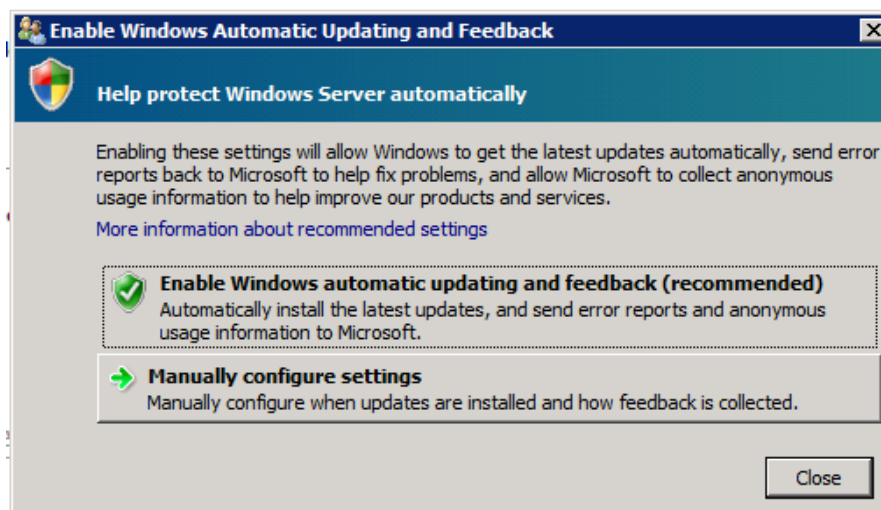
Σημειώνουμε ότι: «Δεν χρειάζεται να κάνουμε πρώτα join στο domain κάποιον server που σκοπεύουμε να κάνουμε domain controller. Το DCPromo.exe θα κάνει όλη την απαραίτητη δουλειά για εμάς».

Μετά την επανεκκίνηση του δεύτερου server, θα δούμε τη γνώριμη πλέον οθόνη του ICT που θα κάνουμε και πάλι τις γνωστές ρυθμίσεις.



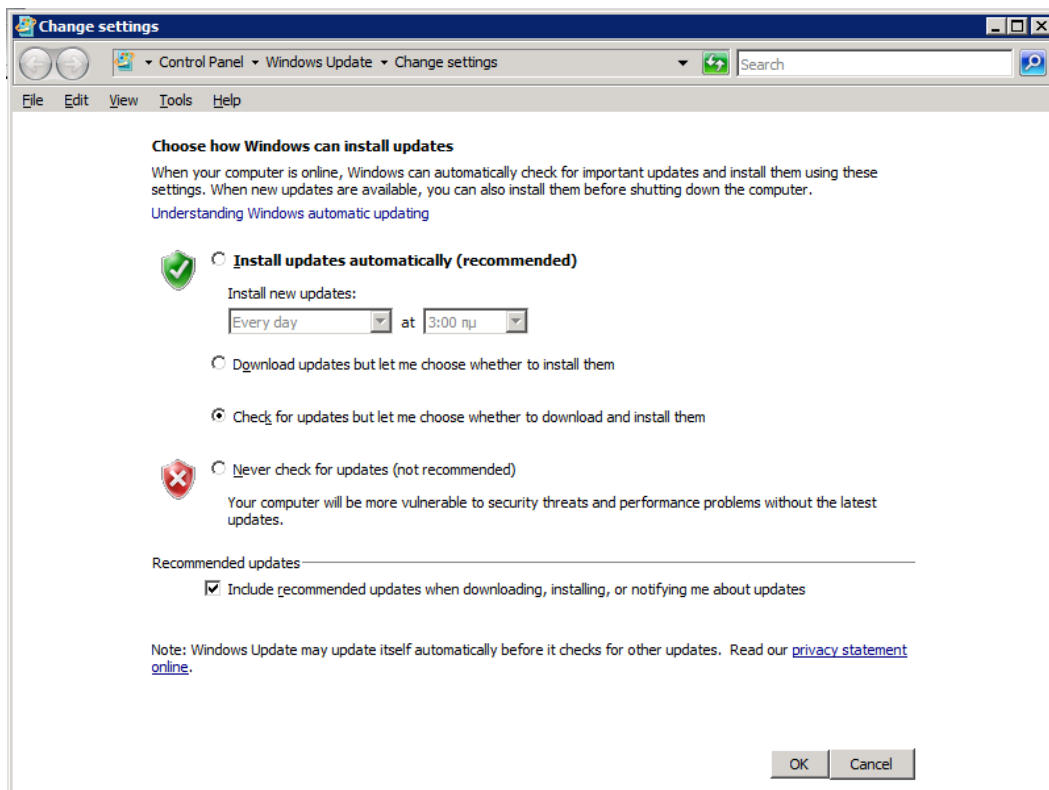
Εικ..3.117

Ξεκινάμε με το “Enable automatic updating and feedback”, που πατάμε στο “Manually configure settings”.



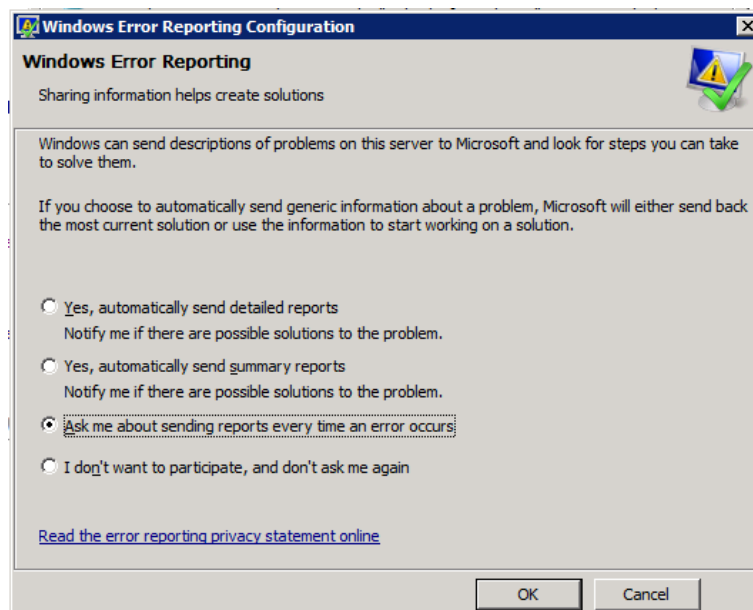
Εικ..3.118

Και επιλέγουμε το “Check for updates but let me choose whether to download and install them”. Δεν ξεχνάμε να επιλέξουμε το “Include recommended updates when downloading, installing, or notifying me about updates”.



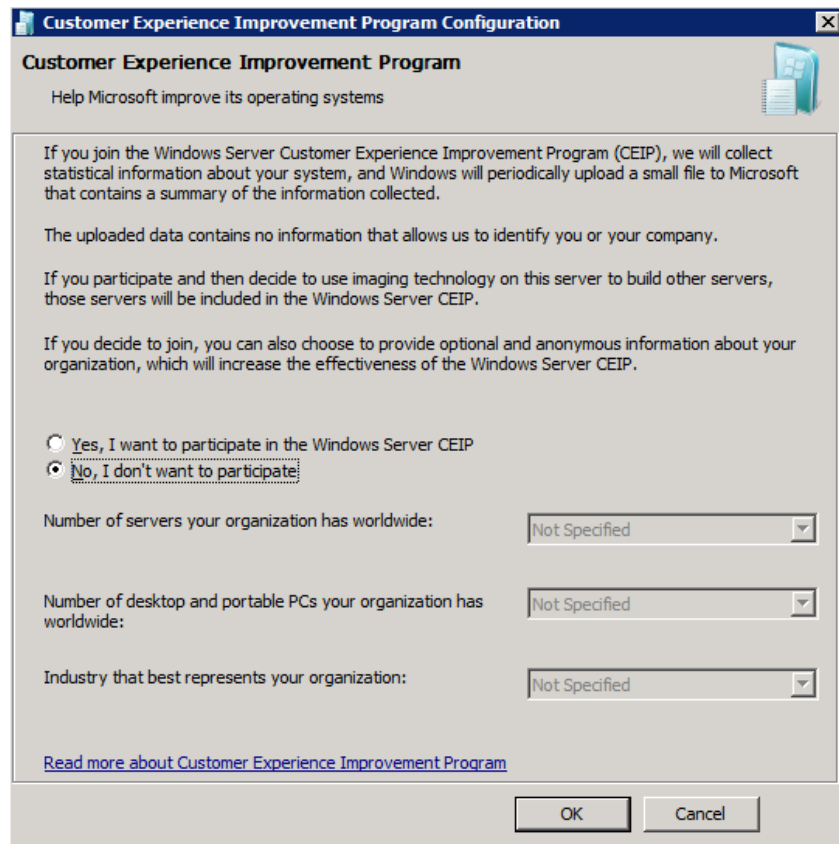
Εικ.3.119

Στο Windows Error Reporting Configuration, επιλέγουμε το “Ask me about sending reports every time an error occurs”



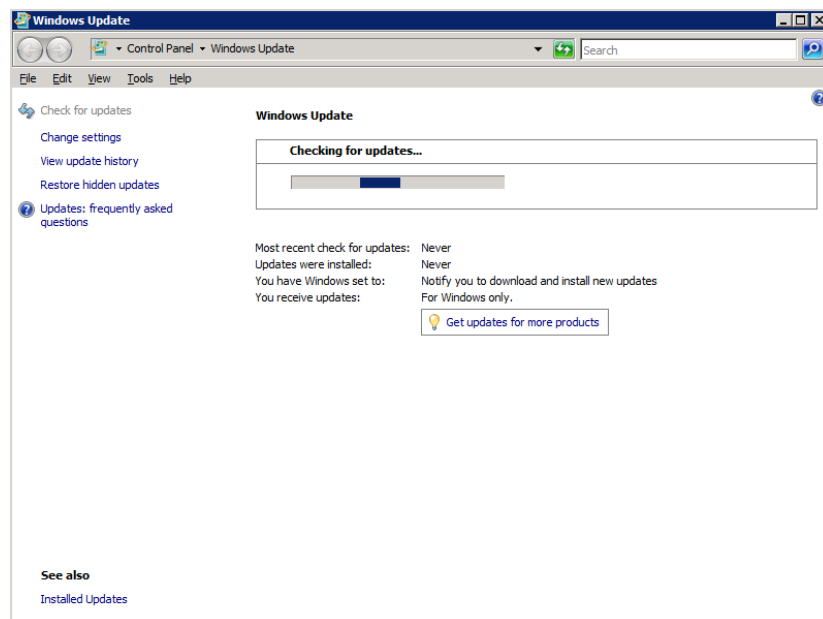
Εικ.3.120

Και στο “Customer Experience Improvement Program Configuration” επιλέγουμε να μην συμμετέχουμε σε αυτό.



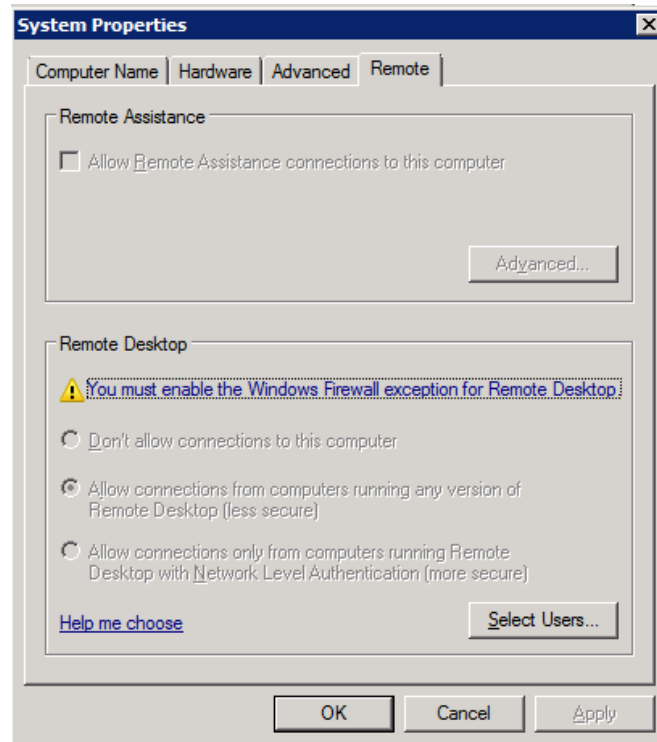
Εικ.3.121

Δεν αμελούμε να εκτελέσουμε όλες τις διαθέσιμες ενημερώσεις των Windows πριν από την εκτέλεση του dcprmo.exe



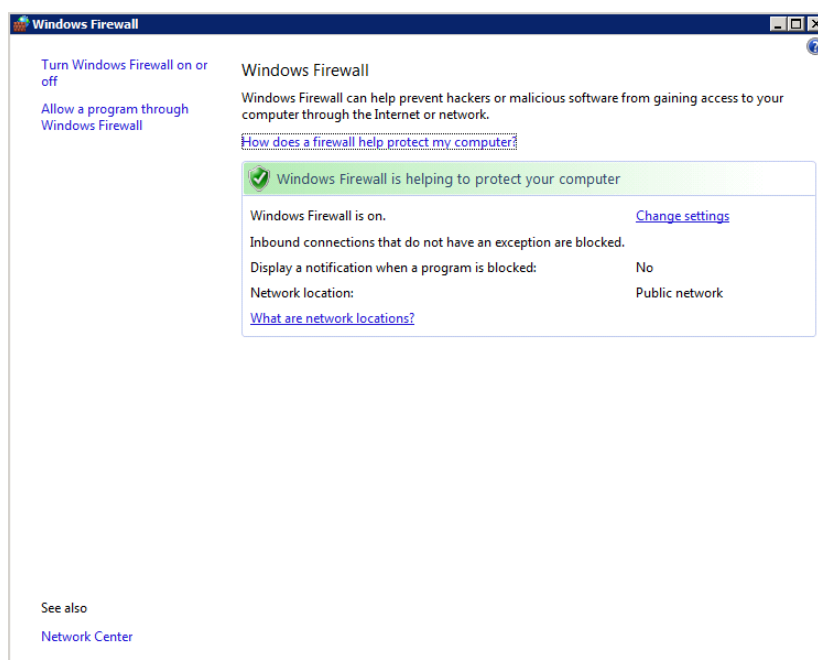
Εικ.3.122

Ρυθμίζω την απομακρυσμένη πρόσβαση στον server μου, δηλαδή το remote desktop, το οποίο απαιτεί την ρύθμιση του Windows Firewall προκειμένου να επιτραπεί αυτή η πρόσβαση. Πατάω λοιπόν πάνω στο “You must enable the Windows Firewall exception for Remote Desktop”



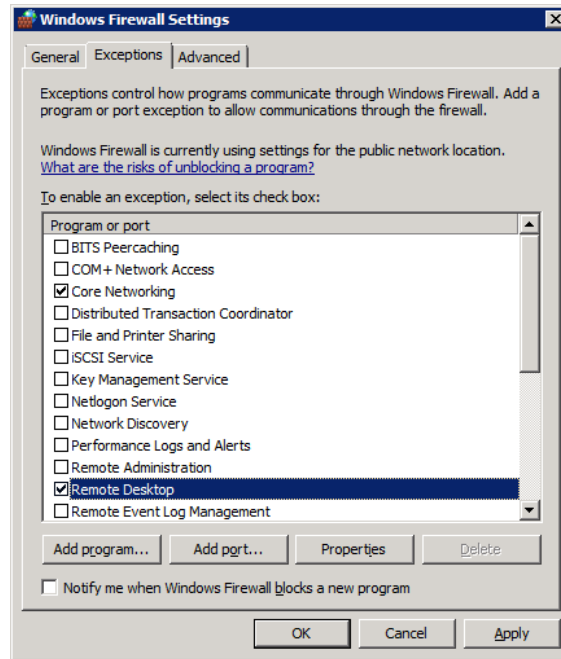
Εικ.3.123

Ανοίγει η σελίδα ρύθμισης του Windows Firewall.



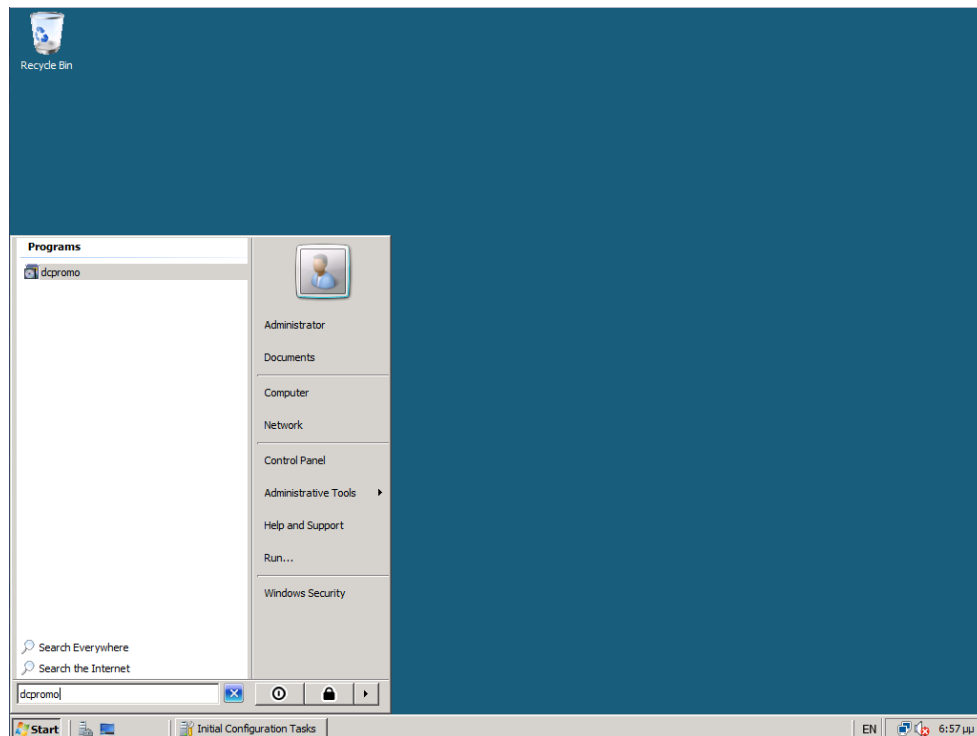
Εικ.3.124

Πατάμε στο “Change Settings” και μετά στο “Exceptions” προκειμένου να δημιουργήσουμε μια εξαίρεση στο τοίχος προστασίας και να επιτρέψουμε την εισερχόμενη θύρα του Remote Desktop. Επιλέγω από την έτοιμη λίστα το “Remote Desktop”, μετά “ok” και είμαστε έτοιμοι για την εγκατάσταση του Active Directory και σε αυτόν το Server.



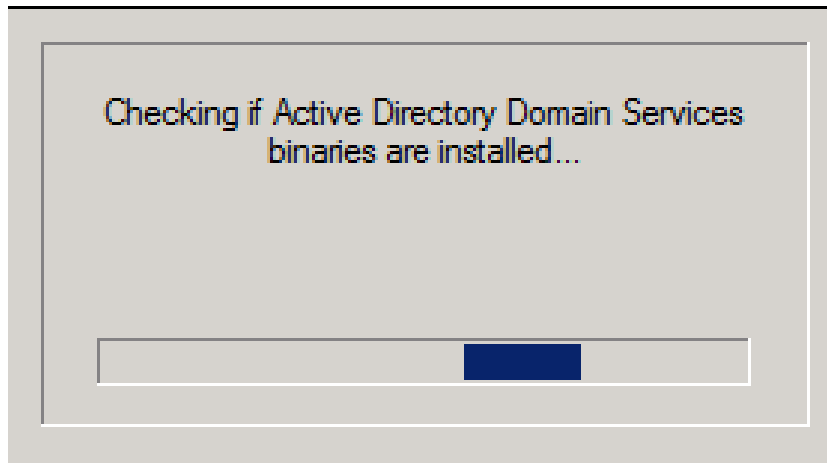
Εικ.3.125

Από το κουμπί “Start” γράφω κατευθείαν το “dcpromo” και πατάω Enter.



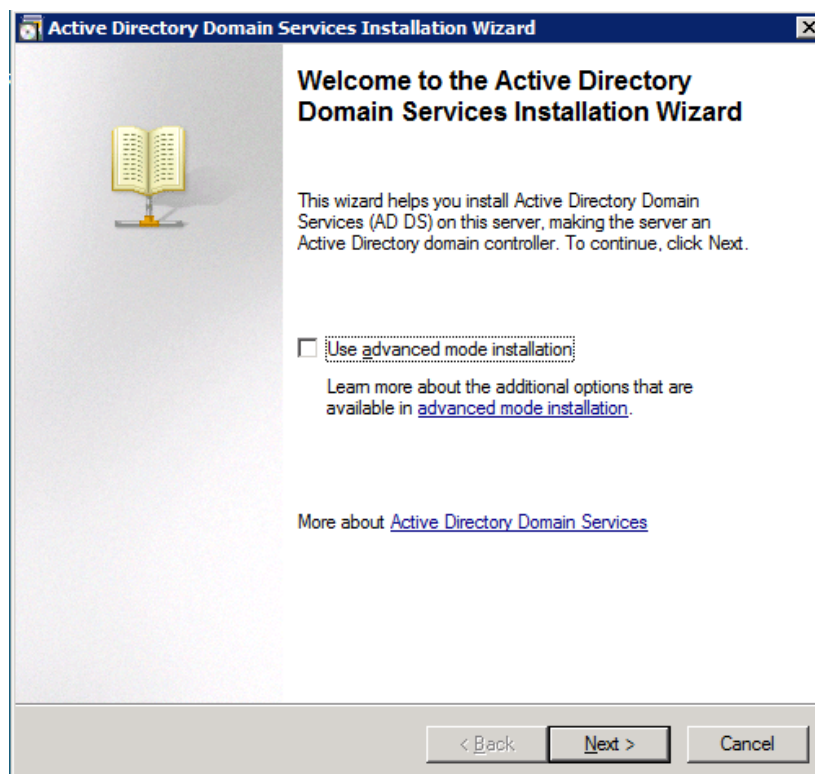
Εικ.3.126

Ξεκινάει η εγκατάσταση όπως ακριβώς γινόταν και στα Windows Server 2003. Ελέγχει πρώτα αν υπάρχουν τα εκτελέσιμα αρχεία για το ADDS, και επειδή δεν θα τα βρει, θα τα εγκαταστήσει πρώτα και μετά θα προχωρήσει στην εγκατάσταση του Active Directory.



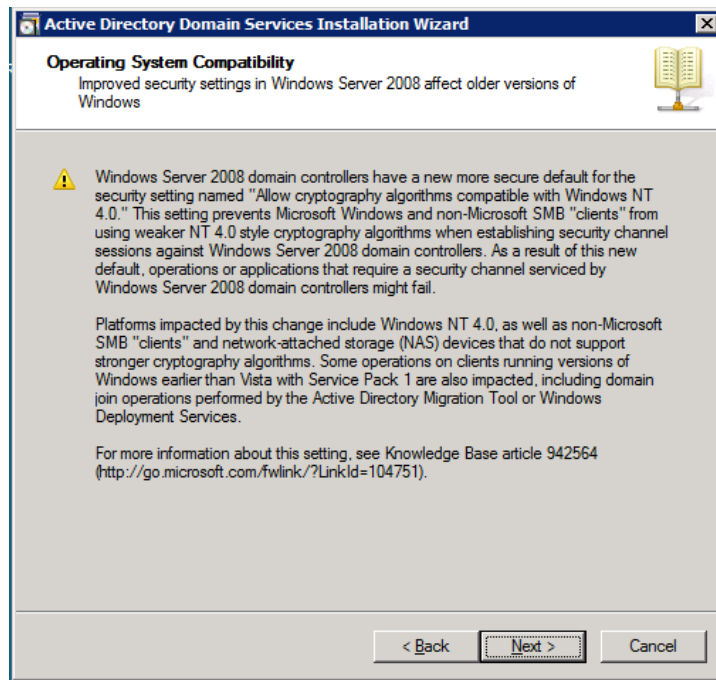
Εικ..3.127

Ξεκινάει ο γνωστός wizard, πατάμε “Next”,



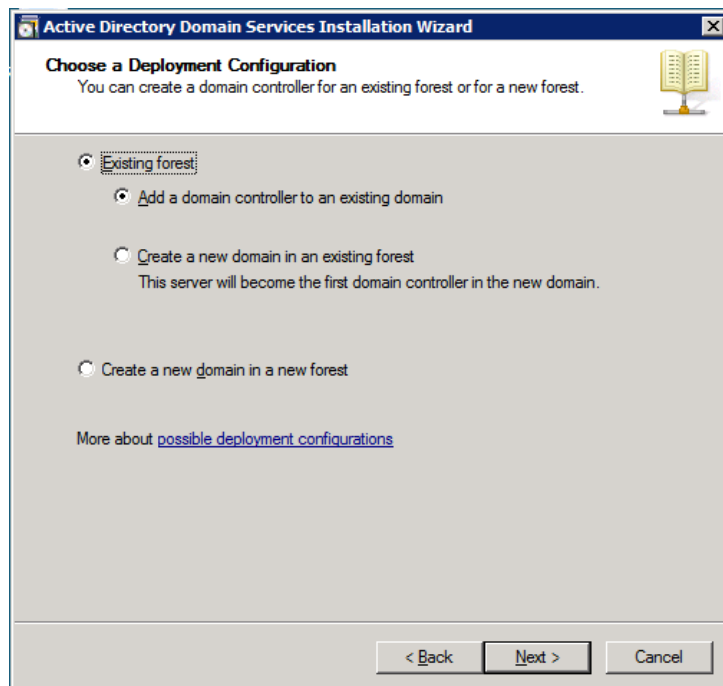
Εικ..3.128

Και στην επόμενη οθόνη ξανά “Next”,



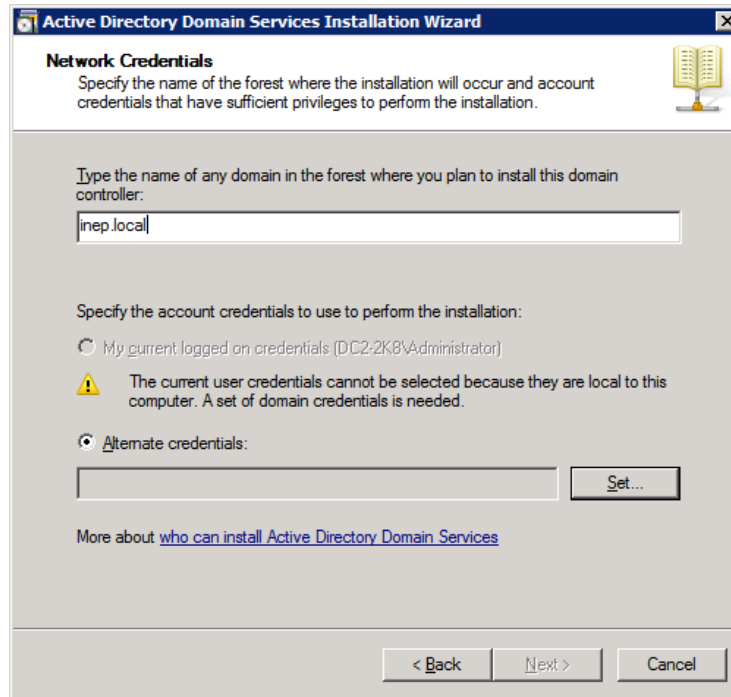
Εικ..3.129

Και εδώ θα επιλέξουμε “Existing forest”, “Add a domain controller to an existing forest” έτσι ώστε ο server μας να γίνει ο δεύτερος domain controller στο domain που ορίσαμε στον πρώτο server όπως στην Εικ.3.130.



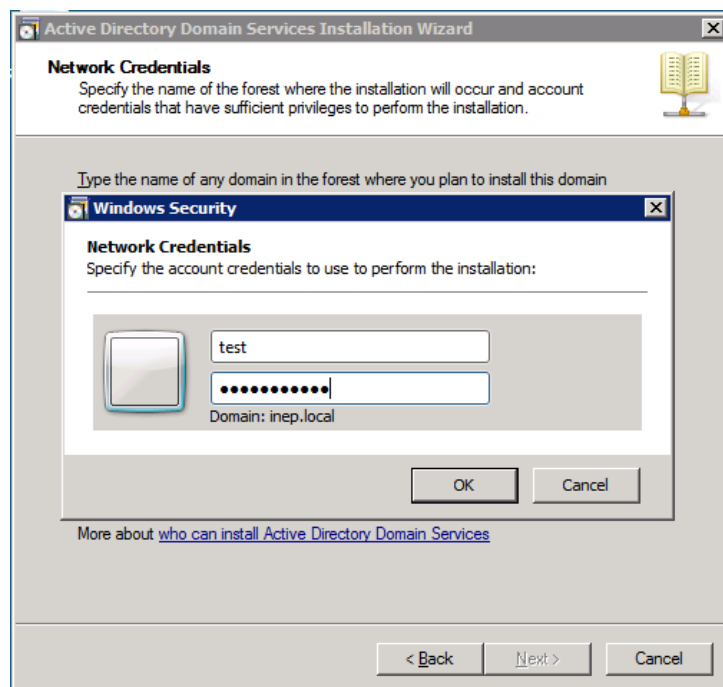
Εικ..3.130

Στην επόμενη οθόνη συμπληρώνουμε το όνομα του domain που θα εγκαταστήσουμε τον server αυτόν, δηλαδή το “inep.local”. Επιλέγουμε “Alternate credentials” και πατάμε “set”



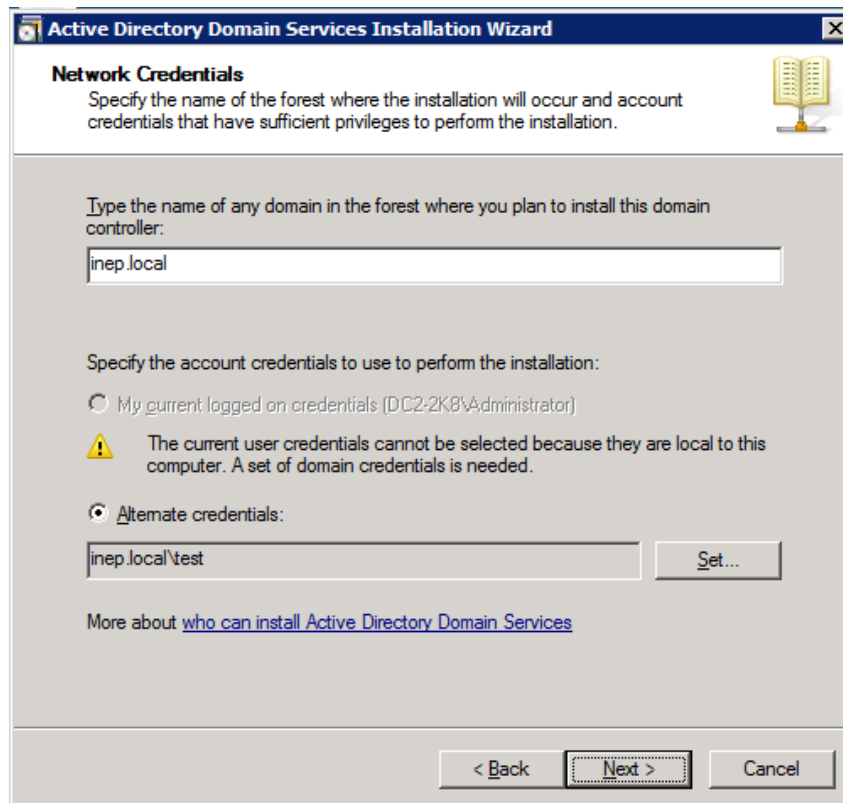
Εικ.3.131

Προκειμένου να εισάγουμε τα credentials ενός χρήστη που έχει δικαίωμα να κάνει την εισαγωγή ενός δεύτερου domain controller. Δίνουμε τα credentials δηλαδή user name και password, του domain administrator τον οποίο τον έχουμε μετονομάσει σε “Test”.



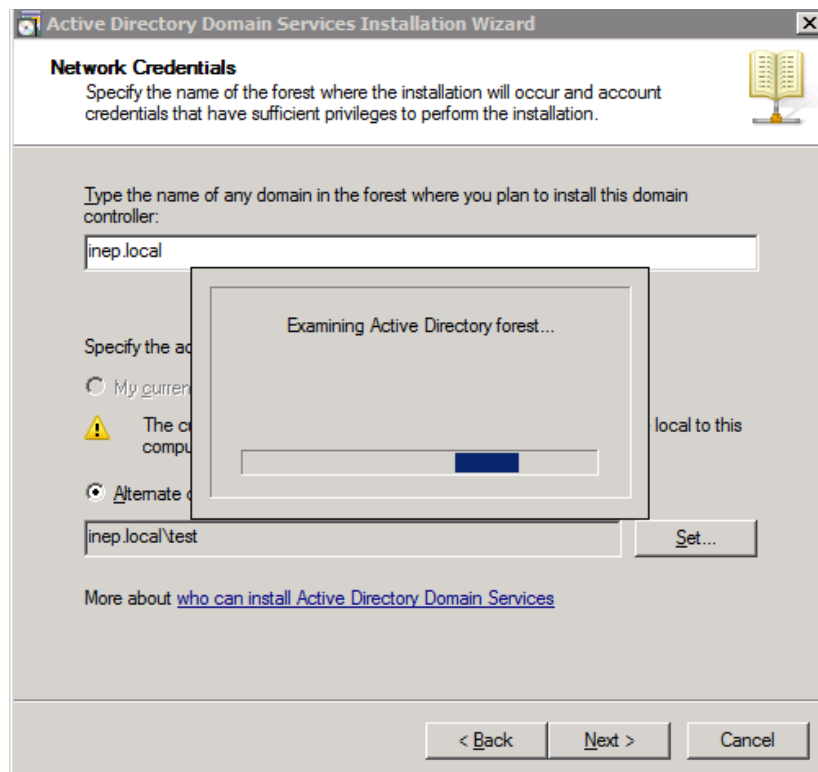
Εικ.3.132

Παρατηρούμε το “inep.local\test” που έχει λάβει θέση στα Alternate Credential, και κάνουμε κλικ στο ok.



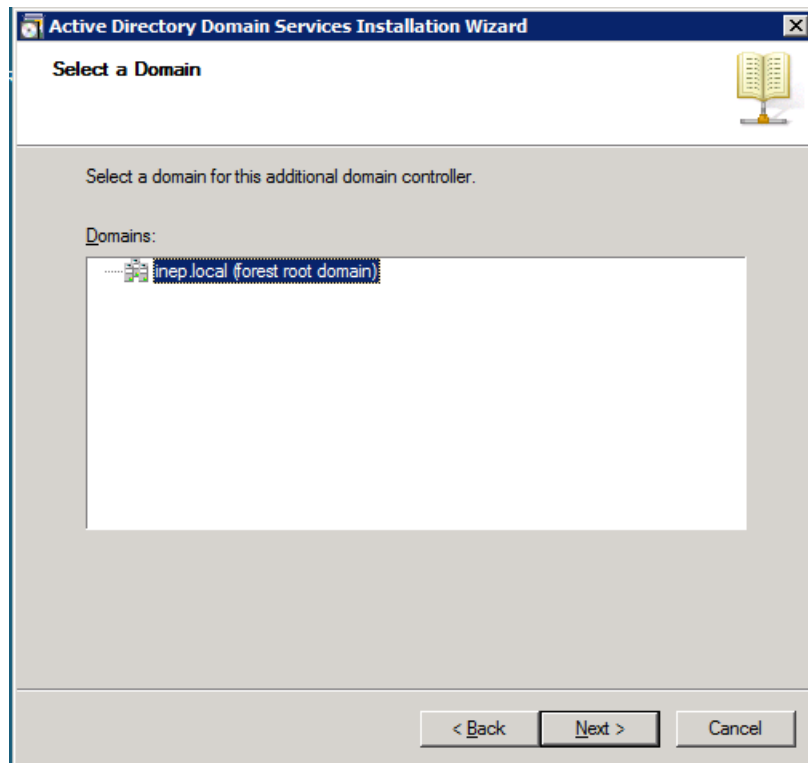
Εικ..3.133

Περιμένουμε λίγο να ελέγξει το forest:



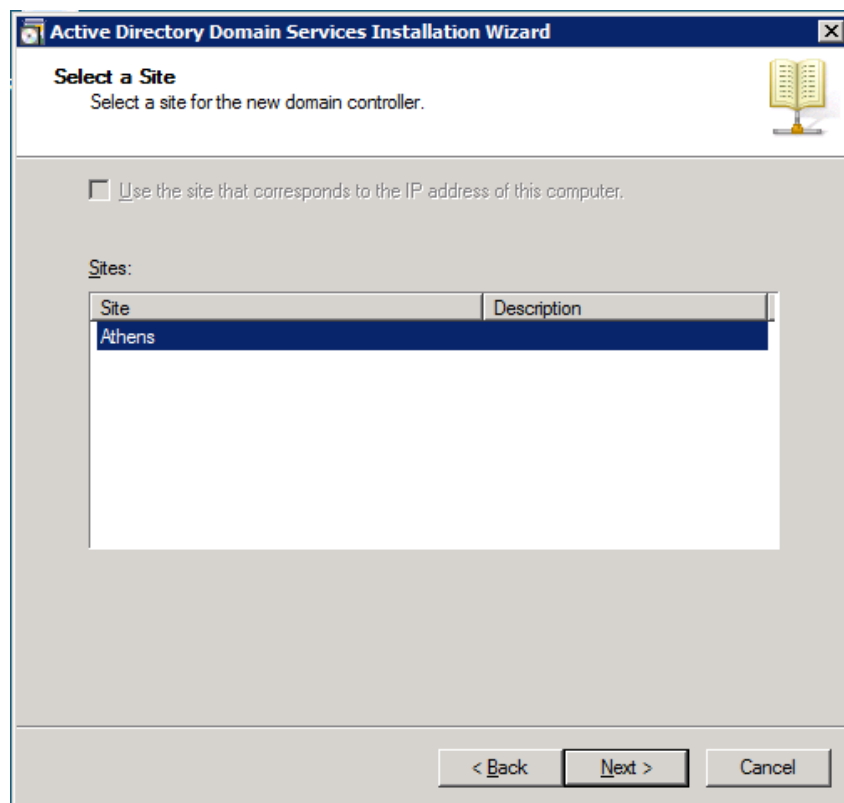
Εικ..3.134

Πατάμε πάλι “Next”, για να επιλέξουμε το μοναδικό domain μέσα στο forest μας.



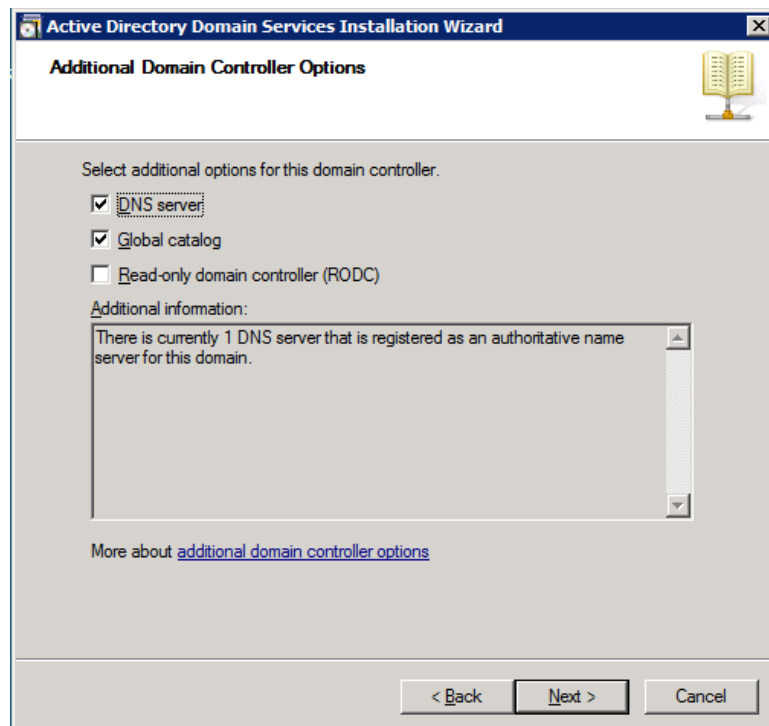
Εικ..3.135

Επιλέγουμε το site για τον domain controller μας, και εδώ είναι το “Athens” που είχαμε ρυθμίσει, και πατάμε “Next”.



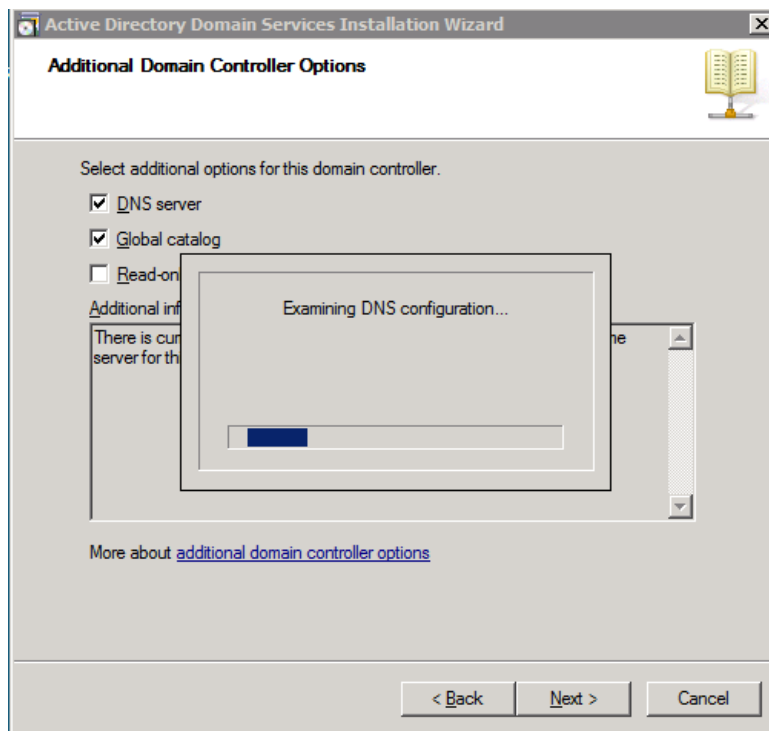
Εικ..3.136

Επιλέγουμε τις υπηρεσίες “DNS server” και “Global catalog” έτσι ώστε ο Domain Controller που στήνουμε να έχει ακριβώς τις ίδιες υπηρεσίες με τον πρώτο και να μπορεί να δουλέψει πλήρως σε περίπτωση που ο πρώτος δεν είναι διαθέσιμος.



Εικ.3.137

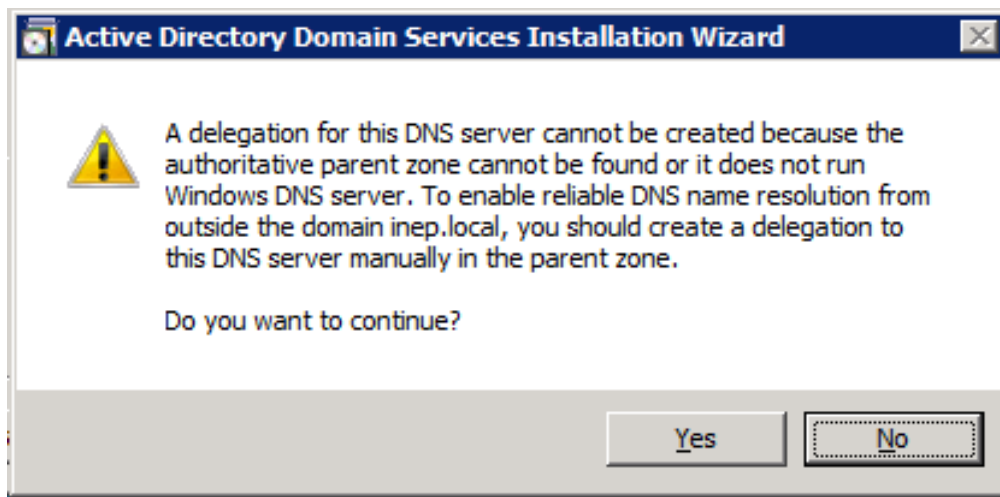
Πατάμε “Next” και περιμένουμε να ελεγχτούν οι ρυθμίσεις DNS.



Εικ.3.138

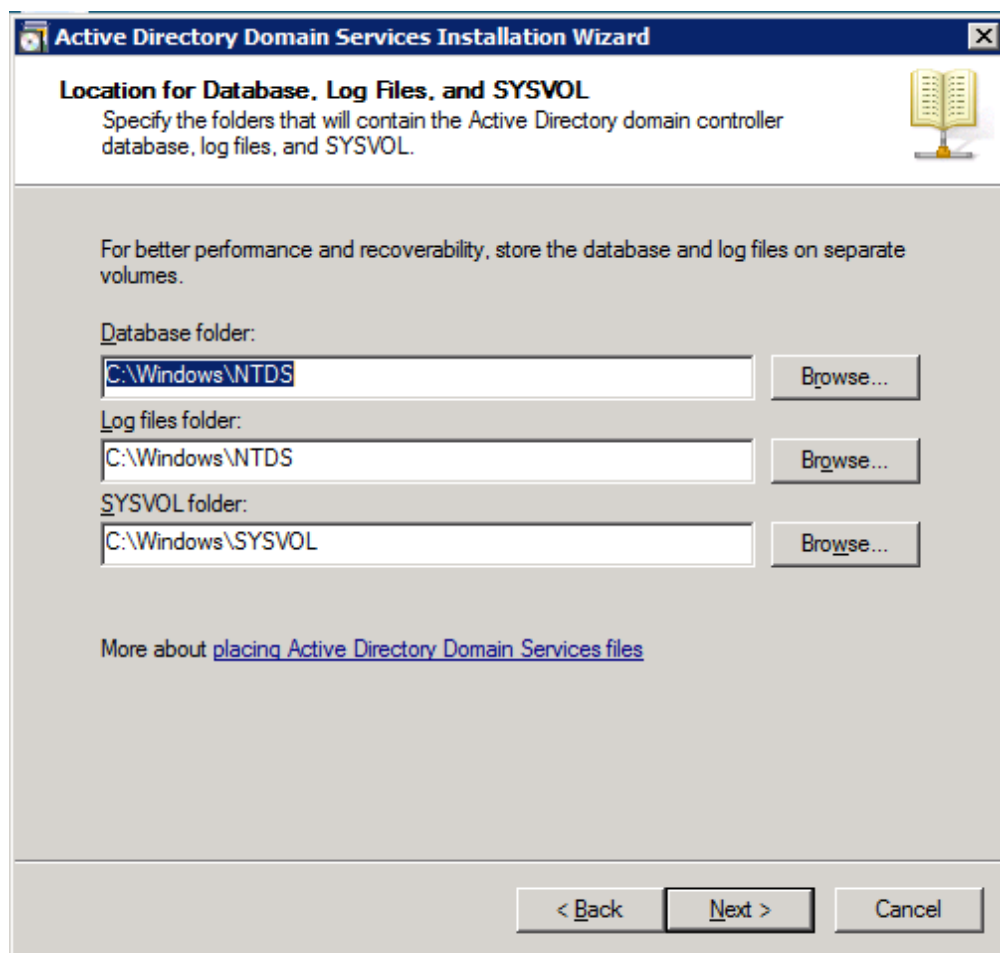
Βγαίνει και πάλι η γνώριμη ειδοποίηση, την οποία μπορούμε να αγνοήσουμε με

ασφάλεια και να πατήσουμε “Next” για να συνεχίσουμε.



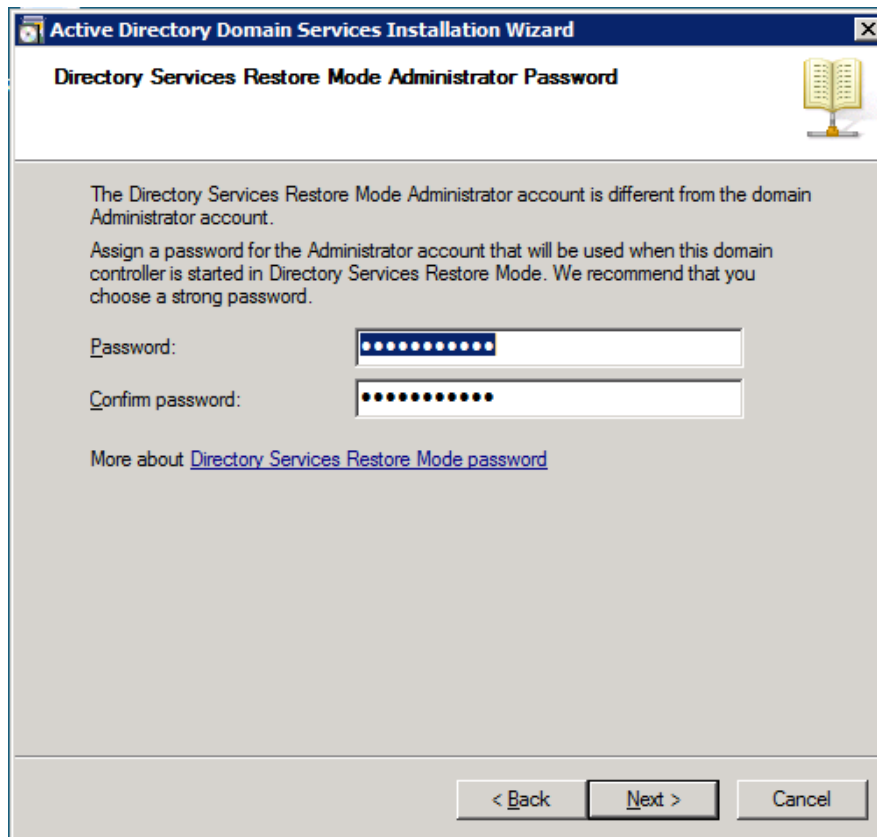
Εικ.3.139

Ρυθμίζουμε και πάλι την τοποθεσία των τριών βασικών φακέλων. Εμείς τους αφήνουμε ως έχουν.



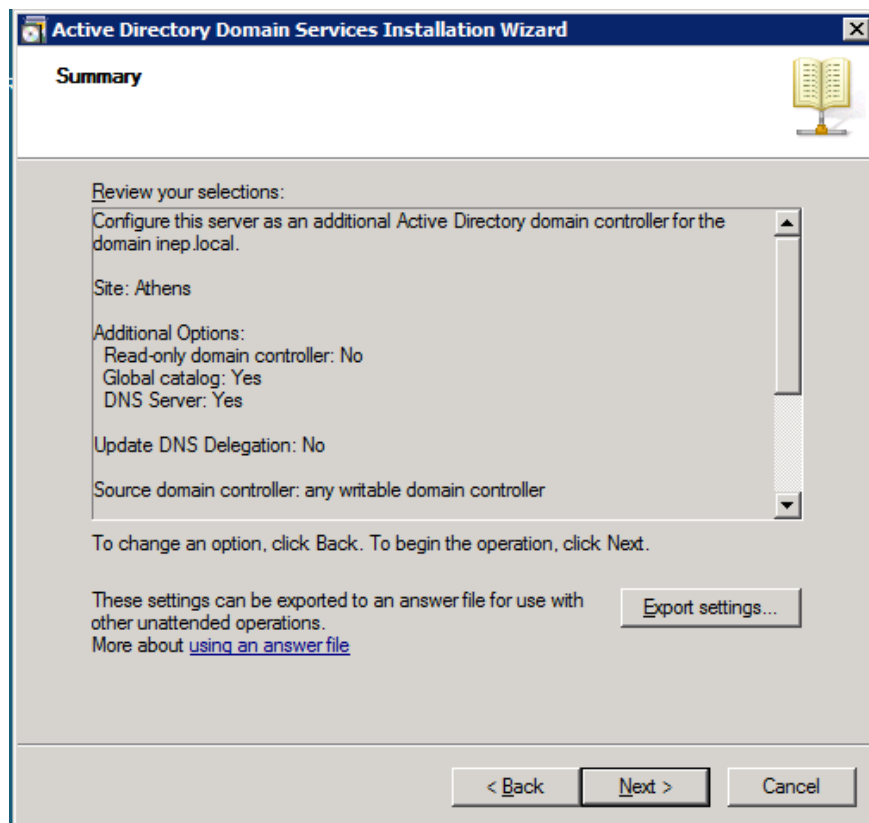
Εικ.3.140

Εδώ δίνουμε το “Restore Mode Administrator Password”. Στο lab που κάνουμε θα βάλουμε τον ίδιο που είχαμε βάλει και στον πρώτο Domain Controller.



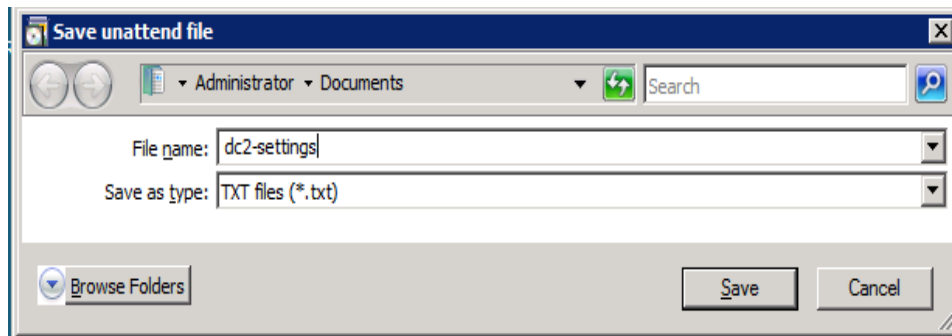
Εικ..3.141

Πατάμε “Next” και βλέπουμε την οθόνη σύνοψης:



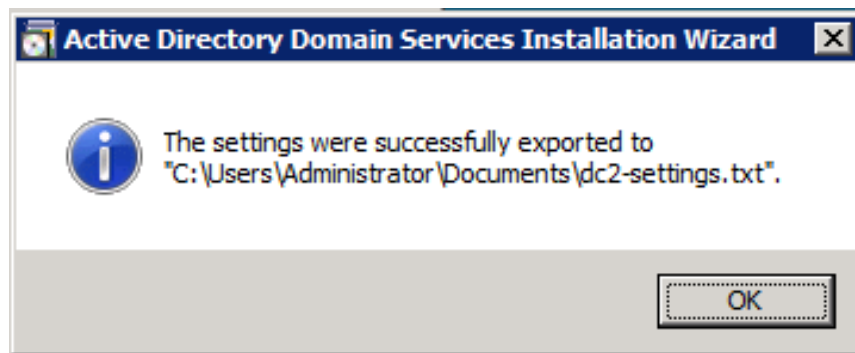
Εικ..3.142

Κάνουμε “Export settings” και για τον δεύτερο Domain Controller”



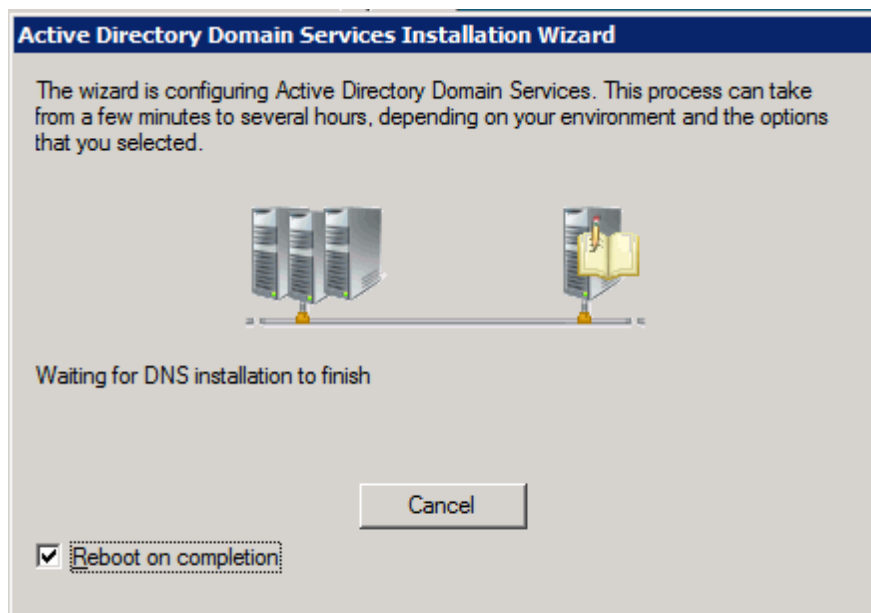
Εικ..3.143

Και πατάμε “ok” για να συνεχίσουμε:



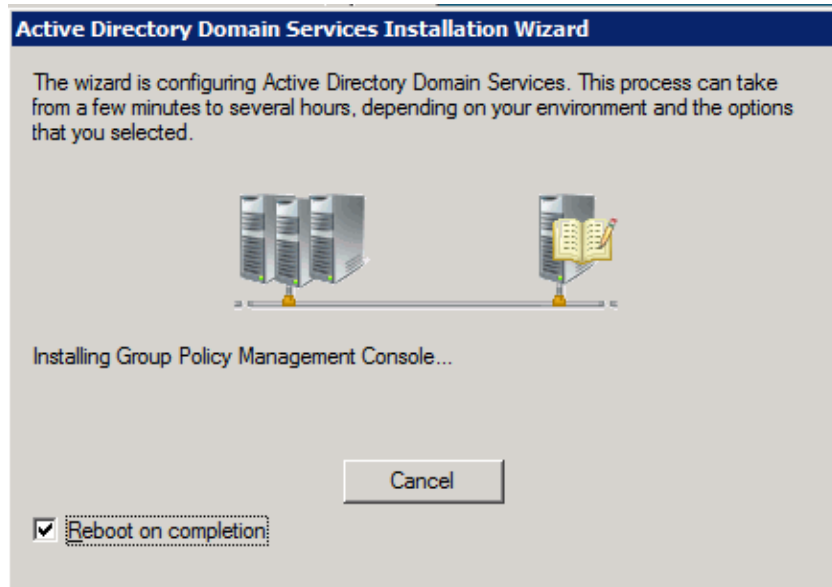
Εικ..3.144

Επιλέγουμε το “Reboot on completion” και αφήνουμε την εγκατάσταση να συνεχίσει μόνη της.



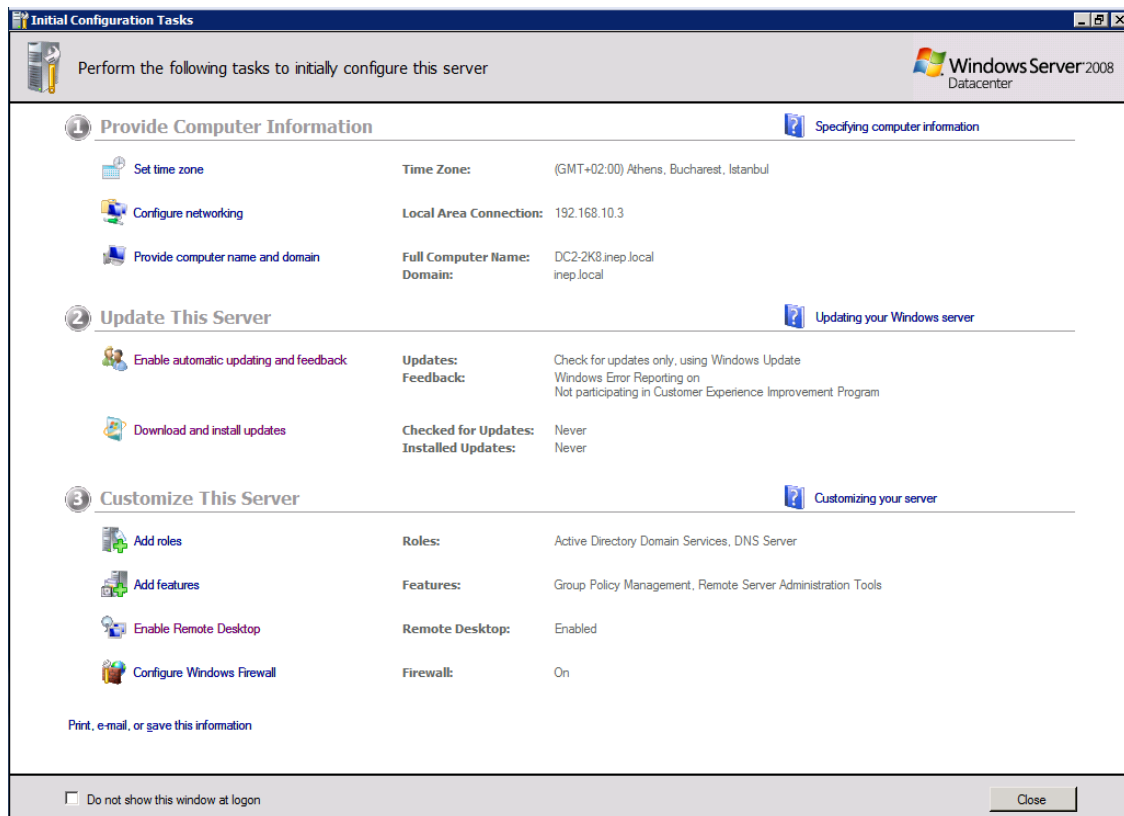
Εικ..3.145

Η οθόνη εγκαθιστά όλα τα απαραίτητα και στο τέλος κάνει επανεκκίνηση του server.



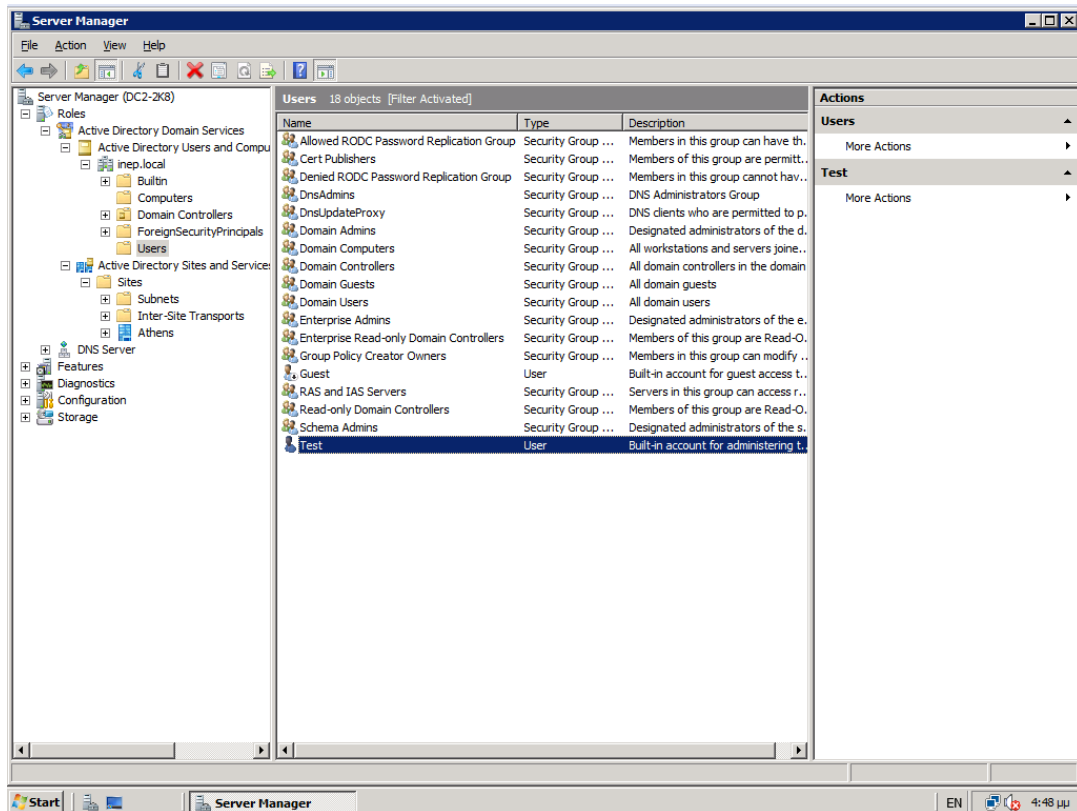
Εικ..3.146

Ο server εκτελεί επανεκκίνηση και κάνουμε login σαν user “Test” του domain που είναι ο λογαριασμός του διαχειριστή του domain.



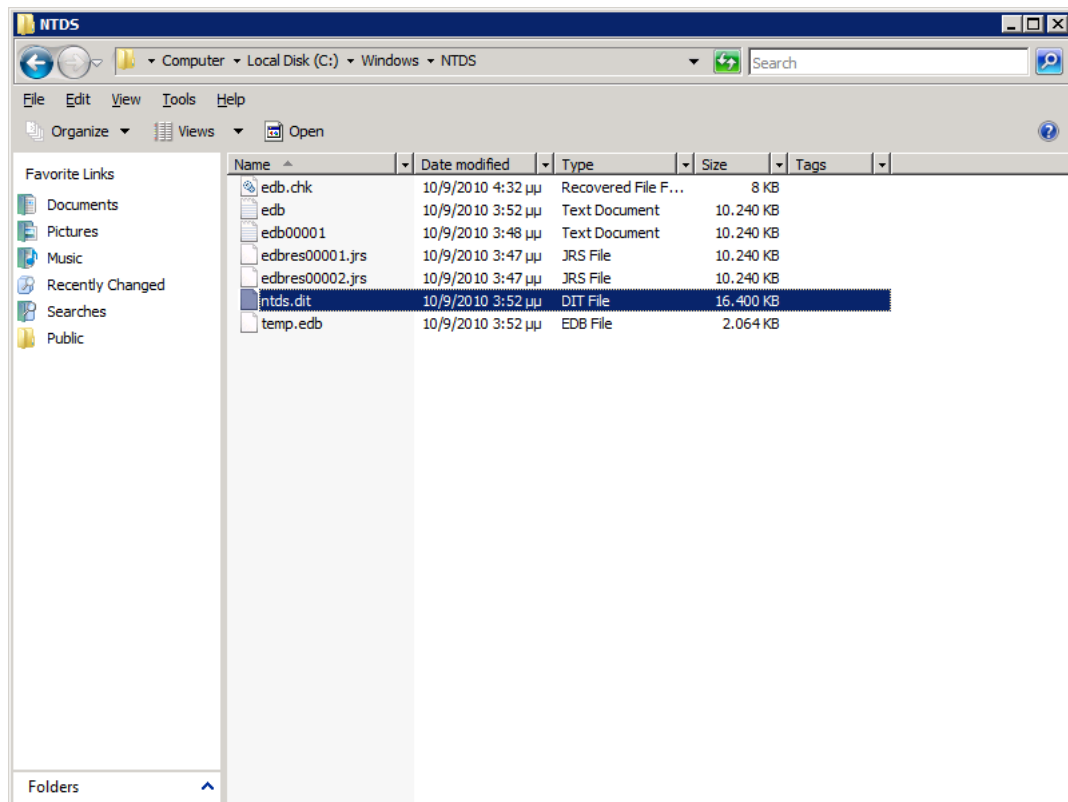
Εικ..3.147

Στον server manager βλέπουμε τα ακόλουθα, και επαληθεύουμε την ύπαρξη των ρόλων και των αντιγράφων των λογαριασμών που ρυθμίσαμε στον πρώτο DC.



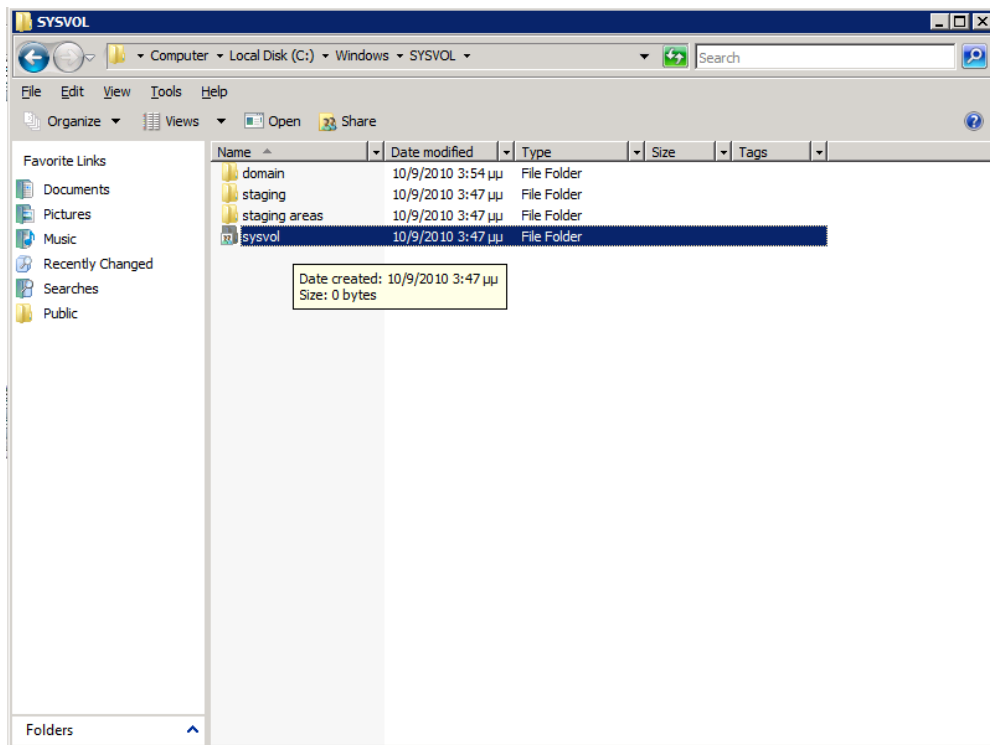
Εικ..3.148

Επίσης επαληθεύουμε την ορθή δημιουργία των φακέλων του AD, όπως είναι ο NTDS που περιέχει το αρχείο “ntds.dit”



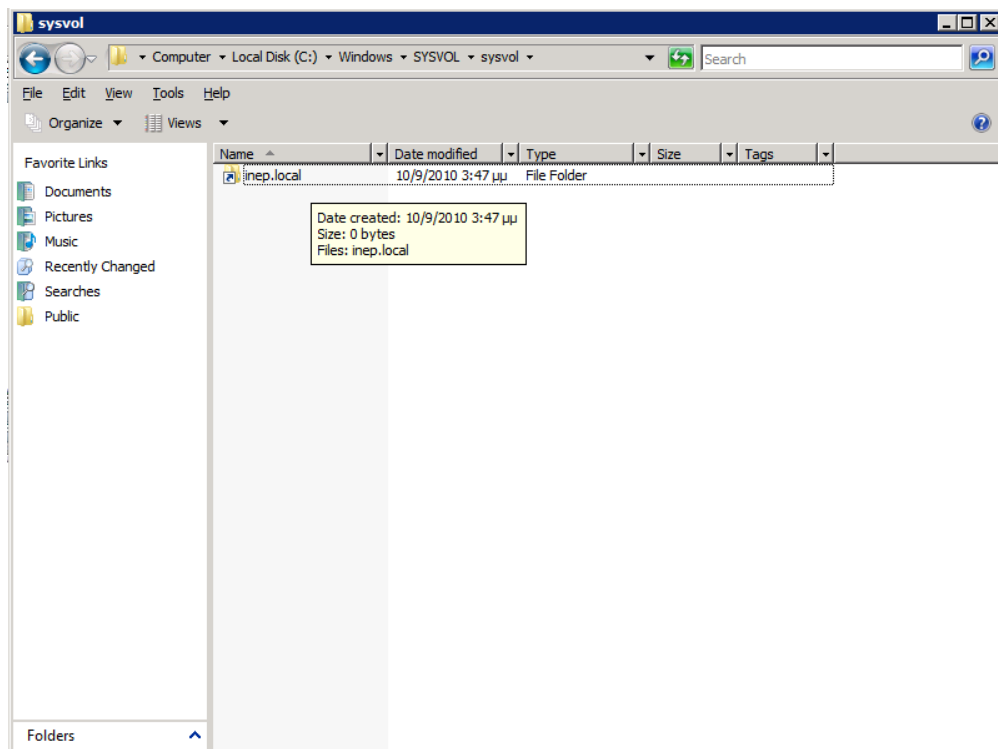
Εικ..3.149

Και ο φάκελος SYSVOL που περιέχει τους φακέλους domain, staging και staging areas και τον shared φάκελο sysvol.



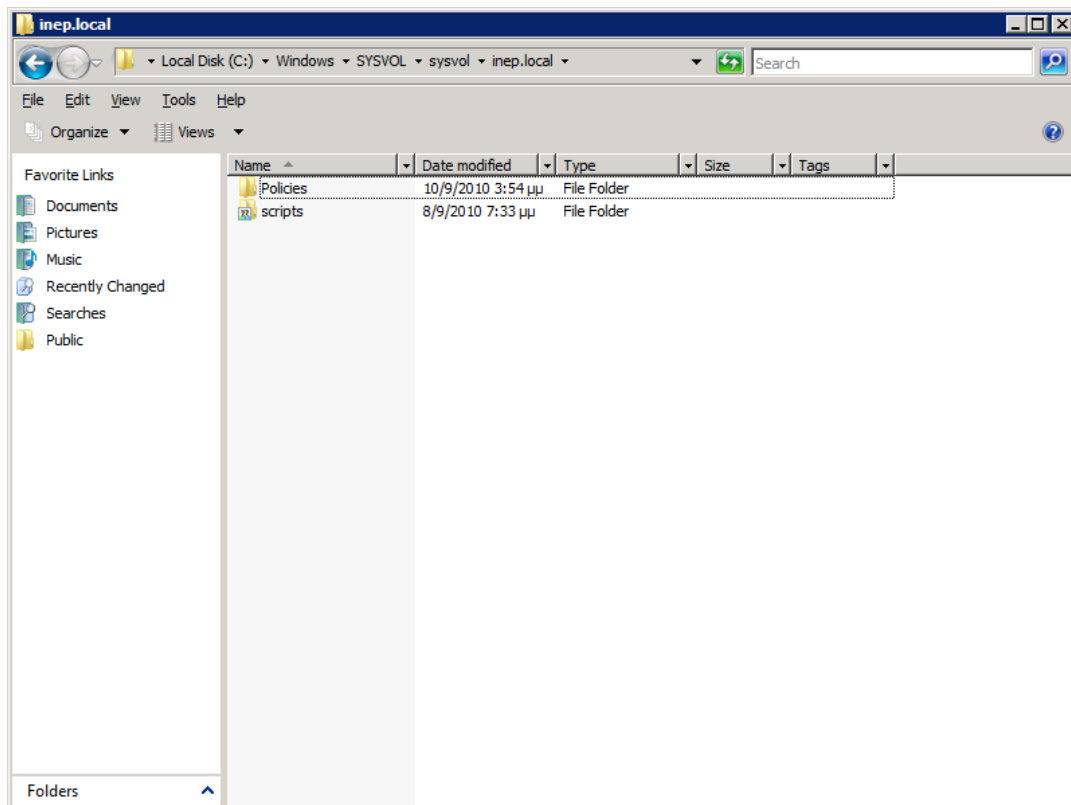
Εικ..3.150

Εσωτερικά στο sysvol θα υπάρχει και πάλι shortcut στο inet.local



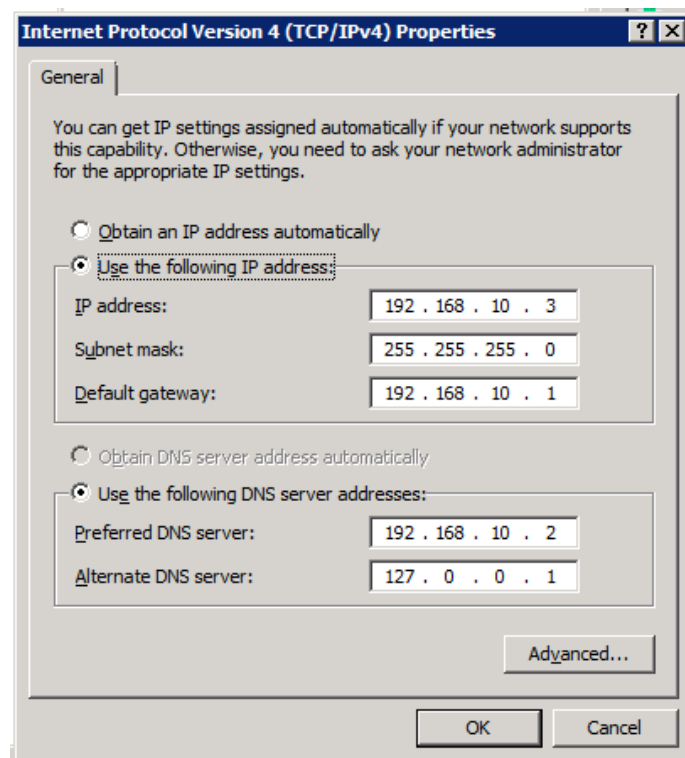
Εικ..3.151

Και μέσα στο inet.local θα πρέπει να υπάρχουν οι φάκελοι Policies και Scripts.



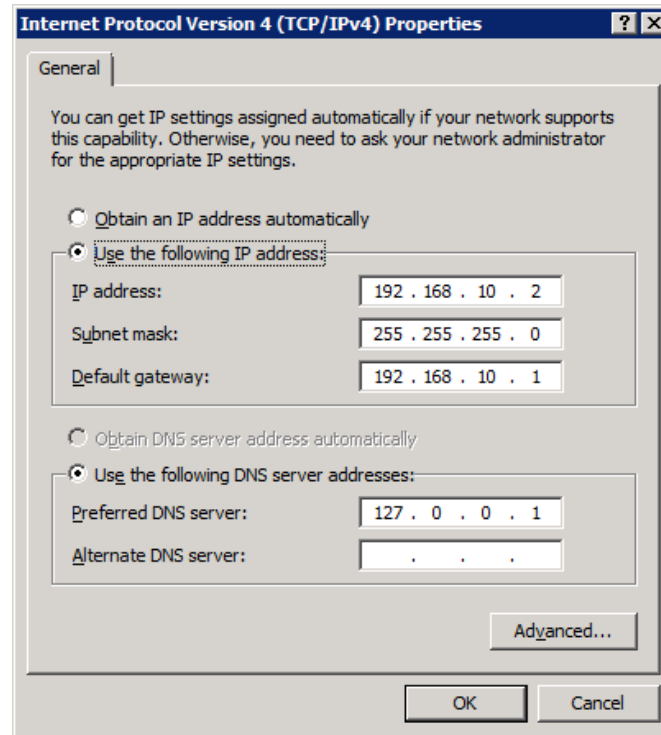
Εικ.3.152

Εξετάζοντας τις δικτυακές ρυθμίσεις του DC2, βλέπουμε ότι ως preferred DNS υπάρχει ο πρώτος όπως είχαμε ορίσει, αλλά ως Alternate υπάρχει πλέον ο εαυτός του!



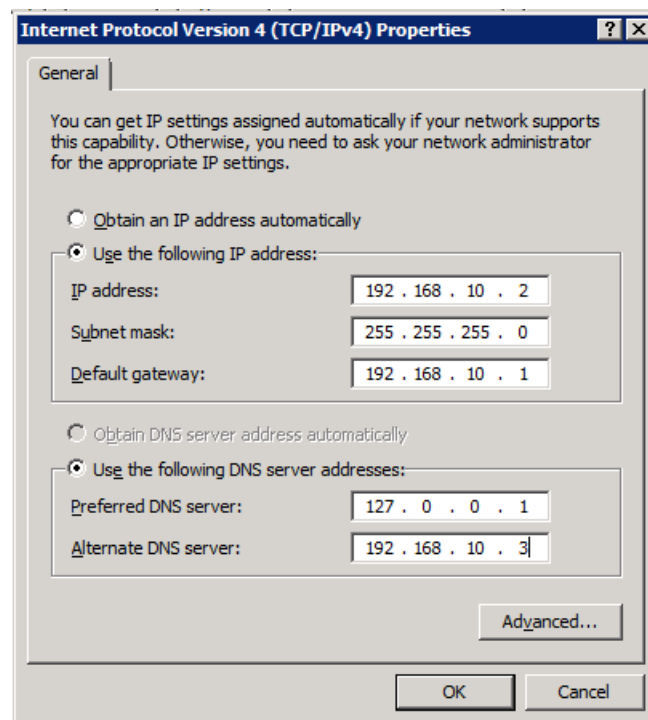
Εικ.3.153

Πηγαίνουμε στον DC1 για να θυμηθούμε τις ρυθμίσεις αυτές:



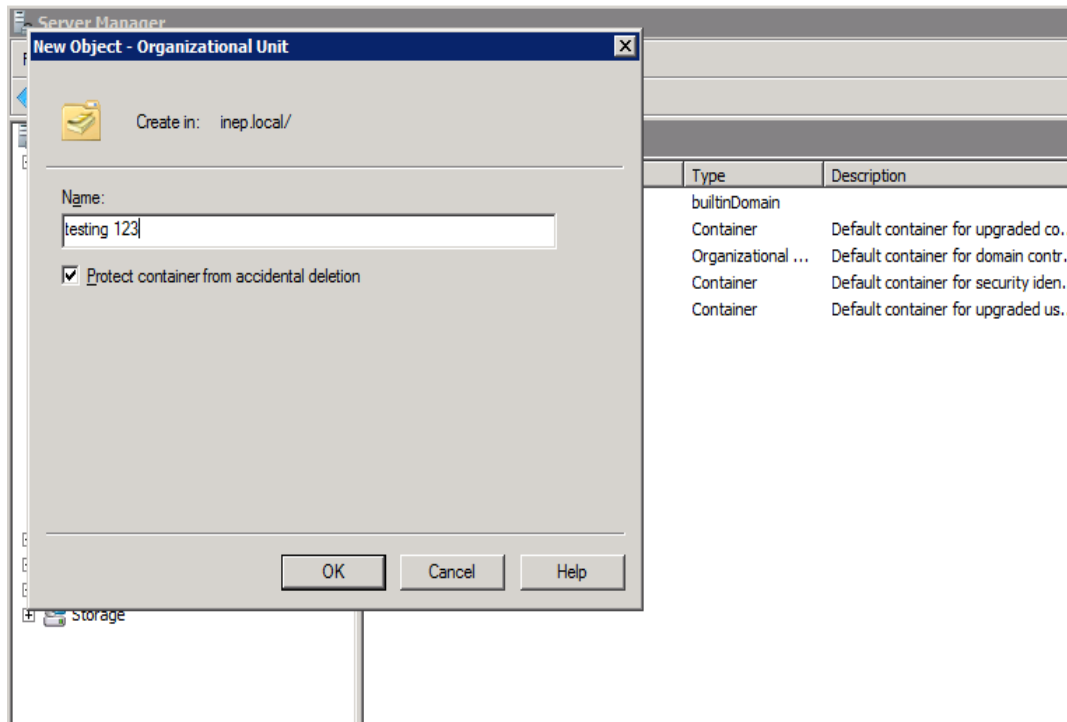
Εικ..3.154

Και για να έχουμε failover λειτουργία ρυθμίζουμε ως Alternate τον DC2!



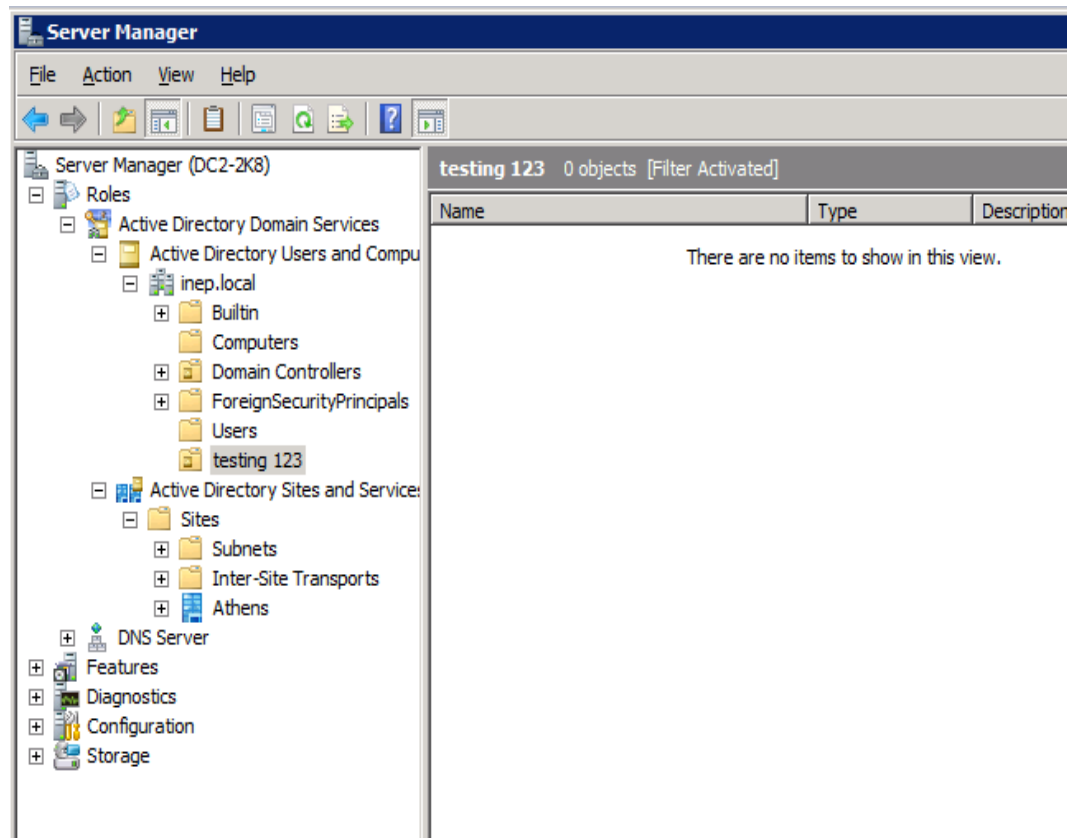
Εικ..3.155

Τώρα είμαστε έτοιμοι να ελέγξουμε το Replication μεταξύ των δύο DCs. Πηγαίνουμε στον δεύτερο DC και φτιάχνουμε ένα Organizational Unit μέσα στο Active Directory Users and Computers, με δεξί κλικ, new OU, έστω το testing 123.



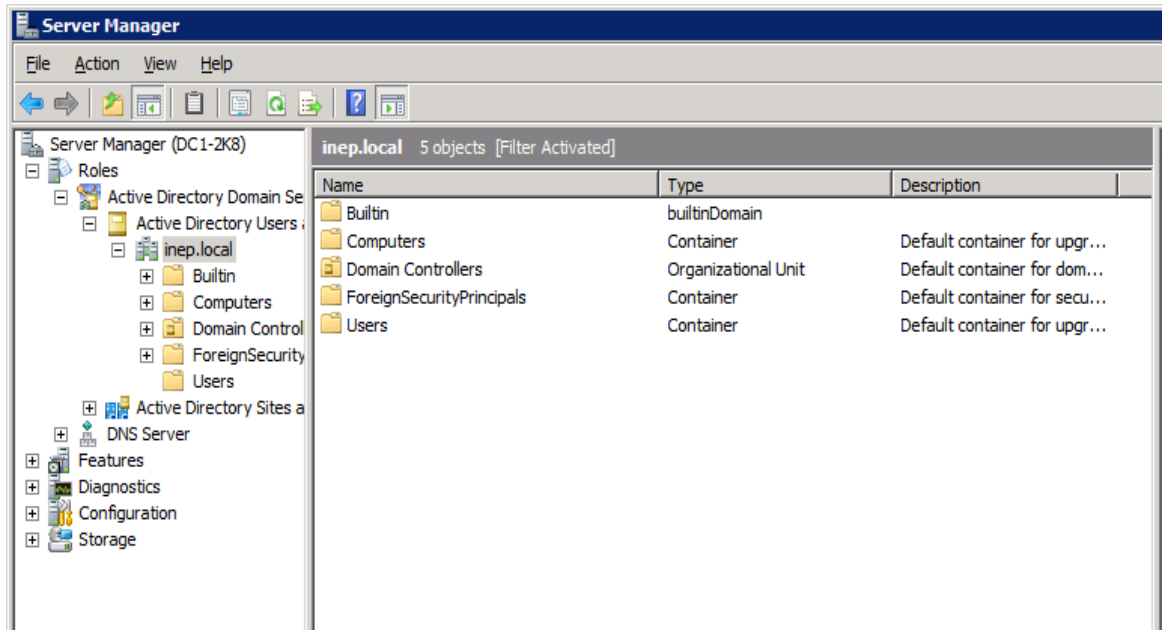
Εικ..3.156

Το βλέπουμε στην ακόλουθη θέση



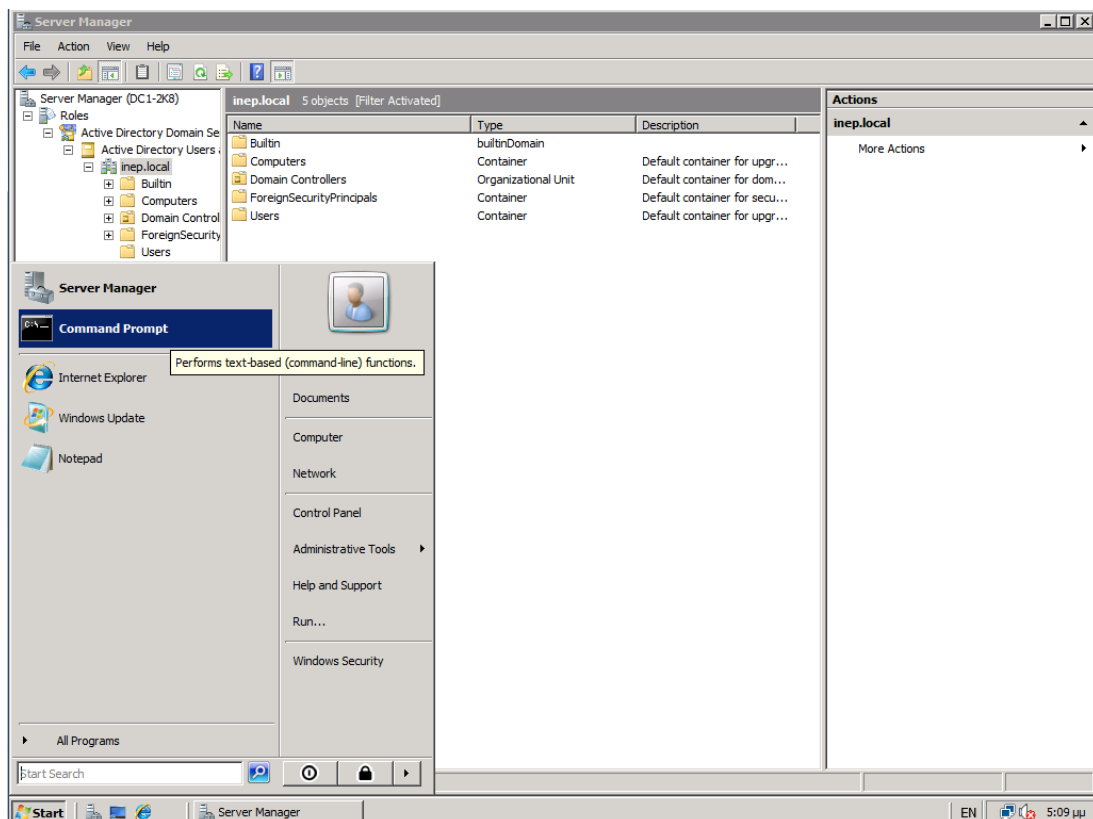
Εικ..3.157

Στη συνέχεια πάμε στον πρώτο να δούμε αν υπάρχει.



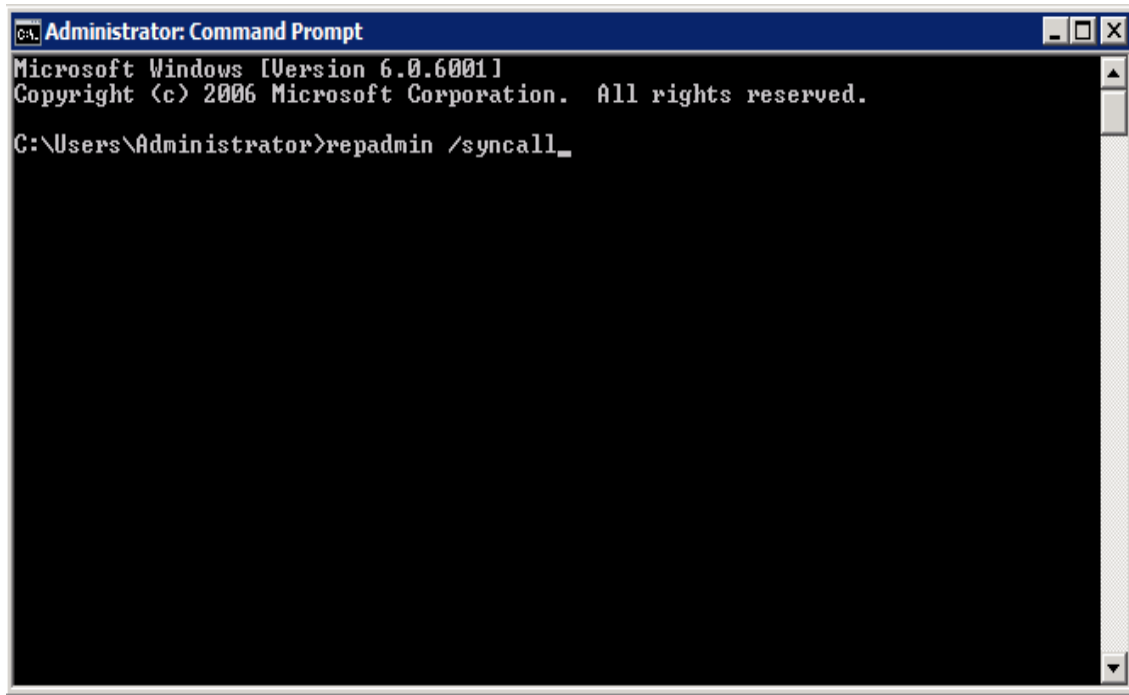
Εικ..3.158

Βλέπουμε ότι δεν έχει δημιουργηθεί στον πρώτο DC. Για να εξαναγκάσουμε την λειτουργία του replication και να ελέγξουμε αν όντως λειτουργεί σωστά ανοίγουμε ένα παράθυρο CMD,



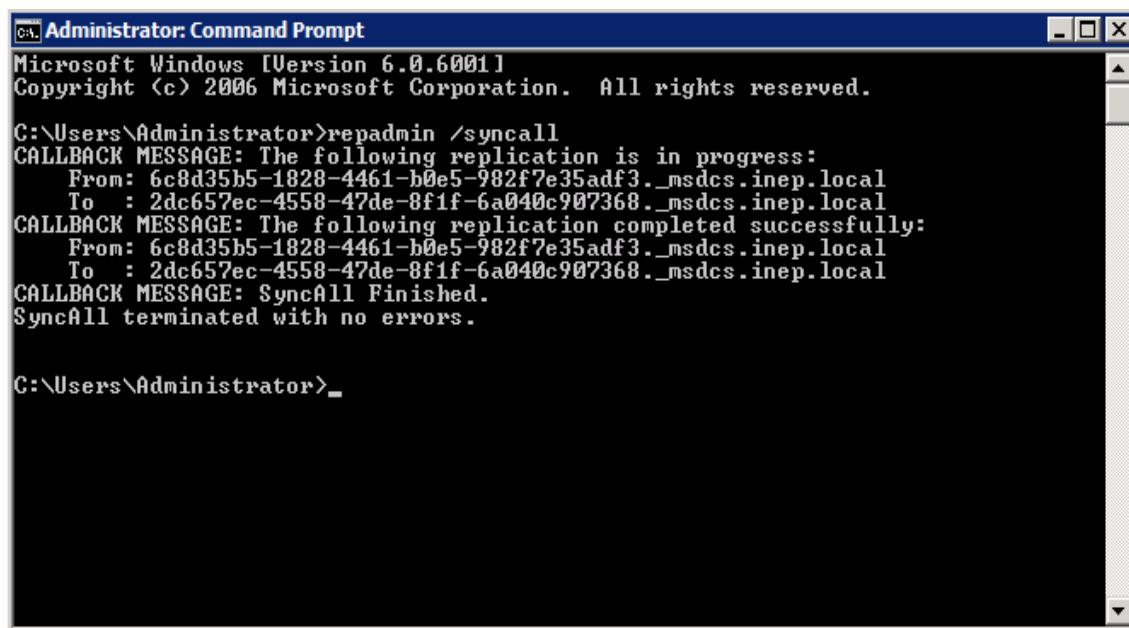
Εικ..3.159

Και γράφουμε: repadim /syncall



Εικ.3.160

Πατάμε Enter και βλέπουμε ότι η διαδικασία τερμάτισε με επιτυχία!

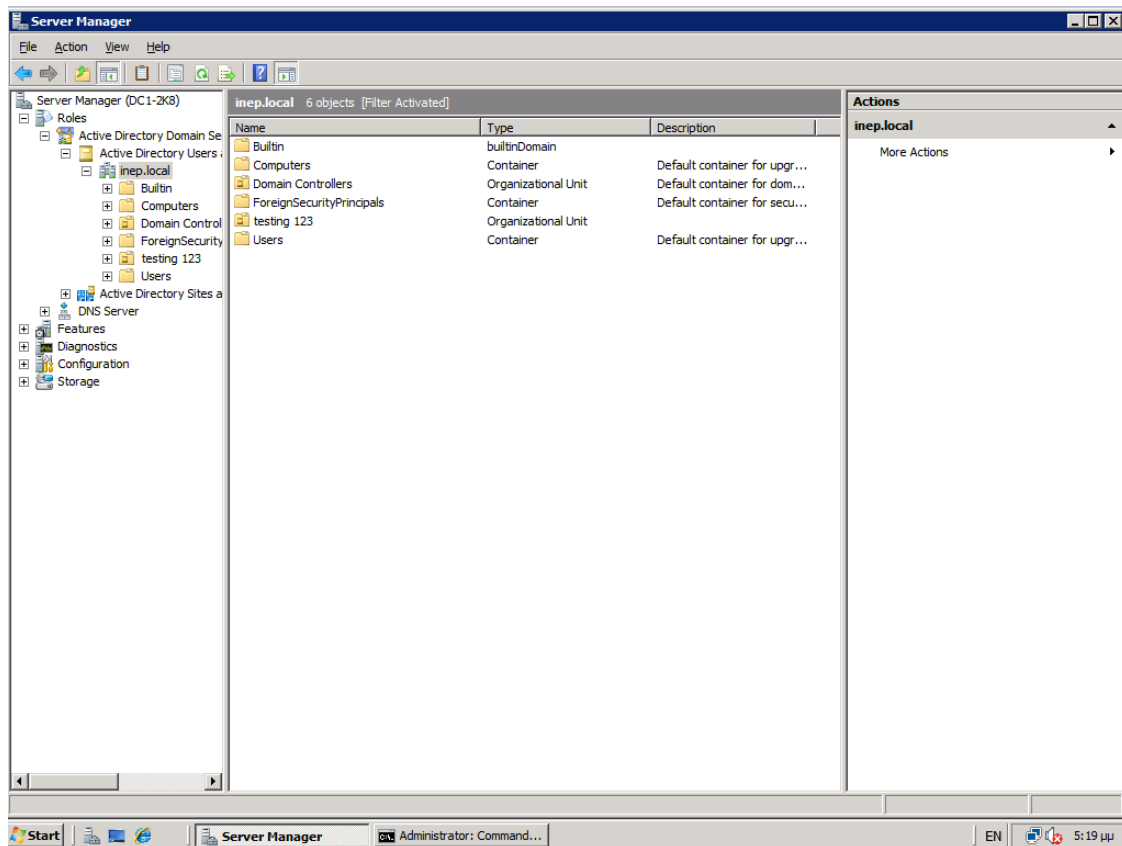


Εικ.3.161

Στον Server Manager, στο Active Directory Users and Computers υπάρχει πλέον το νέο OU.

Το domain μας είναι πλέον λειτουργικό και έτοιμο για χρήση.

Να σημειώσουμε τέλος ότι πολλές φορές οι MMCs κολλάνε και δεν δείχνουν τα σωστά στοιχεία. Για να είμαστε σίγουροι ότι απεικονίζονται τα τελευταία δεδομένα, μπορούμε να κάνουμε refresh της MMC πατώντας το πλήκτρο F5.



Εικ..3.162

ΥΛΟΠΟΙΗΣΗ, ΔΙΑΧΕΙΡΙΣΗ, ΣΥΝΤΗΡΗΣΗ ΔΙΚΤΥΑΚΗΣ ΥΠΟΔΟΜΗΣ

4.1 Εισαγωγή

Οι επιθυμητές γνώσεις και δεξιότητες που θα αποκτήσουν οι επιμορφωμένοι στην ενότητα «Υλοποίηση, Διαχείριση, Συντήρηση Δικτυακής Υποδομής» θα τους καταστήσουν ικανούς να:

- Περιγράφουν τα επίπεδα του μοντέλου αναφοράς δικτύων TCP/IP.
- Γνωρίζουν τη λειτουργία και τη σημασία της υπηρεσίας DHCP.
- Ρυθμίζουν το ρόλο του DHCP Server σε υπολογιστή Windows Server 2008
- Εκτελούν επιμέρους διαχειριστικές ενέργειες στον DHCP Server, όπως ρυθμίσεις scope, address ranges, exxclusions, reservations, DHCP oprtions, client configuration, start, stop, restart, resume.

4.2 Εισαγωγή στα TCP/IP δίκτυα.

Όταν ρυθμίσουμε τις παραμέτρους του πρωτοκόλλου TCP/IP σε έναν υπολογιστή Microsoft Windows, χρειάζεται να δώσουμε μια διεύθυνση IP, μια μάσκα υποδικτύου και συνήθως μια προεπιλεγμένη πύλη στις ρυθμίσεις παραμέτρων του πρωτοκόλλου TCP/IP, μέσω της κατάλληλης διαδρομής η οποία εξαρτάται συνήθως από το λειτουργικό σύστημα που εκτελεί ο υπολογιστής.

Προκειμένου να ρυθμιστούν σωστά οι παράμετροι του πρωτοκόλλου TCP/IP, είναι απαραίτητο να γνωρίζουμε πώς δημιουργούνται οι διευθύνσεις των δικτύων TCP/IP και πώς διαιρούνται σε δίκτυα και υποδίκτυα.

Η επιτυχία του πρωτοκόλλου TCP/IP ως του πρωτοκόλλου δικτύου του Internet οφείλεται κυρίως στη δυνατότητά του να συνδέει δίκτυα διαφόρων μεγεθών και συστήματα διαφορετικών τύπων. Αυτά τα δίκτυα ορίζονται αυθαίρετα σε τρεις κύριες κλάσεις: Class A, Class B, Class C (μαζί με μερικές άλλες δηλ. Class D και Class E) που έχουν προκαθορισμένα μεγέθη, καθένα από τα οποία μπορεί να διαιρεθεί σε μικρότερα υποδίκτυα από τους διαχειριστές συστήματος.

Μια μάσκα υποδικτύου χρησιμοποιείται για να διαιρέσει μια διεύθυνση IP σε δύο μέρη: Το ένα μέρος προσδιορίζει τον κεντρικό υπολογιστή, ενώ το άλλο μέρος προσδιορίζει το δίκτυο στο οποίο ανήκει.

Για να κατανοήσουμε καλύτερα τον τρόπο με τον οποίο λειτουργούν οι διευθύνσεις IP και οι μάσκες υποδικτύου, ας εξετάσουμε μια διεύθυνση IP (Πρωτοκόλλου

Internet) για να δούμε πώς είναι οργανωμένη.

4.2.1 Διευθύνσεις IP: Δίκτυα και κεντρικοί υπολογιστές

Μια διεύθυνση IP (version 4) είναι ένας αριθμός μεγέθους 32 bit που προσδιορίζει μοναδικά έναν κεντρικό υπολογιστή (υπολογιστή ή άλλη δικτυακή συσκευή, όπως εκτυπωτή ή δρομολογητή) σε ένα δίκτυο TCP/IP.

Οι διευθύνσεις IP εκφράζονται κανονικά σε μορφή δεκαδικών διευθύνσεων με τελείες, με τέσσερις δεκαδικούς αριθμούς (ομάδες από 8bit) να χωρίζονται από τελείες, όπως: **192.168.123.132**. Για να κατανοήσουμε πώς χρησιμοποιούνται οι μάσκες υποδικτύου για τη διάκριση μεταξύ κεντρικών υπολογιστών, δικτύων και υποδικτύων, ας εξετάσουμε μια διεύθυνση IP σε δυαδική μορφή.

Για παράδειγμα, η δεκαδική διεύθυνση IP με τελείες 192.168.123.132 (σε δυαδική μορφή) είναι ο αριθμός 32 bit 110000000101000111101110000100. Αυτός ο αριθμός μπορεί να είναι δυσνόητος, για αυτό συνήθως τον χωρίζουμε σε τέσσερα μέρη των οκτώ δυαδικών ψηφίων.

Αυτές οι ενότητες των οκτώ bit είναι γνωστές ως οκτάδες. Το δείγμα διεύθυνσης IP γίνεται τότε 11000000.10101000.01111011.10000100. Αυτός ο αριθμός είναι απλώς λίγο πιο κατανοητός, επομένως για τις περισσότερες χρήσεις, μετατρέπουμε τη δυαδική διεύθυνση αυτή σε μορφή δεκαδικής διεύθυνσης με τελείες και γίνεται 192.168.123.132. Οι δεκαδικοί αριθμοί που χωρίζονται από τελείες είναι οι οκτάδες που μετατράπηκαν από δυαδική σε δεκαδική μορφή.

Για να λειτουργήσει αποδοτικά ένα ευρύτερο δίκτυο (wide area network - WAN) TCP/IP ως συλλογή δικτύων, οι δρομολογητές που μεταβιβάζουν πακέτα δεδομένων μεταξύ δικτύων δεν γνωρίζουν την ακριβή θέση του κεντρικού υπολογιστή για τον οποίο προορίζεται ένα πακέτο πληροφοριών. Οι δρομολογητές γνωρίζουν μόνο σε ποιο δίκτυο ανήκει ο κεντρικός υπολογιστής και χρησιμοποιούν τις πληροφορίες που είναι αποθηκευμένες στον πίνακα διαδρομών τους, για να καθορίσουν τον τρόπο μεταβίβασης του πακέτου στο δίκτυο που υπάρχει ο κεντρικός υπολογιστής προορισμού. Μετά την παράδοση του πακέτου στο δίκτυο προορισμού, το πακέτο παραδίδεται στον κατάλληλο κεντρικό υπολογιστή.

Για να λειτουργήσει αυτή η διαδικασία, μια διεύθυνση IP έχει δύο μέρη. Το πρώτο μέρος μιας διεύθυνσης IP χρησιμοποιείται ως διεύθυνση δικτύου και το τελευταίο μέρος ως διεύθυνση κεντρικού υπολογιστή. Εάν πάρουμε το παράδειγμα 192.168.123.132 και το χωρίσουμε σε αυτά τα δύο μέρη, έχουμε τα εξής:

192.168.123.	Δίκτυο
--------------	--------

.132 Κεντρικός υπολογιστής

Ή αλλιώς

192.168.123.0 - διεύθυνση δικτύου.

0.0.0.132 - διεύθυνση κεντρικού υπολογιστή.

4.2.2 Μάσκα υποδικτύου

Το δεύτερο στοιχείο, που απαιτείται για να λειτουργήσει το TCP/IP, είναι η μάσκα υποδικτύου ή αλλιώς subnet mask. Η μάσκα υποδικτύου χρησιμοποιείται από το πρωτόκολλο TCP/IP για να προσδιορίσει αν ένας κεντρικός υπολογιστής βρίσκεται στο τοπικό υποδίκτυο ή σε απομακρυσμένο δίκτυο.

Στο TCP/IP, τα μέρη της διεύθυνσης IP που χρησιμοποιούνται ως το δίκτυο και οι διευθύνσεις κεντρικού υπολογιστή δεν είναι σταθερές, επομένως το δίκτυο και οι διευθύνσεις κεντρικού υπολογιστή παραπάνω δεν μπορούν να καθοριστούν, εκτός αν έχετε περισσότερες πληροφορίες.

Αυτές οι πληροφορίες παρέχονται σε έναν άλλο αριθμό 32 bit, που ονομάζεται μάσκα υποδικτύου. Σε αυτό το παράδειγμα, η μάσκα υποδικτύου είναι 255.255.255.0. Δεν είναι προφανές τι σημαίνει αυτός ο αριθμός, εκτός αν αναλογιστούμε ότι το 255 σε δυαδική μορφή ισούται με 11111111. Επομένως, η μάσκα υποδικτύου είναι:

11111111.11111111.11111111.00000000

Στοιχίζοντας τη διεύθυνση IP και τη μάσκα υποδικτύου μαζί, τα τμήματα του δικτύου και του κεντρικού υπολογιστή της διεύθυνσης μπορούν να διαχωριστούν:

11000000.10101000.01111011.10000100 -- Διεύθυνση IP (192.168.123.132)

11111111.11111111.11111111.00000000 -- Μάσκα υποδικτύου (255.255.255.0)

Τα πρώτα 24 bit (το πλήθος των αριθμών 1 στη μάσκα υποδικτύου) προσδιορίζονται ως η διεύθυνση δικτύου, με τα τελευταία 8 bit (το πλήθος των μηδενικών που απομένουν στη μάσκα υποδικτύου) να προσδιορίζονται ως η διεύθυνση του κεντρικού υπολογιστή. Αυτό σας δίνει τα εξής:

11000000.10101000.01111011.00000000 -- Διεύθυνση δικτύου:
(192.168.123.0)

00000000.00000000.00000000.10000100 -- Διεύθυνση κεντρικού υπολογιστή:
(000.000.000.132)

Επομένως, τώρα γνωρίζουμε, για αυτό το παράδειγμα που χρησιμοποιεί μια μάσκα υποδικτύου 255.255.255.0, ότι το αναγνωριστικό δικτύου είναι 192.168.123.0 και ότι η διεύθυνση κεντρικού υπολογιστή είναι 0.0.0.132. Όταν ένα πακέτο φθάσει στο υποδίκτυο 192.168.123.0 (από το τοπικό υποδίκτυο ή ένα απομακρυσμένο δίκτυο) και έχει διεύθυνση προορισμού 192.168.123.132, ο υπολογιστής σας θα το λάβει από το δίκτυο και θα το επεξεργαστεί.

Σχεδόν όλες οι δεκαδικές μάσκες υποδικτύου μετατρέπονται σε δυαδικούς αριθμούς που είναι όλοι ο αριθμός ένα στα αριστερά και όλα τα μηδενικά στα δεξιά. Μερικές άλλες κοινές μάσκες υποδικτύου είναι οι εξής:

Δεκαδική	Δυαδική
255.255.255.192	1111111.11111111.1111111.11000000
255.255.255.224	1111111.11111111.1111111.11100000

Το Internet RFC 1878 (διαθέσιμο από την τοποθεσία <http://www.internic.net>) περιγράφει τα έγκυρα υποδίκτυα και μάσκες υποδικτύου που μπορούν να χρησιμοποιηθούν σε δίκτυα TCP/IP.

4.2.3 Κλάσεις δικτύου

Οι διευθύνσεις Internet εκχωρούνται από την InterNIC (<http://www.internic.net>), τον οργανισμό που διαχειρίζεται το Internet. Αυτές οι διευθύνσεις IP διαιρούνται σε κλάσεις. Οι πιο κοινές από αυτές είναι οι κλάσεις A, B και C. Οι κλάσεις D και E υπάρχουν, αλλά γενικά δεν χρησιμοποιούνται από τελικούς χρήστες.

Κάθε κλάση διεύθυνσης έχει διαφορετική προεπιλεγμένη μάσκα υποδικτύου. Μπορούμε να προσδιορίσουμε την κλάση μιας διεύθυνσης IP, εξετάζοντας την πρώτη οκτάδα της. Ακολουθούν οι περιοχές των διευθύνσεων Internet για τις κλάσεις A, B και C, μαζί με παραδείγματα διευθύνσεων για την καθεμία:

- Τα δίκτυα της κλάσης A χρησιμοποιούν μια προεπιλεγμένη μάσκα υποδικτύου 255.0.0.0 και έχουν την περιοχή 0-127 ως την πρώτη οκτάδα τους. Η διεύθυνση 10.52.36.11 είναι μια διεύθυνση της κλάσης A. Η πρώτη οκτάδα της είναι 10, που είναι μεταξύ 1 έως και 126.
- Τα δίκτυα της κλάσης B χρησιμοποιούν μια προεπιλεγμένη μάσκα υποδικτύου 255.255.0.0 και έχουν την περιοχή 128-191 ως την πρώτη οκτάδα τους. Η διεύθυνση 172.16.52.63 είναι μια διεύθυνση κλάσης B. Η πρώτη οκτάδα της είναι 172, που είναι μεταξύ 128 έως και 191.

- Τα δίκτυα της κλάσης C χρησιμοποιούν μια προεπιλεγμένη μάσκα υποδικτύου 255.255.255.0 και έχουν την περιοχή 192-223 ως την πρώτη οκτάδα τους. Η διεύθυνση 192.168.123.132 είναι μια διεύθυνση της κλάσης C. Η πρώτη οκτάδα της είναι 192, που είναι μεταξύ 192 έως και 223.

Σε ορισμένα σενάρια, οι τιμές της προεπιλεγμένης μάσκας υποδικτύου δεν ικανοποιούν τις ανάγκες της εταιρείας, λόγω της φυσικής τοπολογίας του δικτύου ή επειδή οι αριθμοί των δικτύων (ή των κεντρικών υπολογιστών) δεν υπόκεινται στους περιορισμούς της προεπιλεγμένης μάσκας υποδικτύου. Η επόμενη ενότητα επεξηγεί πώς μπορούν να διαιρεθούν τα δίκτυα χρησιμοποιώντας μάσκες υποδικτύου.

4.2.4 Δημιουργία υποδικτύων

Ένα δίκτυο TCP/IP κλάσης A, B ή C μπορεί να διαιρεθεί περαιτέρω ή να διακριθεί σε υποδίκτυα από ένα διαχειριστή συστήματος. Αυτό γίνεται απαραίτητο, καθώς επιλύουμε το συνδυασμό λογικής διεύθυνσης του Internet (τον αφηρημένο κόσμο των διευθύνσεων IP και των υποδικτύων) με τα φυσικά δίκτυα που χρησιμοποιούνται από τον πραγματικό κόσμο.

Ένας διαχειριστής συστήματος στον οποίο έχει εκχωρηθεί ένα μπλοκ διευθύνσεων IP μπορεί να διαχειρίζεται δίκτυα που δεν είναι οργανωμένα με τρόπο που να ταιριάζει εύκολα σε αυτές τις διευθύνσεις. Για παράδειγμα, έχουμε ένα ευρύτερο δίκτυο με 150 κεντρικούς υπολογιστές σε τρία δίκτυα (σε διαφορετικές πόλεις) που συνδέονται από ένα δρομολογητή TCP/IP. Καθένα από αυτά τα τρία δίκτυα διαθέτει 50 κεντρικούς υπολογιστές. Σας εκχωρείται το δίκτυο κλάσης C 192.168.123.0. (Πληροφορικά, αυτή η διεύθυνση προέρχεται στην πραγματικότητα από μια περιοχή που δεν είναι εκχωρημένη στο Internet.) Αυτό σημαίνει ότι μπορείτε να χρησιμοποιήσετε τις διευθύνσεις 192.168.123.1 έως 192.168.123.254 για τους 150 κεντρικούς υπολογιστές σας.

Οι δύο διευθύνσεις που δεν μπορούν να χρησιμοποιηθούν στο παράδειγμά μας είναι 192.168.123.0 και 192.168.123.255, επειδή οι δυαδικές διευθύνσεις με τμήμα διεύθυνσης κεντρικού υπολογιστή με όλους τους αριθμούς ένα (1) ή όλους μηδεν (0) δεν είναι έγκυρες:

- Η μηδενική διεύθυνση δεν είναι έγκυρη, επειδή χρησιμοποιείται για να καθορίσει ένα δίκτυο χωρίς να καθορίζει έναν κεντρικό υπολογιστή.
- Η διεύθυνση 255 (σε δυαδική μορφή, μια διεύθυνση κεντρικού υπολογιστή για όλους τους αριθμούς ένα) χρησιμοποιείται για να αναμεταδώσει ένα

μήνυμα σε κάθε κεντρικό υπολογιστή ενός δικτύου.

Απλώς συγκρατούμε ότι: η πρώτη και η τελευταία διεύθυνση σε οποιοδήποτε δίκτυο ή υποδίκτυο δεν μπορεί να αντιστοιχιστεί σε κανένα μεμονωμένο κεντρικό υπολογιστή.

Τώρα, πρέπει να μπορούμε να δώσουμε διευθύνσεις IP σε 254 κεντρικούς υπολογιστές. Αυτό λειτουργεί καλά, σε περίπτωση που και οι 150 υπολογιστές βρίσκονται σε ένα δίκτυο. Ωστόσο, οι 150 υπολογιστές σας βρίσκονται σε τρία ξεχωριστά φυσικά δίκτυα.

Αντί να ζητήσουμε περισσότερα μπλοκ διευθύνσεων για κάθε δίκτυο, διαιρούμε το δίκτυό μας σε υποδίκτυα που μας επιτρέπουν να χρησιμοποιούμε ένα μπλοκ διευθύνσεων σε πολλά φυσικά δίκτυα.

Σε αυτήν την περίπτωση, διαιρούμε το δίκτυό σας σε τέσσερα υποδίκτυα, χρησιμοποιώντας μια μάσκα υποδικτύου που κάνει τη διεύθυνση δικτύου μεγαλύτερη και την πιθανή περιοχή διευθύνσεων κεντρικού υπολογιστή μικρότερη. Δηλαδή, «δανειζόμαστε» ορισμένα από τα bit που συνήθως χρησιμοποιούνται για τη διεύθυνση κεντρικού υπολογιστή και τα χρησιμοποιούμε για το τμήμα της διεύθυνσης δικτύου.

Η μάσκα υποδικτύου 255.255.255.192 μας δίνει τέσσερα δίκτυα, καθένα από τα οποία διαθέτει 62 κεντρικούς υπολογιστές. Αυτό λειτουργεί, επειδή σε δυαδική μορφή το 255.255.255.192 είναι το ίδιο με το 1111111.11111111.1111111.11000000. Τα πρώτα δύο ψηφία της τελευταίας οκτάδας γίνονται διευθύνσεις δικτύου, επομένως λαμβάνουμε τα πρόσθετα δίκτυα 00000000 (0), 01000000 (64), 10000000 (128) και 11000000 (192). (Ορισμένοι διαχειριστές χρησιμοποιούν μόνο δύο από τα υποδίκτυα, χρησιμοποιώντας το 255.255.255.192 ως μάσκα υποδικτύου. Για περισσότερες πληροφορίες σχετικά με αυτό το θέμα, ανατρέξτε στο RFC 1878.) Σε αυτά τα τέσσερα δίκτυα, τα τελευταία 6 δυαδικά ψηφία μπορούν να χρησιμοποιηθούν για διευθύνσεις κεντρικών υπολογιστών.

Χρησιμοποιώντας μια μάσκα υποδικτύου 255.255.255.192, το δίκτυο 192.168.123.0 μεταβάλλεται στα εξής τέσσερα δίκτυα: 192.168.123.0, 192.168.123.64, 192.168.123.128 και 192.168.123.192. Αυτά τα τέσσερα δίκτυα έχουν τις εξής έγκυρες διευθύνσεις κεντρικών υπολογιστών:

192.168.123.1-62

192.168.123.65-126

192.168.123.129-190

192.168.123.193.254

Υπενθυμίζουμε ξανά, ότι οι δυαδικές διευθύνσεις κεντρικού υπολογιστή με όλους τους αριθμούς (1) ένα ή όλους μηδενικά (0) δεν είναι έγκυρες, επομένως δεν μπορούμε να χρησιμοποιήσουμε διευθύνσεις με την τελευταία οκτάδα 0, 63, 64, 127, 128, 191, 192 ή 255.

Μπορούμε να δούμε πώς λειτουργεί αυτό, εξετάζοντας δύο διευθύνσεις κεντρικού υπολογιστή, 192.168.123.71 και 192.168.123.133. Εάν χρησιμοποιήσουμε την προεπιλεγμένη μάσκα υποδικτύου κλάσης C δηλαδή της 255.255.255.0, και οι δύο διευθύνσεις βρίσκονται στο δίκτυο 192.168.123.0. Ωστόσο, αν χρησιμοποιήσουμε τη μάσκα υποδικτύου 255.255.255.192, βρίσκονται σε διαφορετικά δίκτυα. Το 192.168.123.71 βρίσκεται στο δίκτυο 192.168.123.64, ενώ το 192.168.123.133 βρίσκεται στο δίκτυο 192.168.123.128.

4.2.5 Προεπιλεγμένες πύλες (Default Gateway)

Εάν ένας υπολογιστής TCP/IP χρειάζεται να επικοινωνήσει με έναν κεντρικό υπολογιστή σε άλλο δίκτυο, συνήθως επικοινωνεί μέσω μιας συσκευής που ονομάζεται δρομολογητής. Σύμφωνα με τους όρους του TCP/IP, ένας δρομολογητής που καθορίζεται σε έναν κεντρικό υπολογιστή, ο οποίος συνδέει το υποδίκτυο του κεντρικού υπολογιστή με άλλα δίκτυα, ονομάζεται προεπιλεγμένη πύλη. Αυτή η ενότητα επεξηγεί τον τρόπο με τον οποίο το TCP/IP καθορίζει αν θα στείλει πακέτα στην προεπιλεγμένη πύλη του για να προσεγγίσει έναν άλλο υπολογιστή ή συσκευή στο δίκτυο.

Όταν ένας κεντρικός υπολογιστής προσπαθεί να επικοινωνήσει με μια άλλη συσκευή χρησιμοποιώντας το TCP/IP, εκτελεί μια διαδικασία σύγκρισης χρησιμοποιώντας την καθορισμένη μάσκα υποδικτύου και τη διεύθυνση IP προορισμού, αντί για τη μάσκα υποδικτύου και τη δική του διεύθυνση IP. Το αποτέλεσμα αυτής της σύγκρισης υποδεικνύει στον υπολογιστή αν ο προορισμός είναι τοπικός ή απομακρυσμένος κεντρικός υπολογιστής.

Εάν το αποτέλεσμα αυτής της διαδικασίας προσδιορίζει ότι ο προορισμός είναι ένας τοπικός κεντρικός υπολογιστής, τότε ο υπολογιστής απλώς θα αποστείλει το πακέτο στο τοπικό υποδίκτυο. Εάν το αποτέλεσμα της σύγκρισης προσδιορίζει ότι ο προορισμός είναι ένας απομακρυσμένος κεντρικός υπολογιστής, τότε ο υπολογιστής θα προωθήσει το πακέτο στην προεπιλεγμένη πύλη, που ορίζεται στις ιδιότητες

TCP/IP. Κατόπιν, είναι ευθύνη του δρομολογητή να προωθήσει το πακέτο στο σωστό υποδίκτυο.

4.2.6 Αντιμετώπιση προβλημάτων

Τα προβλήματα δικτύου TCP/IP συχνά προκαλούνται από εσφαλμένη ρύθμιση παραμέτρων των τριών κύριων καταχωρήσεων στις ιδιότητες TCP/IP ενός υπολογιστή. Κατανοώντας τον τρόπο με τον οποίο τα σφάλματα της ρύθμισης παραμέτρων TCP/IP επηρεάζουν τις λειτουργίες του δικτύου, μπορούμε να επιλύσουμε πολλά κοινά προβλήματα του TCP/IP.

4.2.6.1 Εσφαλμένη μάσκα υποδικτύου

Εάν ένα δίκτυο χρησιμοποιεί μια μάσκα υποδικτύου διαφορετική από την προεπιλεγμένη μάσκα για την κλάση διευθύνσεών του και οι παράμετροι ενός προγράμματος-πελάτη εξακολουθούν να είναι ρυθμισμένες με την προεπιλεγμένη μάσκα υποδικτύου για την κλάση διευθύνσεων, η επικοινωνία θα αποτύχει σε ορισμένα κοντινά δίκτυα αλλά όχι σε μακρινά.

Για παράδειγμα, αν δημιουργήσουμε τέσσερα υποδίκτυα (όπως στο παράδειγμα δημιουργίας υποδικτύων) αλλά χρησιμοποιήσουμε την εσφαλμένη μάσκα υποδικτύου 255.255.255.0 στη ρύθμιση παραμέτρων TCP/IP, οι κεντρικοί υπολογιστές δεν θα μπορέσουν να προσδιορίσουν ότι ορισμένοι υπολογιστές βρίσκονται σε διαφορετικά υποδίκτυα από το δικό τους. Όταν συμβεί αυτό, τα πακέτα που προορίζονται για κεντρικούς υπολογιστές σε διαφορετικά φυσικά δίκτυα που ανήκουν στην ίδια διεύθυνση κλάσης C δεν θα σταλούν σε μια προεπιλεγμένη πύλη για παράδοση. Ένα κοινό σύμπτωμα για αυτό είναι όταν ένας υπολογιστής μπορεί να επικοινωνήσει με κεντρικούς υπολογιστές που βρίσκονται στο τοπικό του δίκτυο και μπορεί να "συνομιλήσει" με όλα τα απομακρυσμένα δίκτυα εκτός από εκείνα που βρίσκονται κοντά και έχουν την ίδια διεύθυνση κλάσης A, B ή C. Για να διορθώσουμε αυτό το πρόβλημα, απλώς πληκτρολογούμε τη σωστή μάσκα υποδικτύου στη ρύθμιση παραμέτρων TCP/IP για αυτόν τον κεντρικό υπολογιστή.

4.2.6.2 Εσφαλμένη διεύθυνση IP

Εάν τοποθετήσουμε μαζί υπολογιστές με διευθύνσεις IP που πρέπει να βρίσκονται σε ξεχωριστά υποδίκτυα σε ένα τοπικό δίκτυο, δεν θα είναι σε θέση να επικοινωνήσουν. Θα προσπαθήσουν να στείλουν πακέτα ο ένας στον άλλο μέσω ενός δρομολογητή που δεν θα μπορεί να τα προωθήσει σωστά. Ένα σύμπτωμα αυτού του προβλήματος είναι ένας υπολογιστής που μπορεί να "συνομιλήσει" με κεντρικούς υπολογιστές σε απομακρυσμένα δίκτυα, αλλά δεν μπορεί να επικοινωνήσει με κάποιους ή όλους τους

υπολογιστές στο τοπικό τους δίκτυο. Για να διορθώσουμε αυτό το πρόβλημα, βεβαιωνόμαστε ότι όλοι οι υπολογιστές στο ίδιο φυσικό δίκτυο έχουν διευθύνσεις IP στο ίδιο υποδίκτυο IP. Εάν δεν έχουμε διαθέσιμες άλλες διευθύνσεις IP σε ένα μεμονωμένο τμήμα δικτύου, υπάρχουν λύσεις που όμως δεν αποτελεί αντικείμενο αυτής της σύνοψης.

4.2.6.3 Εσφαλμένη προεπιλεγμένη πύλη

Ένας υπολογιστής ρυθμισμένος με εσφαλμένη προεπιλεγμένη πύλη θα μπορεί να επικοινωνήσει με κεντρικούς υπολογιστές στο τμήμα του δικτύου του, αλλά δεν θα καταφέρει να επικοινωνήσει με κεντρικούς υπολογιστές σε ορισμένα ή όλα τα απομακρυσμένα δίκτυα. Εάν ένα μεμονωμένο φυσικό δίκτυο διαθέτει περισσότερους από έναν δρομολογητές και ο εσφαλμένος δρομολογητής είναι ρυθμισμένος ως η προεπιλεγμένη πύλη, ένας κεντρικός υπολογιστής θα μπορεί να επικοινωνήσει με κάποια απομακρυσμένα δίκτυα, αλλά όχι με άλλα. Αυτό το πρόβλημα είναι κοινό, αν μια επιχείρηση έχει ένα δρομολογητή σε ένα εσωτερικό δίκτυο TCP/IP και έναν άλλο δρομολογητή συνδεδεμένο στο Internet.

Αναφορές:

"TCP/IP Illustrated, Volume 1: The Protocols," Richard Stevens, Addison Wesley, 1994

"Internetworking with TCP/IP, Volume 1: Principles, Protocols, and Architecture," Douglas E. Comer, Prentice Hall, 1995

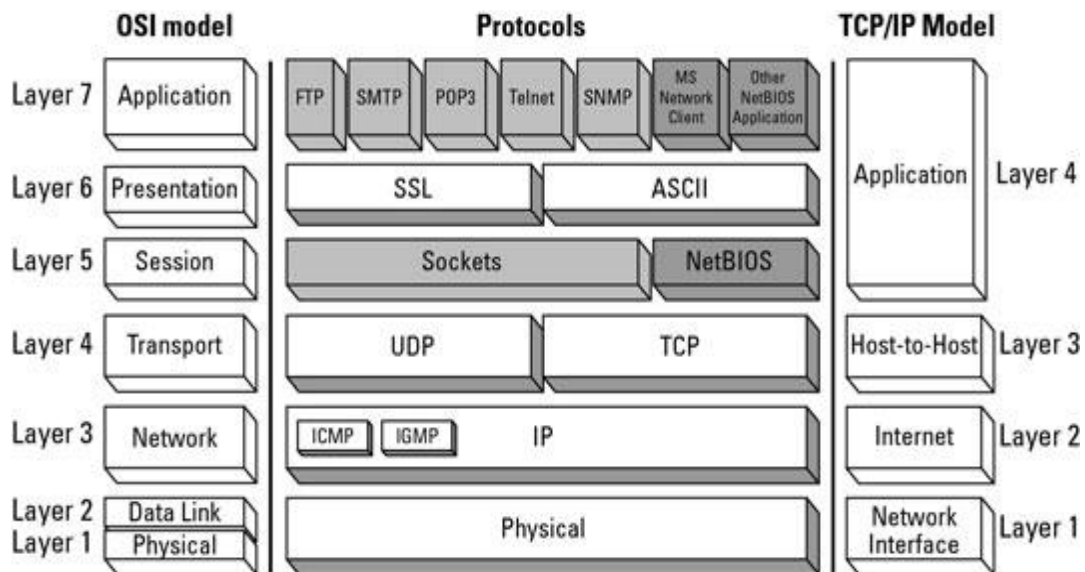
www.microsoft.com

<http://support.microsoft.com/kb/164015/el>

4.3 TCP/IP δίκτυα και OSI

Το Internet Protocol (IP) version 4 (IPv4) είναι το τρέχον στάνταρντ πρωτόκολλο "IP" που χρησιμοποιείται με το TCP/IP — Transmission Control Protocol/Internet Protocol — που είναι το πρωτόκολλο για διευθυνσιοδότηση στο διαδίκτυο (Internet addressing). Όπως και το OSI (Open System Interconnection) έχει ένα μοντέλο 7 στρωμάτων, το TCP/IP έχει και αυτό το δικό του μοντέλο.

Το μοντέλο OSI και το TCP/IP δημιουργήθηκαν και τα δύο ανεξάρτητα. Το μοντέλο δικτύων TCP/IP, αναπαριστά την πραγματικότητα στον κόσμο των δικτύων, ενώ το μοντέλο OSI αντιπροσωπεύει ένα ιδανικό κόσμο που όμως δεν υπάρχει. Εντούτοις το μοντέλο TCP/IP καλύπτει το διαστρωματομένο μοντέλο δικτύων όπως και θα έπρεπε. Ακολούθως φαίνεται μια αντιστοίχιση των δύο μοντέλων:



Το μοντέλο OSI έχει 7 στρώματα και από κάτω προς τα επάνω έχουμε:

- Φυσικό στρώμα (Physical Layer)
 - Μετάδοση ακατέργαστων bits (0 ή 1) από τον αποστολέα στον δέκτη.
- Στρώμα Ζεύξης Δεδομένων (Data Link Layer)
 - Τεμαχίζει τα δεδομένα σε πλαίσια δεδομένων (frames)
 - Επιβεβαιώνει ότι η επικοινωνία του Φυσικού στρώματος είναι αξιόπιστη (Πλαίσια επαλήθευσης -acknowledgement frames)
 - Ανίχνευση και επιδιόρθωση λαθών (Error detection and correction).
 - Έλεγχος ροής (flow control).
- Στρώμα Δικτύου (Network Layer)
 - Δρομολόγηση πακέτων
 - Έλεγχος συμφόρησης
 - Έκδοση λογαριασμών (billing)
- Στρώμα Μεταφοράς (Transport Layer)
 - Τεμαχίζει τα μηνύματα σε μικρότερες μονάδες
 - Επιβεβαιώνει ότι όλες οι μονάδες φτάνουν στο άλλο άκρο και επανασυναρμολογεί το μήνυμα.
 - Πολυπλεξία συνδέσεων/συρμών (steams)
 - Υπηρεσίες μεταφοράς πακέτων από άκρο σε άκρο (end-to-end). (π.χ., αξιόπιστη μεταφορά δεδομένων στον δέκτη).
 - Έλεγχος συμφόρησης (congestion) και ροής πακέτων

- Στρώμα Συνόδου (Session Layer)
 - Αποκατάσταση συνόδων μεταξύ διαφόρων μηχανών (sessions)
 - Διαχείριση σκυτάλης (token management)
 - Συγχρονισμός (synchronization)
- Στρώμα Παρουσίασης (Presentation Layer)
 - Κωδικοποίηση δεδομένων
- Στρώμα Εφαρμογής (Application Layer)
 - Συμβατότητα μεταξύ εφαρμογών

Το μοντέλο TCP/IP έχει τέσσερα βασικά στρώματα από κάτω προς τα πάνω:

- **Στρώμα Προσαρμογέα Δικτύου (Network interface):** Ασχολείται με όλα τα φυσικά εξαρτήματα της δικτυακής σύνδεσης μεταξύ του δικτύου και του πρωτοκόλλου IP.
- **Στρώμα Δικτύου (Internet):** Περιέχει όλη τη λειτουργικότητα που διαχειρίζεται την μετακίνηση πληροφορίας μεταξύ δύο δικτυακών συσκευών πάνω από ένα routed network
- **Στρώμα Host-to-host:** Διαχειρίζεται τη ροή πληροφορίας μεταξύ δύο hosts ή συσκευών, εξασφαλίζοντας ότι τα δεδομένα φτάνουν στην εφαρμογή του host στην οποία απευθύνονται.
- **Στρώμα εφαρμογής (Application):** Λειτουργεί ως τα τελικά σημεία της συνόδου επικοινωνίας μεταξύ δύο hosts.

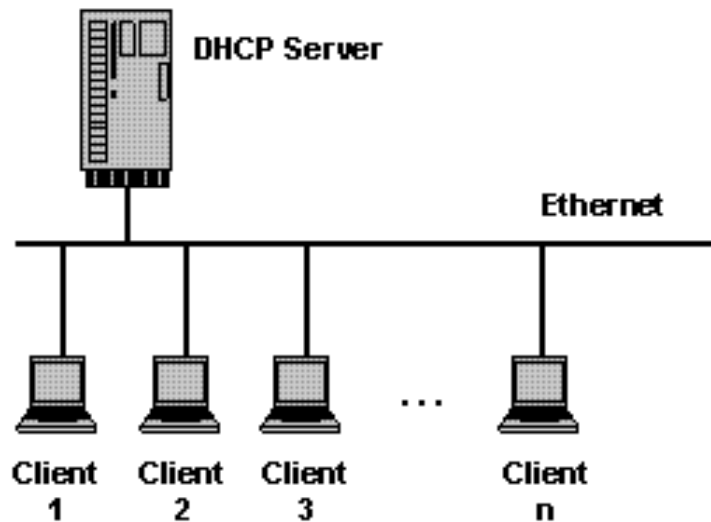
Με μία πρώτη παρατήρηση βλέπουμε ότι το επίπεδο 1 του TCP/IP ενσωματώνει τα δύο πρώτα επίπεδα 1 και 2 του OSI. Επίσης το επίπεδο 4 του TCP/IP ενσωματώνει την λειτουργικότητα των τριών επιπέδων 5, 6 και 7 του OSI. Στα άλλα δύο επίπεδα έχουμε αντιστοίχιση 1-προς-1.

Αναφορές:

<http://www.dummies.com/how-to/content/network-basics-tcpip-and-osi-network-model-compari.html>

4.4 Dynamic Host Configuration Protocol (DHCP)

Ένας DHCP Server αναθέτει διευθύνσεις IP σε δικτυακές συσκευές πελάτες. Πολύ συχνά χρησιμοποιείται σε εταιρικά δίκτυα έτσι ώστε να ελαχιστοποιήσει τις ανάγκες πραγματοποίησης δικτυακών ρυθμίσεων. Όλες οι διευθύνσεις IP όλων των υπολογιστών που έχουν δοθεί στο δίκτυο μέσω του DHCP είναι αποθηκευμένες στην βάση δεδομένων που υπάρχει στον server.

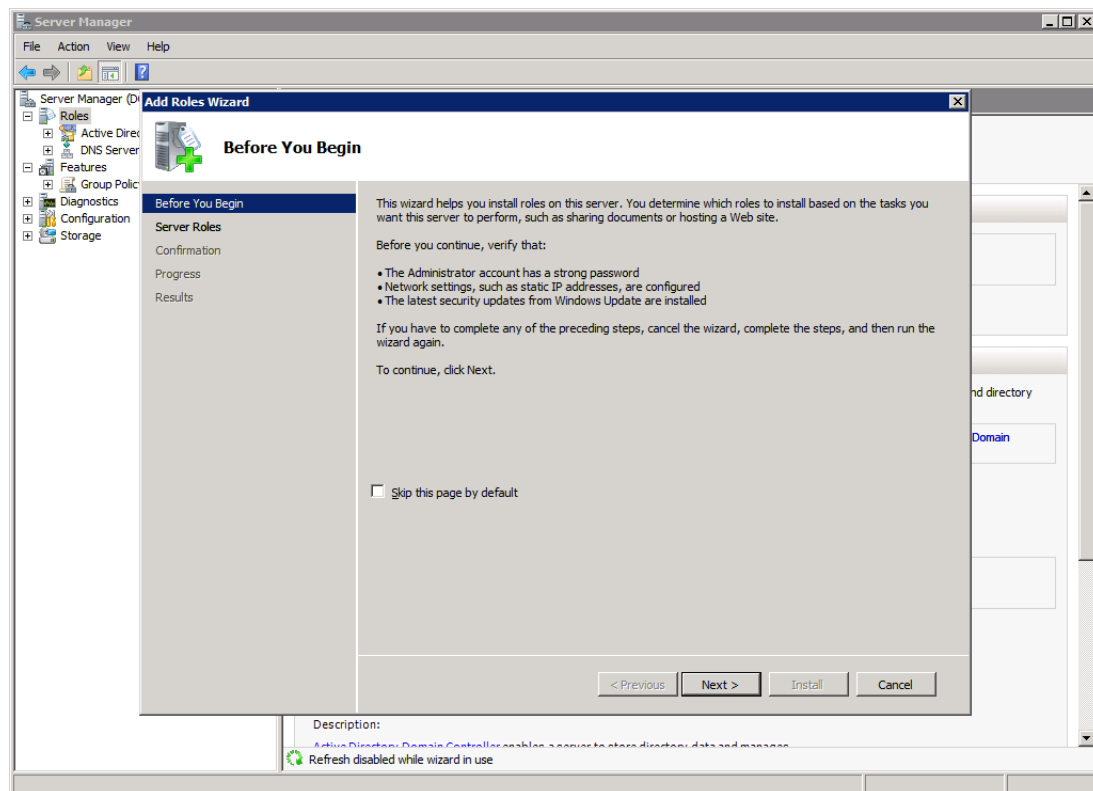


Εικ.4.1

Προκειμένου να εγκαταστήσουμε τον ρόλο του DHCP Server, θα πρέπει να πάμε στον Server Manager ως εξής:

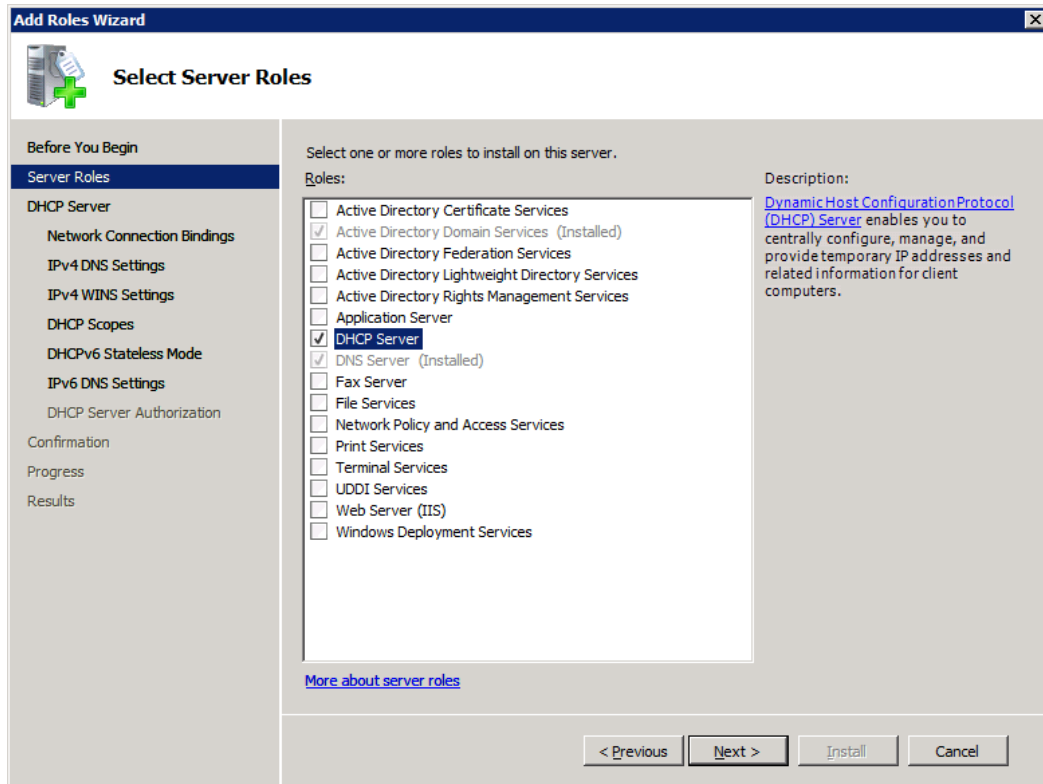
Start—>Administrative tools—>Server Manager

Μόλις ανοίξει ο server manager, κάνουμε κλικ στους Roles από το αριστερό τμήμα του παραθύρου, και εν συνεχεία από το δεξί τμήμα του παραθύρου κάνουμε κλικ στο Add Roles, και έχουμε μπροστά μας την Εικ.4.2.



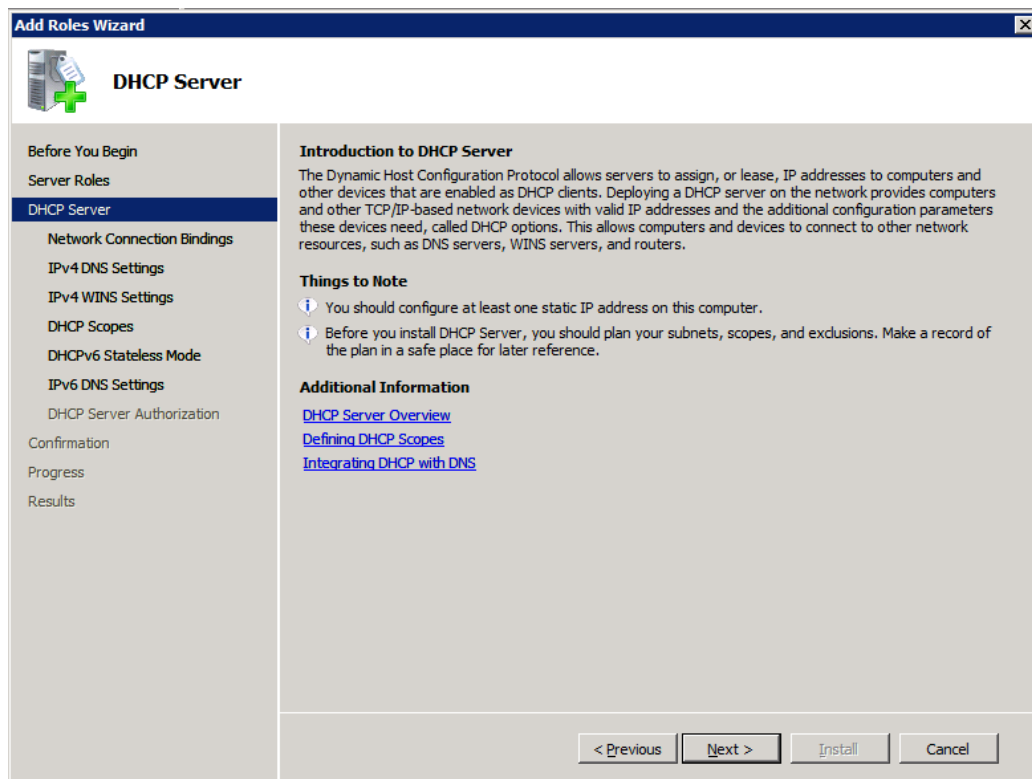
Εικ.4.2

Αριστερό κλικ στο Next.



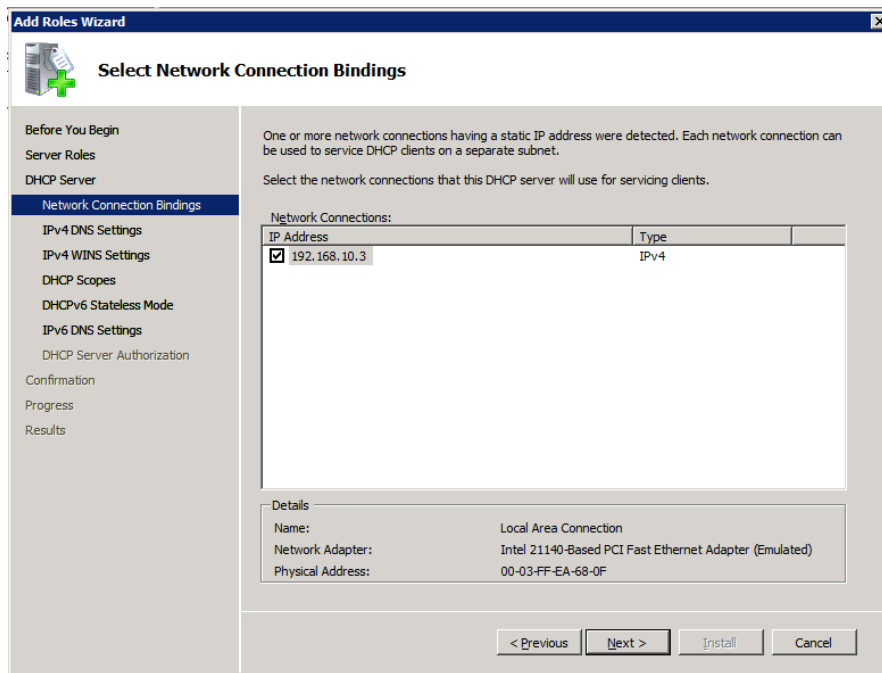
Εικ.4.3

Επιλέγουμε τον ρόλο “DHCP Server και κάνουμε κλικ στο Next (Εικ.4.3).



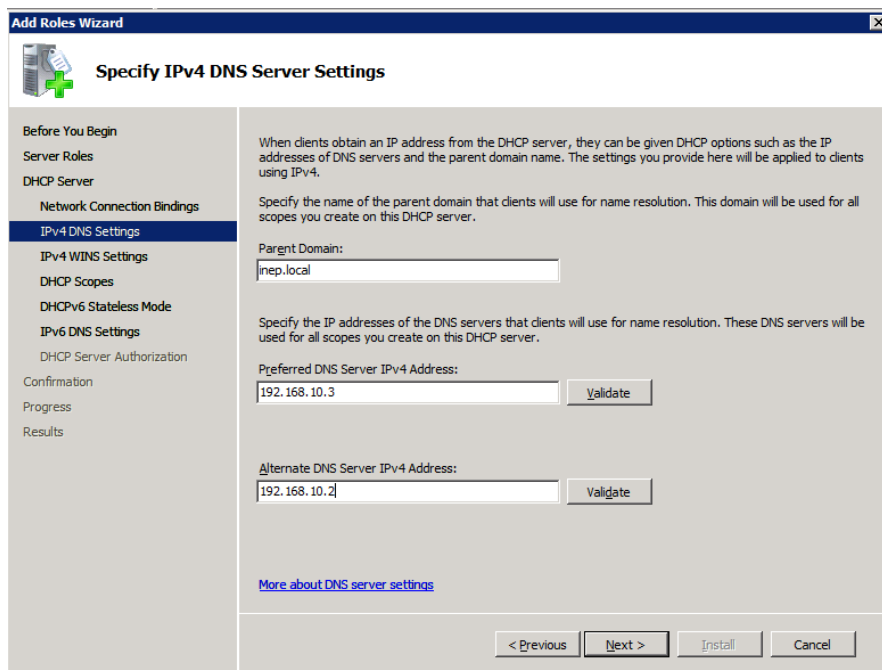
Εικ.4.4

Πατάμε και πάλι στο Next, αφού διαβάσουμε τα πληροφοριακά στοιχεία.



Εικ.4.5

Επιλέγουμε την σύνδεση (NIC) η οποία έχει static IP και θα χρησιμοποιηθεί να μοιράζει διευθύνσεις στο δίκτυο. Σε περίπτωση που έχουμε πολλά subnets είναι σαφές ότι θα χρειαστεί να επιλέξουμε από μία static IP ανά adapter (είτε πραγματικό είτε virtual) που θα βρίσκεται σε κάθε subnet που θέλουμε να διαμοιράσουμε δυναμικά διευθύνσεις. Είναι υποχρεωτικό να έχει static IP ο προσαρμογέας δικτύου (NIC) που θα διαμοιράζει IPs. Εμείς στο παράδειγμά μας έχουμε μόνο μια κάρτα, οπότε αυτή θα είναι που θα διαμοιράσει τις dynamic IPs στο εικονικό μας δίκτυο.



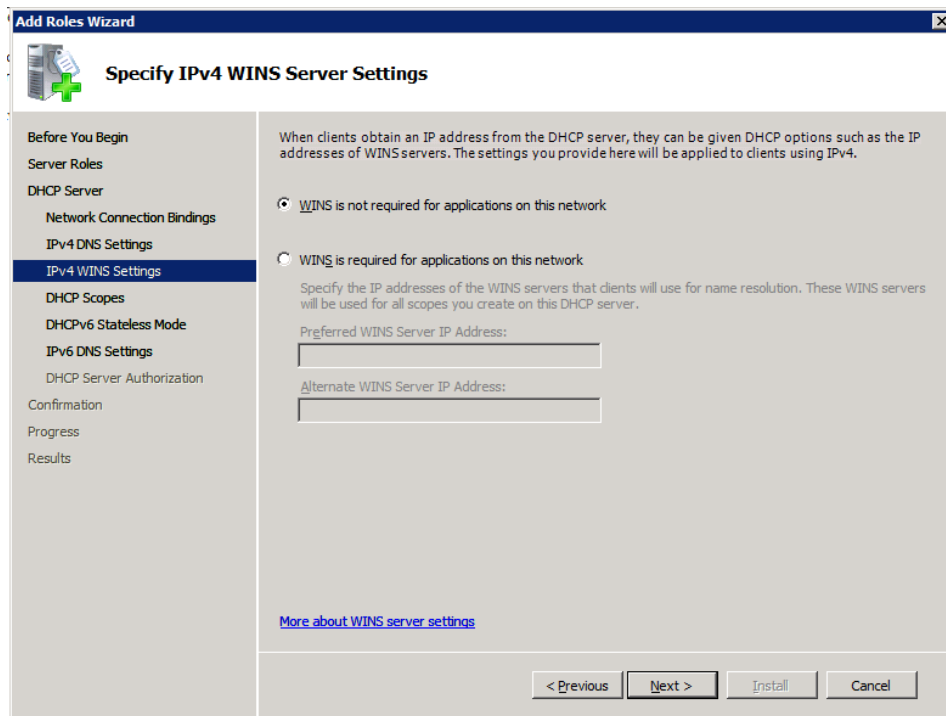
Εικ.4.6

Επειδή υπάρχει ήδη domain στους server μας, ο DHCP που θα στήσουμε θα αυθεντικοποιηθεί στο domain αυτό και θα μπορεί να δημιουργεί αυτόματα εγγραφές στους DNS servers, έτσι ώστε να μας απλοποιεί το έργο. Σημειώνουμε ότι με το να πάρει κάποιος client IP διεύθυνση από τον DHCP δεν σημαίνει σε καμία περίπτωση ότι θα γίνει και join στο domain. Στα πεδία: “Preferred DNS Server” και “Alternate DNS Server” ορίζουμε ποιοι θα είναι οι DNS Server οι οποίοι θα διαμοιράζονται ως πληροφορία στους clients που θα συνδέονται μέσω DHCP, προκειμένου να ρυθμιστούν εξαρχής από τον wizard. (Εικ.4.6)

Εικ.4.7

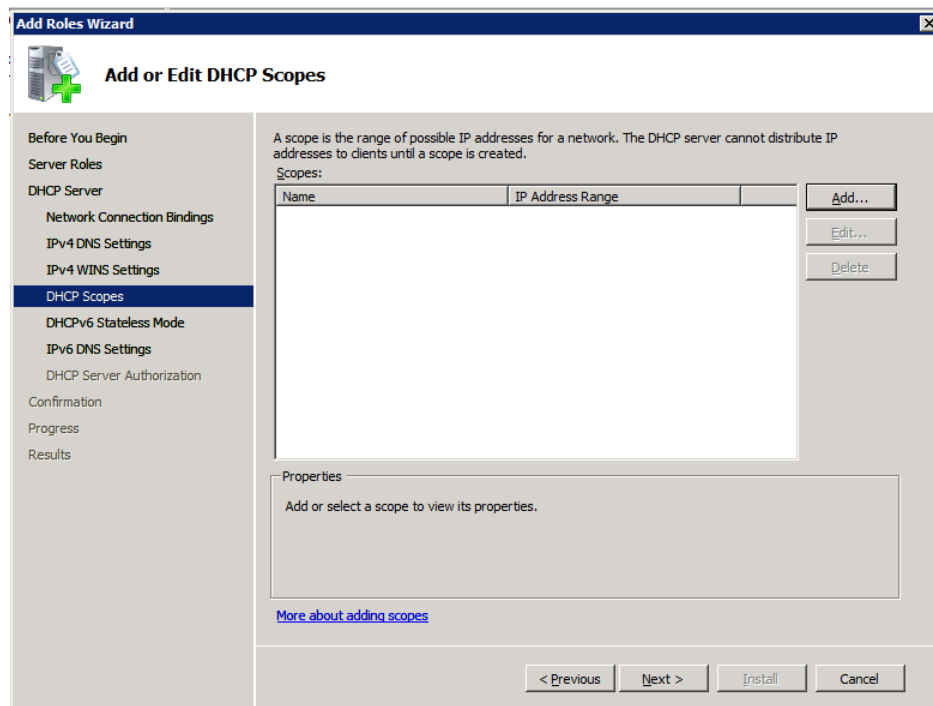
Στη συνέχεια πατώντας τα δύο πλήκτρα “Validate” ελέγχουμε αν υπάρχει σύνδεση με τους DNS και αν όντως οι IP που δώσαμε αντιστοιχούν σε DNS servers. Εφόσον τα test είναι έγκυρα πατάμε Next.

Στην περίπτωσή μας δεν θα ρυθμίσουμε WINS Server Settings για το δίκτυό μας, οπότε κάνουμε κλικ στο “WINS is not required for applications on this network” και Next.



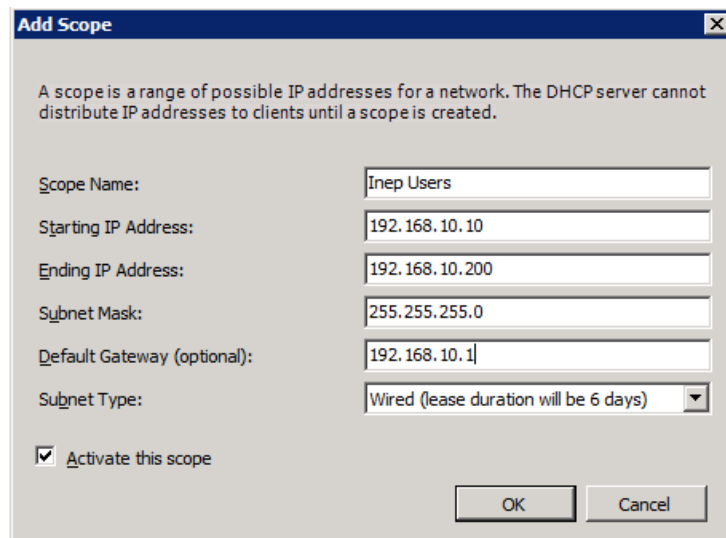
Εικ.4.8

Σημειώνουμε ότι ο WINS Server, έχει αντικατασταθεί από τα Windows 2000 και μετά με την υπηρεσία DNS οπότε δεν χρησιμοποιείται σε καινούρια δίκτυα, ο μόνος λόγος να εγκατασταθεί θα ήταν αν τον απαιτούσε κάποια ειδική (πολύ παλιά) εφαρμογή.



Εικ.4.9

Με το add θα προσθέσουμε DHCP scopes, δηλαδή IP διευθύνσεις προς διαμοιρασμό.



Add Scope

A scope is a range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.

Scope Name: Inep Users

Starting IP Address: 192.168.10.10

Ending IP Address: 192.168.10.200

Subnet Mask: 255.255.255.0

Default Gateway (optional): 192.168.10.1

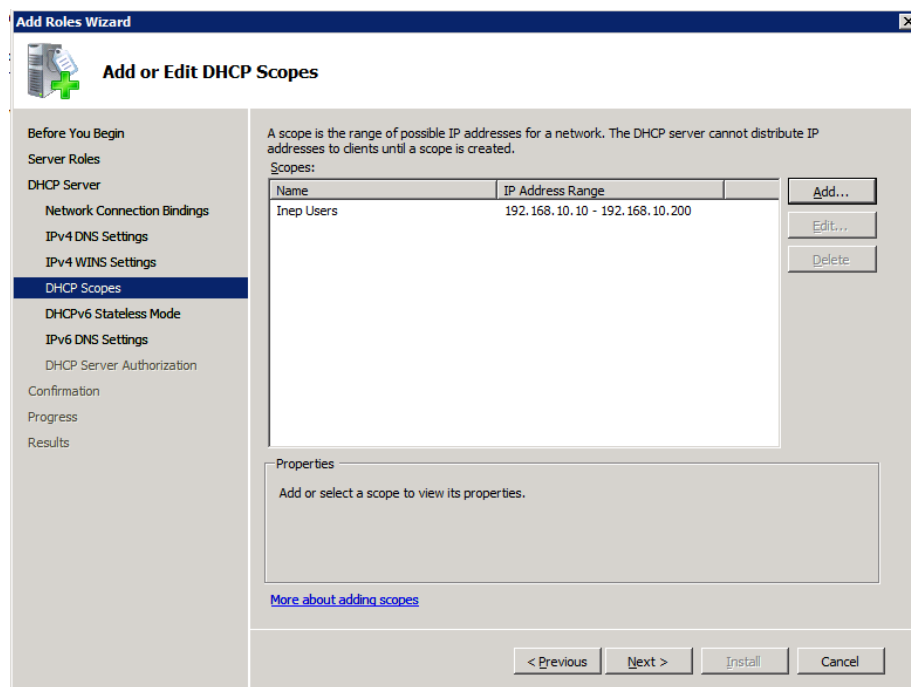
Subnet Type: Wired (lease duration will be 6 days)

☒ Activate this scope

OK Cancel

Εικ.4.10

Δίνουμε ένα όνομα στο Scope Name που να χαρακτηρίζει το scope που θα προσθέσουμε π.χ. “Inep Users”. Ρυθμίζουμε το εύρος διαμοιρασμού των IPs από 192.168.10.10 μέχρι 192.168.10.200, την Subnet Mask (μασκα υποδικτύου) και το Default Gateway να δείχνει στον router μας δηλαδή στο 192.168.10.1. Στο Subnet Type ορίζω Wired, μιας και απευθυνόμαστε σε ενσύρματο δίκτυο (και όχι σε ασύρματο που είναι η άλλη επιλογή). Δεν ξεχνώ να κάνω κλικ στο “Activate this scope” και να πατήσω ok.



Add Roles Wizard

Add or Edit DHCP Scopes

Before You Begin

Server Roles

DHCP Server

Network Connection Bindings

IPv4 DNS Settings

IPv4 WINS Settings

DHCP Scopes

DHCPv6 Stateless Mode

IPv6 DNS Settings

DHCP Server Authorization

Confirmation

Progress

Results

A scope is the range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.

Scopes:

Name	IP Address Range
Inep Users	192.168.10.10 - 192.168.10.200

Add... Edit... Delete

Properties

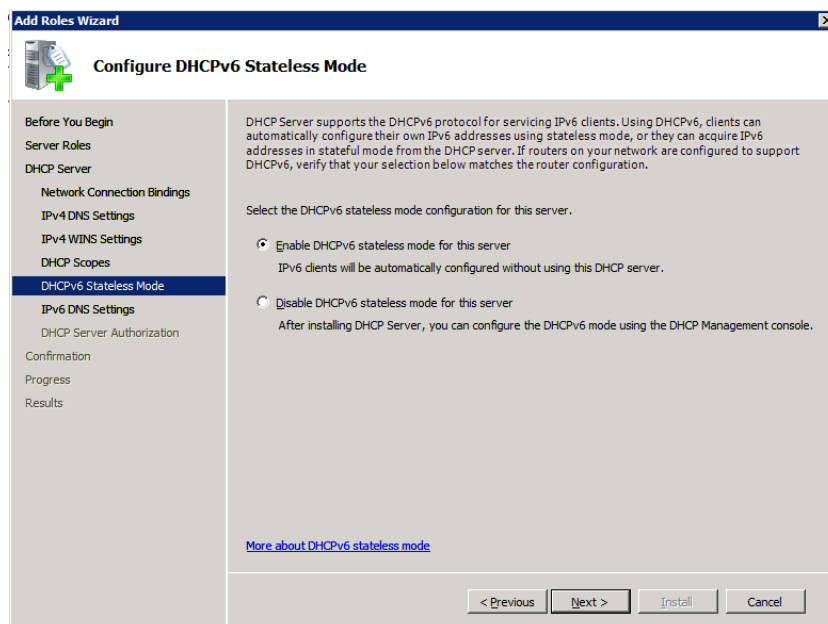
Add or select a scope to view its properties.

[More about adding scopes](#)

< Previous Next > Install Cancel

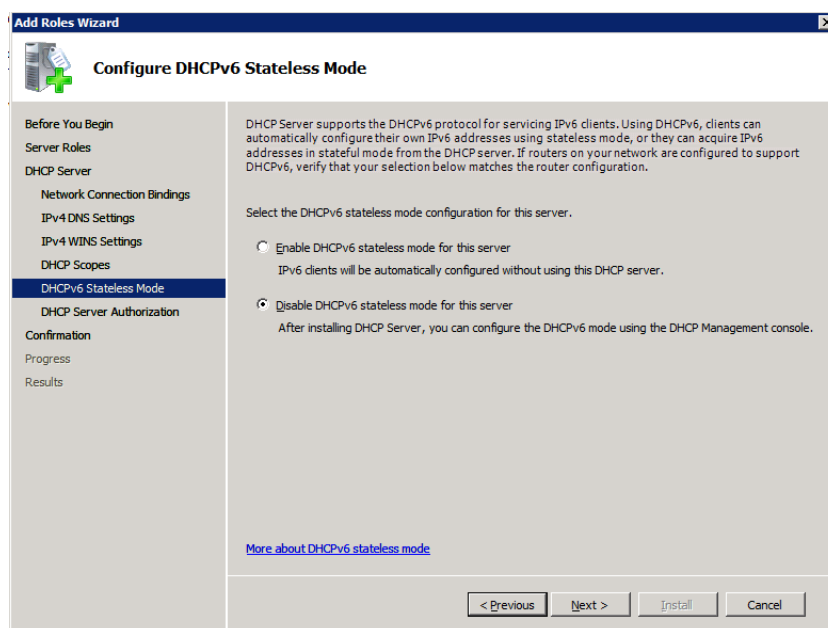
Εικ.4.11

Αν επιθυμώ μπορώ να προσθέσω και άλλα scopes, ή να αλλάξω ή και να διαγράψω. Όταν ολοκληρώσω τις ρυθμίσεις πατάω στο Next και συνεχίζω.



Εικ.4.12

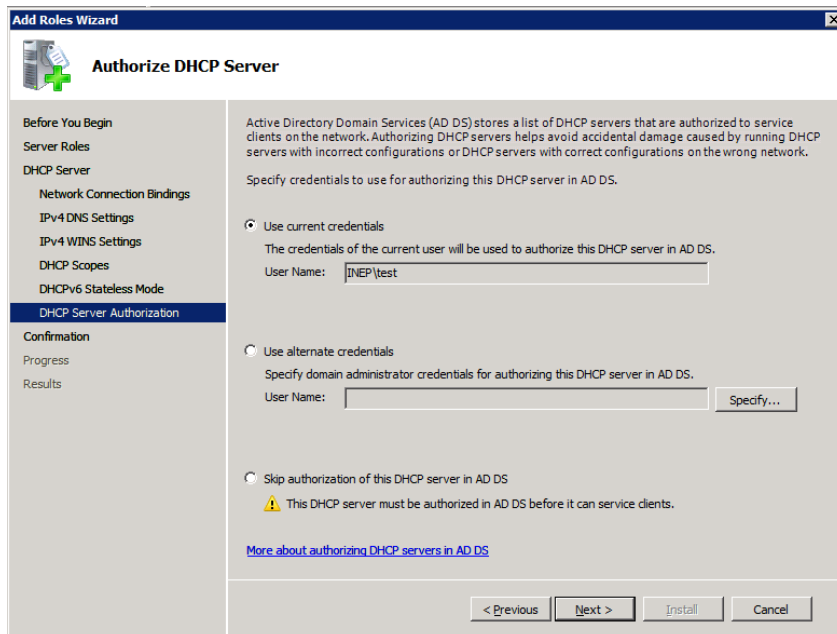
Στην επιλογή για το DHCPv6 Stateless Mode, θα πατήσουμε Disable, οπότε και θα παρακάμψουμε τις ρυθμίσεις για IPv6 DNS που ακολουθούν, μιας και δεν θα έχουμε support για IPv6 δίκτυα (βλέπε Εικ.4.13), και μετά κλικ στο Next.



Εικ.4.13

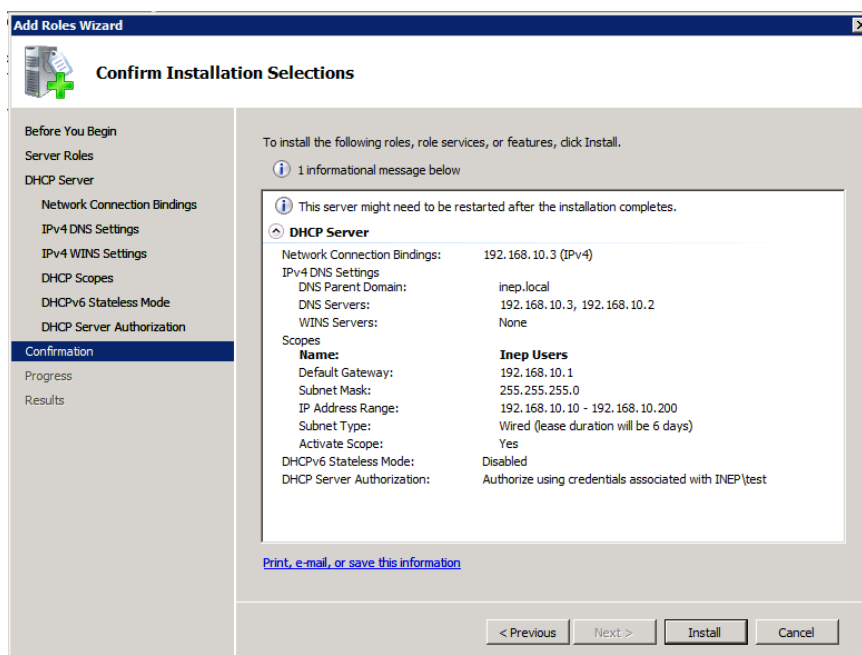
Ακολουθεί το authorization του DHCP Server στο AD DS, χρησιμοποιώντας κάποια credentials. Συνήθως αφήνουμε την επιλογή “use current credentials” για να χρησιμοποιήσει τον λογαριασμό που είναι ήδη ενεργός, αν και για λόγους ασφαλείας

κάποιοι συνιστούν να δημιουργηθεί ένας λογαριασμός ειδικά για αυτή τη δουλειά. Εμείς θα προχωρήσουμε με τα current credentials όπως φαίνεται και στην εικόνα Εικ.4.14, δηλαδή με τον domain administrator που θυμίζω ότι τον έχουμε μετονομάσει σε test.



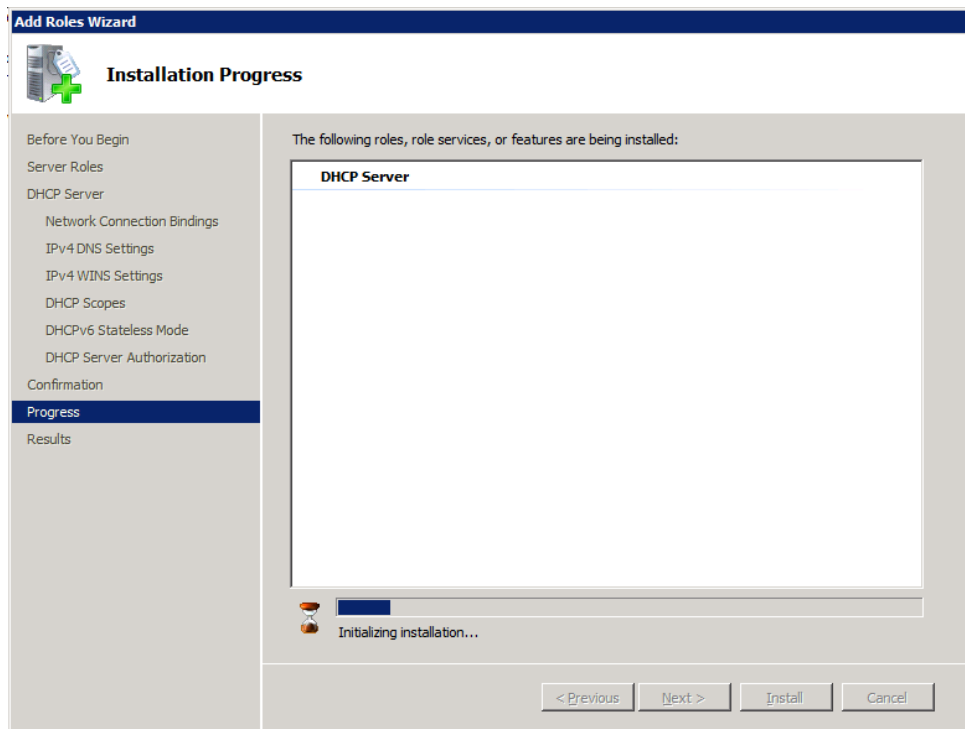
Εικ.4.14

Πατάμε Next και προχωράμε στην σύνοψη των ρυθμίσεων. Αν είμαστε εντάξει πατάμε Install για να προχωρήσουμε με την εγκατάσταση του Ρόλου DHCP με τις ρυθμίσεις που κάναμε.



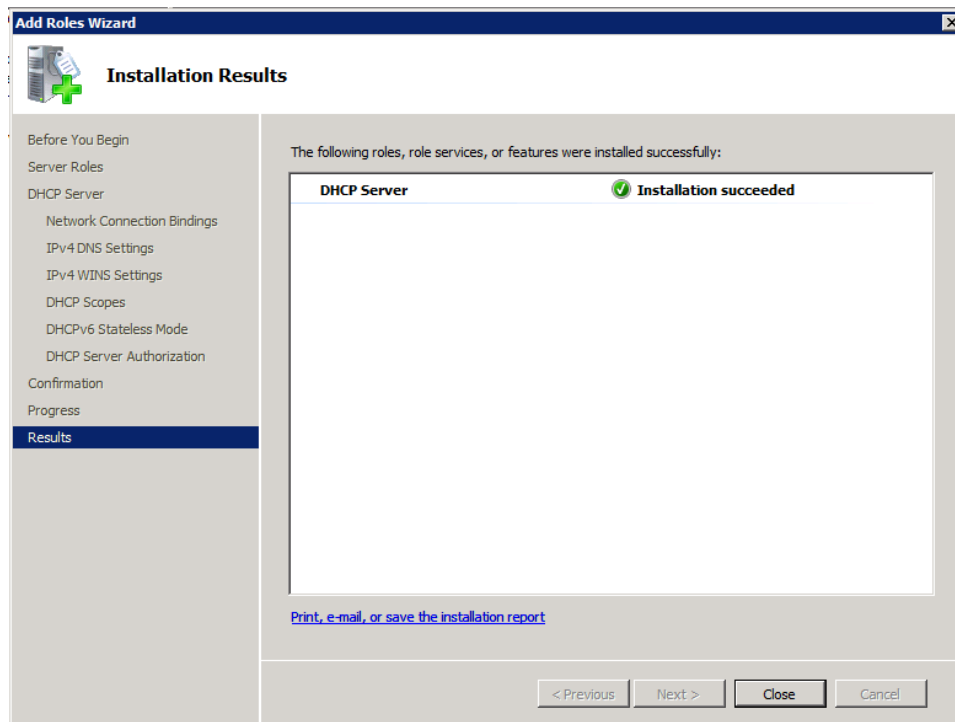
Εικ.4.15

Η εγκατάσταση προχωράει κανονικά.



Εικ.4.16

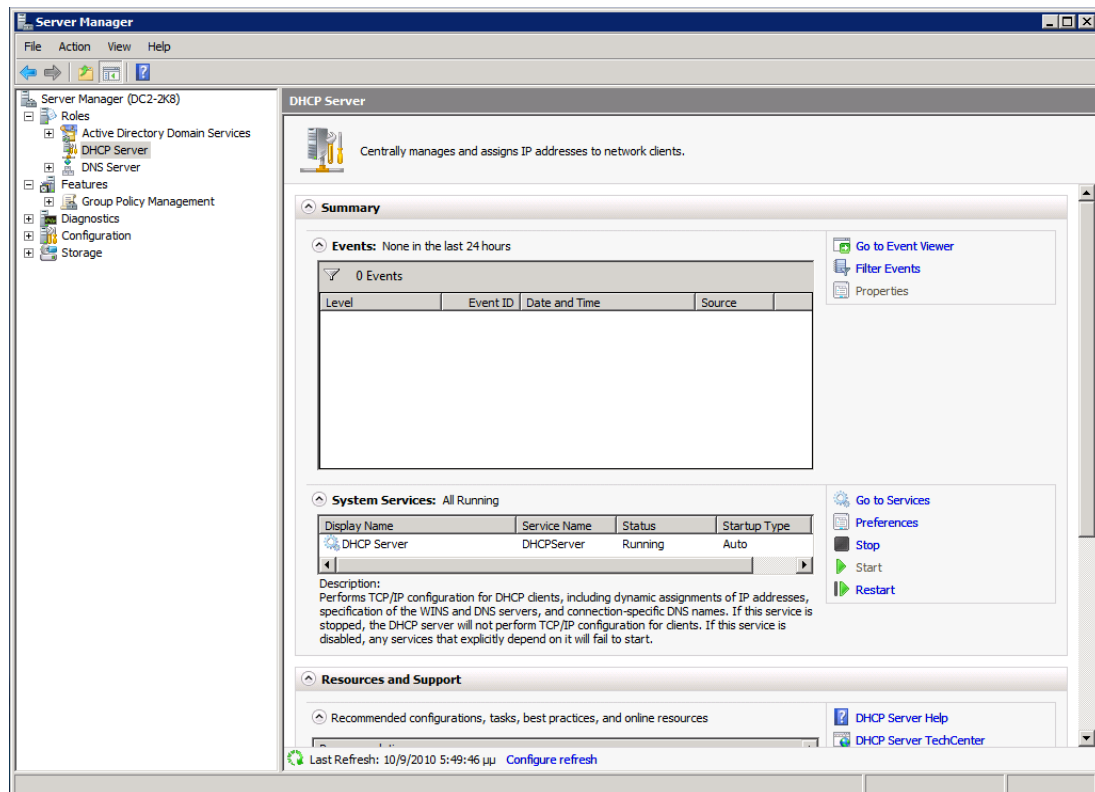
Και μόλις ολοκληρωθεί μας δίνει το αντίστοιχο μήνυμα (Εικ.4.17)



Εικ.4.17

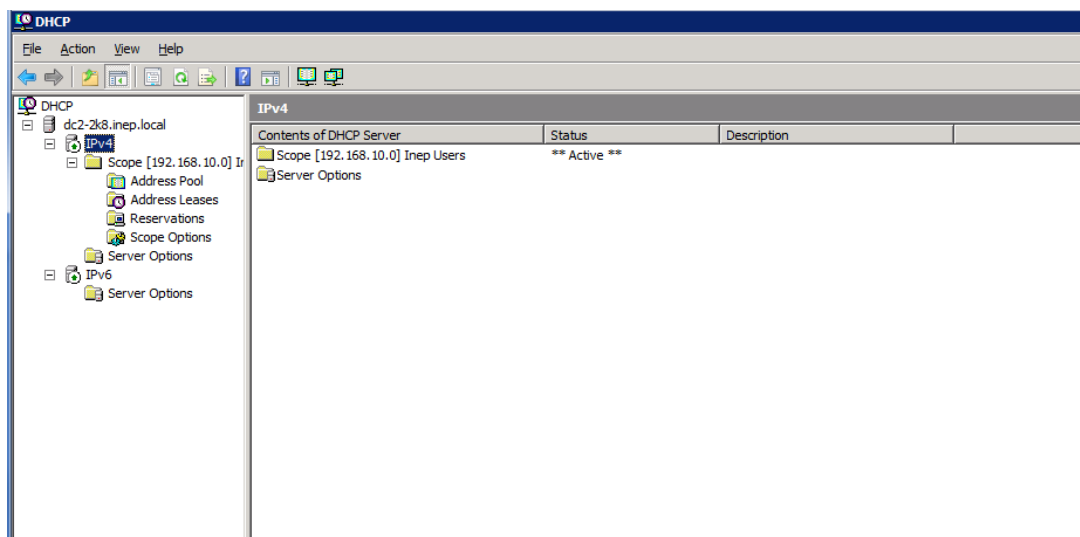
Στη συνέχεια ανοίγοντας τον Server Manager, θα δούμε ότι υπάρχει ο αντίστοιχος ρόλος στο σωστό σημείο. Με κλικ στην αριστερή πλευρά του παραθύρου θα πάρουμε τις πληροφορίες και τις δυνατότητες που φαίνονται στην Εικ.4.18. Μπορούμε να δούμε κάποια Events από την λειτουργία του ρόλου, και να κάνουμε Start, Stop και

Restart το service του DHCP όποτε και αν αυτό κριθεί αναγκαίο από εμάς (τους διαχειριστές).



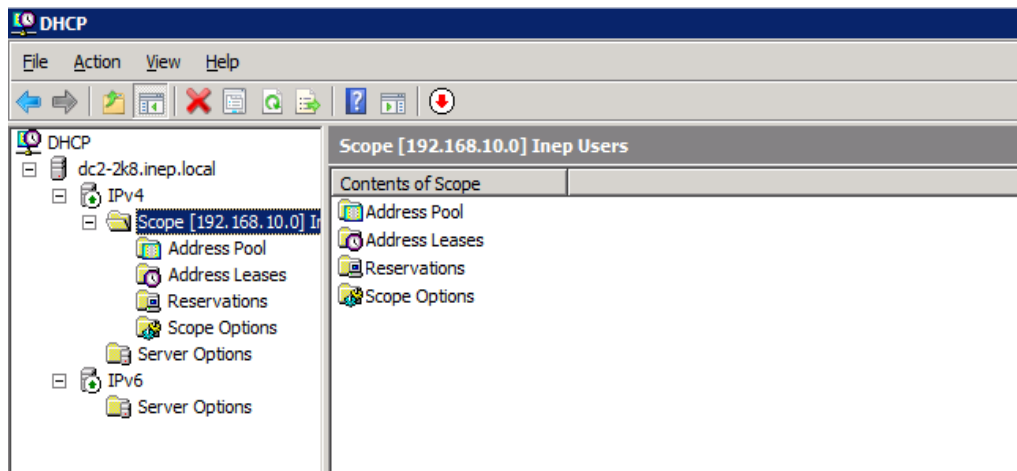
Εικ.4.18

Ανοίγοντας από το Administrative Tools το MMC που λέγεται DHCP έχω πλήρη πρόσβαση στα στοιχεία του DHCP όπως φαίνεται και ακολούθως Εικ.4.19.



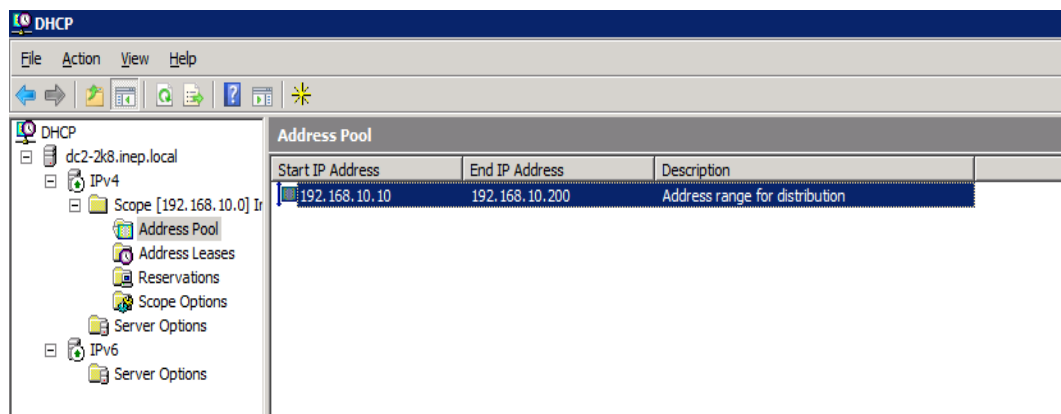
Εικ.4.19

Επιλέγοντας στο αριστερό τμήμα του παραθύρου το Scope που έχουμε δημιουργήσει, στο δεξί τμήμα του παραθύρου εμφανίζονται οι επιλογές: “Address Pool”, “Address Leases”, “Reservations”, “Scope Options” όπως φαίνονται στην Εικ.4.20.



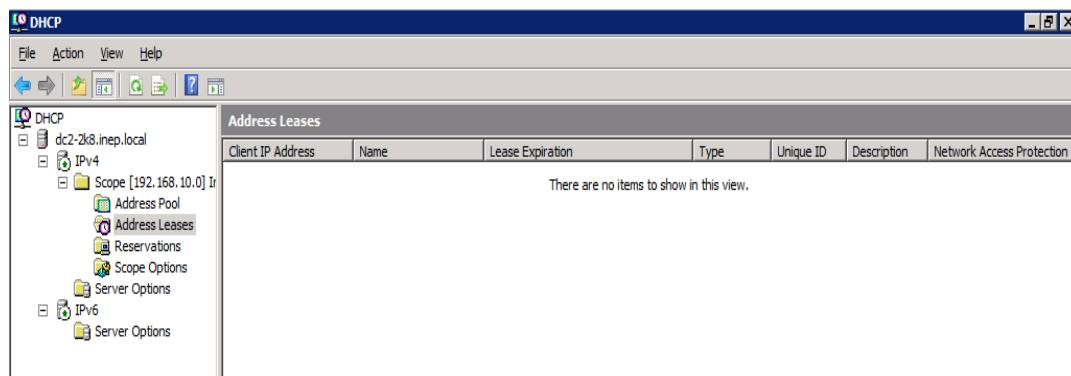
Εικ.4.20

Επιλέγοντας το “Address Pool” βλέπουμε την ρύθμιση που δώσαμε κατά την διαδικασία εγκατάστασης. Μπορούμε να προσθέσουμε ή και να μεταβάλουμε τις ρυθμίσεις αυτές.



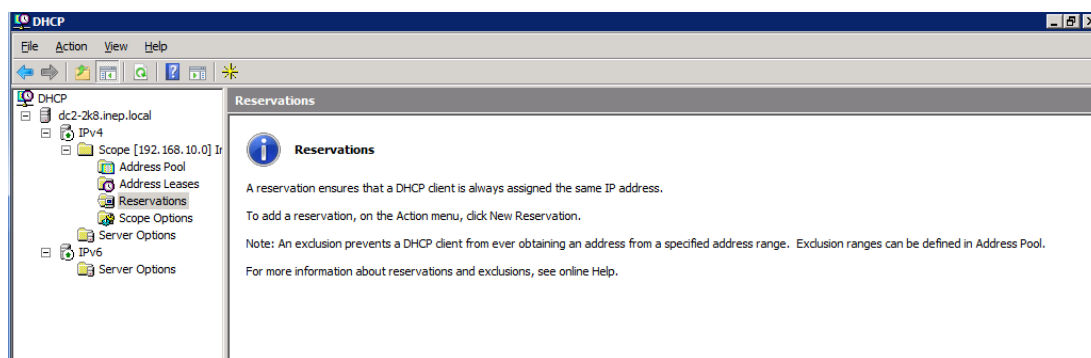
Εικ.4.21

Στο “Address Leases” εμφανίζονται οι πελάτες του DHCP, με πολλές πληροφορίες όπως το όνομα, το πότε λήγει ο δανεισμός της IP που του αποδόθηκε, τον τύπο του πελάτη, το Unique ID δηλαδή την φυσική του διεύθυνση (ή αλλιώς MAC address) μια περιγραφή του, κ.λπ.. Επειδή δεν υπάρχουν πελάτες αυτή τη στιγμή θα είναι κενό.



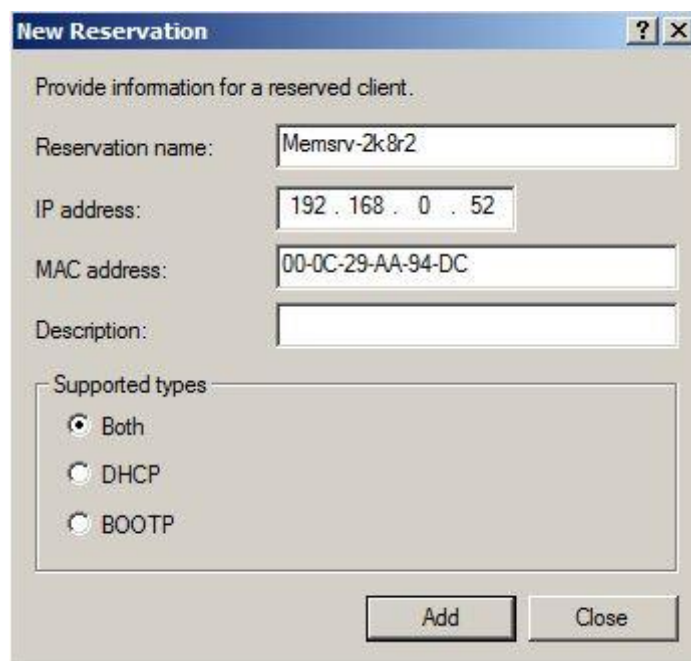
Εικ.4.22

Στη συνέχεια στο αριστερό menu υπάρχει το container με ονομασία Reservations.



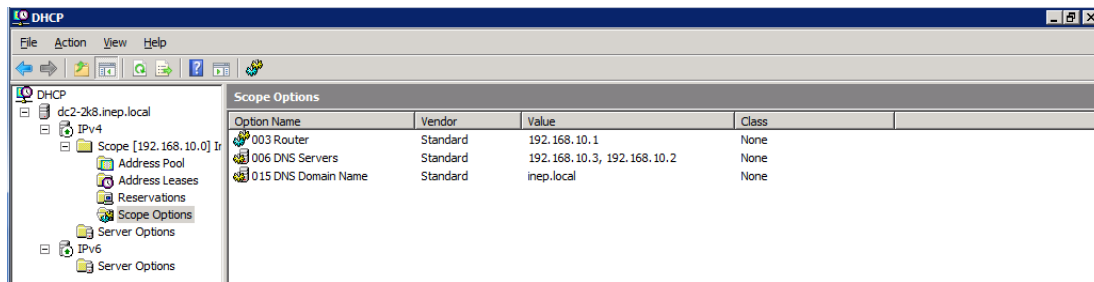
Εικ.4.23

Τα DHCP reservation είναι μια διαδικασία με την οποία μια συγκεκριμένη IP address συσχετίζεται με ένα και μόνο υπολογιστή, συνήθως ένα server, ο οποίος πρέπει να έχει μόνιμα την ίδια IP address. Όταν αυτό γίνει, όποτε ο υπολογιστής αυτός και να ζητήσει μια IP address από τον DHCP server, θα του ανατεθεί η συγκεκριμένη IP. Επειδή η IP address είναι δεσμευμένη για ένα συγκεκριμένο υπολογιστή, δεν πρόκειται να ανατεθεί σε άλλο υπολογιστή ακόμα και αν είναι η μόνη ελεύθερη διεύθυνση διαθέσιμη στο DHCP address pool. Προκειμένου να εξασφαλιστεί η μοναδικότητα της ανάθεσης IP αλλά και λόγω του γεγονότος ότι η IP ζητείται με request από τον DHCP client, ως αναγνωριστικό απαιτείται η γνώση της φυσικής διεύθυνσης MAC address με την οποία θα δηλώσουμε ότι για την συγκεκριμένη MAC θα δίδεται πάντα η συγκεκριμένη IP και μόνο, όπως φαίνεται και στο τυχαίο παράδειγμα στην Εικ.4.24



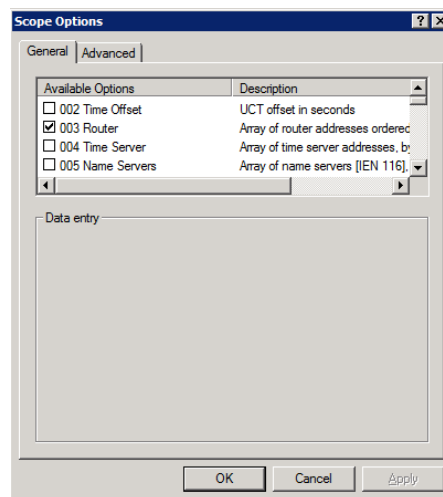
Εικ.4.24

Κάτω από το “Reservations” υπάρχει το “Scope Options” στο οποίο και μπορούμε να ρυθμίζουμε όλες τις παραμέτρους του DHCP που θέλουμε να διαμοιράζει.



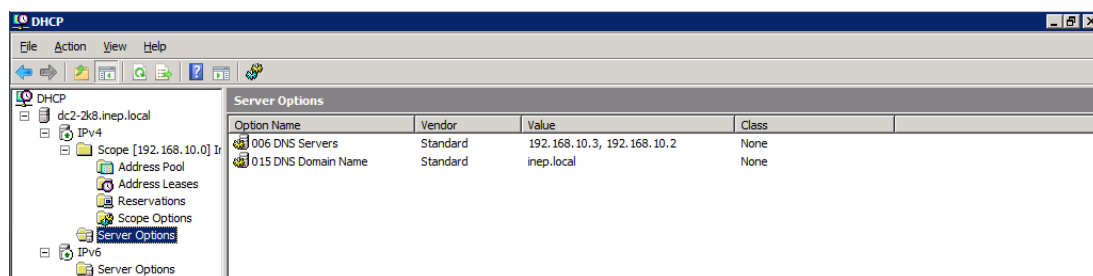
Εικ.4.25

Στην Εικ.4.25 βλέπουμε ήδη τις ρυθμίσεις που έχει κάνει ο Wizard της εγκατάστασης του ρόλου του DHCP server.



Εικ.4.26

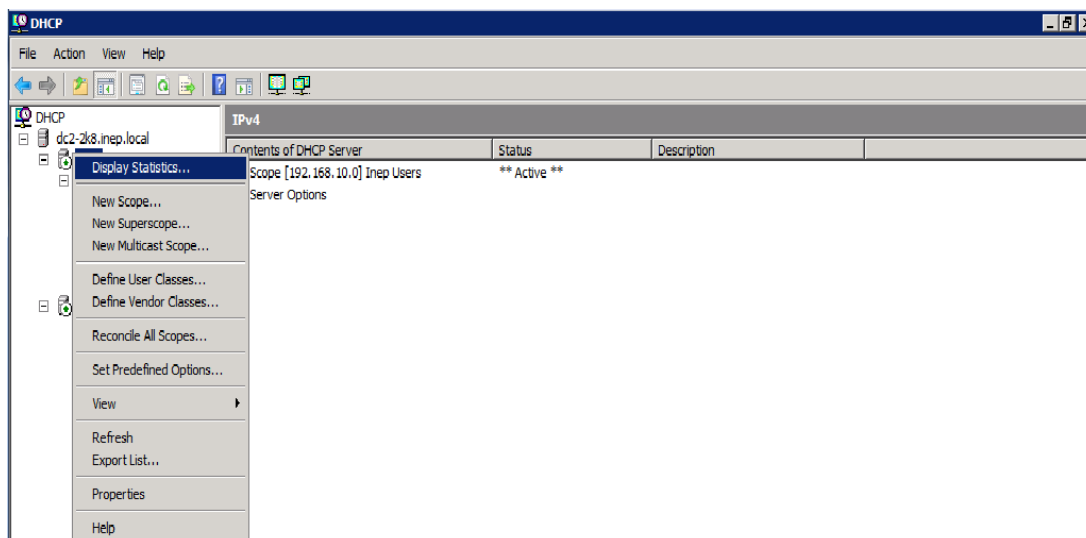
Όπως γίνεται εύκολα αντιληπτό μπορούμε να προσθέσουμε στο Scope Options πολλές ακόμα ρυθμίσεις που θέλουμε να διαμοιράζονται από τον DHCP server, όπως π.χ. την διεύθυνση κάποιου Time server και άλλα πολλά.



Εικ.4.27

Στο Server Options ρυθμίζουμε παράμετρους που έχουν να κάνουν με τον DHCP Server και όχι μόνο με το Scope, αν και το scope υιοθετεί τις ρυθμίσεις αυτές.

Τέλος μας δίνει δυνατότητες να πάρουμε κάποιες στατιστικές σχετικά με τον DHCP server όπως φαίνεται και στην εικόνα Εικ.4.28



Εικ.4.28

Γλωσσάρι

NIC: Network Interface Card ή Κάρτα Δικτύου

Διεύθυνση αναμετάδοσης: Μια διεύθυνση IP με ένα τμήμα κεντρικού υπολογιστή που περιέχει μόνο αριθμούς ένα.

Κεντρικός υπολογιστής: Ένας υπολογιστής ή άλλη συσκευή σε ένα δίκτυο TCP/IP.

Internet: Η παγκόσμια συλλογή δικτύων που είναι συνδεδεμένα μεταξύ τους και κάνουν κοινή χρήση μιας κοινής περιοχής διευθύνσεων IP.

InterNIC: Ο οργανισμός που είναι υπεύθυνος για τη διαχείριση των διευθύνσεων IP στο Internet.

IP: Το πρωτόκολλο δικτύου που χρησιμοποιείται για την αποστολή πακέτων δικτύου μέσω ενός δικτύου TCP/IP ή του Internet.

Διεύθυνση IP: Μια μοναδική διεύθυνση 32 bit για έναν κεντρικό υπολογιστή σε ένα δίκτυο TCP/IP ή διαδίκτυο.

Δίκτυο: Υπάρχουν δύο χρήσεις του όρου "δίκτυο" σε αυτό το άρθρο. Η μία είναι μια ομάδα υπολογιστών σε ένα τμήμα μεμονωμένου φυσικού δικτύου. Η άλλη είναι μια περιοχή διευθύνσεων δικτύου IP που εκχωρείται από ένα διαχειριστή συστήματος.

Διεύθυνση δικτύου: Μια διεύθυνση IP με ένα τμήμα κεντρικού υπολογιστή που περιέχει μόνο μηδενικά.

Οκτάδα: Ένας αριθμός 8 bit, 4 από τα οποία αποτελούν μια διεύθυνση IP 32 bit.

Έχουν μια περιοχή 00000000-11111111, που αντιστοιχεί στις δεκαδικές τιμές 0- 255.

Πακέτο: Μια μονάδα δεδομένων που μεταβιβάζεται μέσω ενός δικτύου TCP/IP ή ευρύτερου δικτύου.

RFC (Request for Comment): Ένα έγγραφο που χρησιμοποιείται για τον ορισμό προτύπων στο Internet.

Δρομολογητής: Μια συσκευή που μεταβιβάζει την κίνηση στο δίκτυο ανάμεσα σε διαφορετικά δίκτυα IP.

Μάσκα υποδικτύου: Ένας αριθμός 32 bit που χρησιμοποιείται για να διακρίνει τα τμήματα δικτύου και κεντρικού υπολογιστή μιας διεύθυνσης IP.

Υποδίκτυο: Ένα μικρότερο δίκτυο που δημιουργείται από τη διαίρεση ενός μεγαλύτερου δικτύου σε ίσα μέρη.

TCP/IP: Χρησιμοποιείται ευρέως, το σύνολο των πρωτοκόλλων, προτύπων και βοηθητικών προγραμμάτων που χρησιμοποιούνται κοινά στο Internet και στα μεγάλα δίκτυα.

Ευρύτερο δίκτυο (Wide area network - WAN): Ένα μεγάλο δίκτυο, που είναι μια συλλογή από μικρότερα δίκτυα διαχωρισμένα από δρομολογητές. Το Internet είναι ένα παράδειγμα ενός πολύ μεγάλου WAN.

ΥΠΗΡΕΣΙΕΣ ΚΑΤΑΛΟΓΟΥ

5.1 Εισαγωγή στις υπηρεσίες καταλόγου και στην υπηρεσία DNS - Αρχιτεκτονική του Active Directory

5.1.1 Τι είναι το Active Directory;

Το Active Directory είναι ουσιαστικά μια βάση δεδομένων δικτύων πόρων (γνωστών και ως αντικείμενα-objects) και πληροφοριών για κάθε ένα από αυτά τα αντικείμενα. Ο κατάλογος του κάθε τομέα μπορεί να αποθηκεύσει μέχρι και 10 εκατομμύρια αντικείμενα που είναι αρκετά για να φιλοξενήσουν εκατομμύρια χρηστών ανά τομέα.

Το Active Directory, ιεραρχικά αποθηκεύει πληροφορίες που αφορούν τα αντικείμενα του δικτύου και που βρίσκονται στη διάθεση των διαχειριστών, των χρηστών και των εφαρμογών.

5.1.2 Τι είναι το DNS;

Οι τοποθεσίες Web διαθέτουν μια "φιλική" διεύθυνση που ονομάζεται Ενιαίο αναγνωριστικό πόρου (URL) και μια διεύθυνση IP. Οι χρήστες χρησιμοποιούν τα URL για να εντοπίσουν τις τοποθεσίες Web, ενώ οι υπολογιστές χρησιμοποιούν για το σκοπό αυτό τις διευθύνσεις IP. Το DNS μεταφράζει τα URL σε διευθύνσεις IP (και αντίστροφα). Για παράδειγμα, εάν πληκτρολογήσουμε <http://www.microsoft.com> στη γραμμή διευθύνσεων του προγράμματος περιήγησης Web, ο υπολογιστής μας θα στείλει μια αίτηση στο διακομιστή DNS. Ο διακομιστής DNS μεταφράζει το URL σε διεύθυνση IP, ώστε ο υπολογιστής μας να μπορεί να εντοπίσει το διακομιστή Web της Microsoft.

5.1.3 Περιεχόμενα Καταλόγου

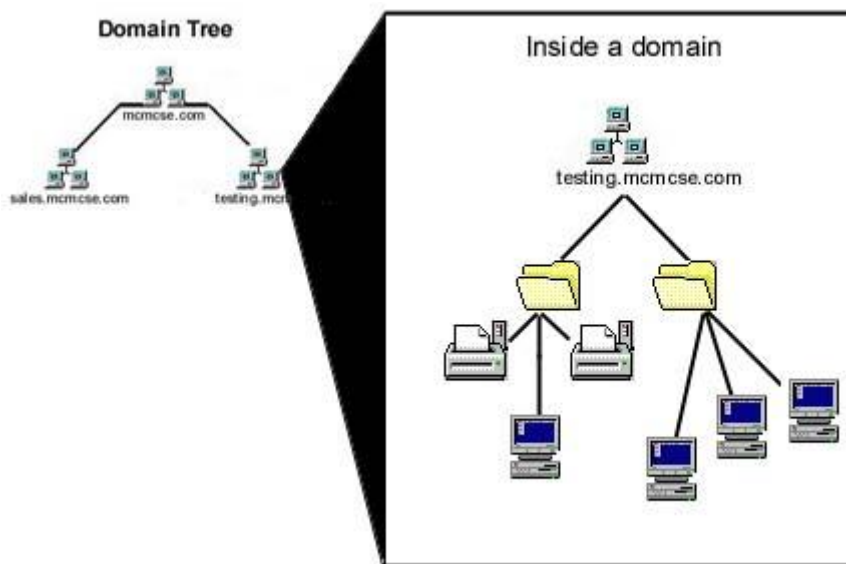
Μια κοινή αναλογία για έναν κατάλογο είναι ένας τηλεφωνικός κατάλογος. Και τα δύο περιλαμβάνουν λίστες των διαφόρων αντικειμένων, των πληροφοριών και των ιδιοτήτων σχετικών με αυτές. Μέσα στον κατάλογο περιλαμβάνονται

- **Αντικείμενα** – objects, τα αντικείμενα σε μια βάση δεδομένων μπορεί να περιλαμβάνουν εκτυπωτές, χρήστες, servers, υπηρεσίες, κοινούς φακέλους κ.λπ., και είναι το πιο βασικό συστατικό του καταλόγου.
- **Χαρακτηριστικά**-attributes Ένα χαρακτηριστικό περιγράφει ένα αντικείμενο. Για παράδειγμα, οι κωδικοί πρόσβασης και τα ονόματα είναι τα χαρακτηριστικά των αντικειμένων χρήστη. Διαφορετικά αντικείμενα θα έχουν ένα διαφορετικό σύνολο χαρακτηριστικών, ωστόσο, διαφορετικά

αντικείμενα μπορούν επίσης να έχουν κοινά χαρακτηριστικά. Για παράδειγμα, ένας εκτυπωτής και ένας υπολογιστής ενδέχεται να έχουν και οι δύο μια διεύθυνση IP ως ένα κοινό χαρακτηριστικό.

- **Σχήμα-** Schema Ένα σχήμα καθορίζει τον κατάλογο των χαρακτηριστικών που περιγράφουν ένα συγκεκριμένο τύπο αντικειμένου. Για παράδειγμα, ας υποθέσουμε ότι όλα τα αντικείμενα του εκτυπωτή ορίζονται με βάση το όνομα, PDL τύπο και χαρακτηριστικά ταχύτητας εκτύπωσης. Αυτός ο κατάλογος των χαρακτηριστικών γνωρισμάτων περιλαμβάνει τη διάταξη-schema για την κλάση αντικείμενο "εκτυπωτές". Το σχήμα είναι προσαρμόσιμο, που σημαίνει ότι οι ιδιότητες που χαρακτηρίζουν μια object class μπορούν να τροποποιηθούν.
- **Υποδοχέας-container** - Ένας υποδοχέας είναι έννοια παρόμοια με την έννοια φάκελος στα Windows. Ένας φάκελος περιέχει αρχεία και άλλους φακέλους. Στο Active Directory, ένα container κρατά αντικείμενα και άλλα containers.

Οι Υποδοχείς έχουν χαρακτηριστικά όπως ακριβώς και τα αντικείμενα, ακόμη και αν δεν αποτελούν μια πραγματική οντότητα, όπως ένα αντικείμενο. Οι τρεις τύποι container είναι Domains, Sites και Organizational Units και αναλύονται στη συνέχεια.



Εικ.5.1

- **Domains** – θα αναφερθεί στην επόμενη παράγραφο.
- **Sites** - Μια τοποθεσία είναι μια θέση. Συγκεκριμένα, οι χώροι που χρησιμοποιούνται για τη διάκριση μεταξύ τοπικών και απομακρυσμένων

τοποθεσιών.

- **Organizational Units** – Οι Οργανωτική μονάδα είναι container στο οποίο μπορούμε να τοποθετήσουμε χρήστες, ομάδες, υπολογιστές και άλλες οργανωτικές μονάδες. Η Οργανωτική μονάδα δεν μπορεί να περιέχει αντικείμενα από άλλους τομείς. Οι οργανωτικές μονάδες μπορούν να περιέχουν άλλες οργανωτικές μονάδες. Οι Οργανωτικές μονάδες θα πρέπει να χρησιμοποιηθούν για να συμβάλουν στην ελαχιστοποίηση του αριθμού των τομέων που απαιτούνται σε ένα δίκτυο.

Τα σύμβολα του φάκελου αντιπροσωπεύουν Organizational Units (OU) containers και σε κάθε ένα από αυτά θα βρούμε αντικείμενα, όπως εκτυπωτές, εξυπηρετητές, ηλεκτρονικούς υπολογιστές, χρήστες, κ.λπ. Αντί για αντικείμενα στο εσωτερικό αυτών των οργανωτικών μονάδων, θα μπορούσαν να υπάρχουν περισσότερα OU containers.

5.2 Active Directory Forests και Domains

5.2.1 Βασικές Έννοιες

Η έννοια του "site".

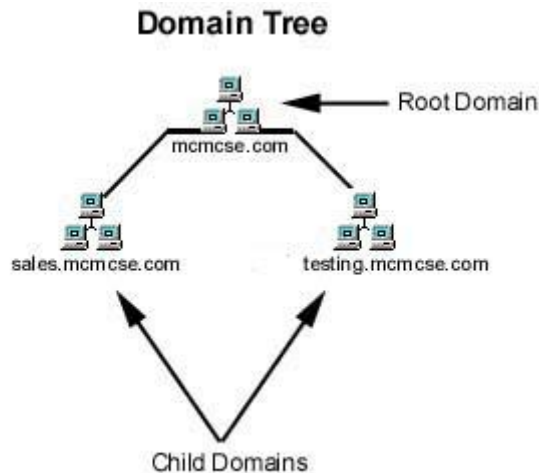
Τοποθεσίες που χρησιμοποιούνται για να καθορίσουν τα φυσικά όρια των συνδέσεων υψηλής ταχύτητας σε ένα δίκτυο που περιέχει Active Directory εξυπηρετητές. Τα Sites βασίζονται σε IP subnets και ορίζονται ως «καλά συνδεδεμένα υποδίκτυα» ή μόνον «υποδίκτυα».

Η έννοια του "domain".

Ένας τομέας-domain είναι το κεντρικό σημείο ενός δικτύου των Windows. Το domain είναι μια λογική ομάδα από υπολογιστές διαχειριζόμενους και προσπελάσιμους από κοινούς κανόνες, που χρησιμοποιούν εκδόσεις του λειτουργικού συστήματος Microsoft Windows και που μοιράζονται μια κεντρική βάση δεδομένων καταλόγου. Αυτή η κεντρική βάση δεδομένων ονομάζεται Active Directory

Το Active Directory υλοποιείται όταν οριστεί ένας εξυπηρετητής σαν εκλεκτής τομέα-domain controller DC. Από προεπιλογή, οι εξυπηρετητές έχουν εγκατασταθεί ως Standalone Member Servers. Με το Active Directory Installation Wizard (**Dcpromo.exe**) μπορούμε να αναβαθμίσουμε ένα Standalone Member Server σε ελεγκτή τομέα-domain και αντίστροφα. Ο οδηγός ζητά όλες τις απαραίτητες πληροφορίες για την εγκατάσταση του Active Directory.

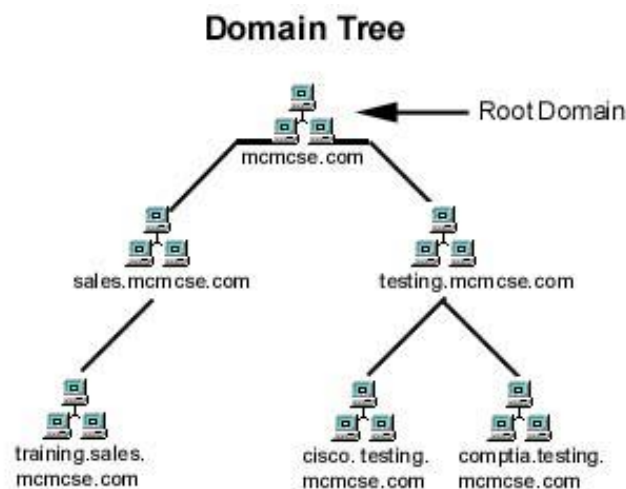
Κάθε ελεγκτής τομέα είναι σε θέση να δέχεται αιτήσεις για αλλαγές στη βάση δεδομένων του τομέα και να αντιγράφει-replicate αυτές τις πληροφορίες στους άλλους DC του τομέα. Ο πρώτος τομέας που δημιουργείται αναφέρεται ως " root domain " και βρίσκεται στην κορυφή του δέντρου καταλόγου-directory tree. Όλοι οι επόμενοι τομείς θα δημιουργούνται κάτω από το ριζικό τομέα και αναφέρονται ως child domains. Τα child domains πρέπει να είναι μοναδικά.



Εικ.5.2

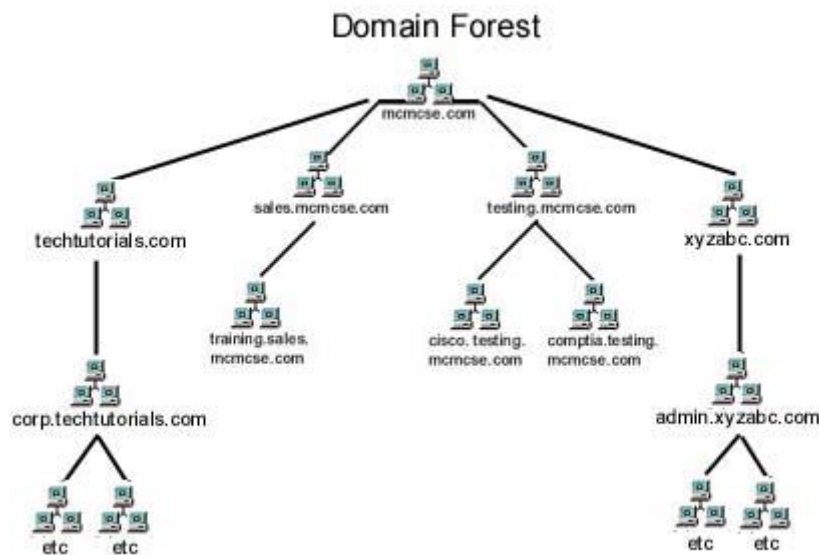
Η έννοια του "Forest".

Όταν ένα ριζικός τομέα και τουλάχιστον ένα child domain έχουν δημιουργηθεί, ένα "δέντρο" σχηματίζεται.



Εικ.5.3

Μπορούμε να δούμε ότι η δομή ξεκινά να παίρνει το σχήμα ενός δέντρου με κλαδιά. Ας υποθέσουμε ότι μια εταιρεία όπως η Microsoft ή η IBM κατέχει διάφορες άλλες εταιρείες. Συνήθως, η κάθε εταιρεία θα έχει το δικό της δέντρο και αυτά θα συνδέονται μαζί με σχέσεις εμπιστοσύνης-trust relationships για τη δημιουργία ενός «δάσους»-forest.



Εικ.5.4

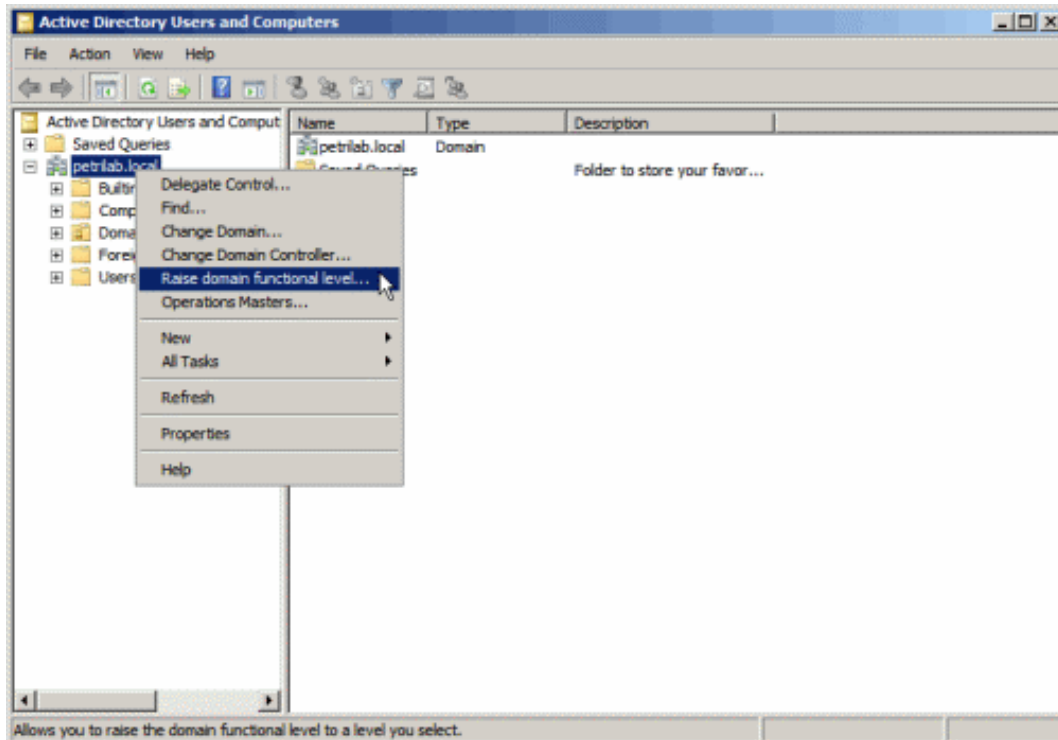
5.2.2 Windows Server 2008 Domain and Forest Functional Levels

Όταν ο πρώτος Windows Server 2008 ελεγκτής τομέα εγκατασταθεί σε έναν τομέα ή σε ένα forest, ο τομέας ή το forest λειτουργεί από προεπιλογή στο χαμηλότερο λειτουργικό επίπεδο το οποίο είναι δυνατό σε αυτό το περιβάλλον δηλαδή στα Windows 2000 Native Mode. Αυτό μας επιτρέπει να επωφεληθούμε από τα προεπιλεγμένα Active Directory χαρακτηριστικά, ενώ χρησιμοποιούμε εκδόσεις των Windows πριν από τα Windows Server 2008. Όταν αυξηθεί το λειτουργικό επίπεδο ενός τομέα ή forest, μια σειρά από προηγμένες δυνατότητες είναι διαθέσιμες.

	2000 native	2003 native	2008 native
επιτρέπονται οι DC	W2K, W2K3, W2K8	W2K3, W2K8	W2K8 μόνο
Χαρακτηριστικά Domain	Universal groups, Group nesting, Group conversions, Security identifier	Δυνατότητα να μετονομάσετε ελεγκτές τομέα μέσω του Netdom.exe,	Distributed File System, υποστήριξη αναπαραγωγής για το SYSVOL,

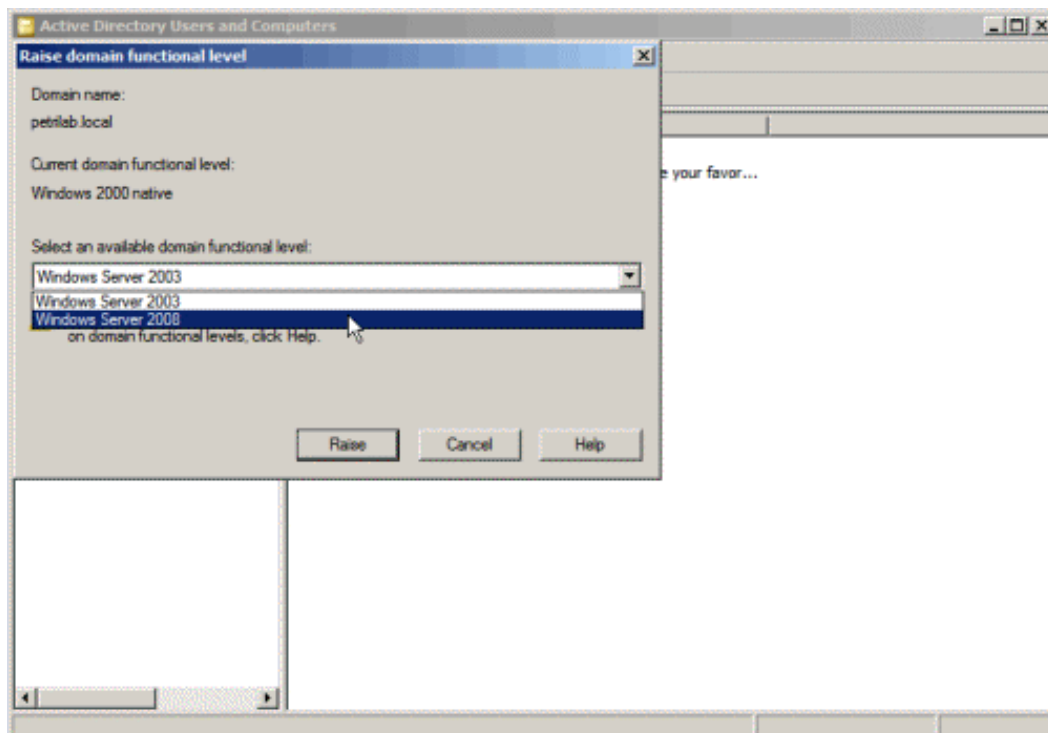
	(SID) history	χρονosφραγίδες Logon, Redirect Χρηστών και Υπολογιστών, Authorization Manager policies in AD, Constrained delegation, Selective authentication	προχωρημένη κρυπτογράφηση, Last Interactive Logon information, Fine-grained password policies
Χαρακτηριστικά Forest	Όλες οι προεπιλεγμένες λειτουργίες AD.	Forest trust, μετονομασία τομέα, linked-value replication, Read-only domain controller deployment, instances of the dynamic auxiliary class named dynamicObject in a domain directory partition, convert inetOrgPerson object instance into a User object instance, create instances of new group types to support role-based authorization, deactivation and redefinition of attributes and classes in the schema	Δεν υπάρχουν νέες πρόσθετες λειτουργίες

Για να αυξηθεί το λειτουργικό επίπεδο ενός τομέα κάνουμε δεξί κλικ στον τομέα από την κονσόλα **Active Directory Users and Computers**



Εικ.5.5

και επιλεγούμε το λειτουργικό επίπεδο που θέλουμε



Εικ.5.6

Αντίστοιχα για να αυξηθεί το λειτουργικό επίπεδο στο forest δεξί κλικ στο forest από το **Active Directory Domains and Trusts** και επιλέγουμε **Raise Forest Functional Level**

5.3 Ρόλοι του AD -Active Directory roles

5.3.1 Object Names

Το Active Directory χρησιμοποιεί το Lightweight Directory Access Protocol (LDAP) προκειμένου να δώσει μια τυποποιημένη ονομασία για τα αντικείμενα. Οι 2 βασικές έννοιες είναι distinguished names και common names. Τα distinguished names είναι η πλήρης «διαδρομή», μέσω της ιεραρχικής δομής δέντρου προς ένα συγκεκριμένο αντικείμενο. Αυτό είναι παρόμοιο με τον προσδιορισμό της πλήρους διαδρομής προς ένα αρχείο από μια γραμμή εντολών του DOS. Αυτή η «διαδρομή» υποδεικνύει τη θέση ενός αντικείμενου στην ιεραρχία. Τα παρακάτω είναι τα στοιχεία που απαρτίζουν ένα distinguished name:

- OU - οργανική μονάδα. Το χαρακτηριστικό αυτό χρησιμοποιείται για να διαιρέσει ένα χώρο ονομάτων-namespaces με βάση την οργανωτική δομή όπως προηγούμενως.
- DC - Domain Component. Ένα distinguished name που χρησιμοποιεί DC χαρακτηριστικά θα έχει ο ελεγκτής για κάθε επίπεδο κάτω του root. Δηλαδή υπάρχει ένα χαρακτηριστικό DC για κάθε τμήμα που χωρίζεται από μια τελεία στο όνομα τομέα.
- CN - Common Name. Αυτό το χαρακτηριστικό αποτελεί το ίδιο το αντικείμενο, εντός της υπηρεσίας καταλόγου.

CN =JacktheRipper, CN = Users, DC=ekdd, DC=gr μέλος του τομέα teachers.ekdd.gr.

Το DN distinguished name μου θα είναι: CN =JacktheRipper, CN=Users, DC=teachers, DC=ekdd, DC=gr

Ο υπολογιστής μου CN=blade, CN=Computers, DC=ekdd, DC=gr

5.3.2 Global Catalog

Η ονοματοδοσία μπορεί να είναι πολύπλοκη και δύσκολα διαχειρίσιμη αλλά υπάρχει ένα εργαλείο που την καθιστά εφικτή. Το Active Directory χρησιμοποιεί μια υπηρεσία με την ονομασία Global Catalog (GC), που χρησιμοποιείται για να εντοπίσει οποιαδήποτε αντικείμενα ενός δίκτυο στο οποίο ένας συγκεκριμένος χρήστης έχει πρόσβαση. πχ το Global Catalog μας επιτρέπει να κάνουμε αναζήτηση στο δίκτυο για έναν εκτυπωτή που έχει συγκεκριμένα χαρακτηριστικά. Όταν ένα νέο αντικείμενο δημιουργείται στο A.D., τού αποδίδεται ένας μοναδικός αριθμός που

ονομάζεται GUID (παγκοσμίως μοναδικό αναγνωριστικό globally unique identifier). Το GUID είναι χρήσιμο διότι παραμένει το ίδιο για οποιοδήποτε αντικείμενο, ακόμη και αν το αντικείμενο μετακινηθεί. Το GUID είναι ένα αναγνωριστικό μεγέθους 128-bit.

5.3.3 Replication

Τα Windows δίκτυα εξαρτώνται σε μεγάλο βαθμό από το AD και ως εκ τούτου, είναι πολύ σημαντικό η υπηρεσία να λειτουργεί γρήγορα και είναι προσβάσιμη ανά πάσα στιγμή. Για να επιτευχθεί αυτό, η βάση δεδομένων AD πρέπει να υπάρχει σε πολλούς διακομιστές, έτσι ώστε αν ένας server αποτύχει, ένας πελάτης να μπορεί να επικοινωνήσει με ένα άλλο εξυπηρετητή με πανομοιότυπες υπηρεσίες και πληροφορίες. Αυτό δεν δημιουργεί μόνο διαθεσιμότητα, αλλά μειώνει το φορτίο στους μεμονωμένους διακομιστές. Το μόνο που χρειάζεται να γίνει σε έναν ελεγκτή τομέα προκειμένου να καταστεί replication partner είναι να τον προσθέσετε στον τομέα.

Ένα από τα πιο δύσκολα σημεία στην επίτευξη διαθεσιμότητας βρίσκεται στο να έχουν οι εξυπηρετητές τις πιο πρόσφατες πληροφορίες. Το Active Directory χρησιμοποιεί αναπαραγωγή τύπου multimaster, το οποίο σημαίνει ότι η ενημέρωση μπορεί να συμβεί σε οποιονδήποτε εξυπηρετητή που έχει το Active Directory. Αυτό σημαίνει επίσης, ότι δεν υπάρχει ελεγκτής τομέα πρωτεύων όπως στα NT και ότι όλοι οι ελεγκτές είναι ισότιμοι. Αυτό επιτυγχάνεται μέσω της χρήσης των μοναδικών αριθμών ακολουθίας unique sequence numbers (USN). Κάθε φορά που γίνεται μια ενημέρωση, θα αποδίδεται ένας μοναδικός αύξων αριθμός από ένα μετρητή που αυξάνεται κάθε φορά που γίνεται η αλλαγή.

5.3.4 Flexible Single Master

Για την πρόληψη των συγκρούσεων κατά την διάρκεια της ενημέρωσης-replication, το Active Directory εκτελεί ενημερώσεις συγκεκριμένων αντικείμενων με τη μέθοδο του single-master. Σε ένα μοντέλο δικτύου τύπου single-master, μόνο ένας Active Directory ελεγκτής τομέα χειρίζεται τις ενημερώσεις. Το Active Directory επεκτείνει το μοντέλο single-master ώστε να περιλαμβάνει πολλαπλούς ρόλους και τη δυνατότητα μεταφοράς ρόλων σε οποιονδήποτε ελεγκτή. Δεδομένου ότι ένας ρόλος Active Directory δεν είναι συνδεδεμένος με έναν μεμονωμένο ελεγκτή τομέα, αναφέρεται ως Flexible Single Master Operation ρόλο. Υπάρχουν πέντε ρόλοι FSMO ως εξής:

Schema Master

Όπως προαναφέρθηκε το σχήμα είναι μια λίστα των χαρακτηριστικών που προσδιορίζουν ένα συγκεκριμένο τύπο αντικειμένου. Ο Schema Master ρόλος σε έναν εκλεκτή τομέα είναι ο DC υπεύθυνος για την εκτέλεση των ενημερώσεων στο σχήμα της υπηρεσίας καταλόγου. Αυτός ο DC είναι ο μόνος που μπορεί να επεξεργαστεί ενημερώσεις για το σχήμα της υπηρεσίας καταλόγου. Μόλις ολοκληρωθεί η ενημέρωση σχήματος, αυτό αναπαράγεται από τον schema master σε όλους τους άλλους ελεγκτές τομέα του καταλόγου. Υπάρχει μόνο ένας ρόλος schema master ανά κατάλογο.

Domain Naming Master

Ο Domain Naming Master ελέγχει την προσθήκη Domains σε ένα forest. Αυτός ο DC είναι ο μόνος που μπορεί να προσθέσει ή να αφαιρέσει έναν τομέα από τον κατάλογο.

RID Master

Ο RID Master ((Relative Identifier Master) συνεργάζεται με τους ελεγκτές τομέα για την απόδοση αποκλειστικών SID σε κάθε αντικείμενο που απαιτεί ένα. Κάθε αντικείμενο παίρνει ένα SID τομέα που είναι κοινό για όλα τα αντικείμενα του τομέα. Αυτό που κάνει μοναδικό το SID είναι το RID οποία είναι μοναδικό για τα αντικείμενα στον τομέα. Ο RID Master είναι επίσης υπεύθυνος όταν ένα αντικείμενο μετακινηθεί, για τη διαγραφή ενός αντικειμένου από τον τομέα και τη μετακίνηση του σε έναν άλλο τομέα, όταν.

PDC emulator

Ο PDC Emulator δρα σαν PDC (server με Windows NT 4.0) και είναι απαραίτητος σε τομείς που δεν είναι native (δηλαδή, έχουν πελάτες Windows 95/98/NT-). Βεβαίως κάνει πολύ περισσότερα από αυτό. Ο PDC Emulator είναι ο root time server για το συγχρονισμό των ρολογιών στους υπολογιστές Windows στο forest και ο οποίος επιλύει προβλήματα αυθεντικοποίησης. Μια άλλη λειτουργία του PDC Emulator είναι ότι αυτός είναι ο ελεγκτής τομέα στον οποίο όλες οι αλλαγές στην πολιτική ομάδας αποθηκεύονται αρχικά και από εκεί το GPO θα αναπαραχθεί σε όλους τους άλλους ελεγκτές τομέα του τομέα μας. Όλες οι αλλαγές password και θέματα κλειδώματος λογαριασμού- account lockout, γίνονται από τον PDC Emulator

Infrastructure Daemon

Ενημερώσεις συμμετοχής χρηστών σε ομάδες-groups όταν γίνονται αλλαγές.

5.4 Active Directory Services & Server Roles

Το Active Directory services στον Windows Server 2008 καλύπτει πολλές και διαφορετικές υπηρεσίες:

- Active Directory Domain Services (AD DS)
- Active Directory Federation Services (AD FS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Rights Management Services (AD RMS).
- Active Directory Certificate Services (AD CS)

Κάθε μια από τις παραπάνω υπηρεσίες αποτελεί και Server role.

Active Directory Domain Services (AD DS)

Το Active Directory Domain Services (AD DS) των Windows Server 2008, περιλαμβάνει πολλές βελτιώσεις και νέα χαρακτηριστικά σε σύγκριση με το Windows Server 2003 με κυριότερα τα παρακάτω

- Active Directory Domain Services - Read-Only Domain Controllers
- Active Directory Domain Services - Restartable Active Directory Domain Services
- Active Directory Domain Services - Fine-Grained Password Policies
- Identity Management για UNIX

Το Active Directory Read-Only Domain Controller (RODC) είναι ένας νέος τύπος domain controller στα Windows Server 2008. Με ένα RODC, οι οργανισμοί μπορούν να αναπτύξουν εύκολα έναν domain controller σε θέσεις όπου η φυσική ασφάλεια δεν είναι εγγυημένη.

Βασικός σκοπός της RODC είναι να βελτιωθεί η ασφάλεια στα υποκαταστήματα. Στα υποκαταστήματα είναι συχνά δύσκολο να υπάρχει η φυσική ασφάλεια που χρειάζεται για μια IT υποδομή, ειδικά για τους domain controllers που περιέχουν ευαίσθητα δεδομένα. Συχνά ένας domain controller μπορεί να βρεθεί σε ένα γραφείο ή σε χώρους με εύκολη προσβασιμότητα. Αν κάποιος αποκτήσει φυσική πρόσβαση στο DC, δεν είναι δύσκολο να παρακάμψει το σύστημα ασφαλείας και να αποκτήσει πρόσβαση στα δεδομένα. Το RODC λύνει αυτά τα ζητήματα ασφαλείας.

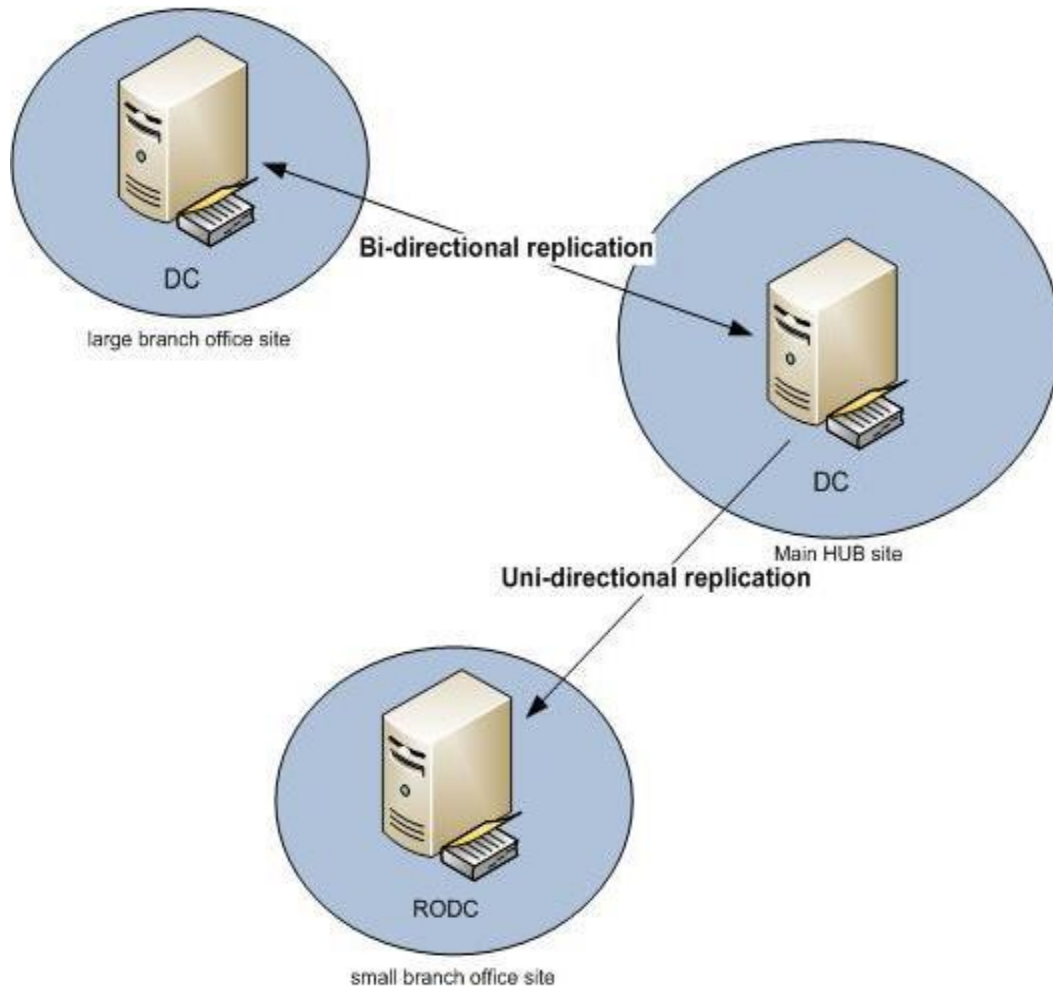
Τα βασικά μέρη του RODC είναι τα εξής:

- Read-Only Domain Controller
- Administrative Role Separation
- Credential Caching

- Read-Only DNS

5.4.1 Read-Only Domain Controller

Ο RODC περιέχει ένα μη εγγράψιμο και μόνο για ανάγνωση αντίγραφο της Active Directory βάσης δεδομένων με όλα της τα αντικείμενα και τα attributes. Ο RODC υποστηρίζει μόνο αναπαραγωγή μιας κατεύθυνσης (uni-directional replication) των τροποποιήσεων του Active Directory, πράγμα που σημαίνει ότι το RODC αναπαράγεται -replicates μόνο με τους Domain Controllers του κεντρικού site.



Εικ.5.7

Replication στον RODC

Το RODC θα επιτελέσει κανονικά την εισερχόμενη αναπαραγωγή -inbound replication από το κεντρικό site για το Active Directory και τις DFS αλλαγές. Το RODC θα λάβει όλα τα δεδομένα από το Active Directory, αλλά ευαίσθητες πληροφορίες όπως τροποποιήσεις σε Domain Admins, Enterprise Admins και Schema Admins αποκλείονται από την αναπαραγωγή στον RODC.

Εάν μια εφαρμογή χρειάζεται πρόσβαση στο Active Directory, ο RODC στέλνει μια LDAP παραπομπή που ανακατευθύνει αυτόματα την εφαρμογή σε ένα Domain Controller με δυνατότητες εγγραφής. Ο RODC είναι επίσης σε θέση να επιτελέσει τον Global Catalog Role για ταχύτερη σύνδεση εάν είναι απαραίτητο.

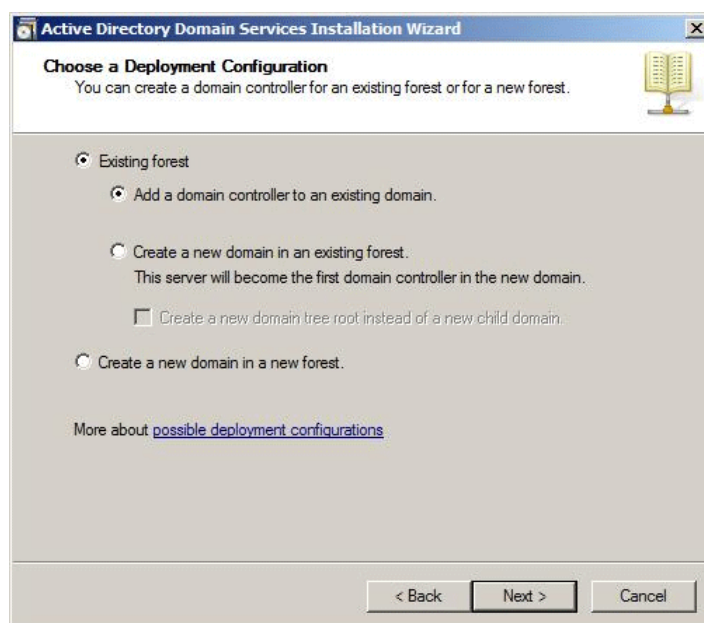
Αυτό είναι ένα μεγάλο πλεονέκτημα για τα υποκαταστήματα και γενικότερα για τα απομακρυσμένα sites, γιατί αν κάποιος αποκτήσει φυσική πρόσβαση στον server ή ακόμα χειρότερα τον κλέψει, αυτός θα είναι σε θέση να σπάσει τους κωδικούς πρόσβασης για τους λογαριασμούς χρηστών στο active directory, αλλά όχι κάποιον από τους ευαίσθητους λογαριασμούς - δεδομένου ότι αυτοί δεν βρίσκονται στο RODC.

Αυτό όμως σημαίνει ότι αυτοί οι ευαίσθητοι λογαριασμοί σαν τον administrator δεν θα είναι σε θέση να συνδεθούν στο RODC εάν η WAN σύνδεση με το κύριο site δεν είναι διαθέσιμη.

Για την εφαρμογή του RODC στο περιβάλλον μας, θα πρέπει να έχουμε το domain και το forest σε Windows Server 2003 native mode και τον domain controller που έχει τον PDC emulator role να έχει εγκατεστημένο Windows Server 2008 λειτουργικό σύστημα.

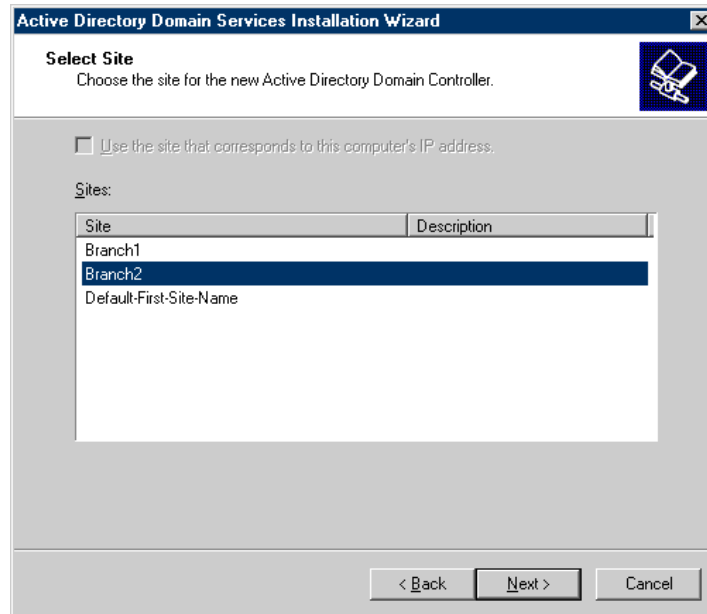
Εγκατάσταση RODC

Αρχίζουμε την εγκατάσταση του AD DS όπως στο **βήμα 1** έως **4** για το **βήμα 5** (παράγραφος 6.3) επιλεγούμε το **Add a domain controller to an existing domain**



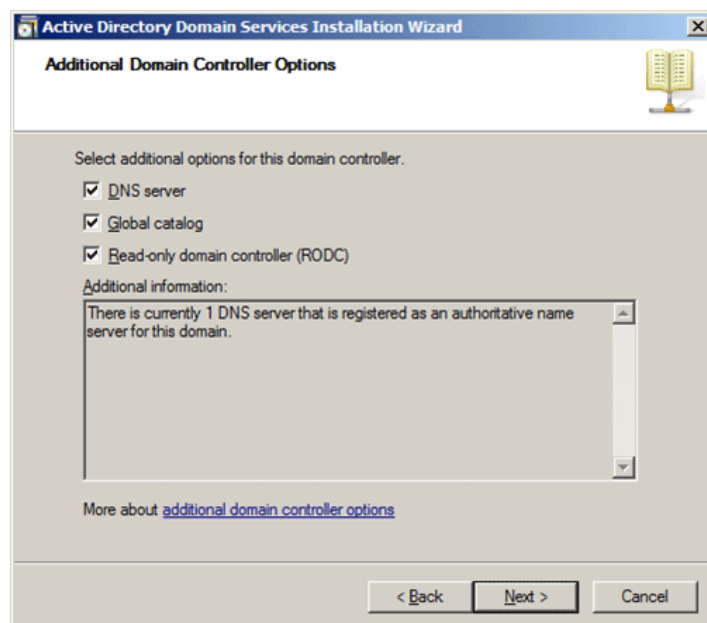
Εικ.5.8

Επιλεγούμε το domain και το active directory site και κάνουμε κλικ στο Next



Εικ.5.9

Επιλεγούμε το Read-only domain controller και κάνουμε κλικ στο Next



Εικ.5.10

Επανεκκινούμε στο τέλος της διαδικασίας.

Administrative Role Separation

Μπορούμε να εκχωρήσουμε δικαιώματα τοπικού διαχειριστή για το RODC εξυπηρετητή σε κάθε χρήστη του Active Directory. Ο εξουσιοδοτημένος λογαριασμός χρήστη θα είναι πλέον σε θέση να συνδεθεί στο εξυπηρετητή και να κάνει εργασίες συντήρησης, χωρίς να έχει δικαιώματα στο AD DS. Επιπλέον ο χρήστης δεν έχει πρόσβαση στους άλλους domain controllers του Active Directory.

Credential Caching

Εξ 'ορισμού, ο RODC δεν αποθηκεύει τοπικά λογαριασμούς χρηστών ή υπολογιστών, εκτός από το λογαριασμό υπολογιστή του ίδιου του RODC και ένα ειδικό λογαριασμό με όνομα «krbtgt» που κάθε RODC έχει.

Το RODC μπορεί όμως να ρυθμιστεί ώστε να αποθηκεύσει κωδικούς πρόσβασης και αυτό γίνεται από το Password Replication Policy. Η Password Replication Policy καθορίζει εάν το Replication από τον εγγράψιμο DC στον RODC επιτρέπεται για τον συγκεκριμένο χρήστη ή υπολογιστή. Σε περίπτωση που αυτό επιτρέπεται, οι πιστοποιήσεις του χρήστη αποθηκεύονται στον RODC κατά την διάρκεια του login.

Όταν ένας λογαριασμός επικυρώνεται με επιτυχία στο RODC, το RODC επιχειρεί να επικοινωνήσει με ένα εγγράψιμο ελεγκτή τομέα στο κεντρικό site. Εάν ένας κωδικός πρόσβασης δεν είναι προσωρινά αποθηκευμένος, ο RODC θα διαβιβάσει την αίτηση ελέγχου ταυτότητας σε ένα εγγράψιμο DC. Το DC κατά την παραλαβή του αιτήματος αναγνωρίζει ότι η αίτηση προέρχεται από RODC και ελέγχει τη Password Replication Πολιτική.

Το όφελος της προσωρινής αποθήκευσης των διαπιστευτηρίων είναι ότι βοηθά την προστασία του κωδικού πρόσβασης σε υποκαταστήματα και ελαχιστοποιεί την έκθεση τους, σε περίπτωση που το RODC εκτεθεί σε κίνδυνο.

Read-Only DNS

Εκτός από το RODC, είναι επίσης δυνατό να εγκατασταθεί μια υπηρεσία R.O. DNS. Ένας εξυπηρετητής DNS που εκτελείται σε έναν RODC δεν υποστηρίζει δυναμικές ενημερώσεις. Αλλά οι πελάτες μπορούν να χρησιμοποιούν το DNS server για την επίλυση ονομάτων.

Δεδομένου ότι το DNS είναι μόνο για ανάγνωση, οι πελάτες δεν μπορούν να ενημερώσουν τις εγγραφές σε αυτόν. Αλλά αν ο πελάτης επιθυμεί να ενημερώσει το δικό του DNS record, ο RODC θα στείλει μια LDAP παραπομπή προς ένα εγγράψιμο DNS server. Το ενημερωμένο αρχείο στη συνέχεια θα αναπαραχθεί-replicate από το εγγράψιμο εξυπηρετητή DNS στο εξυπηρετητή DNS του RODC.

5.4.2 Restartable Active Directory Domain Services.

Το Windows Server 2008, Active Directory Domain Services (AD DS) έχει την δυνατότητα να σταματήσει προσωρινά να λειτουργεί. Αυτό σημαίνει ότι μπορούμε να σταματήσουμε το AD DS για να εκτελέσουμε κάποιες λειτουργίες ή διαδικασίες ή και για συντήρηση, κάτι το οποίο σε προηγούμενες εκδόσεις των Windows Server

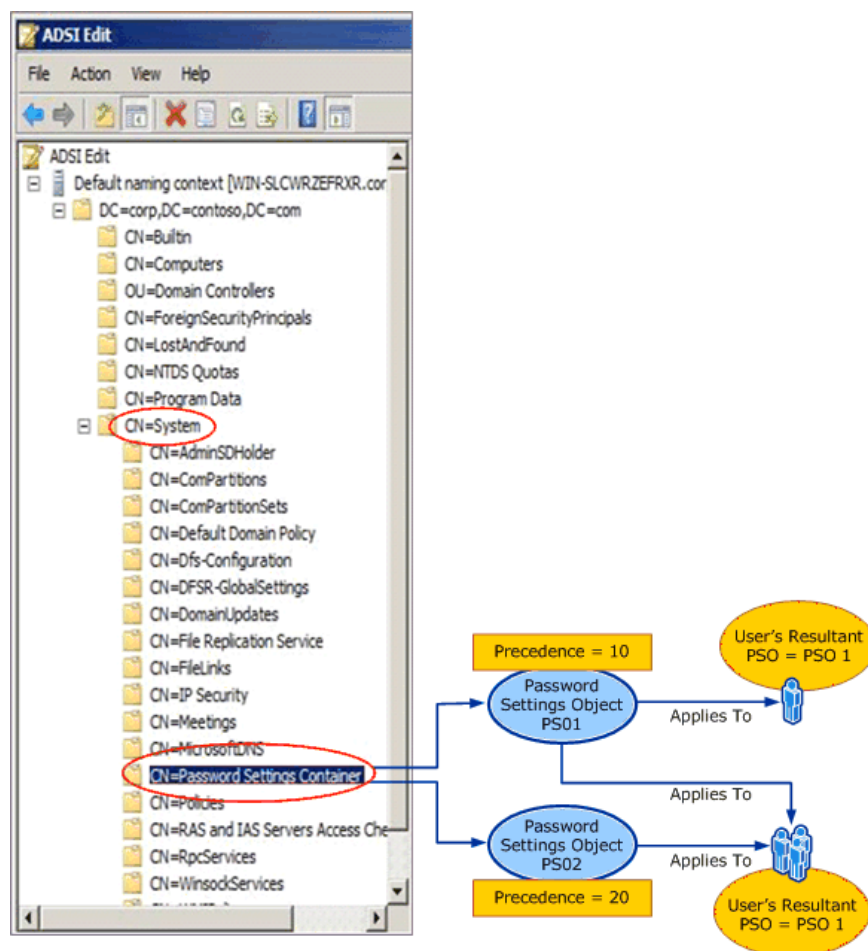
απαιτούσαν επανεκκίνηση σε Directory Services Restore Mode (DSRM). Αυτό γίνεται από την κονσόλα των services-> stop active directory domain services

Τις πιθανές καταστάσεις για το AD DS είναι οι εξής:

- AD DS – started
- AD DS – stopped
- AD DS Restore Mode (DSRM)

Fine-Grained Password Policies

Πριν από τα Windows Server 2008, μπορούσαμε να έχουμε μόνο μια πολιτική κλειδώματος λογαριασμών και password ανά τομέα, η οποία ίσχυε για όλους τους χρήστες του τομέα. Στα Windows Server 2008 AD. DS, είναι δυνατόν τώρα με Fine-Grained Password πολιτικές να καθορίσουν διαφορετικά set πολιτικών κωδικού πρόσβασης ή account lockout για διαφορετικά σύνολα χρηστών στον ίδιο τομέα. Για να γίνει αυτό θα πρέπει να δημιουργηθεί ένα Password Settings object (PSO) με την χρήση του ADSI Edit.



Εικ.5.111

5.4.3 Identity Management για UNIX

Το Identity Management για UNIX είναι ένα service role του AD DS που μπορεί να εγκατασταθεί μόνον δε ελεγκτές τομέα. Δυο τεχνολογίες η Server for NIS (Network Information Service) και το Password Synchronization διευκολύνουν την ενσωμάτωση των windows σε περιβάλλον Unix.

5.5 Εγκατάσταση της υπηρεσίας AD DS

Για την εγκατάσταση του ρόλου Active Directory Domain Services (AD DS) σε εξυπηρετητή είναι απαραίτητο να έχει εγκατασταθεί και ο Domain Name System (DNS) ρόλος σε αυτόν τον εξυπηρετητή ή σε κάποιο άλλο γι' αυτόν τον λόγο η εγκατάσταση θα γίνει μετά από τον σωστό σχεδιασμό του DNS

Domain Name System (DNS) είναι ένα σύστημα ονοματοδοσίας για υπολογιστές και για δικτυακές υπηρεσίες που αντιστοιχίζει ονόματα σε διευθύνσεις δικτύου και τα οργανώνει σε μια ιεραρχική δομή (τομείς, ζώνες περιοχές). Όταν ένας χρήστης εισάγει το DNS όνομα του υπολογιστή σε μια εφαρμογή, η υπηρεσία DNS θα πρέπει να αναζητήσει το όνομα και να παρέχει και άλλες πληροφορίες που συσχετίζονται με τον υπολογιστή, όπως η IP διεύθυνση του ή υπηρεσίες που αυτός παρέχει στο δίκτυο. Αυτή η διαδικασία ονομάζεται επίλυση ονομάτων.

Συστήματα ονοματοδοσίας, όπως το DNS, καθιστούν ευκολότερη τη χρήση των πόρων του δικτύου, παρέχοντας στους χρήστες έναν τρόπο να αναφερθούν σε έναν υπολογιστή ή σε μια υπηρεσία μέσω ενός ονόματος που είναι εύκολο να θυμούνται. Η υπηρεσία DNS μέσω του ονόματος παρέχει την αριθμητική διεύθυνση IP για να γίνει εφικτή η σύνδεση με τον υπολογιστή. Για παράδειγμα, οι χρήστες εισάγουν το www.microsoft.com αντί της IP διεύθυνσης (αριθμητικής) του εξυπηρετητή για τον εντοπισμό του Web server της Microsoft στο Internet.

Το όνομα θα επιλυθεί (στην IP διεύθυνση του), όταν το λογισμικό-πελάτη DNS του χρήστη, θα στείλει μια αίτηση σε ένα DNS server που ο υπολογιστής του χρήστη έχει ρυθμιστεί να χρησιμοποιεί. Εάν ο εξυπηρετητής DNS έχει ρυθμιστεί ώστε να απαντήσει authoritatively με τη IP διεύθυνση του ζητούμενου ονόματος, θα απαντήσει στο αίτημα άμεσα. Σε αντίθετη περίπτωση, ο DNS server περνάει το αίτημα σε άλλο DNS server που μπορεί να παρέχει τη διεύθυνση ή την παραπομπή σε άλλους DNS servers που μπορούν να βοηθήσουν την επίλυση της διεύθυνσης.

Εάν ο τοπικός DNS εξυπηρετητής δεν γνωρίζει ποιος εξυπηρετητής έχει επιφορτιστεί με την επίλυση των συγκεκριμένων διευθύνσεων, μπορεί να ζητήσει την διεύθυνση

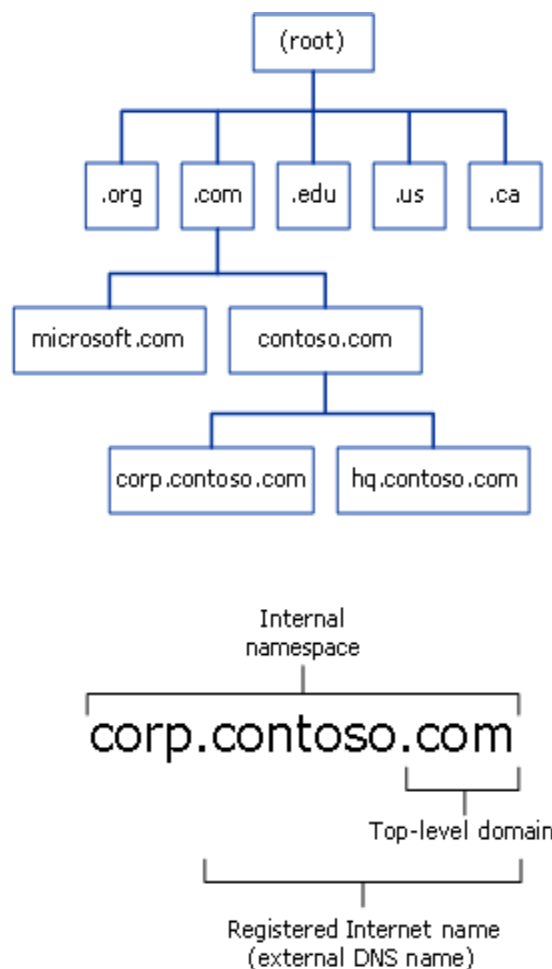
του από τον DNS εξυπηρετητή που είναι υπεύθυνος της ρίζας-root του δέντρου του DNS domain namespace. Για παράδειγμα, αν το DNS server δεν γνωρίζει ο εξυπηρετητής είναι υπεύθυνος για το εξυπηρετητή που ονομάζεται `www.microsoft.com`, ο εξυπηρετητής DNS μπορεί να ζητήσει από τον εξυπηρετητή που είναι υπεύθυνος για το `.com domain` την παροχή της IP διεύθυνσης του εξυπηρετητή που είναι υπεύθυνος για την παροχή διευθύνσεων του domain `microsoft.com`. Στη συνέχεια μόλις πάρει αυτήν την διεύθυνση ο αρχικός- τοπικός DNS εξυπηρετητής μπορεί να υποβάλει ερώτημα σε αυτόν τον DNS εξυπηρετητή για τη διεύθυνση του υπολογιστή με το όνομα `www.microsoft.com`. Τα DNS records που οδηγούν στους προαναφερόμενους (13) εξυπηρετητές ανώτερου επιπέδου root ονομάζονται και root hints.

ΥΠΗΡΕΣΙΕΣ ΟΝΟΜΑΤΩΝ- ΣΧΕΔΙΑΣΜΟΣ DNS

Το Domain Name System (DNS) είναι η κύρια μέθοδος για την επίλυση ονομάτων στα Windows Server 2008 όπως και για άλλες εκδόσεις των λειτουργικών συστημάτων Windows της Microsoft, όπως τα Windows 2000, Windows XP, Windows Server 2003 και τα Windows Vista. Όπως προαναφέρθηκε DNS είναι απαιτούμενο για την εγκατάσταση του ρόλου Active Directory Domain Services (AD DS) στον εξυπηρετητή.

6.1 Η κατανόηση των ονομάτων DNS

Η παρακάτω εικόνα δείχνει τον τρόπο που το DNS είναι ιεραρχικά οργανωμένο.



Εικ.6.1

Ένα όνομα DNS αποτελείται από δύο ή περισσότερα μέρη που χωρίζονται από τελείες (.). Το τελευταίο (δεξιό), μέρος του ονόματος ονομάζεται top-level domain (TLD). Άλλα μέρη του ονόματος είναι υποτομείς του TLD ή αλλιώς subdomain. Τα ονόματα των TLD προσδιορίζονται είτε λειτουργικά είτε γεωγραφικά.

Λειτουργικά TLD	Συνήθως χρησιμοποιούνται από ...
. com	Εμπορικές οντότητες, όπως επιχειρήσεις
. edu	Ξένα Εκπαιδευτικά ιδρύματα, όπως τα κολέγια, και τα δημόσια και ιδιωτικά σχολεία των ΗΠΑ
. gov	Κυβερνητικές υπηρεσίες των ΗΠΑ, όπως είναι οι ομοσπονδιακές και τοπικές κυβερνήσεις
. net	Οργανισμοί που παρέχουν υπηρεσίες Internet, όπως οι πάροχοι υπηρεσιών Διαδικτύου (ISP)
. org	Ιδιωτικές, μη κερδοσκοπικές οργανώσεις

Γεωγραφικές TLDs με την ένδειξη της χώρας ή της περιοχής από όπου ο οργανισμός που καταχωρήθηκε το domain βρίσκεται. Για παράδειγμα, μια οργάνωση που θέλει να δείξει ότι βρίσκεται στην Ελλάδα καταχωρεί το domain name στο .GR TLD και μια επιχείρηση που θέλει να δείξει ότι είναι εγκατεστημένη στη Βραζιλία καταχωρεί το domain name του στο .BR TLD

Οι περισσότεροι οργανισμοί που θέλουν να έχουν παρουσία στο Διαδίκτυο μέσω μιας ιστοσελίδας Web ή που θέλουν να στείλουν ή να λάβουν μηνύματα ηλεκτρονικού ταχυδρομείου, επιλέγουν να καταχωρίσουν ένα όνομα που συνήθως βασίζεται στο όνομα τους, όπως microsoft.com ή ekdd.gr

6.2 Σχεδιάζοντας ένα χώρο ονομάτων DNS

Μπορούμε να σχεδιάσουμε έναν “εξωτερικό” χώρο ονομάτων DNS που να είναι ορατός στους χρήστες του Διαδικτύου ή να σχεδιάσουμε ένα “εσωτερικό” χώρο ονομάτων που είναι ορατός μόνο σε χρήστες και υπολογιστές που βρίσκονται εσωτερικά στο δίκτυό μας.

Οργανισμοί που απαιτούν παρουσία στο Διαδίκτυο, καθώς και εσωτερικό χώρο ονομάτων πρέπει να αναπτύξουν τόσο μια εσωτερική όσο και μια εξωτερική DNS ονοματοδοσία και να διαχειριστούν κάθε namespace ξεχωριστά.

6.2.1 Δημιουργία ενός ονόματος τομέα DNS

Εάν θα χρησιμοποιήσουμε ταυτόχρονα μια εσωτερική και μια εξωτερική DNS ονοματοδοσία ελέγχουμε στον τοπικό μας πάροχο- καταχωρητή -registrar ονομάτων εάν το όνομα που επιλέξαμε είναι διαθέσιμο προς αγορά. πχ ekdd.gr

Χρησιμοποιούμε ονόματα υπολογιστών συναφή με την πολιτική ονοματοδοσίας του οργανισμού μας π.χ. Το FQDN – Fully Qualified Domain Name του υπολογιστή της μισθοδοσίας μπορεί να είναι payroll.ekdd.gr με hostname το payroll

Για τους τομείς μας εσωτερικά, δημιουργούμε ονόματα που σχετίζονται με το DNS όνομα που έχει καταχωρηθεί. Πχ για το καταχωρημένο ekdd.gr χρησιμοποιούμε πάλι το ίδιο ως όνομα τομέα των windows (domain). Και με χρήση του ekdd, σαν το NetBIOS domain name.

6.2.2 Δημιουργία ονόματα υπολογιστών DNS

Θα πρέπει να ακολουθούμε τα παρακάτω όταν δημιουργούμε DNS ονόματα:

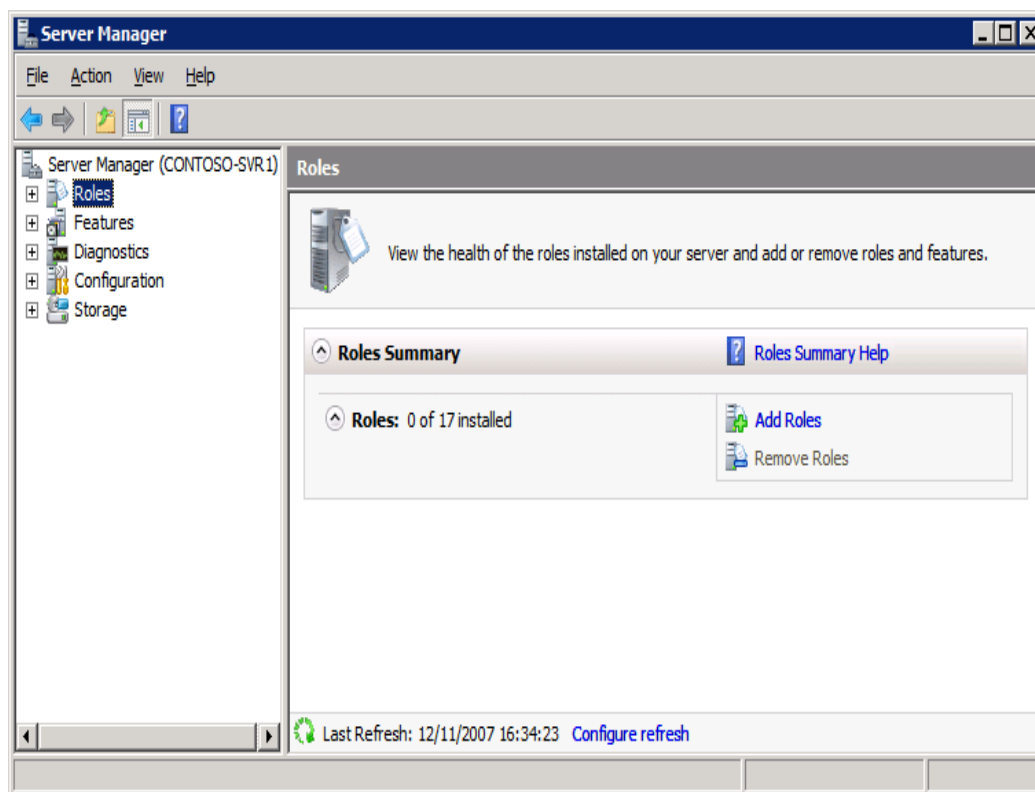
- Επιλογή ονομάτων υπολογιστών που θα είναι εύκολο στους χρήστες να τα θυμούνται.
- Ορίζουμε τον ιδιοκτήτη του υπολογιστή ή την θέση εργασίας στο όνομα του υπολογιστή.
- Χρησιμοποιούμε μοναδικά ονόματα για όλους τους υπολογιστές της εταιρείας/οργανισμού μας.
- Χρησιμοποιούμε χαρακτήρες ASCII για να εξασφαλιστεί η διαλειτουργικότητα με τους υπολογιστές που χρησιμοποιούν εκδόσεις των Windows πριν από τα Windows 2000 εάν φυσικά έχουμε τέτοιους.
- Για τον υπολογιστή και τα ονόματα τομέα, θα χρησιμοποιηθούν μόνο οι χαρακτήρες Α έως το Ω, 0 έως 9, καθώς και η παύλα (-). Ειδικότερα, οι παρακάτω χαρακτήρες δεν επιτρέπονται στην ονοματοδοσία του DNS:
 - Κόμμα (,)
 - Περισπωμένη (~)
 - Άνω και κάτω τελεία (:)
 - Θαυμαστικό (!)
 - Το σύμβολο (@)
 - Το σύμβολο αριθμού (#)
 - Το σύμβολο του δολαρίου (\$)
 - Σύμβολο του ποσοστού (%)
 - Ύψωση σε δύναμη (^)
 - Ampersand (&)
 - Απόστροφος (')

- Τελεία (.), Εκτός από διαχωριστικό μεταξύ των ονομάτων
- Παρενθέσεις (())
- Άγκιστρα ({})
- Υπογράμμιση (_)
- Ο αριθμός των χαρακτήρων σε ένα όνομα πρέπει να είναι μεταξύ 2 και 24.

6.3 Εγκατάσταση και ρύθμιση ADDS και DNS

Όταν δημιουργούμε ένα νέο Active Directory Domain Services (AD DS) domain, ο Active Directory Domain Services οδηγός εγκατάστασης εγκαθιστά το ρόλο Domain Name System (DNS) από προεπιλογή. Αυτό διασφαλίζει ότι οι DNS και AD DS έχουν ρυθμιστεί σωστά.

Στον Windows Server 2008, σε αντίθεση με προηγούμενες εκδόσεις, ένα επιπλέον βήμα πρέπει να ληφθεί πριν από την εκτέλεση του DCPROMO για να προβιβάσουμε το εξυπηρετητή σε ελεγκτή τομέα και για την εγκατάσταση του Active Directory σε αυτό. Αυτό το βήμα είναι η εγκατάσταση του ρόλου Active Directory Domain Services (AD-DS), στον εξυπηρετητή. Στην πραγματικότητα, ο ρόλος AD-DS είναι αυτό που επιτρέπει στον server να ενεργεί ως ελεγκτής τομέα, και μετά θα πρέπει να εκτελέσουμε το DCPROMO.exe



Εικ.6.2

Πριν από την εγκατάσταση και ρύθμιση του AD DS και DNS στον πρώτο domain controller σε ένα νέο τομέα-domain, θα πρέπει να βεβαιωθούμε ότι η διεύθυνση IP του εξυπηρετητή είναι στατική. Δηλαδή, ότι δεν έχει ανατεθεί από κάποιο Dynamic Host Configuration Protocol (DHCP) server, ή ότι έχει γίνει explicit reservation της IP αυτής με την MAC Address του server (σπανιότερα).

Για να εγκαταστήσουμε το DNS με AD DS σε ένα νέο Domain

Βήμα 1

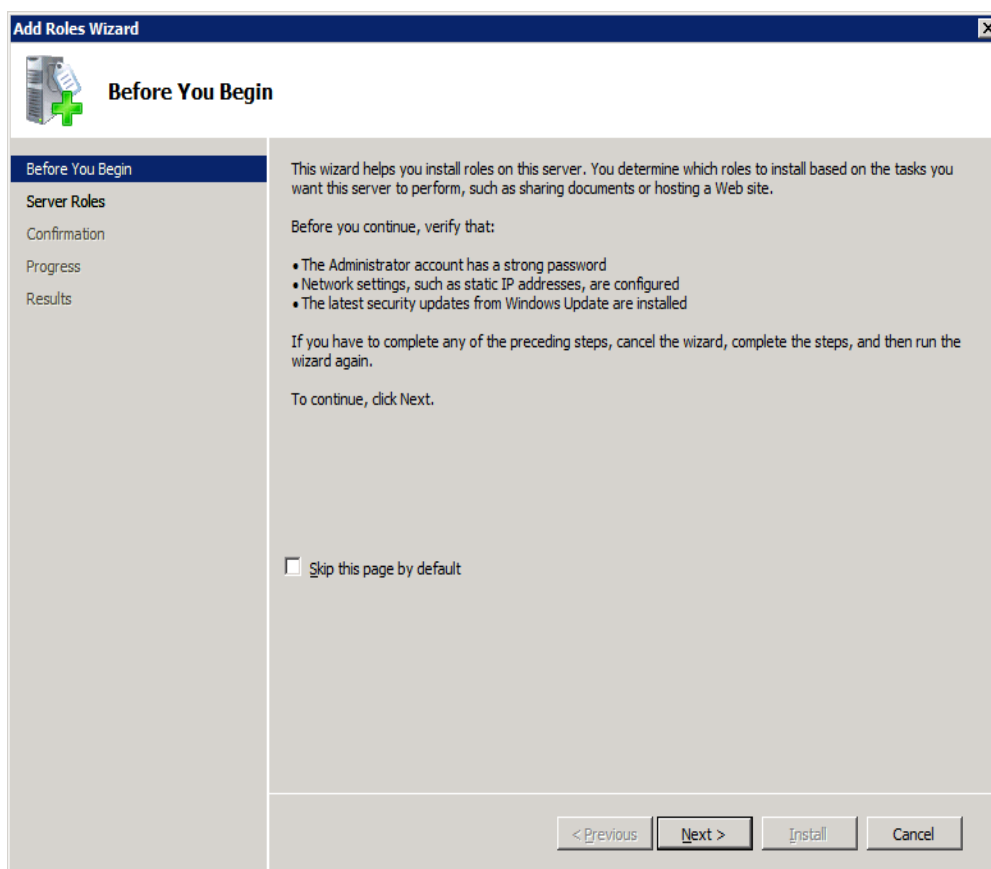
Κάνουμε κλικ στο κουμπί Start, Administrative Tools και στη συνέχεια κάνουμε κλικ στην επιλογή Server Manager.

Στο παράθυρο δέντρο, κάνουμε κλικ στην εντολή **Roles**.

Στο παράθυρο αποτελεσμάτων, κάνουμε κλικ στο κουμπί **Add Roles**.

Βήμα 2

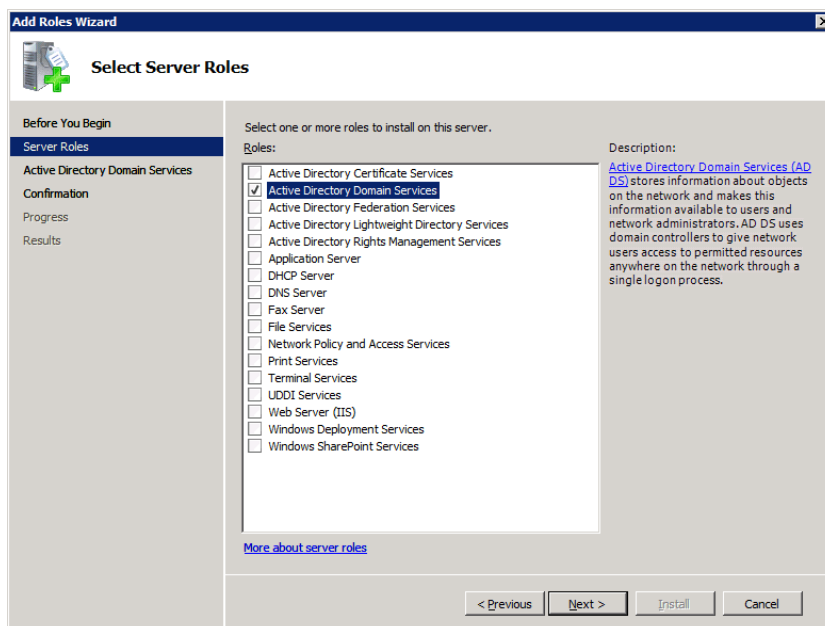
Στη σελίδα **Before You Begin**, κάνουμε κλικ στο κουμπί Next.



Εικ.6.3

Βήμα 3

Στη σελίδα Select Server Roles, κάνουμε κλικ στο Active Directory Domain Services και κατόπιν κάνουμε κλικ στο **Next**.



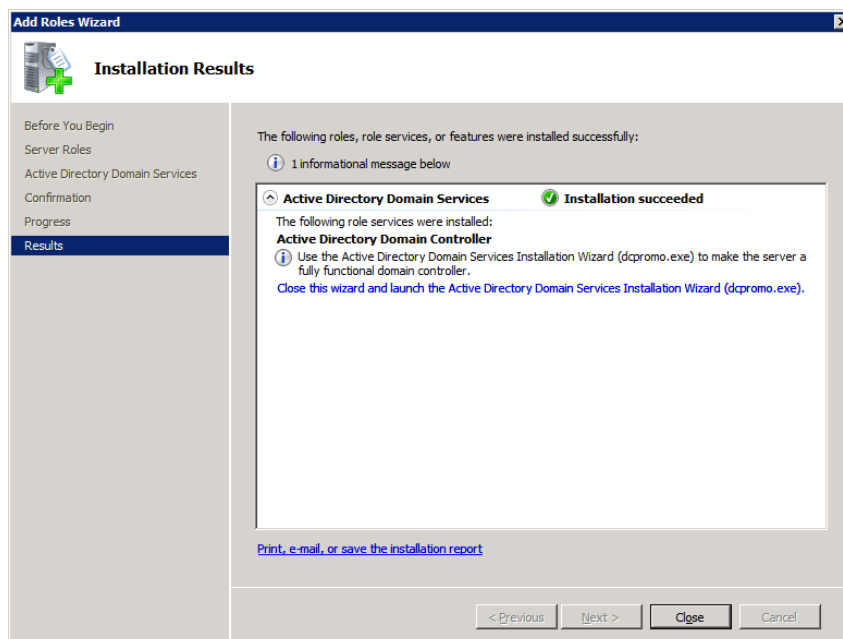
Εικ.6.4

Βήμα 4

Από την σελίδα **Active Directory Domain Services**, διαβάζουμε τις πληροφορίες και στη συνέχεια κάνουμε κλικ στο **Next**.

Από την σελίδα **Confirm Installation Selections**, διαβάζουμε τις πληροφορίες και στη συνέχεια κάνουμε κλικ στο κουμπί **Install**.

Μετά την ολοκλήρωση της εγκατάστασης, στην σελίδα **Installation Results**, κάνουμε κλικ στο κουμπί **Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe)**.

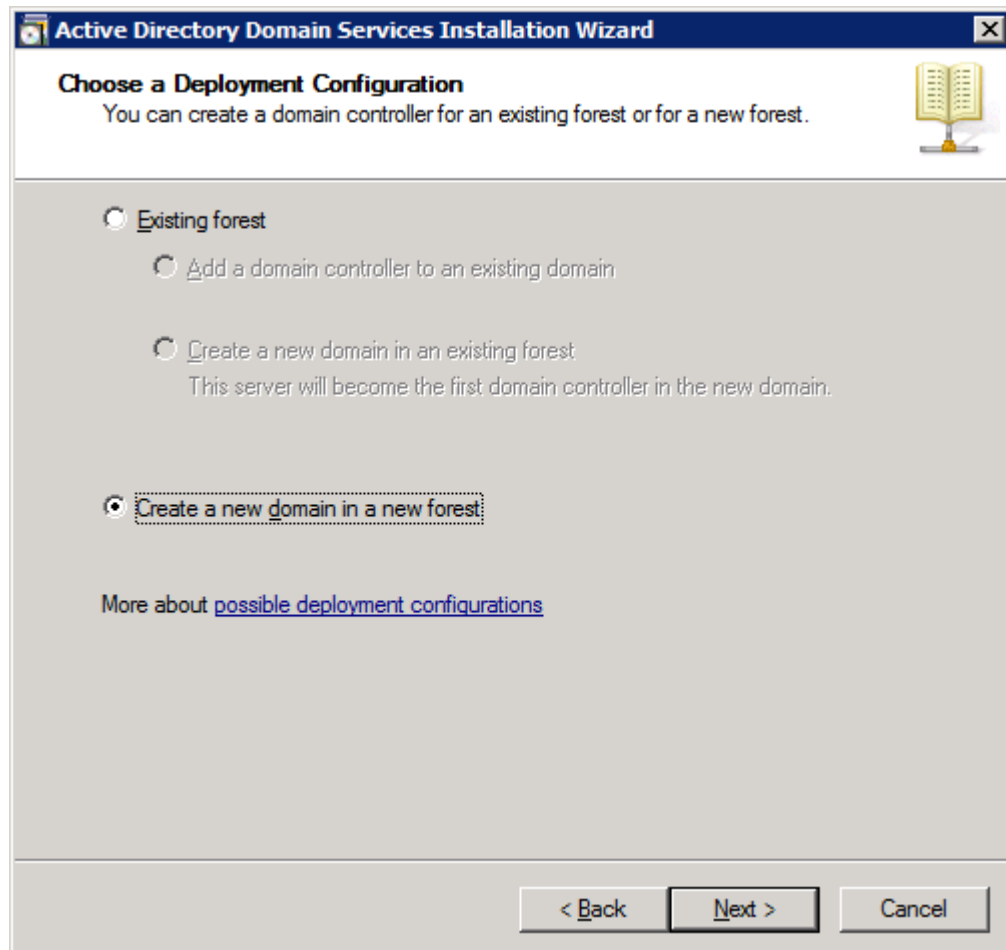


Εικ.6.5

Βήμα 5

Στην σελίδα **Welcome to the Active Directory Domain Services Installation Wizard**, κάνουμε κλικ στο κουμπί **Next**.

Στην σελίδα **Choose a Deployment Configuration**, κάνουμε κλικ στην επιλογή **Create a new domain in a new forest** και στη συνέχεια κάνουμε κλικ στο **Next**.



Εικ.6.6

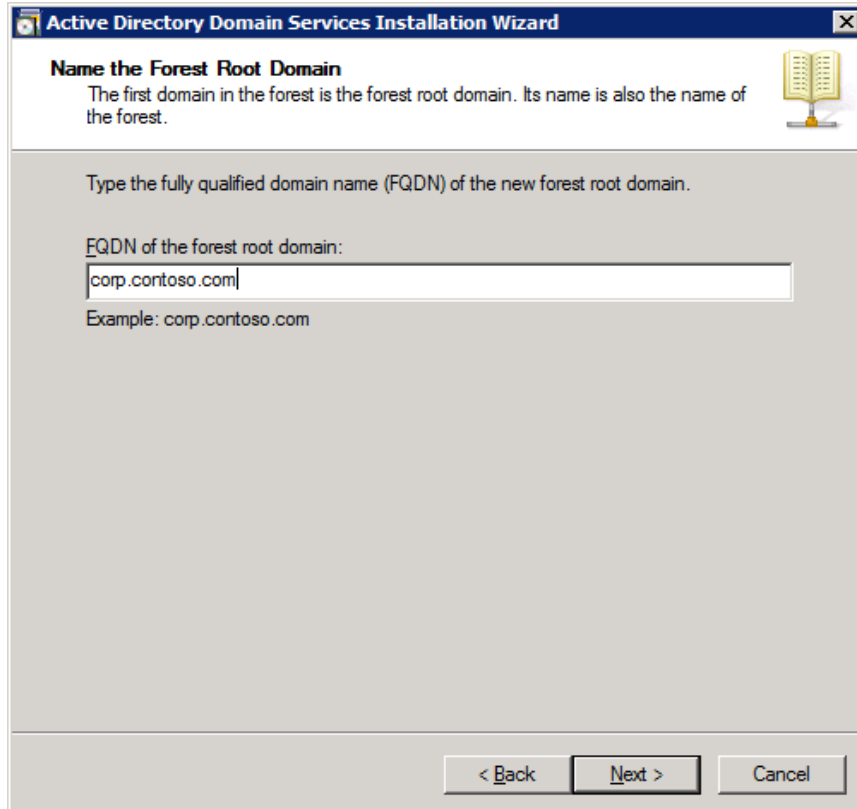
Βήμα 6

Στη σελίδα **Name the Forest Root Domain**, πληκτρολογούμε το πλήρες όνομα DNS (FQDN) για το νέο τομέα και κατόπιν κάνουμε κλικ στο **Next**.

Βήμα 7

Στη σελίδα **Set Forest Functional Level**, επιλέγουμε το Windows Server 2008, και στη συνέχεια κάνουμε κλικ στο κουμπί **Next**.

Στη σελίδα **Additional Domain Controller Options**, βεβαιωνόμαστε ότι το DNS server είναι επιλεγμένο και κατόπιν κάνουμε κλικ στο **Next**.



Active Directory Domain Services Installation Wizard

Name the Forest Root Domain

The first domain in the forest is the forest root domain. Its name is also the name of the forest.

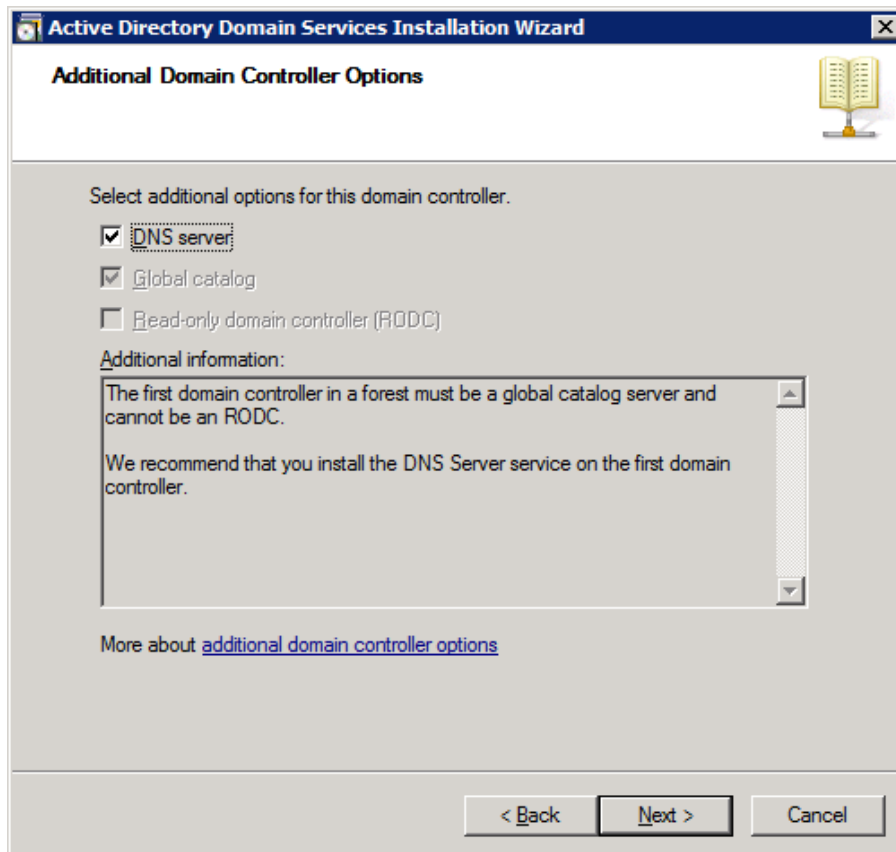
Type the fully qualified domain name (FQDN) of the new forest root domain.

FQDN of the forest root domain:

Example: corp.contoso.com

< Back Next > Cancel

Εικ.6.7



Active Directory Domain Services Installation Wizard

Additional Domain Controller Options

Select additional options for this domain controller.

☒ DNS server

☒ Global catalog

☐ Read-only domain controller (RODC)

Additional information:

The first domain controller in a forest must be a global catalog server and cannot be an RODC.

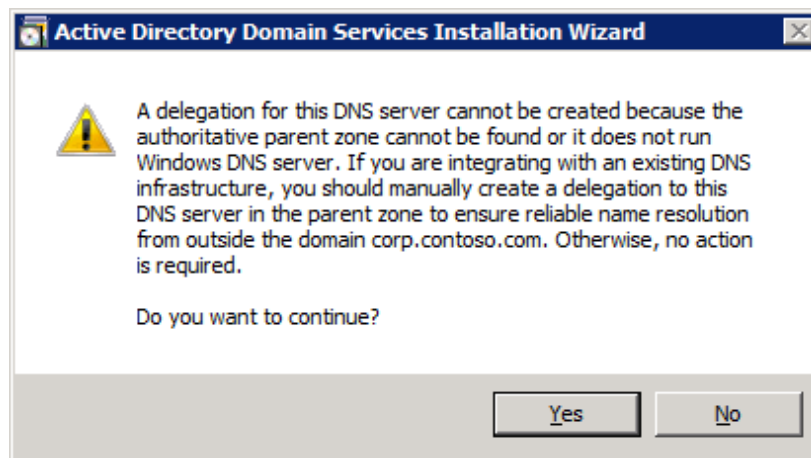
We recommend that you install the DNS Server service on the first domain controller.

More about [additional domain controller options](#)

< Back Next > Cancel

Εικ.6.8

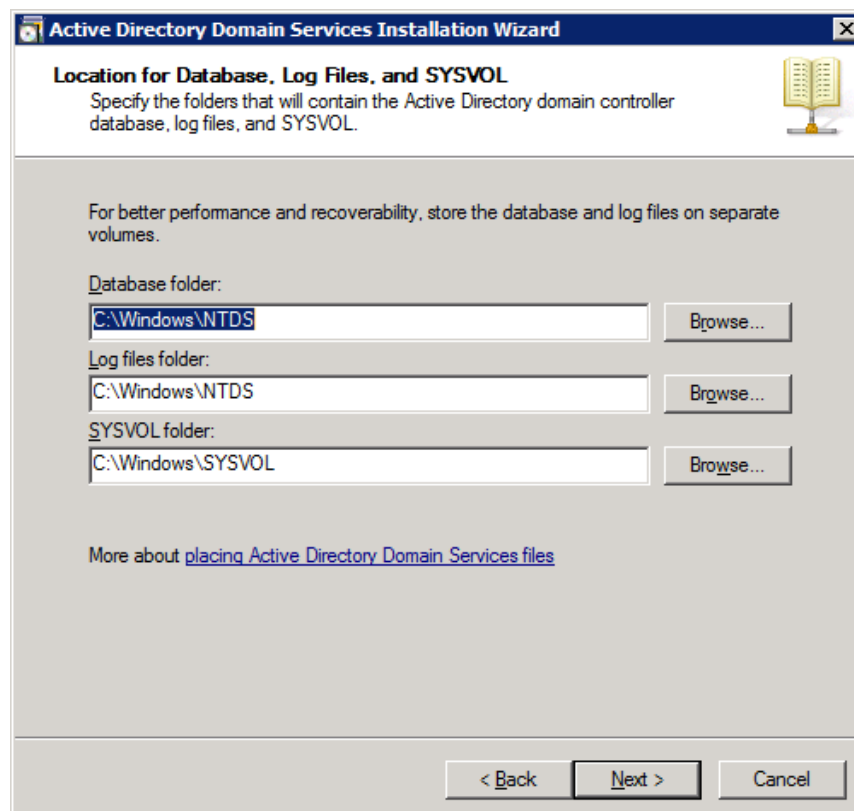
Ένα πλαίσιο μηνύματος μας ενημερώνει ότι delegation για αυτό το εξυπηρετητή DNS δεν μπορεί να δημιουργηθεί. Αυτό είναι φυσιολογικό και αναμενόμενο για το πρώτο ελεγκτή τομέα σε ένα νέο forest. Κάνουμε κλικ στο κουμπί **YES** για να συνεχίσουμε.



Εικ.6.9

Βήμα 8

Στη σελίδα που ζητάει τη θέση για τη βάση δεδομένων, των αρχείων καταγραφής **Log Files** και του SYSVOL, πληκτρολογούμε τη θέση την οποία θέλουμε, ή επιλέγουμε **Browse** για να επιλέξουμε μια νέα θέση, και στη συνέχεια κάνουμε κλικ στο **Next**.



Εικ.6.10

Βήμα 9

Στη σελίδα Directory Services Restore Mode Administrator Password, πληκτρολογούμε έναν κωδικό πρόσβασης που θα χρησιμοποιήσουμε για να συνδεθούμε με το εξυπηρετητή σε Directory Services Restore Mode, επιβεβαιώνουμε τον κωδικό πρόσβασης και στη συνέχεια, κάνουμε κλικ στο **Next**.

Εικ.6.11

Ελέγχουμε τα δεδομένα της σελίδας **Summary** και στη συνέχεια κάνουμε κλικ στο κουμπί **Next** για να ξεκινήσει η εγκατάσταση.

Μετά το τέλος της εγκατάστασης, κάνουμε κλικ στο κουμπί OK για να επανεκκινήσουμε τον υπολογιστή.

Εναλλακτική εγκατάσταση AD DS – Servermanagercmd.exe

Το Servermanagercmd.exe είναι το αντίστοιχο σε command line του Add Roles and Add Features wizard στον Server Manager. Με τη χρήση των διαφόρων επιλογών της γραμμής εντολών, μπορούμε γρήγορα και εύκολα να προσθέσουμε ή να αφαιρέσουμε λειτουργίες και ρόλους στον ή από τον κεντρικό υπολογιστή, συμπεριλαμβανομένου του ρόλου AD-DS.

Για την εγκατάσταση AD-DS με τη χρήση Servermanagercmd.exe, πληκτρολογούμε την ακόλουθη εντολή στο παράθυρο της γραμμής εντολών:

Servermanagercmd.exe -I ADDS-Domain-Controller

6.4 Διαχείριση της Υπηρεσίας DNS

6.4.1 DNS κονσόλα και διαμόρφωση

Μετά την εγκατάσταση του DNS, μπορούμε να βρούμε την DNS κονσόλα από το Έναρξη -> Όλα τα Προγράμματα -> Administrative Tools -> DNS. Το Windows 2008 παρέχει έναν οδηγό για να μας βοηθήσει να ρυθμίσουμε το DNS.

Κατά τη ρύθμιση των παραμέτρων του DNS server, θα πρέπει να είμαστε εξοικειωμένοι με τις ακόλουθες έννοιες:

- Forward lookup zone
- Reverse lookup zone
- Zone types

Μια Forward lookup zone είναι απλά ένας τρόπος για την επίλυση των ονομάτων υπολογιστών σε διευθύνσεις IP.

Μια Reverse lookup zone επιτρέπει σε ένα εξυπηρετητή DNS να ανακαλύψει το όνομα DNS του υπολογιστή από την IP του. Ουσιαστικά, πρόκειται για το ακριβώς αντίθετο μιας Forward lookup zone.

Μια reverse lookup zone δεν απαιτείται, αλλά είναι εύκολο να ρυθμιστεί και θα επιτρέψει τον Windows 2008 Server να έχει πλήρη DNS λειτουργικότητα.

Κατά την επιλογή ενός τύπου ζώνης -Zone type στον DNS server έχουμε τις εξής επιλογές:

Active Directory (AD) Integrated, Standard Primary και Standard Secondary

Η πρώτη επιλογή αποθηκεύει τις πληροφορίες της βάσης δεδομένων στο AD και επιτρέπει την ασφαλή ενημέρωση της. Αυτή η επιλογή θα εμφανιστεί μόνο αν το AD έχει εγκατασταθεί. Σε περίπτωση που έχει εγκατασταθεί και κάνουμε αυτήν την επιλογή, το AD θα αποθηκεύσει και την αναπαραγωγή-replication των αρχείων ζώνης μας.

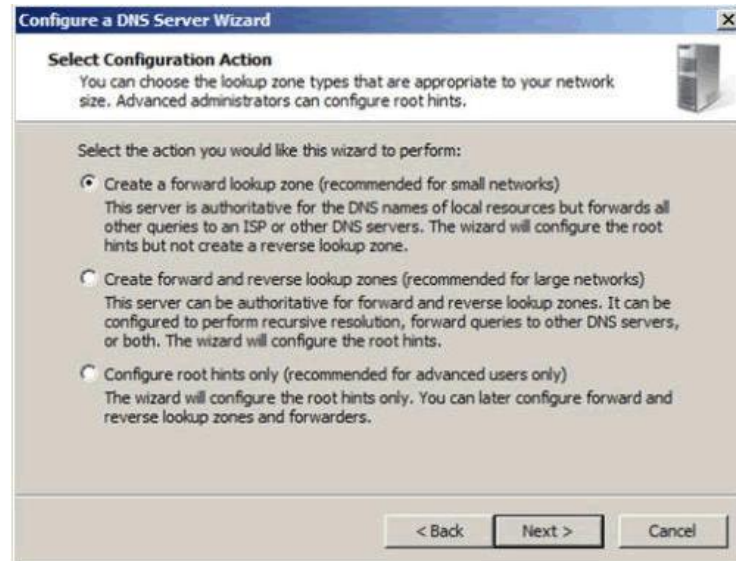
Μια Standard Primary ζώνη αποθηκεύει τη βάση δεδομένων σε ένα αρχείο κειμένου. Αυτό το αρχείο κειμένου μπορεί να διαμοιραστεί με άλλους διακομιστές DNS που αποθηκεύουν τις πληροφορίες τους σε ένα αρχείο κειμένου. Τέλος, μια Standard Secondary ζώνη δημιουργεί απλώς ένα αντίγραφο της υπάρχουσας βάσης δεδομένων από έναν άλλο DNS server τον primary. Χρησιμοποιείται κυρίως για load balancing.

Για να ανοίξουμε το εργαλείο παραμετροποίησης του DNS server:

Επιλέγουμε DNS από το φάκελο Administrative Tools για να ανοίξουμε την κονσόλα DNS.

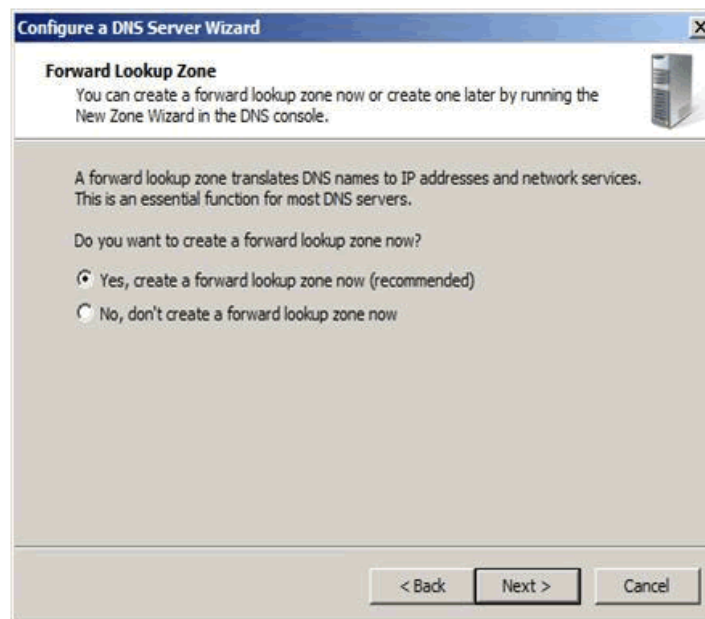
Επισημάνουμε το όνομα του server μας και επιλέγουμε Action -> Configure a DNS Server για την έναρξη του Configure DNS Server Wizard.

Κάνουμε κλικ στο **Next** και επιλέγουμε ένα από: forward lookup zone, forward and reverse lookup zone, root hints only



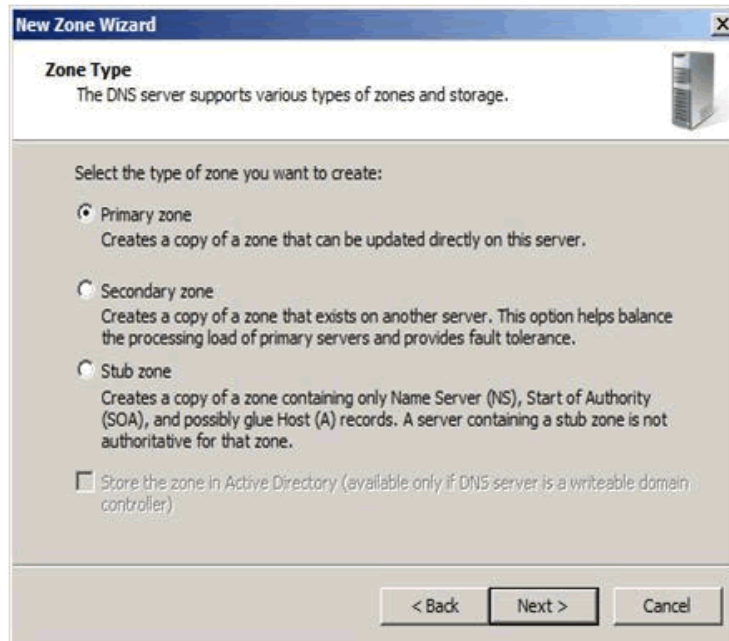
Εικ.6.12

Κάνουμε κλικ στο κουμπί **Next** και στη συνέχεια κάνουμε κλικ στο κουμπί **Yes** για να δημιουργήσουμε μια forward lookup zone



Εικ.6.13

Επιλέγουμε το κατάλληλο κουμπί για να εγκαταστήσουμε τα επιθυμητά Zone Types

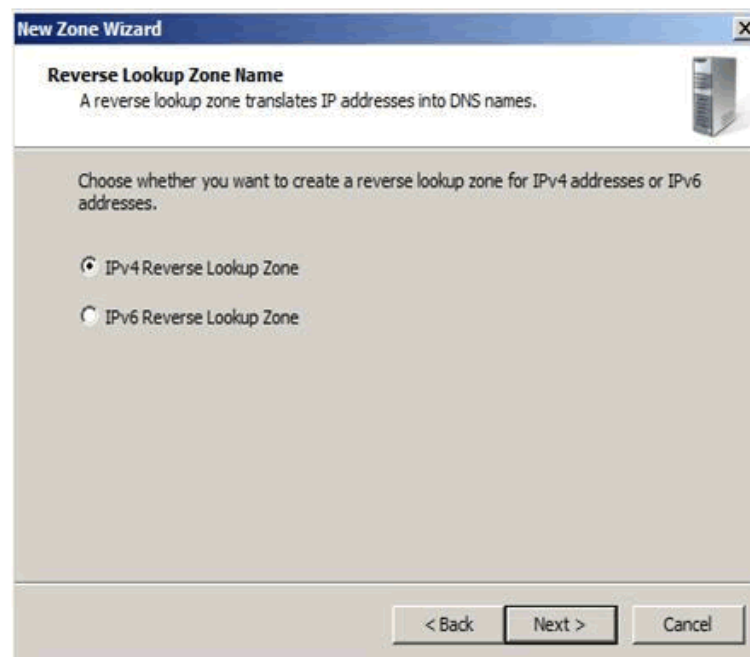


Εικ.6.14

Κάνουμε κλικ στο κουμπί **Next** και πληκτρολογούμε το όνομα της ζώνης που δημιουργούμε.

Κάνουμε κλικ στο κουμπί **Next** και στη συνέχεια κάνουμε κλικ στο κουμπί **Yes** για να δημιουργήσουμε μια reverse lookup zone

Επιλέγουμε μεταξύ μιας IPv4 ή IPv6 Reverse Lookup Zone



Εικ.6.15

New Zone Wizard

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

☒ Network ID:

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☐ Reverse lookup zone name:

< Back Next > Cancel

Εικ.6.16

Κάνουμε κλικ στο κουμπί **Next** και εισάγουμε τις πληροφορίες που προσδιορίζουν την reverse lookup zone

Μπορούμε να επιλέξουμε να δημιουργήσετε ένα νέο αρχείο ή να χρησιμοποιήσουμε ένα ήδη υπάρχον αρχείο DNS

New Zone Wizard

Zone File
You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

☒ Create a new file with this file name:

☐ Use this existing file:

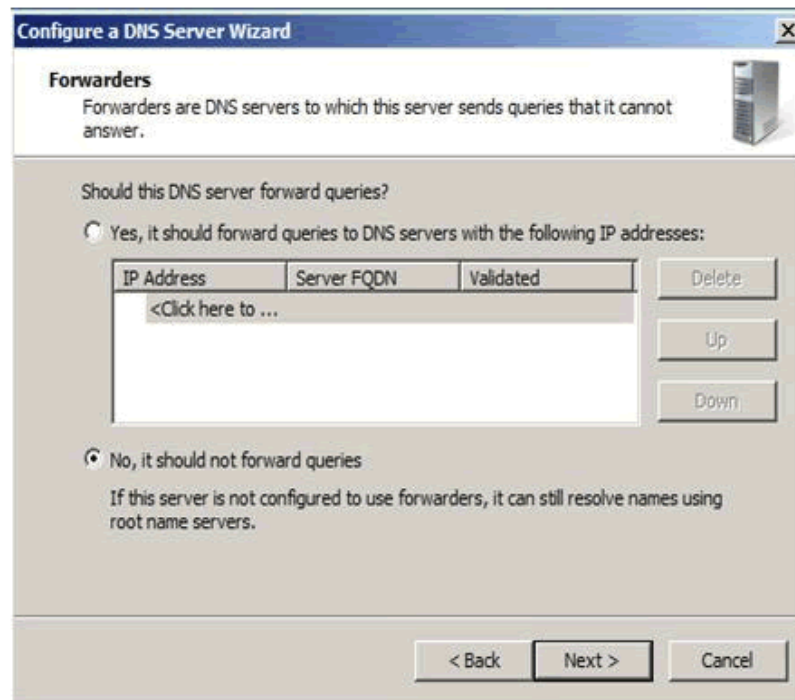
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

< Back Next > Cancel

Εικ.6.17

Στο παράθυρο της δυναμικής ενημέρωσης, πρέπει να επιλεγεί πώς ο DNS δέχεται ασφαλείς, nonsecure, ή δεν δέχεται δυναμικές ενημερώσεις.

Εάν θα πρέπει να εισαχθεί ένας DNS, forwarder μπορούμε να τον εισάγουμε στο παράθυρο Forwarders.



Εικ.6.18

Κάνουμε κλικ στο κουμπί Finish

6.4.2 Διαχείριση DNS

Διαχείριση DNS Records (εγγραφές)

Υπάρχουν πολλά είδη DNS records, τα περισσότερα από τα οποία δε χρησιμοποιούνται και τόσο συχνά. Αυτά που χρησιμοποιούνται περισσότερο είναι τα παρακάτω:

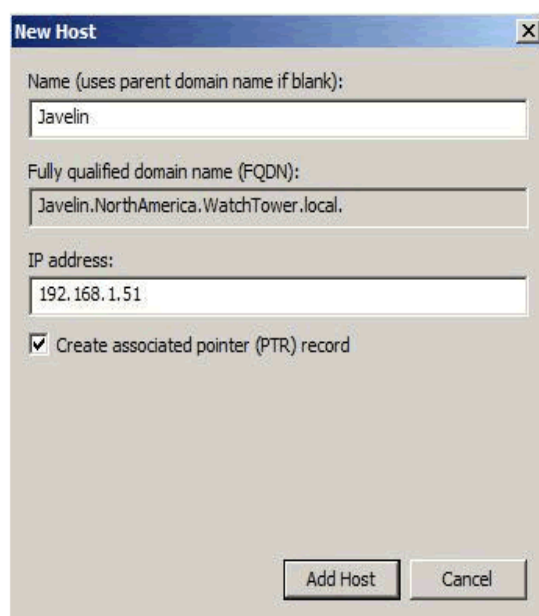
- A (Address) – Αντιστοιχίζει όνομα υπολογιστή υπηρεσίας σε διεύθυνση IP (πολλαπλές IP διευθύνσεις για τον ίδιο υπολογιστή πολλαπλά A records)
- CNAME (Canonical Name) – Ορίζει alias (ψευδώνυμο) για ένα όνομα υπολογιστή (π.χ. ο υπολογιστής corpserver01.microsoft.com μπορεί να έχει το ψευδώνυμο www.microsoft.com)
- MX (Mail eXchange) – Ορίζει στο domain ένα server ανταλλαγής αλληλογραφίας ο οποίος φροντίζει για τη μεταφορά της αλληλογραφίας στο σωστό mail server

- NS (Name Server) – Ορίζει στο domain ένα ή/και περισσότερους DNS servers (primary, secondary)
- PTR (PoinTeR) – Δημιουργεί δείκτη που αντιστοιχίζει IP σε όνομα υπολογιστή ώστε να είναι δυνατή η αντίστροφη αναζήτηση (reverse lookup)
- SOA (Start Of Authority) – Δηλώνει ποιος υπολογιστής είναι η «πιο εξουσιοδοτημένη» πηγή πληροφοριών DNS

Κάθε ζώνη πρέπει να έχει και ένα SOA record (δημιουργείται αυτόματα κατά τη δημιουργία της ζώνης).

Προσθήκη A και PTR Records

Ένα A και ένα PTR record μπορούν να δημιουργηθούν είτε ταυτόχρονα, είτε ξεχωριστά.



Εικ.6.19

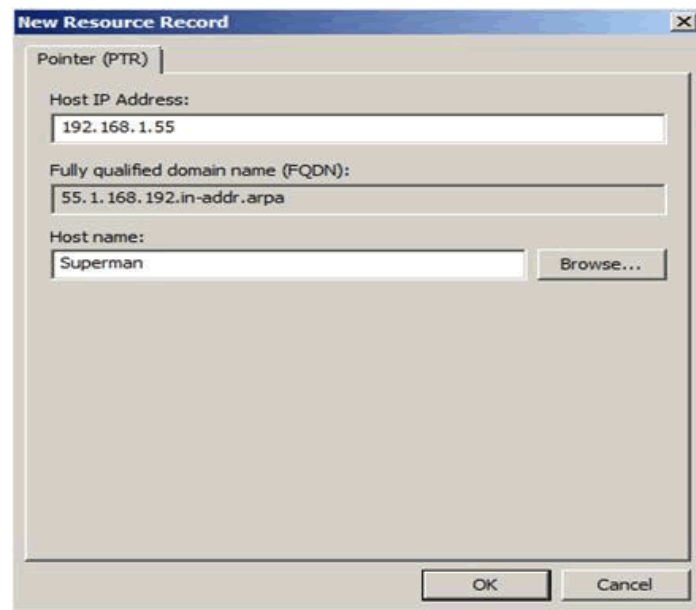
Ταυτόχρονα:

- Forward Lookup Zones -> δεξί κλικ στο domain -> New Host
- Πληκτρολόγηση ονόματος υπολογιστή (π.χ. Javelin) και μετά την IP Address
- Επιλογή Create associated pointer (PTR) record (σημ. η δημιουργία PTR είναι δυνατή μόνο όταν είναι διαθέσιμο το αντίστοιχο reverse lookup zone)
- Add Host (επανάληψη αυτών των βημάτων για κάθε υπολογιστή που πρόκειται να προστεθεί), Done

Ξεχωριστά (εκ των υστέρων):

- Reverse Lookup Zone -> δεξί κλικ στο σωστό υποδίκτυο -> New Pointer

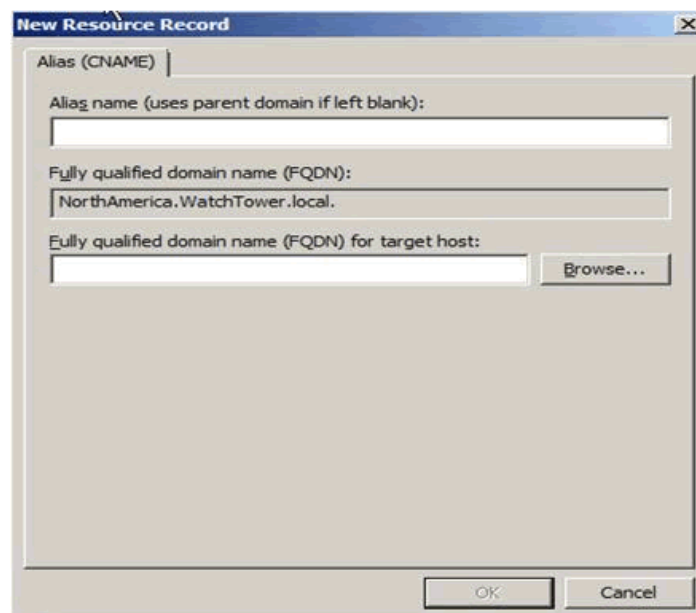
- Πληκτρολόγηση αναγνωριστικού αριθμού δικτύου του υπολογιστή (επίθεμα στο IP Address) -> Πληκτρολόγηση FQDN υπολογιστή π.χ
superman.sales.microsoft.com -> OK



Εικ.6.20

Προσθήκη CNAME Records

- Forward Lookup Zones -> δεξί κλικ στο domain -> New Alias
- Πληκτρολόγηση Ψευδωνύμου (π.χ. www) -> πληκτρολόγηση FQDN του υπολογιστή για τον οποίο δημιουργείται το ψευδώνυμο -> OK



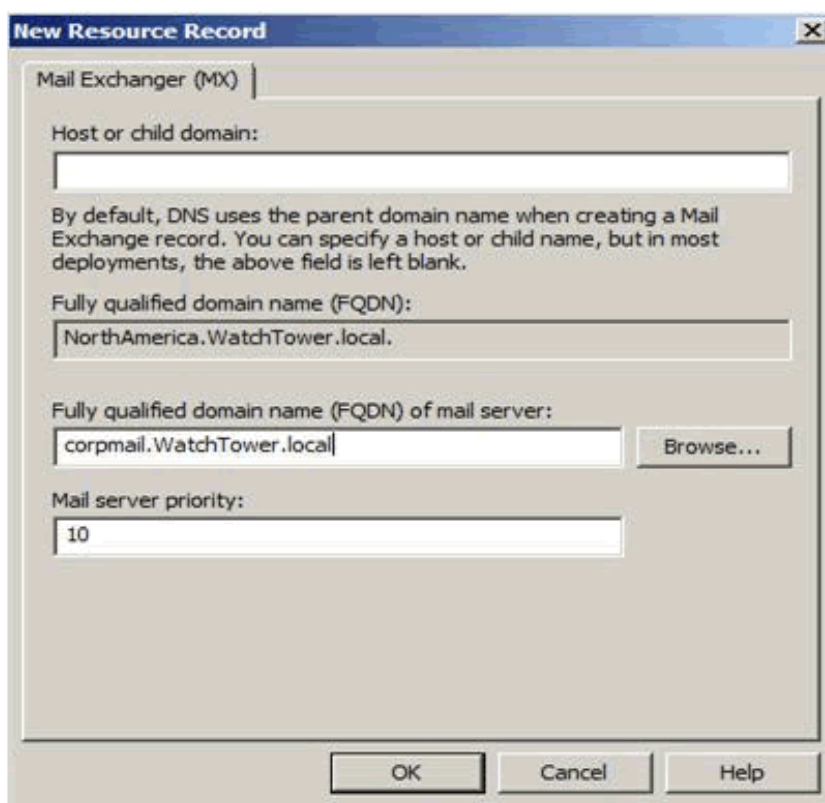
Εικ.6.21

Προσθήκη MX Records

Οι συγκεκριμένες εγγραφές προσδιορίζουν τους mail exchange servers του domain. Αυτοί οι servers ευθύνονται για τη επεξεργασία και προώθηση της αλληλογραφίας στο domain. Όταν δημιουργείται ένα MX record πρέπει να καθορίζεται ένας αριθμός προτίμησης (preference number) για το mail server ο οποίος (αριθμός) στην ουσία καθορίζει την προτεραιότητα του mail server στο domain (0 – 65535). Μικρότερο preference number σημαίνει μεγαλύτερη προτεραιότητα.

Forward Lookup Zones -> δεξί κλικ στο domain -> New Mail Exchanger

Πληκτρολόγηση του FQDN του mail server (π.χ. corpmail.microsoft.com),
πληκτρολόγηση του αριθμού προτεραιότητας (0 – 65535), OK

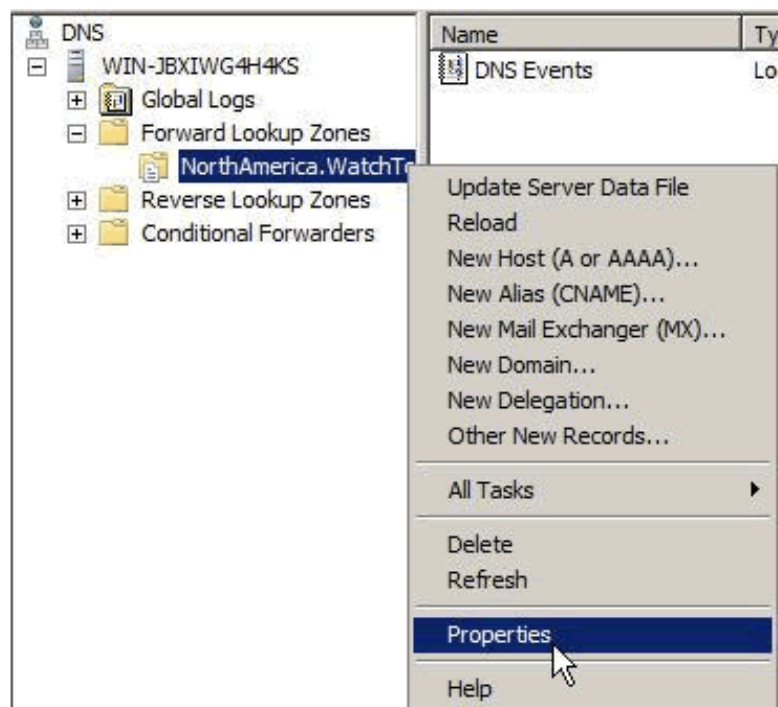


Εικ.6.22

Προσθήκη NS Records

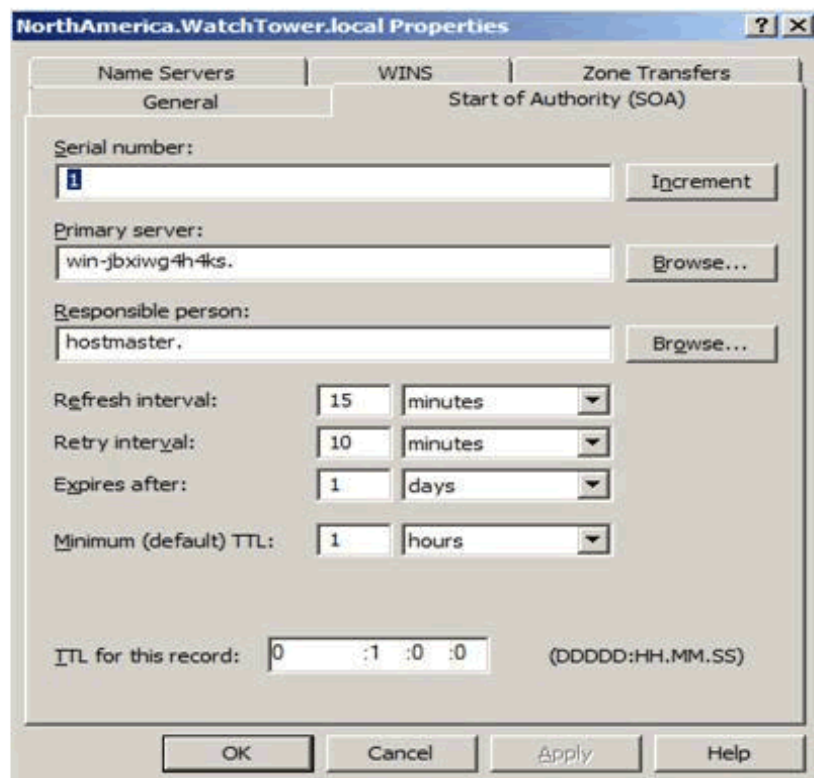
Forward Lookup Zones -> Άνοιγμα φακέλου domain -> δεξί κλικ σε name server -> Properties-> Καρτέλα Name Servers -> Add

Πληκτρολόγηση του FQDN του name server -> Πληκτρολόγηση της πρωτεύουσας IP διεύθυνσης του server -> Add (επανάληψη για πρόσθετες IP διευθύνσεις Up & Down για αλλαγή σειράς) -> OK



Εκ.6.23

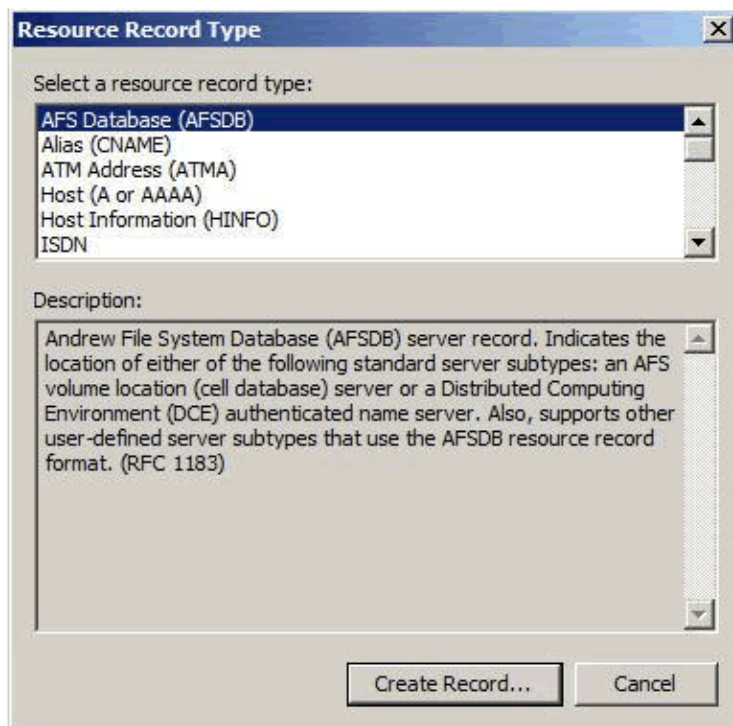
Προσθήκη SOA και υπευθύνου ατόμου



Εκ.6.24

Άλλες νέες εγγραφές

Μπορούμε να δημιουργήσουμε και πολλούς άλλους τύπους αρχείων. Για μια πλήρη περιγραφή, επιλέγουμε action -> other new records από την κονσόλα DNS. Επιλέγουμε το αρχείο της επιλογής μας και ελέγχουμε την περιγραφή.



Εικ.6.25

6.5 Active Directory & DNS

Προτείνεται στις περισσότερες των περιπτώσεων να χρησιμοποιείται η πλήρη ενοποίηση της υπηρεσίας DNS με την υπηρεσία καταλόγου Active Directory. Η αντίθετη περίπτωση είναι αυτή του μερικού συνδυασμού DNS με Active Directory η διαφορά της οποίας από την πλήρη ενοποίηση εξηγείται παρακάτω:

Μερικός Συνδυασμός

Με το μερικό συνδυασμό το domain (μιλάμε πάντα για DNS) χρησιμοποιεί τον τυπικό τρόπο αποθήκευσης των αρχείων. Οι πληροφορίες DNS αποθηκεύονται σε αρχεία κειμένου που έχουν επέκταση .dns στην προεπιλεγμένη θέση που είναι ο φάκελος %SystemRoot%\System32\DNS. Οι ενημερώσεις του DNS γίνονται από ένα μόνο εξουσιοδοτημένο server ο οποίος έχει καθοριστεί ως Primary DNS Server για το συγκεκριμένο domain ή για τμήμα του (zone). Η παραμετροποίηση των clients που χρησιμοποιούν δυναμικές ενημερώσεις DHCP πρέπει να είναι τέτοια ώστε να χρησιμοποιούν αυτόν τον server. Αν δε γίνει αυτό δε θα ενημερώνονται σ' αυτούς οι

πληροφορίες DNS.

Επίσης δε θα είναι δυνατές οι δυναμικές ενημερώσεις μέσω DHCP όταν ο Primary DNS Server είναι εκτός λειτουργίας.

Πλήρης Ενοποίηση

Χρησιμοποιώντας πλήρη ενοποίηση οι πληροφορίες του DNS αποθηκεύονται κατευθείαν στο Active Directory και είναι διαθέσιμες για τον αποδέκτη για το αντικείμενο dnsZone. Σαν μέρος του Active Directory, οι πληροφορίες DNS είναι διαθέσιμες σε κάθε domain controller χρησιμοποιώντας έτσι το DHCP για τις δυναμικές ενημερώσεις. Αυτό πρακτικά επιτρέπει, αφενός σε όποιο domain controller εκτελεί το DNS Server να χειρίζεται τις δυναμικές ενημερώσεις, αφετέρου στα clients που χρησιμοποιούν δυναμικές ενημερώσεις DNS μέσω DHCP να χρησιμοποιούν οποιοδήποτε DNS Server της ζώνης. Η πλήρης ενοποίηση πλεονεκτεί επίσης έναντι του μερικού συνδυασμού στο ότι μπορεί να χρησιμοποιηθεί η λειτουργία ασφαλείας του Active Directory για τον έλεγχο πρόσβασης στο DNS. Τέλος, μια ακόμη σημαντική διαφορά μεταξύ των δύο υλοποιήσεων (πλεονέκτημα για την πλήρη ενοποίηση) είναι ο τρόπος αναπαραγωγής των πληροφοριών DNS στο δίκτυο και η επίδρασή του στην απόκριση του δικτύου. Οι πληροφορίες αυτές, με το μερικό συνδυασμό, αποθηκεύονται και αναπαράγονται ξεχωριστά από το Active Directory. Η ύπαρξη δύο ξεχωριστών δομών μειώνει την αποτελεσματικότητα τόσο του DNS όσο και του Active Directory και κάνει τη διαχείριση πιο πολύπλοκη.

Επειδή το DNS είναι λιγότερο αποδοτικό από το Active Directory στο θέμα της αναπαραγωγής των αλλαγών, μπορεί να αυξηθεί σ' αυτή την περίπτωση το κυκλοφοριακό στο δίκτυο καθώς επίσης και ο χρόνος αντιγραφής των αλλαγών από το DNS σε όλο το δίκτυο

Δημιουργία θυγατρικών περιοχών σε ξεχωριστές ζώνες

Καθώς μεγαλώνει το δίκτυο μιας εταιρείας ή οργανισμού, ενδέχεται να παρουσιαστεί η ανάγκη οργάνωσης των DNS σε ξεχωριστές ζώνες, π.χ. στα κεντρικά της εταιρείας να υπάρχει το parent domain microsoft.com και στα υποκαταστήματα της Νέας Υόρκης, του Λος Άντζελες και της Βοστώνης να υπάρχουν τα child domains newyork.microsoft.com, la.microsoft.com και boston.microsoft.com αντίστοιχα.

Για τη δημιουργία child domain σε ξεχωριστή ζώνη ακολουθείται η παρακάτω διαδικασία:

Εγκατάσταση DNS Server σε κάθε θυγατρική περιοχή και δημιουργία των απαραίτητων forward & reverse lookup zones για τη θυγατρική περιοχή. Στον

εξουσιοδοτημένο DNS Server (authoritative) του parent domain πρέπει να γίνει πιστοποίηση εξουσιοδότησης (delegation of authority) για κάθε child domain, διαδικασία που επιτρέπει στα child domains να αναλύουν και να απαντούν σε DNS ερωτήματα από υπολογιστές μέσα και έξω από το τοπικό υποδίκτυο

Ανάπτυξη Forward Lookup Zones > δεξί κλικ στο parent domain > New Delegation > Next

Πληκτρολόγηση ονόματος child domain (π.χ. newyork) > Next Add > Πληκτρολόγηση στο πεδίο Server το FQDN του DNS Server της θυγατρικής περιοχής (π.χ. ns1.newyork.microsoft.com)

Στο πεδίο IP Address πληκτρολόγηση της πρωτεύουσας IP του server > Add (επανάληψη διαδικασίας για επιπρόσθετες IP και κουμπιά Up – Down για αλλαγή της σειράς τους). Εναλλακτικά μετά την πληκτρολόγηση του FQDN στο πεδίο ονόματος του server κάνοντας κλικ στο Resolve αναλύεται η IP και προστίθεται αυτόματα.

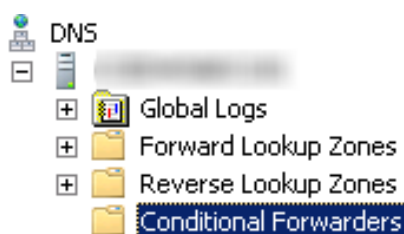
OK (επανάληψη των τριών προηγούμενων βημάτων για πρόσθετους DNS Servers)
Next, Finish

6.6 Forwarders & Conditional Forwarders

Ο Forwarder είναι ένας (συνήθως εξωτερικός) Domain Name System (DNS) εξυπηρετητής που χρησιμοποιείται για να διαβιβάσει τα ερωτήματα DNS που αφορούν τις επιλύσεις εξωτερικών ονομάτων DNS σε διακομιστές DNS εκτός του εν λόγω δικτύου.

Εισαγωγή από την γραμμή εντολών

```
dnscmd <ServerName> /ResetForwarders <MasterIPAddress ...> [/TimeOut <Time>]
[/Slave]
```

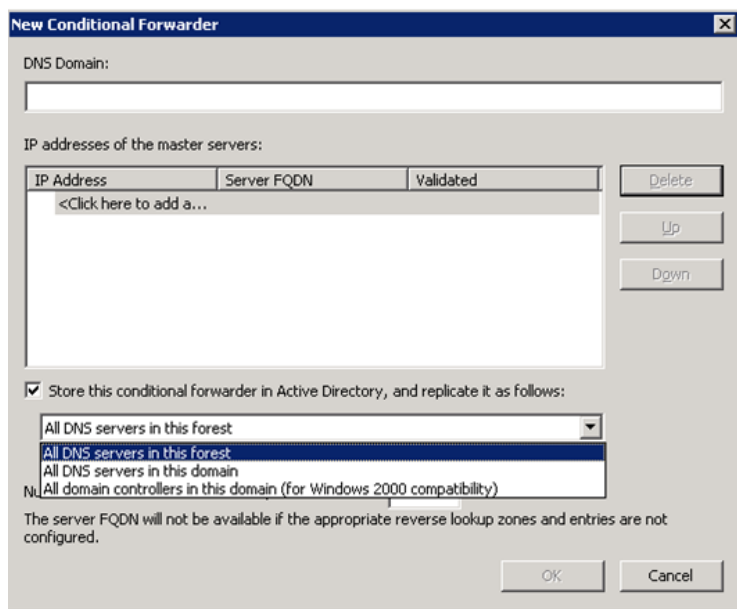


Εικ.6.26

Ενώ από την κονσόλα ανοίγουμε τον DNS Manager κάνουμε κλικ στον αντίστοιχο DNS Server κλικ properties κλικ την καρτέλα forwarders και εκεί προσθέτουμε τον forwarder

Μπορούμε επίσης να ρυθμίσουμε τον εξυπηρετητή μας να διαβιβάζει ερωτήματα, ανάλογα με τα ονόματα τομέα σε διαφορετικούς Forwarder. Αυτοί ονομάζονται conditional forwarders

Και η δημιουργία ενός καινούργιου conditional forwarder με βάση το όνομα τομέα



Εικ.6.27

Ενώ από την γραμμή εντολών `dnscmd <ServerName> /ResetForwarders <MasterIPAddress ...> [/TimeOut <Time>] [/Slave]`

6.7 GlobalNames Zone (GNZ)

Πριν από την έλευση του windows 2008 πολλοί οργανισμοί χρησιμοποιούσαν την υπηρεσία WINS για εναλλακτική επίλυση (netbios NetBT) ονομάτων στο δίκτυο. Με την έλευση του IPv6 το WINS και το NetBT δεν μπορούν να χρησιμοποιηθούν γιατί δεν το υποστηρίζουν. Για την απόσυρση αυτών των παλαιών πρωτοκόλλων και για να περάσει όλη η επίλυση ονομάτων στους DNS servers ο DNS Server role σε ένα Windows Server 2008 υποστηρίζει μια ειδική ζώνη την GlobalNames Zone (GNZ). Αυτή η ζώνη μπορεί να περιέχει στατικά ονόματα (static, single-label names) εξυπηρετητών τα οποία μέχρι τώρα υπήρχαν στη βάση του WINS. Το GNZ είναι δεν αντικαταστάτης του WINS αλλά χρησιμοποιείται για την μετάβαση από το WINS στο DNS γιατί δεν υποστηρίζει δυναμικές εγγραφές.

LLMNR -Τα νέο λειτουργικά συστήματα της Microsoft όπως τα Windows Vista και Windows Server 2008 μπορούν να χρησιμοποιήσει μια νέα μέθοδο επίλυσης ονομάτων που ονομάζεται "Link-Local Multicast Name Resolution" (LLMNR),

γνωστό και ως DNS multicast ή mDNS, για την επίλυση ονομάτων σε ένα τοπικό τμήμα δικτύου, όταν ένας εξυπηρετητής DNS δεν είναι διαθέσιμος. Για παράδειγμα, εάν ένας δρομολογητής αποτύχει, και ένα υποδίκτυο αποκοπεί από όλους τους εξυπηρετητές DNS του δικτύου, οι πελάτες για το δευτερεύον δίκτυο που υποστηρίζει LLMNR μπορούν να συνεχίσουν να επιλύουν ονόματα peer-to-peer μέχρι η σύνδεση με το δίκτυο αποκατασταθεί.

Για να ενεργοποιήσουμε το GNZ κλικ το Start, δεξί κλικ Command Prompt, και μετά κλικ το Run as Administrator.

γράφουμε: `Dnscmd ServerName /config /Enableglobalnamesupport 1`

Μετά φτιάχνουμε μια καινούργια ζώνη που θα γίνεται replicated σε όλους τους ελεγκτές τομέα στο forest δίνοντας της το όνομα GlobalNames.

Για να προσθέσουμε εγγραφές στην ζώνη επιλεγούμε να προσθέσουμε New Alias (CNAME).

ACTIVE DIRECTORY USERS AND COMPUTERS

7.1 Active Directory Users and Computers console

Η κονσόλα Active Directory Users and Computers είναι το κύριο εργαλείο για τη διαχείριση χρηστών, ομάδων, υπολογιστών και άλλων αντικείμενων της υπηρεσία καταλόγου Active Directory. Τα αντικείμενα του Active Directory περιέχουν τις απαραίτητες πληροφορίες περιλαμβάνοντας περιγραφές, δικαιώματα file system, security identifiers κ.α.

Η κονσόλα Active Directory Users and Computers μας επιτρέπει να δημιουργήσουμε, να τροποποιήσουμε και να διαγράψουμε αντικείμενα του καταλόγου. Τα αντικείμενα στο Active Directory συνήθως ομαδοποιούνται και φιλοξενούνται μέσα σε ομάδες που καλούνται οργανωτικές μονάδες -organizational Units (OU) οι οποίες, με τη σειρά τους, μπορεί να φιλοξενήσουν επιπλέον οργανωτικές μονάδες. Ως εκ τούτου, ο κατάλογος του Active Directory έχει δενδροειδή δομή.

7.1.1 Δυνατότητες του Active Directory Users and Computers

Συχνά, οι οργανισμοί δημιουργούν Active Directory οργανωτικές μονάδες (OU) που αντικατοπτρίζουν τις οργανικές δομές τους. Για παράδειγμα, ένας οργανισμός μπορεί να έχει ξεχωριστές οργανωτικές μονάδες όπως διοίκησης, πωλήσεων και τεχνικής υποστήριξης με διαφορετικές πολιτικές για τη καθεμιά από αυτές. Σε άλλες περιπτώσεις οι οργανωτικές μονάδες (OU) αντικατοπτρίζουν την θέση του οργανισμού και των υποκαταστημάτων του π.χ. Αθήνα, Θεσσαλονίκη, Ιωάννινα, Ηράκλειο. Με αυτόν τον τρόπο δίνεται η δυνατότητα να δημιουργηθούν δομές που εξυπηρετούν τον οργανισμό και μέσω αυτών να μεταβιβαστούν διαχειριστικά δικαιώματα (delegate administration) εκεί που πρέπει και πάντα με ασφάλεια.

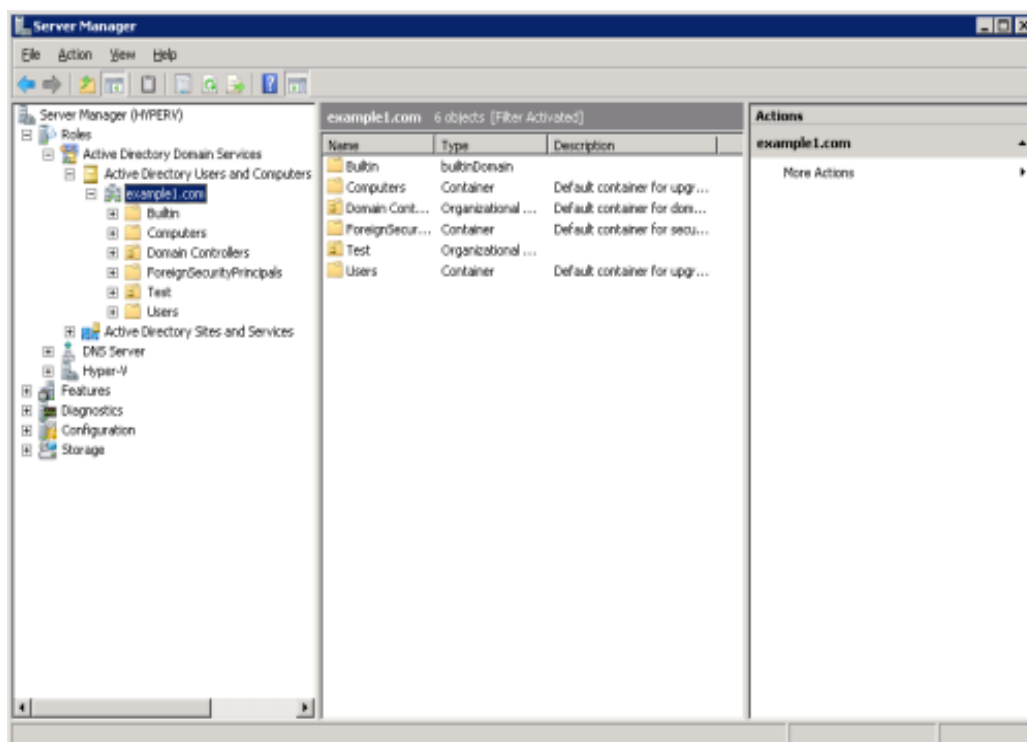
Μερικές από τις συνήθεις εργασίες που επιτυγχάνονται με την κονσόλα του Active Directory Users and Computers περιλαμβάνουν:

- Τη προσθήκη νέων χρηστών στο Active Directory
- Την αλλαγή κωδικών πρόσβασης
- Τη χορήγηση δικαιωμάτων πρόσβασης σε κοινόχρηστους φακέλους
- Τον έλεγχο της απομακρυσμένης πρόσβασης στο δίκτυο
- Τις ρυθμίσεις σύνδεσης, αποσύνδεσης και εκτέλεσης των scripts
- Την πρόσβαση των χρηστών στο δίκτυο
- Δημιουργία ομάδων ασφαλείας -security groups
- Τη διαχείριση του τομέα

- Τη διαχείριση των οργανωτικών μονάδων

Πολλές εφαρμογές, συμπεριλαμβανομένων των, Exchange Server, Terminal Services και System Center προσθέτουν νέες δυνατότητες στο Active Directory. Μερικές φορές, οι εφαρμογές αυτές προσθέτουν επεκτάσεις στο Active Directory Users and Computers για να είναι δυνατή η διαχείριση των αντικειμένων που σχετίζονται με αυτές. Για παράδειγμα, αν προσθέσουμε την υπηρεσία Terminal Services στο δίκτυό μας, μπορούμε να χρησιμοποιήσουμε το Active Directory Users and Computers για να ελέγξουμε τον χρόνο που ο χρήστης μπορεί να παραμείνει συνδεδεμένος στον Terminal Server.

Σε σχέση με τα windows 2000 και 2003 η κονσόλα Active Directory Users and Computers έχει υποστεί κάποια βελτίωση. Επιπλέον στα Windows Server 2008, θα βρούμε μερικά νέα αντικείμενα καθώς και τις ιδιότητες τους, αντικείμενα που δεν ήταν διαθέσιμα σε παλαιότερες εκδόσεις του Windows Server.



Εικ.7.1

Πιο συγκεκριμένα, η Microsoft έχει προσθέσει μια καρτέλα Attribute Editor για κάθε αντικείμενο που επιτρέπει στους διαχειριστές με εύκολο τρόπο να αλλάξουν γρήγορα την τιμή των χαρακτηριστικών γνωρισμάτων κάθε Active Directory αντικειμένου.

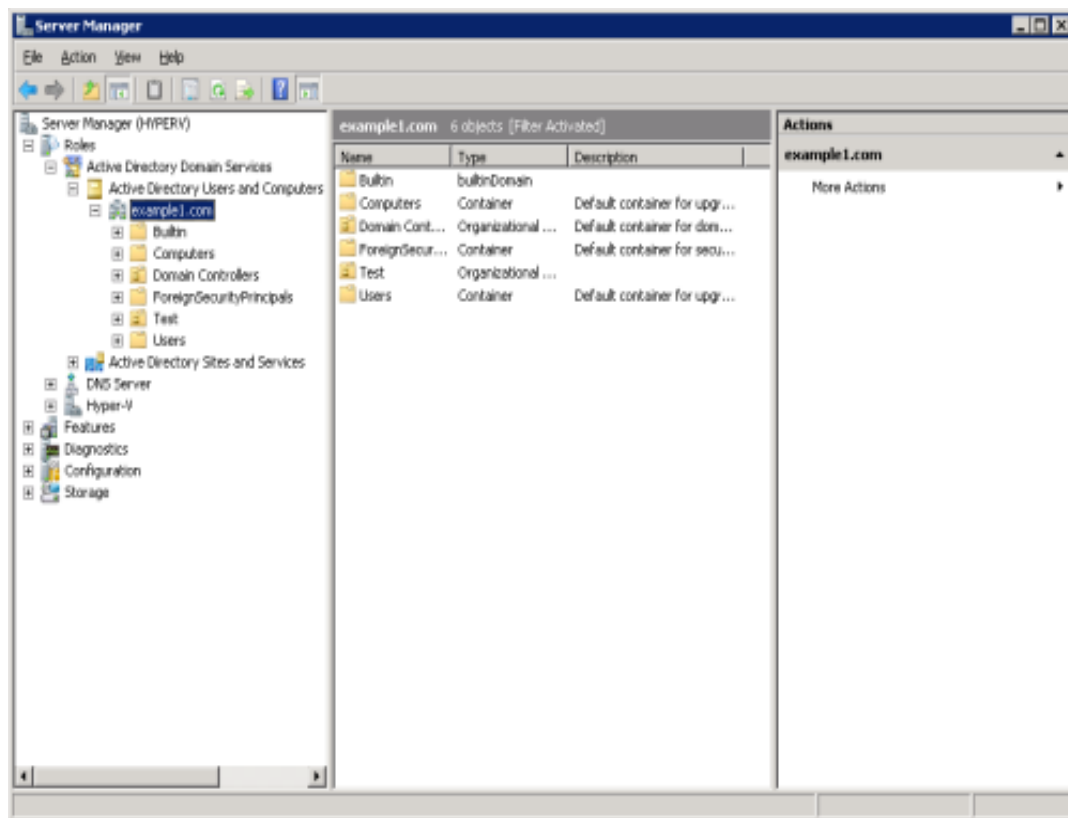
Υπάρχουν πολλοί τρόποι για να χρησιμοποιήσουμε τις δυνατότητες του Active Directory Users and Computers του Windows Server 2008. Ανεξάρτητα από τη μέθοδο που θα χρησιμοποιήσουμε, θα πρέπει να συνδεθούμε στο εξυπηρετητή ως

χρήστης με δικαιώματα διαχειριστή είτε απομακρυσμένα ή από το μηχάνημα (interactively).

7.1.2 Πρόσβαση στο Active Directory Users and Computers

Κατ' αρχήν, μπορούμε να χρησιμοποιήσουμε το νέο εργαλείο Server Manager | Roles | Active Directory Domain Services | Active Directory Users and Computers.

Η δεύτερη μέθοδος πρόσβασης στο Active Directory Users and Computers είναι να εκτελέσουμε το Active Directory Users and Computers όπως σε προηγούμενες εκδόσεις των Windows. Κάνουμε κλικ στο κουμπί Start | All Programs | Administrative Tools | Active Directory Users and Computers.



Εικ.7.2

Εμφανίζεται μια κονσόλα διαχείρισης Microsoft Management Console (MMC). Στην πάνω γραμμή του παραθύρου υπάρχει μια γραμμή μενού με τα -FILE-ACTION-VIEW-HELP. Κάτω από τη γραμμή μενού είναι μία γραμμή κουμπιών που παρέχει γρήγορη πρόσβαση σε συχνά χρησιμοποιούμενες διαδικασίες. Τέλος, θα δούμε δύο παράθυρα. Στο αριστερό τμήμα του παράθυρου παρέχει μια προβολή δέντρου της δομής του Active Directory. Η δεξιά πλευρά δείχνει τα αντικείμενα για τους επιλεγμένους υποδοχείς -containers του αριστερού παράθυρου.

7.1.3 Επιλογές του Μενού

FILE: Στο μενού File βρίσκεται το μενού Options, το οποίο μας επιτρέπει να καθορίσουμε τις πληροφορίες της κονσόλας MMC. Μπορούμε επίσης να κλείσουμε το Active Directory Users and Computers κάνοντας κλικ στο κουμπί Έξοδος.

ACTION: Το μενού αυτό μας επιτρέπει να εκτελέσουμε διάφορες ενέργειες ανάλογα με το ποιο αντικείμενο ή υποδοχέα- container έχουμε επιλέξει. Για παράδειγμα, αν επιλέξαμε τον υποδοχέα χρήστες-Users, μπορούμε να δούμε το Delegate Control μενού, όπως και επιλογές που μας επιτρέπουν να δημιουργήσουμε νέους χρήστες και ομάδες αλλά αν επιλέξουμε ένα συγκεκριμένο αντικείμενο χρήστη θα δούμε τι μπορούμε να κάνουμε για να χρήστη, όπως η επαναφορά κωδικών πρόσβασης και η απενεργοποίηση λογαριασμών. Όταν το αντικείμενο που είναι επιλεγμένο είναι ο τομέας-Domain αυτό το μενού περιέχει επιλογές για raise the domain functional level αλλά και τροποποίησης των διακομιστών που είναι-PDC emulator και του κύριου σχήματος -schema master.

VIEW: Αυτή η επιλογή μενού μας επιτρέπει να προσαρμόσουμε την εμφάνιση του Active Directory Users and Computers. Μπορούμε να αλλάξουμε τον τρόπο που τα αντικείμενα φαίνονται και να φιλτράρουμε τα αντικείμενα που δεν θέλουμε να εμφανίζονται.

Window: Αυτή η επιλογή μενού μας επιτρέπει να εμφανίζουμε πολλά MMC παράθυρα και να ελέγχουμε πώς αυτά τα παράθυρα θα εμφανίζονται.

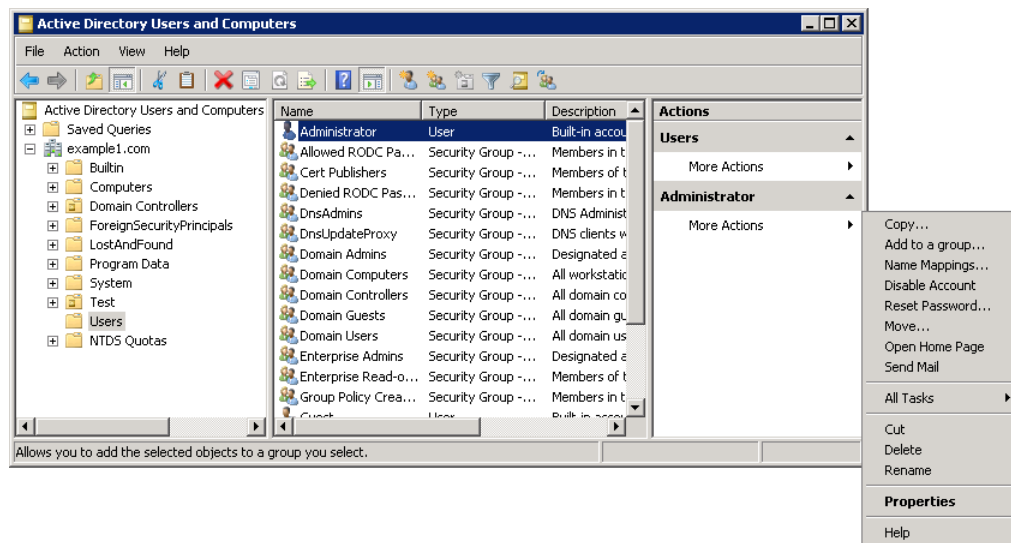
HELP: Αυτή η επιλογή μας επιτρέπει να έχουμε πρόσβαση στα αρχεία βοήθειας του Active Directory Users and Computers.

7.1.4 Τα κουμπιά πλοήγησης-button bar

Το Active Directory Users and Computers είναι μια MMC κονσόλα. Αριστερά προς τα δεξιά βρίσκουμε τα κουμπιά:

- Back to previous selection: Πίσω στην προηγούμενη επιλογή
- Forward to next selection (if you previously used Back): Προς τα εμπρός στην επόμενη επιλογή
- Move up one level in the Active Directory hierarchy: Μετακινηθείτε στο αμέσως ανώτερο επίπεδο στην ιεραρχία του Active Directory
- Show/Hide console tree: Εμφάνιση / Απόκρυψη κονσόλας
- Paste: Επικόλληση
- Get properties for current object: Ιδιότητες στο τρέχον αντικείμενο

- Refresh: Ανανέωση
- Export List: Κατάλογος εξαγωγής
- Help: Βοήθεια
- Show/Hide action pane: Εμφάνιση / Απόκρυψη περιοχής παραθύρου
- Create a new user object in the current container: Δημιουργήστε ένα νέο αντικείμενο χρήστη στο τρέχοντα υποδοχέα
- Create a new group in the current container: Δημιουργήστε μια νέα ομάδα στο τρέχοντα υποδοχέα
- Create a new organizational unit in the current container: Δημιουργήστε μια νέα οργανωτική μονάδα στο τρέχοντα υποδοχέα
- Create a filter to see only specific types of objects: Δημιουργήστε ένα φίλτρο για να δείτε μόνο συγκεκριμένους τύπους αντικειμένων
- Find objects: Εύρεση αντικειμένων
- Add selected objects to a group: Προσθήκη επιλεγμένων αντικειμένων σε μια ομάδα



Εικ.7.3

Θα παρατηρήσουμε ότι καθώς πηγαίνουμε από υποδοχέα σε υποδοχέα στο αριστερό παράθυρο, νέα κουμπιά ανάλογα με την περίσταση θα καταστούν διαθέσιμα. Για παράδειγμα, αν πάμε στον υποδοχέα υπολογιστές, δεν μπορούμε να χρησιμοποιήσουμε τη Δημιουργία Νέας οργανωτικής μονάδας.

Στο πιο κάτω σχήμα, ο χρήστης αντικείμενο που ονομάζεται Administrator είναι επιλεγμένος. Στο παράθυρο δεξιά, Δράση-Action υπάρχουν δύο More Actions ενέργειες. Η μια είναι κάτω από την επικεφαλίδα Χρήστες-Users και παρέχει

σύντομη πρόσβαση στις ίδιες επιλογές που θα ήταν διαθέσιμες εάν κάναμε δεξί κλικ στον υποδοχέα χρήστες. Ομοίως, κάτω από το Διαχειριστή, |Administrator το κουμπί Περισσότερες Ενέργειες -More Actions παρέχει γρήγορη πρόσβαση στις επιλογές που θα ήταν διαθέσιμες, αν επρόκειτο να κάνουμε δεξί κλικ στο χρήστη Administrator. Δηλαδή το Action Pane παρέχει γρήγορη πρόσβαση στις λειτουργίες που είναι διαθέσιμες σε ένα αντικείμενο αφού προηγουμένως βεβαιωθούμε ότι έχουμε επιλέξει το Advanced view, το οποίο μας δίνει περισσότερες πληροφορίες.

Για να ενεργοποιήσουμε το Advanced mode, επιλέγουμε View | Advanced Features.

7.1.5 To Console Tree

Το αριστερό τμήμα της κονσόλας ονομάζεται Console Tree. Από αυτή τη δομή δέντρου εμφανίζονται όλα τα αντικείμενα του υποδοχέα για το Active Directory. Μπορούμε να προηγηθούμε στο Console Tree κάνοντας κλικ στο σήμα συν (+) να αναπτύξουμε τις διάφορες επιλογές / υποδοχές. Τα default αντικείμενα που θα βρούμε στο Console Tree των Windows Server 2008 είναι τα εξής:

- **Saved Queries Αποθηκευμένες Αναζητήσεις:** Μας επιτρέπει να αποθηκεύσουμε τα ερωτήματα που εκτελούν αναζητήσεις για ομάδες αντικειμένων. Οι αποθηκευμένες αναζητήσεις θα μας δώσουν έναν τρόπο να έχουμε γρήγορη πρόσβαση σε αντικείμενα που χρησιμοποιούμε σε τακτική βάση.
- **Domain:** Το όνομα του Active Directory domain μας εμφανίζεται εδώ. Αυτό το αντικείμενο είναι ο κύριος υποδοχέας κοντέινερ; για το Active Directory και περιέχει όλους τους άλλους υποδοχείς και τις οργανωτικές μονάδες.
- **Builtin:** Περιέχει όλες τις προεγκατεστημένες ομάδες ασφαλείας που έρχονται με τον Windows Server 2008, οι οποίες περιγράφονται παρακάτω:
 - Account Operators: Τα μέλη μπορούν να διαχειρίζονται χρήστες του τομέα και ομάδες
 - Administrators: Οι διαχειριστές έχουν πλήρη και απεριόριστη πρόσβαση στον τομέα και στους υπολογιστές του τομέα
 - Backup Operators: Οι Backup Operators μπορεί να παρακάμψουν τους περιορισμούς ασφαλείας με μοναδικό σκοπό την δημιουργία αντιγράφων ασφαλείας ή την αποκατάσταση των αρχείων
 - Certificate Service DCOM Access: Μέλη αυτής της ομάδας μπορούν να συνδεθούν με τις Αρχές Πιστοποίησης του τομέα -domain/enterprise

- Cryptographic Operators: Τα μέλη επιτρέπεται να εκτελούν κρυπτογραφικές διαδικασίες.
- Distributed COM Users: Τα μέλη έχουν τη δυνατότητα να ξεκινήσουν, να ενεργοποιήσουν και να χρησιμοποιήσουν Distributed COM αντικείμενα σε αυτό το μηχάνημα.
- Event Log Readers: Τα μέλη αυτής της ομάδας μπορούν να διαβάσουν αρχεία καταγραφής συμβάντων από το τοπικό μηχάνημα
- Guests: Οι επισκέπτες έχουν την ίδια πρόσβαση με τα μέλη της ομάδας Users από προεπιλογή, εκτός από το λογαριασμό Guest που είναι ακόμη πιο περιορισμένος
- IIS_IUSRS: Built-in ομάδα που χρησιμοποιείται από τις υπηρεσίες Internet Information Services.
- Incoming Forest Trust Builders: Μέλη αυτής της ομάδας μπορεί να δημιουργήσουν σχέσεις one-way trust στο forest
- Network Configuration Operators: Μέλη αυτής της ομάδας μπορούν να έχουν ορισμένα δικαιώματα διαχειριστή για να διαχειριστούν δικτυακές παραμέτρους
- Performance Log Users: Μέλη αυτής της ομάδας μπορούν να προγραμματίσουν την καταγραφή μετρητών επιδόσεων και να επιτρέψουν την συλλογή event traces, τόσο τοπικά όσο και μέσω απομακρυσμένης πρόσβασης σε κάποιον υπολογιστή
- Performance Monitor Users: Μέλη της ομάδας αυτής μπορούν να έχουν πρόσβαση σε δεδομένα μετρητών επιδόσεων τοπικά και απομακρυσμένα
- Pre-Windows 2000 Compatible Access: Μια ομάδας συμβατότητας με τα windows 2000 που επιτρέπουν read πρόσβαση σε όλους τους χρήστες και τις ομάδες στον τομέα
- Print Operators: Τα μέλη της μπορούν να διαχειριστούν εκτυπωτές του τομέα
- Remote Desktop Users: Τα μέλη αυτής της ομάδας έχουν το δικαίωμα να συνδεθούν εξ αποστάσεως στον υπολογιστή
- Replicator: Υποστηρίζει αναπαραγωγή-αντιγραφή αρχείων σε έναν τομέα
- Server Operators: Τα μέλη μπορούν να διαχειρίζονται domain servers

- Terminal Server License Servers: Μέλη αυτής της ομάδας μπορούν να ενημερώνουν τους λογαριασμούς χρήστη στο Active Directory με πληροφορίες αδειοδότησης, για σκοπούς παρακολούθησης και υποβολής εκθέσεων ανά (Computer Access Licence) χρήστη
 - Users: Στους χρήστες δεν δίνεται δυνατότητα αλλαγών στο σύστημα είτε από λάθος ή εσκεμμένα. Συνήθως μπορούν να εκτελέσουν τις περισσότερες εφαρμογές
 - Windows Authorization Access Group: Μέλη αυτής της ομάδας έχουν πρόσβαση στο tokenGroupsGlobalAndUniversal χαρακτηριστικό-attribute για το αντικείμενο User
- **Computers:** Περιέχει όλους τους σταθμούς εργασίας και τους εξυπηρετητές που είναι μέλη στο Active Directory. Εδώ είναι το default σημείο που θα εμφανίζονται οι νέοι υπολογιστές που θα προστίθενται στο domain.
 - **Domain Controllers:** Περιέχει όλους τους ελεγκτές τομέα που χρησιμοποιούνται στο Active Directory domain μας.
 - **ForeignSecurityPrincipals:** Διαθέτει τα αναγνωριστικά ασφαλείας -security identifiers που σχετίζονται με αντικείμενα από εξωτερικούς, αξιόπιστους τομείς.
 - **LostAndFound:** Εδώ βρίσκονται τα αντικείμενα που θα έπρεπε να αναπαραχθούν-replicate στον κατάλογο, αλλά δεν μπόρεσαν για κάποιο λόγο. Ακόμα τα αντικείμενα που θα εμφανιστούν εδώ, συνήθως δημιουργήθηκαν ταυτόχρονα στον υποδοχέα που τα περιείχε ο οποίος και διαγράφηκε. Αυτό θα συμβεί μόνο όταν υπάρχουν πολλοί διαχειριστές δικτύου που εργάζονται ταυτόχρονα στο Active Directory.
 - **Program Data:** Περιέχει πληροφορίες για αντικείμενα σχετικές με εφαρμογές δικτυακές, ειδικότερα δεδομένων που αποθηκεύονται απευθείας στο Active Directory.

- **System:** Περιέχει επιπλέον υποδοχείς που αποθηκεύουν πληροφορίες συστήματος για το Active Directory, όπως πολιτικές ομάδας, DNS, IPSec, και DFS διαμορφώσεις.
- **Users:** Αυτό είναι το προεπιλεγμένο κοντέινερ-υποδοχέας για Active Directory χρήστες.
- **NTDS Quotas:** Αποθηκεύει αντικείμενα Quota –ποσόστωσης, η οποία περιορίζει τον αριθμό των αντικειμένων που ένας χρήστης μπορεί να δημιουργήσει σε έναν υποδοχέα.
- **Additional organizational units:** Η ιεραρχία του Active Directory μπορεί να διαμορφωθεί έτσι ώστε να ομοιάζει αυτήν της οργανωτική δομή μας. Δεν είναι απαραίτητο τα αντικείμενα users να υπάρχουν μόνο στον υποδοχέα Users. Μπορούμε να δημιουργήσουμε υποδοχείς για κάθε αντικείμενο και για κάθε δομή που θέλουμε.

7.2 Active Directory objects

Σε κάθε υποδοχέα υπάρχουν Active Directory αντικείμενα, τα οποία αντιπροσωπεύουν κάθε πόρο που έχει προστεθεί στην υπηρεσία καταλόγου Active Directory. Εάν περιηγηθούμε στους υποδοχείς που αναφέρθηκαν παραπάνω, θα δούμε τα αντικείμενα να εμφανίζονται στο δεξιό τμήμα του παραθύρου.

Η Microsoft έχει δώσει στα αντικείμενα συναφή ονόματα. Συνήθως, μπορούμε να μαντέψουμε γρήγορα την χρήση ενός αντικείμενο από το όνομά του. Για παράδειγμα, το DHCP Users αντικείμενο είναι μια ομάδα που περιέχει τα μέλη που έχουν πρόσβαση read only σε DHCP εξυπηρετητές.

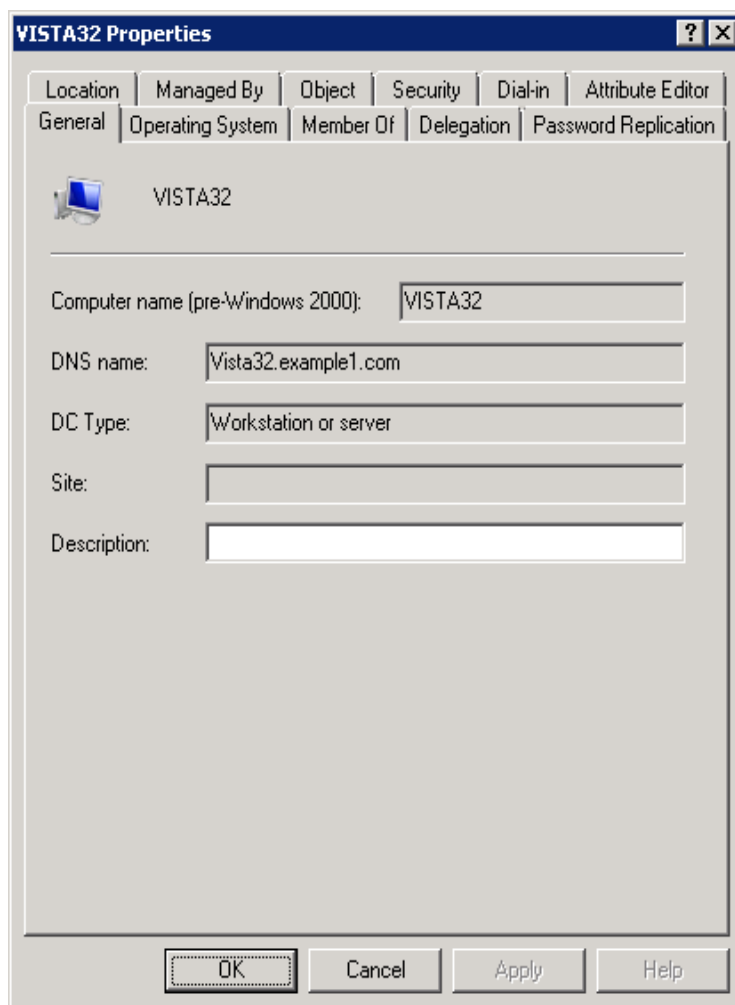
Κάθε αντικείμενο αποτελείται από μια ομάδα ιδιοτήτων που περιγράφουν το αντικείμενο αλλά και το τι μπορεί να κάνει. Μπορούμε να προβάλουμε τις ιδιότητες για ένα αντικείμενο, κάνοντας δεξί κλικ στο αντικείμενο και επιλέγοντας Properties.

Ιδιότητες κυριότερων αντικειμένων

7.2.1 Computer Objects:

- Το Computer Objects περιγράφει υπολογιστές που έχουν δικαιώματα πρόσβασης στο δίκτυο. Μπορεί να περιγράψει ελεγκτές τομέα, εξυπηρετητές που ανήκουν στον τομέα ή σταθμούς εργασίας. Θα βρούμε τους ελεγκτές τομέα μέσα στο υποδοχέα Domain Controllers. Οι εξυπηρετητές που ανήκουν στον τομέα και οι

σταθμοί εργασίας εμφανίζονται στο κοντέινερ Computers. Όταν κάνουμε δεξί κλικ σε ένα αντικείμενο Computer και επιλέξουμε Properties, θα δείτε στην οθόνη αυτό που φαίνεται στο σχήμα.



Εικ.7.4

Η σελίδα Properties του υπολογιστή που ονομάζεται VISTA32.

- **Properties** Η σελίδα περιλαμβάνει τις καρτέλες:
 - **General:** Η καρτέλα αυτή παρέχει βασικές πληροφορίες σχετικά με το αντικείμενο, συμπεριλαμβανομένων τόσο του NetBIOS ονόματος, του ονόματος DNS, του τύπου, Active Directory site και την περιγραφή.
 - **Operating System:** Η καρτέλα αυτή εμφανίζει το λειτουργικό σύστημα που τρέχει στον υπολογιστή και τι Service Pack υπάρχουν.
 - **Member Of:** Εδώ, προβάλλονται οι ιδιότητες μέλους ομάδας του υπολογιστή και οι αναγκαίες προσαρμογές. Από προεπιλογή, όλοι οι νέοι υπολογιστές προστίθεται στην ομάδα με το όνομα Domain Computers.

- **Delegation:** Σε παλαιότερες εκδόσεις του Windows Server, τα στοιχεία αυτά βρίσκονται στην καρτέλα General. Θα πρέπει να επιλεγεί ένα από τα trust options, αν θέλουμε ο υπολογιστής να είναι σε θέση να ζητήσει υπηρεσίες από έναν άλλο υπολογιστή.
- **Password Replication:** Η καρτέλα διατηρεί μια λίστα read only ελεγκτών τομέα που αποθηκεύουν προσωρινές (cached) εκδόσεις του καταλόγου.
- **Location:** Εδώ εισάγονται τα στοιχεία που περιγράφουν φυσική τοποθεσία του υπολογιστή.
- **Managed By:** Παροχή πληροφοριών σχετικά με τα πρόσωπα που είναι υπεύθυνα για την διαχείριση του υπολογιστή απευθείας από το Active Directory.
- **Object:** Αυτή η καρτέλα εμφανίζει πληροφορίες σχετικά με το αντικείμενο, συμπεριλαμβανομένου του ονόματος του, πότε δημιουργήθηκε, πότε ενημερώθηκε για τελευταία φορά, και τα Update Sequence Numbers. Σε αυτή την καρτέλα, μπορούμε επίσης να αναφέρουμε ότι το αντικείμενο θα πρέπει να προστατεύεται από μια τυχαία διαγραφή.
- **Security:** Η καρτέλα αυτή ελέγχει τα Active Directory δικαιώματα των άλλων αντικειμένων που έχουν σε αυτό το αντικείμενο. Το Group ή user names πλαίσιο απαριθμεί τα αντικείμενα με δικαιώματα και το Permissions πλαίσιο περιγράφει τα δικαιώματα που έχουν χορηγηθεί ή απορριφθεί στον επιλεγμένου χρήστη ή στην ομάδα.
- **Dial-in:** Επιλεγούμε εάν οι χρήστες μπορούν να αποκτήσουν απομακρυσμένη πρόσβαση στον υπολογιστή, είτε με dial-up ή VPN. Μπορείτε επίσης να ορίσουμε τις επιλογές επιστροφής κλήσης για επιπλέον ασφάλεια.
- **Attribute Editor** (νέα καρτέλα στο Windows Server 2008): Στον Windows Server 2008, η Microsoft έχει δανειστεί αυτήν την λειτουργία από το βοηθητικό πρόγραμμα ADSI Edit και πρόσθεσε αυτή την καρτέλα, η οποία μας επιτρέπει να χειριστούμε άμεσα το σύνολο των ιδιοτήτων που σχετίζονται με το επιλεγμένο αντικείμενο.

7.2.2 Group Objects

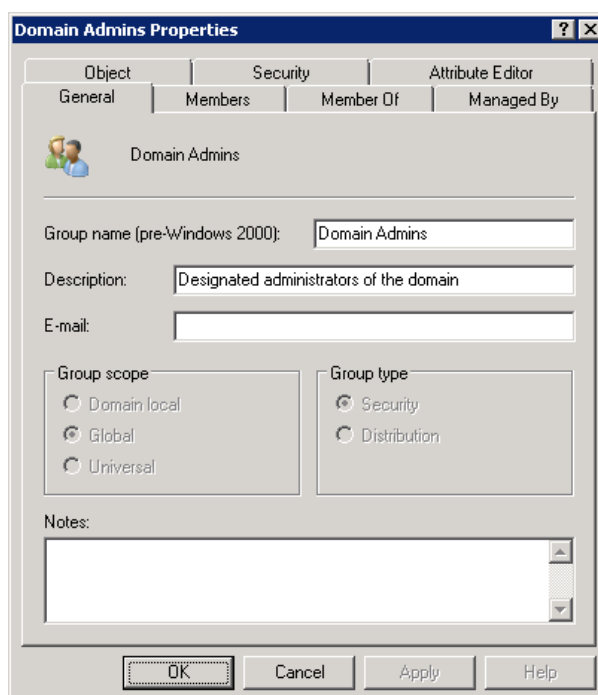
Υπάρχουν δυο είδη αντικειμένων Group-ομάδας που μπορεί να δημιουργηθούν στο Active Directory. Το πρώτο είδος, το security group, παρέχει έναν τρόπο να διαχειρίζονται τα δικαιώματα πρόσβασης για πολλούς χρήστες (ή για άλλα αντικείμενα), ομαδικά. Αντί να εκχωρήσουμε διαφορετικά δικαιώματα πρόσβασης σε ένα κοινόχρηστο αρχείο, για παράδειγμα, μπορούμε να δώσουμε δικαιώματα στην

ομάδα ασφαλείας και στη συνέχεια να προσθέσουμε ή και να αφαιρέσουμε τα μέλη της ομάδας, ανάλογα, όπως απαιτείται. Τα Security groups μπορούν επίσης να χρησιμοποιηθούν και ως ομάδες διανομής ηλεκτρονικού ταχυδρομείου.

Το δεύτερο είδος της ομάδας, που ονομάζεται ομάδα διανομής distribution group, χρησιμοποιείται αποκλειστικά και μόνο ως μια λίστα διανομής ηλεκτρονικού ταχυδρομείου.

Ομάδες ασφαλείας.

Αν κάνουμε δεξί κλικ σε ένα αντικείμενο ομάδας, θα δείτε την παρακάτω εικόνα.



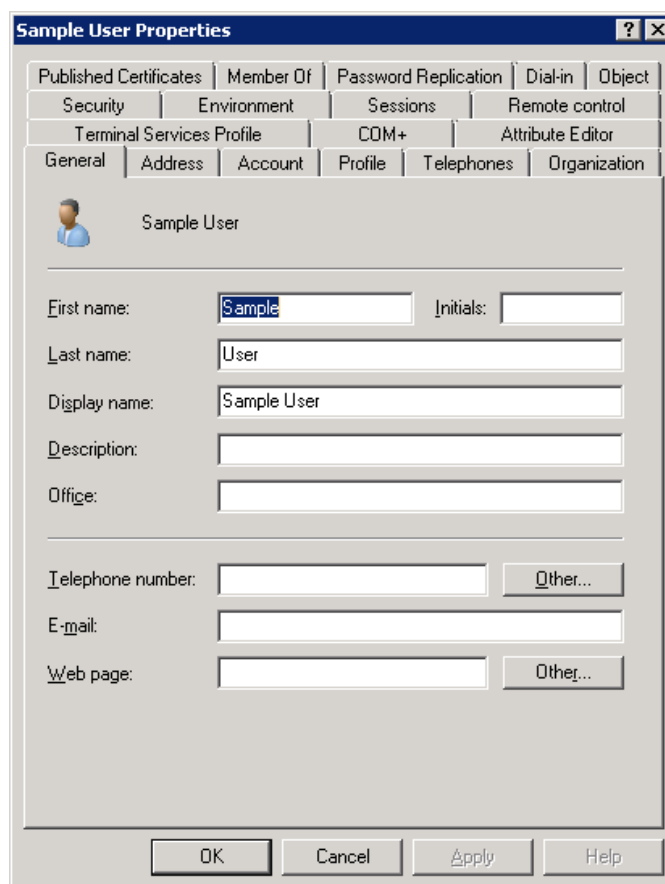
Εικ.7.5

Η σελίδα ιδιοτήτων για την ομάδα Domain Admins.

Οι Καρτέλες για το αντικείμενο Group περιλαμβάνουν:

- **General:** Αυτή η καρτέλα εμφανίζει πληροφορίες σχετικά με το αντικείμενο. Μπορούμε να δούμε, αλλά όχι να τροποποιήσουμε το Group Scope και το Group Type for Groups. Μπορούμε να τροποποιήσουμε όλα τα άλλα πεδία σε αυτή τη σελίδα.
- **Member:** Εδώ μπορούμε να προσθέσουμε και να αφαιρέσουμε τα μέλη μιας ομάδας. Κάνοντας κλικ στο κουμπί Προσθήκη-Add, μπορούμε να προσθέσουμε μεμονωμένα αντικείμενα ή επιλέξουμε πολλαπλά αντικείμενα.
- **Member Of:** Αυτή η καρτέλα παραθέτει τις ομάδες που σε αυτές ανήκει το αντικείμενο. Μπορούμε να προσθέσουμε ή να αφαιρέσουμε ομάδες.

- **Managed By:** Παροχή πληροφοριών σχετικά με τα πρόσωπα που είναι υπεύθυνα για την διαχείριση του υπολογιστή απευθείας από το Active Directory
- **Object:** Αυτή η καρτέλα εμφανίζει πληροφορίες σχετικά με το αντικείμενο, συμπεριλαμβανομένου του ονόματος του, πότε δημιουργήθηκε, πότε ενημερώθηκε για τελευταία φορά και το Update Sequence Numbers του. Σε αυτή την καρτέλα, μπορούμε επίσης να αναφέρουμε ότι το αντικείμενο θα πρέπει να προστατεύεται από τυχαία διαγραφή.
- **Security:** Η καρτέλα αυτή ελέγχει τα Active Directory δικαιώματα των άλλων αντικειμένων που έχουν σε αυτό το αντικείμενο. Το Group ή user names πλαίσιο απαριθμεί τα αντικείμενα με δικαιώματα και το Permissions πλαίσιο περιγράφει τα δικαιώματα που έχουν χορηγηθεί ή απορριφθεί στον επιλεγμένου χρήστη ή στην ομάδα.



Εικ.7.6

- **Attribute Editor** (νέα καρτέλα στο Windows Server 2008): Στον Windows Server 2008, η Microsoft έχει δανειστεί αυτήν την λειτουργία από το βοηθητικό πρόγραμμα ADSI Edit και πρόσθεσε αυτή την καρτέλα, η οποία μας επιτρέπει να

χειριστούμε άμεσα το σύνολο των ιδιοτήτων που σχετίζονται με το επιλεγμένο αντικείμενο.

7.2.3 User Objects.

Όταν κάνουμε δεξί κλικ σε ένα αντικείμενο χρήστη και επιλέξουμε τις ιδιότητες, θα δούμε στην οθόνη ότι φαίνεται στο σχήμα

Η σελίδα Properties για ένα user object.

Το παράθυρο για τους χρήστες περιλαμβάνει τις εξής καρτέλες:

- **General:** Εμφανίζει γενικές περιγραφικές πληροφορίες για τον χρήστη, συμπεριλαμβανομένου του ονόματος, της διεύθυνσης ηλεκτρονικού ταχυδρομείου και του αριθμού τηλεφώνου.
- **Address:** Αυτή η καρτέλα εμφανίζει τις ταχυδρομικές διευθύνσεις για τον επιλεγμένο χρήστη.
- **Account:** Η καρτέλα διαθέτει λεπτομερείς πληροφορίες για το λογαριασμό του χρήστη, συμπεριλαμβανομένου του ονόματος σύνδεσης του χρήστη (logon name) και μέσω του κουμπιού Logon Hours που υπάρχει σε αυτήν την καρτέλα, χρονικοί περιορισμοί στο λογαριασμό. Το Account options τμήμα των επιλογών μας δίνει έναν τρόπο να υποχρεώσουμε τους χρήστες να αλλάξουν τον κωδικό τους κατά την επόμενη σύνδεση ή να τους εμποδίζουν να αλλάζουν τους κωδικούς πρόσβασης, να απαιτείται μια έξυπνη κάρτα για σύνδεση και να καταστεί δυνατό το Delegation - αντιπροσωπεία για αυτόν τον λογαριασμό. Θα χρησιμοποιήσουμε ακόμα αυτήν τη σελίδα, αν ο λογαριασμός κλειδωθεί, λόγω αποτυχημένων προσπαθειών σύνδεσης. Η προσθήκη μιας " Unlock account" επιλογής σε αυτή την καρτέλα μας δίνει την δυνατότητα να ξεκλειδώνουμε εύκολα τον λογαριασμό.
- **Profile:** Η καρτέλα Προφίλ καθορίζει τις διαδρομές για δέσμες ενεργειών σύνδεσης που ο χρήστης πρέπει να έχει πρόσβαση. Μπορούμε επίσης να καθορίσουμε μια διαδρομή στο προφίλ του χρήστη και στον home folder του.
- **Telephones:** Αυτή η καρτέλα χρησιμεύει ως τηλεφωνικός κατάλογος των αριθμών που έχουμε για τον χρήστη, συμπεριλαμβανομένων συσκευών τηλεειδοποίησης, κινητών τηλεφώνων, και IP τηλεφώνων.
- **Organization:** Εδώ, περιλαμβάνονται στοιχεία για την εταιρεία του χρήστη, συμπεριλαμβανομένου του τμήματος, καθώς και του ονόματος της εταιρείας. Μπορούμε επίσης να συνδέσουμε το χρήστη με το διαχειριστή του στο Active Directory.

- **Terminal Services Profile:** Η καρτέλα αυτή είναι παρόμοια με την καρτέλα Profile, αλλά αυτή εδώ ελέγχει μόνον τις πληροφορίες του προφίλ για τη σύνοδο των υπηρεσιών Terminal Services, συμπεριλαμβανομένων της θέσης του home folder
- **COM+:** Μπορείτε να εκχωρήσουμε το δικαίωμα στο χρήστη να είναι μέρος ενός διαμερίσματος -partition COM+. Τα COM+ partition επιτρέπουν στους χρήστες ενός τομέα να έχουν πρόσβαση σε COM+ εφαρμογές σε ολόκληρο τον τομέα.
- **Security:** Η καρτέλα αυτή ελέγχει τα Active Directory δικαιώματα των άλλων αντικειμένων που έχουν σε αυτό το αντικείμενο. Το Group ή user names πλαίσιο απαριθμεί τα αντικείμενα με δικαιώματα και το Permissions πλαίσιο περιγράφει τα δικαιώματα που έχουν χορηγηθεί ή απορριφθεί στον επιλεγμένου χρήστη ή στην ομάδα.
- **Attribute Editor** (νέα καρτέλα στο Windows Server 2008): Στον Windows Server 2008, η Microsoft έχει δανειστεί από το βοηθητικό πρόγραμμα την λειτουργία ADSI Edit και πρόσθεσε αυτή την καρτέλα, η οποία μας επιτρέπει να χειριστούμε άμεσα το σύνολο των ιδιοτήτων που σχετίζονται με το επιλεγμένο αντικείμενο.
- **Environment:** Η καρτέλα αυτή ελέγχει το περιβάλλον εκκίνησης Terminal Services του χρήστη.
- **Sessions:** Με αυτήν την καρτέλα ελέγχουμε τον τρόπο με τον οποίο ο χρήστης αλληλεπιδρά με τις υπηρεσίες Terminal Services, συμπεριλαμβανομένου και του χρονικού διαστήματος που παραμένει συνδεδεμένος και τι θα συμβεί αν αποσυνδεθεί από το εξυπηρετητή.
- **Remote Control:** Αυτή η καρτέλα δείχνει αν η Terminal Server σύνοδος του χρήστη, μπορεί να ελεγχθεί εξ αποστάσεως. Μπορούμε να ρυθμίσουμε τις επιλογές που μας επιτρέπουν να έχουμε συνεδρίες τύπου view-only ή συνεδρίες που καθιστούν δυνατή την αλληλεπίδραση.
- **Published Certificates:** Αυτή η καρτέλα μας επιτρέπει να συσχετίσουμε τα πιστοποιητικά ασφαλείας-certificates X.509 με το χρήστη.
- **Member Of:** Αυτή η καρτέλα παραθέτει τις ομάδες στις οποίες ανήκει ο χρήστης. Μπορούμε να προσθέσουμε ή να διαγράψουμε την ιδιότητα του μέλους εδώ.
- **Password Replication:** Η καρτέλα διατηρεί μια λίστα read only ελεγκτών τομέα που αποθηκεύουν προσωρινά -cached εκδόσεις του καταλόγου.

- **Dial-in:** Επιλεγούμε εάν οι χρήστες μπορούν να αποκτήσουν απομακρυσμένη πρόσβαση στον υπολογιστή, είτε με dial-up ή VPN. Μπορούμε επίσης να ορίσουμε τις επιλογές επιστροφής κλήσης για επιπλέον ασφάλεια.
- **Object:** Αυτή η καρτέλα εμφανίζει πληροφορίες σχετικά με το αντικείμενο, συμπεριλαμβανομένου του ονόματος του, πότε δημιουργήθηκε, πότε ενημερώθηκε για τελευταία φορά και το Update Sequence Numbers για αυτό. Σε αυτή την καρτέλα, μπορούμε επίσης να αναφέρουμε ότι το αντικείμενο θα πρέπει να προστατεύεται από τυχαία διαγραφή.

7.3 Πραγματοποιώντας εργασίες με το Active Directory Users και Computers

7.3.1 Δημιουργώντας έναν νέο χρήστη -new user

Κάνουμε δεξί κλικ στο κοντέινερ όπου θέλουμε το νέο αντικείμενο -χρήστης να αποθηκευτεί. Κάνουμε κλικ στο κουμπί Νέος |χρήστης New | User.

Ακολουθούμε τις υποδείξεις στην οθόνη, για να προσθέσετε πληροφορίες σχετικά με το χρήστη, όπως το όνομα σύνδεσης-logout name και το όνομα χρήστη αλλά και άλλες πληροφορίες. Κάνουμε κλικ στο κουμπί Επόμενο για να δούμε πρόσθετες οθόνες και πληκτρολογούμε τις κατάλληλες πληροφορίες όπου μας ζητούνται.

7.3.2 Δημιουργία νέας ομάδας -new group

Κάνουμε δεξί κλικ στο κοντέινερ όπου θέλουμε το νέο αντικείμενο -ομάδα να αποθηκευτεί. Κάνουμε κλικ στο κουμπί New Group |. Ακολουθούμε τις υποδείξεις στην οθόνη για την δημιουργία του νέου group και προσθέτουμε πληροφορίες σχετικά με την ομάδα, όπως το όνομα της ομάδας και το είδος της ομάδας. Για τις περισσότερες ομάδες που θα δημιουργήσουμε, θα δημιουργήσουμε μια Global Security Group. Κάνουμε κλικ στο OK για να δημιουργήσουμε την ομάδα.

7.3.3 Δημιουργία ενός νέου κοντέινερ ,υποδοχέα - organizational unit

Κάνουμε δεξί κλικ στο κοντέινερ όπου θέλουμε το νέο αντικείμενο –organizational unit να αποθηκευτεί. Κάνουμε κλικ στο κουμπί Νέα | οργανική μονάδα, New | Organizational Unit. Στην οθόνη του Νέου Αντικείμενου - Οργανική Μονάδα, πληκτρολογούμε ένα μοναδικό όνομα. Κάνουμε κλικ στο κουμπί OK .

7.3.4 Προσθήκη ενός χρήστη -user σε μια ομάδα –group

Κάνουμε δεξί κλικ στο αντικείμενο χρήστη. Επιλέγουμε το Add To A Group. Όταν εμφανιστεί το Select Group παράθυρο, πληκτρολογούμε το όνομα της ομάδας στο πλαίσιο Enter The Object Name To Select και κάνουμε κλικ στην επιλογή Έλεγχος

ονομάτων Check Names. Εάν δεν γνωρίζουμε το όνομα, κάνουμε κλικ στο Advanced. Μετά Κάνουμε κλικ στο κουμπί Εύρεση τώρα -Find now για να εμφανίσουμε όλες τις ομάδες ή δίνουμε τα αρχικά της ομάδας που μας ενδιαφέρει και κάνουμε κλικ στο Εύρεση τώρα -Find now.

Επιλέγουμε την ομάδα που θέλουμε ο χρήστης να ανήκει και κάνουμε κλικ στο OK. Κάνουμε ξανά κλικ στο κουμπί OK για να κλείσουμε το παράθυρο Select Group.

7.3.5 Αλλαγή κωδικού πρόσβασης - Change a password

Κάνουμε δεξί κλικ στο αντικείμενο χρήστη. Επιλέγουμε Επαναφορά κωδικού πρόσβασης -Reset Password. Όταν εμφανισθεί η οθόνη, πληκτρολογούμε δυο φορές τον νέο κωδικό στα κατάλληλα πεδία. Για να υποχρεώσουμε τον χρήστη να αλλάξει τον κωδικό πρόσβασης αμέσως, επιλέγουμε Users Must Change Password. Κάνουμε κλικ στο OK.

7.3.6 Για να ξεκλειδώσουμε ένα λογαριασμό

Κάνουμε δεξί κλικ στο αντικείμενο χρήστη. Επιλέγουμε Ιδιότητες -Properties. Κάνουμε κλικ στην καρτέλα Ο λογαριασμός -Account. Αφαιρούμε την επιλογή από το κουτί Account Is Locked Out.

7.3.7 Απενεργοποίηση λογαριασμού

Κάνουμε δεξί κλικ στο αντικείμενο χρήστη. Επιλέγουμε Απενεργοποίηση Λογαριασμού. Ενεργοποίηση λογαριασμού κάνοντας δεξί κλικ στο αντικείμενο χρήστη και την επιλογή Ενεργοποίηση Λογαριασμού.

7.3.8 Μετακίνηση ενός χρήστη

Drag and drop του χρήστη στον υποδοχέα -κοντεινερ.

7.3.9 Περιορισμός χρόνου σύνδεσης -Restrict logon times

Κάνουμε δεξί κλικ στο αντικείμενο χρήστη. Επιλέγουμε Ιδιότητες. Κάνουμε κλικ στην καρτέλα Account. Κάνουμε κλικ στο κουμπί Logon Hours. Όταν η καρτέλα Logon Hours εμφανιστεί η οθόνη, επιλέγουμε Logon Denied και κάνουμε κλικ στις ώρες που δεν θέλουμε ο χρήστης να συνδέεται.

7.3.10 Μεταβίβαση εξουσιών Delegate authority

Κάνουμε δεξί κλικ στο αντικείμενο κοντέινερ από όπου θέλετε την ανάθεση καθηκόντων Delegate authority. Επιλέγουμε Delegate Control. Ο οδηγός Delegation Of Control εμφανίζεται. Ακολουθούμε τις οδηγίες στην οθόνη για να προσθέσουμε τους χρήστες ή τις ομάδες που θέλουμε να δώσουμε τον έλεγχο αλλά και ποιες αρμοδιότητες θέλουμε να χορηγούν στους χρήστες ή στις ομάδες.

7.3.11 Άδεια στους χρήστες να χρησιμοποιούν VPN

Κάνουμε δεξί κλικ στο αντικείμενο χρήστη. Επιλέγουμε Ιδιότητες -Properties. Κάνουμε κλικ στην καρτέλα Dial-in. Επιλέγουμε Allow Access (ή, αν έχετε υλοποιήσει Windows Server 2008 Network Access Protection, κάνουμε κλικ στην εντολή Έλεγχος πρόσβασης μέσω NPS Network Policy. Κάνουμε κλικ στο κουμπί OK.

7.3.12 Για μια αλλαγή σε ένα συγκεκριμένο χαρακτηριστικό ενός αντικείμενου

Κάνουμε δεξί κλικ στο αντικείμενο. Επιλέγουμε Ιδιότητες-Properties. Κάνουμε κλικ στην καρτέλα Editor Attribute. Επιλέγουμε το χαρακτηριστικό που θέλουμε να τροποποιήσουμε. Κάνουμε κλικ στο κουμπί Επεξεργασία. Κάνουμε την αλλαγή και κλικ στο OK.

7.4 Στρατηγικές ομάδων Group strategies

7.4.1 GROUP SCOPE

Το group scope ορίζει την εμβέλεια ενός group σε ένα domain ή σε ένα forest.

Υπάρχουν τρεις επιλογές στο windows 2008 forest

- Domain Local
- Global
- Universal

Group scope	Possible members	Can be a member of	Permissions and rights assignments
Domain local	User accounts, global groups, and universal groups from any domain in the forest Other domain local groups from the same domain User accounts, global groups, and universal groups from trusted domains in another forest	Domain local groups in the same domain Local groups on domain member computers; domain local groups in the Builtin folder can be members only of other domain local groups	Resources on any DC or member computer in the domain; domain local groups in the Builtin folder can be added to DACLS only on DCs, not on member computers
Global	User accounts and global groups (nested) in the same domain	Global groups in the same domain Domain local groups or local groups on member computers in any domain in the forest or trusted domains in another forest	Resources on any DC or member computer in any domain in the forest or trusted domains in another forest
Universal	User accounts, global groups, and universal groups from any domain in the forest	Universal groups from any domain in the forest Domain local groups or local groups on member computers in any domain in the forest or trusted domains in another forest	Resources on any DC or member computer in any domain in the forest or trusted domains in another forest

Εικ.7.7

Και το Local group που ισχύει μόνον στα group που δημιουργούνται στη βάση δεδομένων SAM ενός υπολογιστή που ανήκει στο domain ή ενός stand alone υπολογιστή όπως φαίνονται και από την εικόνα.

7.4.2 Domain Local Groups

Ένα domain local group είναι το βασικό security principal που συνιστάται για εκχώρηση δικαιωμάτων στους πόρους ενός domain.

Global and Universal groups μπορούν να χρησιμοποιηθούν για τον ίδιο σκοπό, αλλά οι βέλτιστες πρακτικές της Microsoft συνιστούν τη χρήση αυτών των ομάδων για τη ομαδοποίηση των χρηστών με παρόμοιες απαιτήσεις πρόσβασης ή δικαιωμάτων.

7.4.3 Global Groups

Για να εκχωρήσουμε δικαιώματα χρήσης πόρων δικτύου σε χρήστες που έχουν κοινές απαιτήσεις στην χρήση των πόρων λόγω του ότι συνήθως κάνουν κοινές εργασίες.

Θεωρείται παγκόσμια **Global** γιατί μπορεί να γίνει μέλος ενός domain local group, σε κάθε τομέα στο forest ή σε trusted domains σε άλλα forests.

7.4.4 Universal Groups

Ένα **Universal Group** μπορεί να περιέχει χρήστες από κάθε domain στο forest και να του εκχωρούνται δικαιώματα σε πόρους, σε κάθε τομέα στο forest.

Των **Universal Group** η ιδιότητα μέλους είναι αποθηκευμένη μόνο σε global catalog servers.

Οι αλλαγές στην ιδιότητα μέλους **Universal Group** απαιτούν αναπαραγωγή σε όλους τους global catalog servers.

7.4.5 Local Groups

Μια τοπική ομάδα LOCAL GROUP δημιουργείται στην τοπική βάση δεδομένων SAM σε ένα member server ή σε έναν σταθμό εργασίας ή σε έναν αυτόνομο υπολογιστή –εκτός του τομέα.

Όταν ένας υπολογιστής ενώνεται σε έναν τομέα, τα Windows αλλάζουν τη ιδιότητα μέλους δύο local groups αυτόματα.

- Στους Administrators: προστίθεται το global group Domain Admin
- Στους Χρήστες: προστίθεται το global group Domain users

Οι τοπικές ομάδες LOCAL GROUPS μπορούν να έχουν τους παρακάτω διαφορετικούς τύπους λογαριασμών χρηστών και ομάδων ως μέλη:

- Local user
- Domain user

- Domain local group
- Global or universal group

7.4.6 Στρατηγικές για την παροχή δικαιωμάτων

Σε ένα περιβάλλον όπου υπάρχει ένας τομέας, single domain environment ή όταν στους χρήστες από έναν μόνο τομέα θα εκχωρηθεί πρόσβαση σε έναν πόρο, η χρήση της στρατηγικής AGDLP συνιστάται από την Microsoft.

AGDLP:

Accounts λογαριασμοί χρηστών γίνονται μέλος των

Global groups, οι οποίες γίνονται μέλη των

Domain Local groups του τομέα, οι οποίες εκχωρούν

Permissions δικαιώματα στους πόρους.

Σε περιβάλλον πολλών τομέων multidomain, όπου χρήστες από διαφορετικούς τομείς θα έχουν πρόσβαση σε έναν πόρο, η χρήση AGGUDLP συνιστάται

AGGUDLP:

Accounts λογαριασμοί χρηστών γίνονται μέλος των

Global groups, οι οποίες γίνονται εμφολεύμενα μέλη άλλων

Global groups, οι οποίες γίνονται μέλη των

Universal groups, οι οποίες γίνονται μέλη των

Domain Local groups, οι οποίες εκχωρούν

Permissions δικαιώματα στους πόρους

Αυτές οι στρατηγικές είναι σχεδιασμένες για να μειώσουν το βάρος της συντήρησης και διαχείρισης του Forest.

ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΣΒΑΣΗΣ ΣΕ ΠΟΡΟΥΣ

8.1 Εισαγωγή

Οι επιθυμητές γνώσεις και δεξιότητες που θα αποκτήσουν οι επιμορφωμένοι στην ενότητα Διαχείριση πρόσβασης σε πόρους & Υλοποίηση και διαχείριση εκτυπώσεων, θα τους καταστήσουν ικανούς να :

- Δημιουργούν κοινούς φακέλους και να εκτελούν βασικές ρυθμίσεις ασφάλειας.
- Εκτελούν ρυθμίσεις με τη χρήση NTFS Permissions και να αποτιμούν τα Effective Permissions.
- Διατηρούν διαθέσιμους τους κοινούς φακέλους για εργασία χωρίς σύνδεση με χρήση Offline Caching.
- Εγκαθιστούν και να διαχειρίζονται εκτυπωτές σε έναν print server για εκτυπώσεις μέσω δικτύου από τους clients.

8.2 Διαχείριση πρόσβασης σε πόρους

Για να μπορούν οι χρήστες στα Windows 2008 Server να εκμεταλλευτούν τις δυνατότητες που παρέχονται από ένα δίκτυο, όπως είναι η κοινή χρήση πόρων, διατίθεται το εργαλείο **Share and Storage management** (Διαχείριση Αποθήκευσης και Κοινής Χρήσης).

Είναι μια κονσόλα (mmc), η οποία παρέχει ένα κεντρικό σημείο διαχείρισης για δύο συγκεκριμένους και σοβαρούς πόρους ενός server:

- Τους φακέλους και τους τόμους που μπορούν να διαμοιραστούν στο δίκτυο.
- Τόμους σε δίσκους και αποθηκευτικά υποσυστήματα στα οποία θα αναφερθούμε συνοπτικά, διότι θα ακολουθήσει περεταίρω ανάλυση σε άλλη ενότητα.

8.3 Βασικές έννοιες

Shared Folder: Είναι ένας φάκελος που βρίσκεται σε δίσκο του Server ή και σε υποσυστήματα δίσκων που είναι συνδεδεμένα στο δίκτυο (SAN, NAS, iSCSI), με τον οποίο μπορούν να «συναναστρέφονται», ανάλογα με τα δικαιώματα που τους παρέχονται, οι χρήστες του δικτύου.

Δικαιώματα (permissions): Καθορίζουν τις επιτρεπόμενες ενέργειες (NTFS permissions) που μπορούν να γίνουν από τους χρήστες σε ένα φάκελο. Ορίζονται τόσο σε κοινόχρηστους όσο και τοπικούς φακέλους (NTFS permissions) και μπορεί να είναι:

- **Read (ανάγνωση):** Δυνατότητα εμφάνισης, προσπέλασης, ανάγνωσης αρχείων και υποφακέλων, ανάγνωσης ιδιοτήτων αρχείων, εκτέλεση προγραμμάτων.
- **Change (τροποποίηση):** Ότι για το Read και επιπρόσθετα, δημιουργία και τροποποίηση αρχείων και υποφακέλων, τροποποίηση ιδιοτήτων και διαγραφή αρχείων και υποφακέλων.
- **Full Control (πλήρης έλεγχος):** Όλα τα παραπάνω και επιπλέον, αλλαγή δικαιωμάτων πρόσβασης αρχείων και υποφακέλων, ανάληψη κατοχής αρχείων και υποφακέλων.
- **Hidden Shares:** Είναι κοινόχρηστοι φάκελοι, οι οποίοι δεν είναι «εμφανείς», δηλαδή, δεν φαίνονται μέσω της περιοχής δικτύου σαν κοινόχρηστοι πόροι, αλλά είναι προσβάσιμοι, αναλόγως δικαιωμάτων, με το Universal Naming Convention (UNC) τους με το χαρακτηριστικό γνώρισμα τους το \$ στο τέλος του φακέλου (\\servername\sharefolder\$).
- **Administrative Shares:** Είναι **Hidden Shares** τα οποία δημιουργούνται από το λειτουργικό σύστημα και χρησιμοποιούνται για διαχειριστικούς λόγους και επιτρέπουν την πρόσβαση σε οποιονδήποτε ανήκει στην ομάδα των administrators.
- **Χαρακτηριστικά Hidden Shares :**
 - ✓ **DriveLetter\$:** Έχουν πρόσβαση οι Administrators και οι Backup Operators όταν πρόκειται για servers & workstations ενώ στην περίπτωση του Domain Controller πρόσβαση έχουν και οι Server Operators.
 - ✓ **ADMIN\$:** Σε αυτά τα στοιχεία πρόσβαση έχουν οι Administrators και οι Backup Operators, όταν πρόκειται για servers & workstations, ενώ στην περίπτωση του Domain Controller πρόσβαση έχουν και οι Server Operators.
 - ✓ **IPC\$:** Inter-Process Communication (IPC) Χρησιμοποιείται για την διευκόλυνση της επικοινωνίας μεταξύ διαδικασιών (processes) και του υπολογιστή, όπως και για την ανταλλαγή δεδομένων μεταξύ υπολογιστών που έχουν αυθεντικοποιηθεί.
 - ✓ **SYSVOL\$:** Χρησιμοποιείται για την αποθήκευση δεδομένων και αντικειμένων του Active Directory.
- **Πρωτόκολλα πρόσβασης σε κοινόχρηστους πόρους:**
 - ✓ **Server Message Block (SMB):** Για συστήματα Windows στα οποία η πρόσβαση ελέγχεται μέσω δικαιωμάτων σε χρήστες και ομάδες (users-groups).
 - ✓ **Network File System (NFS):** Για συστήματα Unix στα οποία η πρόσβαση ελέγχεται μέσω δικαιωμάτων σε συγκεκριμένους υπολογιστές (client computers) και

ομάδες (groups) χρησιμοποιώντας δικτυακά ονόματα.

8.4 Δημιουργία και Διαχείριση

Ένας φάκελος μπορεί να γίνει κοινόχρηστος με δύο τρόπους:

- Με δεξί κλικ στον φάκελο properties και ενεργώντας στις καρτέλες **sharing** και **security**.
- Με την χρήση της κονσόλας διαχείρισης του server 2008, **Share and Storage management**.

Και οι δύο τρόποι οδηγούν στο ίδιο αποτέλεσμα ενώ απαιτούν δικαιώματα administrators ή ισοδύναμα.

8.4.1 Δημιουργία και διαχείριση δικαιωμάτων κοινόχρηστων φακέλων μέσω των ιδιοτήτων του φακέλου

Αν σε έναν φάκελο, τον οποίο θέλουμε να κάνουμε κοινόχρηστο, κάνουμε δεξί κλικ properties, εμφανίζεται η Εικ. 8.1.



Εικ. 8.1. Ιδιότητες Φακέλου.

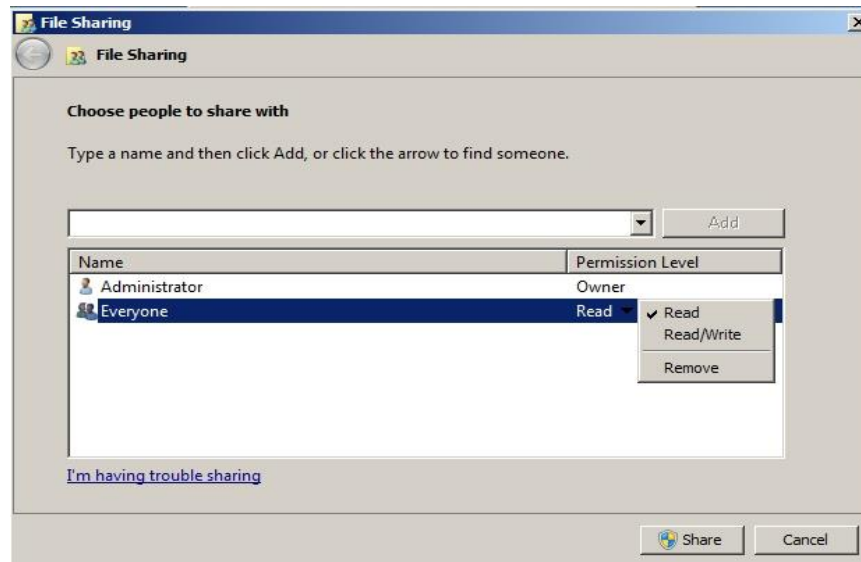
Στην καρτέλα sharing αν επιλέξουμε Share, εμφανίζεται η Εικ. 8.2, που μας ζητά να



Εικ. 8.2. Επιλογή χρηστών.

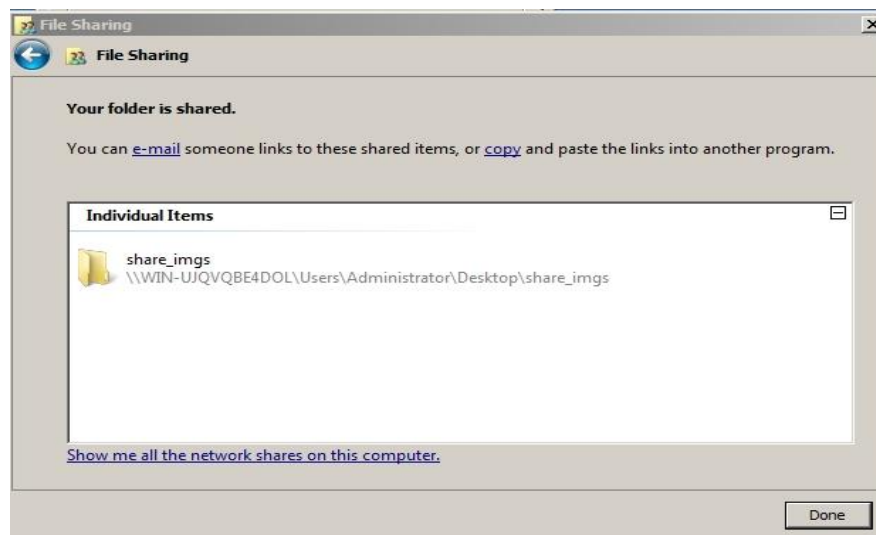
διαλέξουμε τον ή τους χρήστες που θα μπορούν να χρησιμοποιούν τον κοινόχρηστο φάκελο μέσω του δικτύου.

Επιλέγουμε **create a new user** και εμφανίζεται μια σειρά από φόρμες επιλογής η δημιουργίας χρηστών. Όταν επιλεγεί ο χρήστης, επιλέγουμε τα δικαιώματα που θα έχει (Read,Read/Write),



Εικ. 8.3. Επιλογή δικαιωμάτων χρηστών.

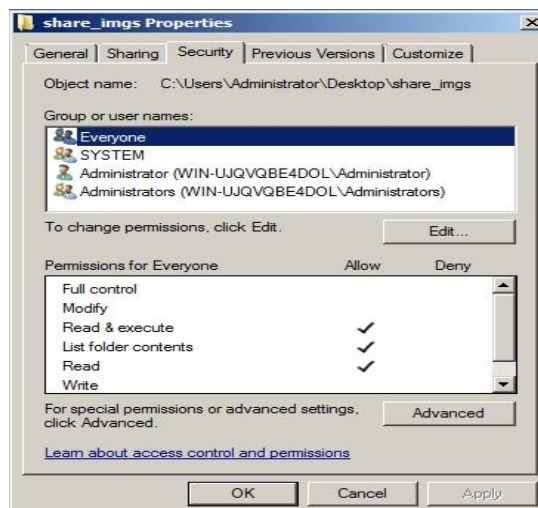
όπως μπορούμε να παρατηρήσουμε στην εικόνα 8.3. Πατώντας Share επιβεβαιώνεται η δημιουργία του κοινόχρηστου φακέλου, αλλά δεν έχει εξασφαλισθεί και η πρόσβαση.



Εικ. 8.4. Επιβεβαίωση δημιουργίας κοινόχρηστου φακέλου.

8.4.2 Διαχείριση δικαιωμάτων φακέλων (NTFS permissions)

Για να εξασφαλίσουμε την πρόσβαση σε κοινόχρηστο φάκελο είναι αναγκαία και η ρύθμιση των δικαιωμάτων της καρτέλας security (Εικ. 8.5).



Εικ. 8.5. Δικαιώματα security.

Μπορούμε να προσθέσουμε ή να αφαιρέσουμε κάποιο δικαίωμα πατώντας στο edit και επιλέγοντας ανάλογα.

Ο συνδυασμός των δικαιωμάτων sharing και security είναι αυτός τελικά που θα μας δώσει την τελική πρόσβαση στον κοινόχρηστο φάκελο. Σε περίπτωση διαφοροποίησης δικαιωμάτων μεταξύ των δύο καρτελών, ισχύουν τελικά τα πλέον απαγορευτικά.

Στον παρακάτω πίνακα 8.1 παρουσιάζονται στοιχεία σχετικά με τα δικαιώματα (NTFS permissions) και την επιρροή που έχουν σε φακέλους και αρχεία.

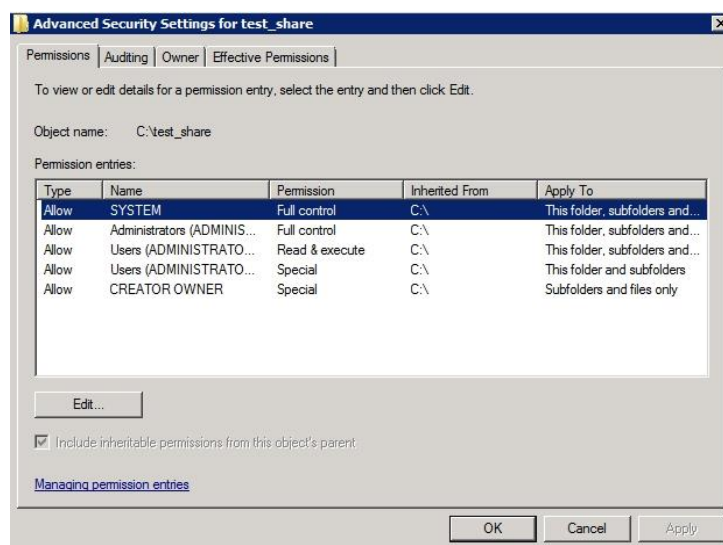
Δικαιώματα	Φάκελος	Αρχείο
Read	Επιτρέπει την εξέταση και εμφάνιση αρχείων και υποφακέλων	Επιτρέπει την εξέταση και την προσπέλαση των περιεχομένων του αρχείου
Write	Επιτρέπει την προσθήκη αρχείων και υποφακέλων	Επιτρέπει την εγγραφή των αρχείων
Read & Execute	Επιτρέπει την εξέταση αρχείων και υποφακέλων, την παρουσίαση τους σε λίστες και την εκτέλεση αρχείων. Κληρονομείται από αρχεία και φακέλους	Επιτρέπει την εξέταση και την προσπέλαση των περιεχομένων του αρχείου και την εκτέλεση αρχείου
List Folder Contents	Επιτρέπει την εξέταση αρχείων και υποφακέλων, την παρουσίαση τους σε λίστες και την εκτέλεση αρχείων. Κληρονομείται μόνο από	--

	φακέλους	
Modify	Επιτρέπει την ανάγνωση και εγγραφή αρχείων και υποφακέλων. Επιτρέπει τη διαγραφή του φακέλου	Επιτρέπει την ανάγνωση και εγγραφή αρχείου. Επιτρέπει τη διαγραφή του αρχείου
Full Control	Πλήρης έλεγχος, ανάγνωση, εγγραφή, τροποποίηση, διαγραφή αρχείων και υποφακέλων	Πλήρης έλεγχος, ανάγνωση, εγγραφή, τροποποίηση, δια-γραφή αρχείου

Πίνακας 8.1. Δικαιώματα σε φακέλους και αρχεία.

Θα πρέπει να αναφερθεί ότι το δικαίωμα Read είναι το μόνο που χρειάζεται για την εκτέλεση scripts ενώ αν σε χρήστη εκχωρηθεί το δικαίωμα Write για κάποιο αρχείο χωρίς τη δυνατότητα διαγραφής του (Modify), ο χρήστης μπορεί να ανοίξει και να διαγράψει τα περιεχόμενα του αρχείου.

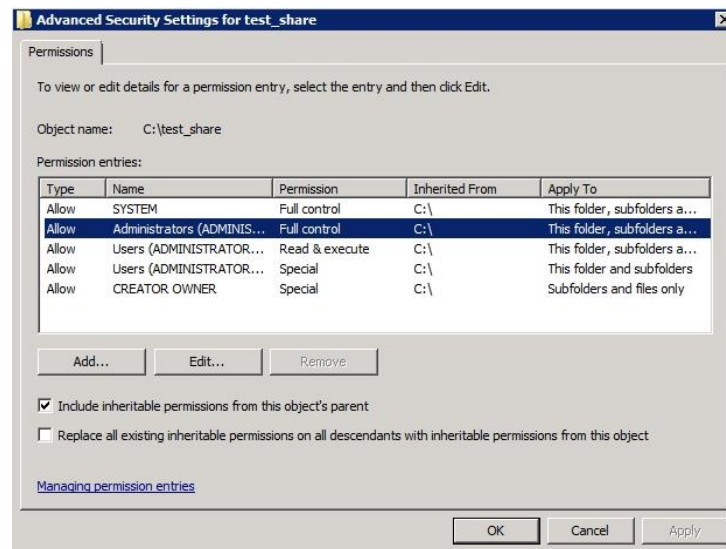
Επιλέγοντας **advanced** (προχωρημένα) δικαιώματα στην Εικ. 8.5, εμφανίζεται η Εικ. 8.6.



Εικ. 8.6. Advanced Δικαιώματα security.

Εδώ μπορούμε να τροποποιούμε «προχωρημένα» δικαιώματα χρηστών, καθώς επιλέγοντας ένα χρήστη και πατώντας edit, παρουσιάζεται η Εικ. 8.7. Παρατηρώντας βλέπουμε την επιλογή **include inheritable permissions from this object's parent** που είναι προεπιλεγμένη και ορίζει ότι κάθε «παιδί» (child) κληρονομεί τα δικαιώματα του «γονέα» (parent).

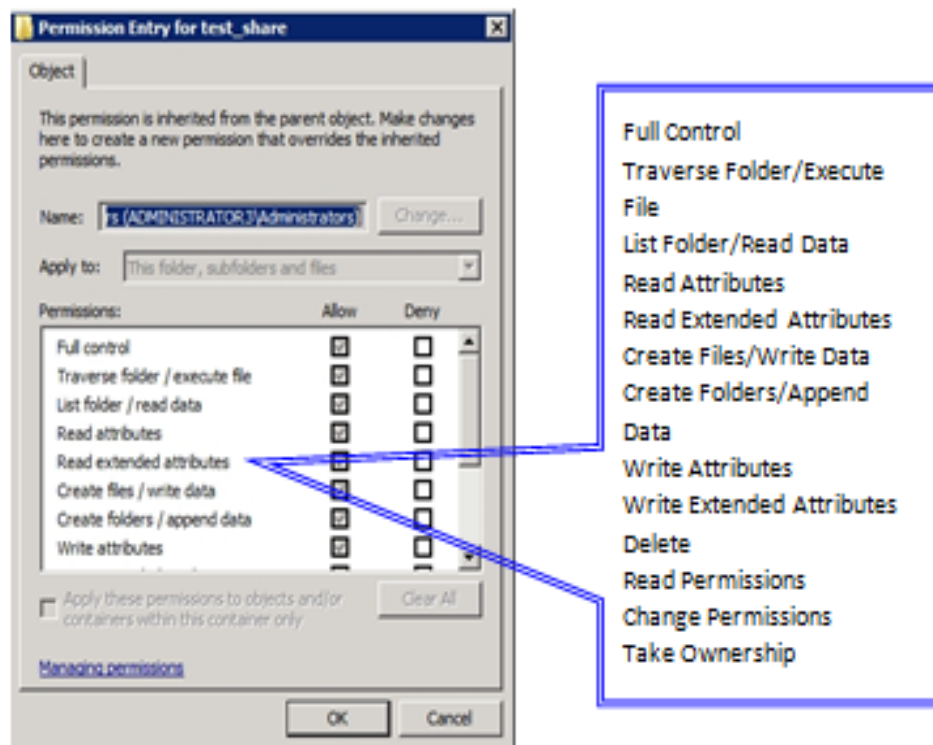
Για να διακόψουμε την κληρονομικότητα πρέπει να το αποεπιλέξουμε.



Εικ. 8.7. Advanced Δικαιώματα.

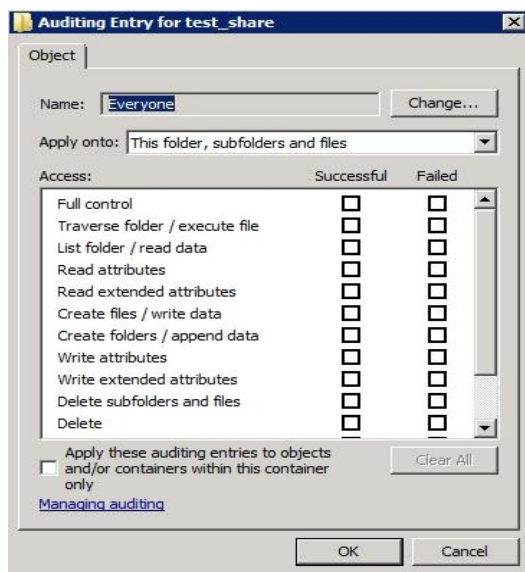
Μια ακόμα επιλογή είναι η **Replace all existing inheritable permissions on all descendants with inheritable permissions from this object**, με την οποία τα δικαιώματα του γονέα (parent) αντικαθιστούν, αν ενεργοποιηθεί, τα αντίστοιχα στους απογόνους του.

Επιλέγοντας edit (Εικ. 8.7) παρουσιάζονται τα προχωρημένα δικαιώματα της Εικ.8.8.



Εικ. 8.8. Προχωρημένα Δικαιώματα.

Explicit allow-deny: Οι επιλογές **allow-deny** λέγονται **Explicit** (ρητές) και επιλέγονται όταν δημιουργείται ένα αντικείμενο. Αν είναι επιλεγμένο και γκρι τότε το

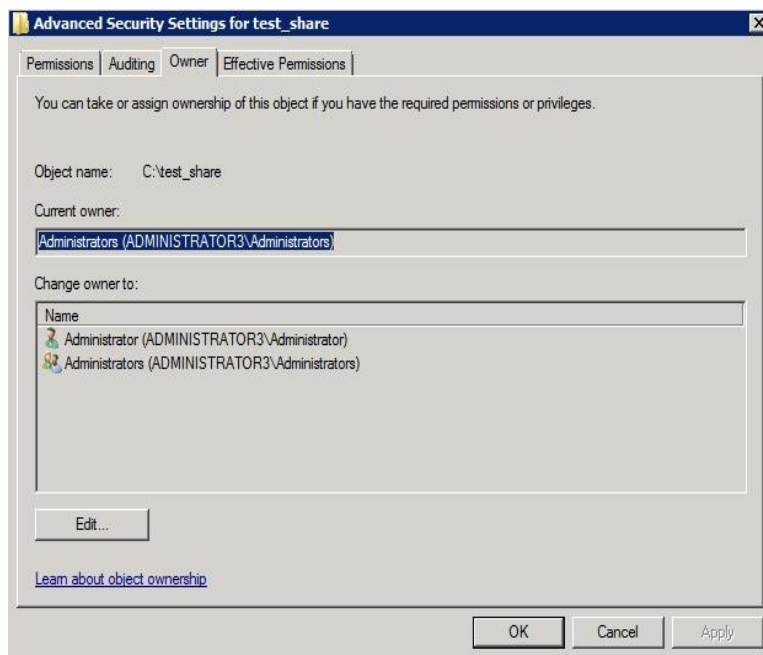


Εικ. 8.9. Παρακολούθηση ενεργειών.

δικαίωμα αυτό έχει κληρονομηθεί, ενώ αν είναι επιλεγμένο σε κανονικό πλαίσιο τότε είναι **Explicit allow** ή **deny** και υπερισχύει για εφαρμογή έναντι οποιασδήποτε κληρονομικότητας.

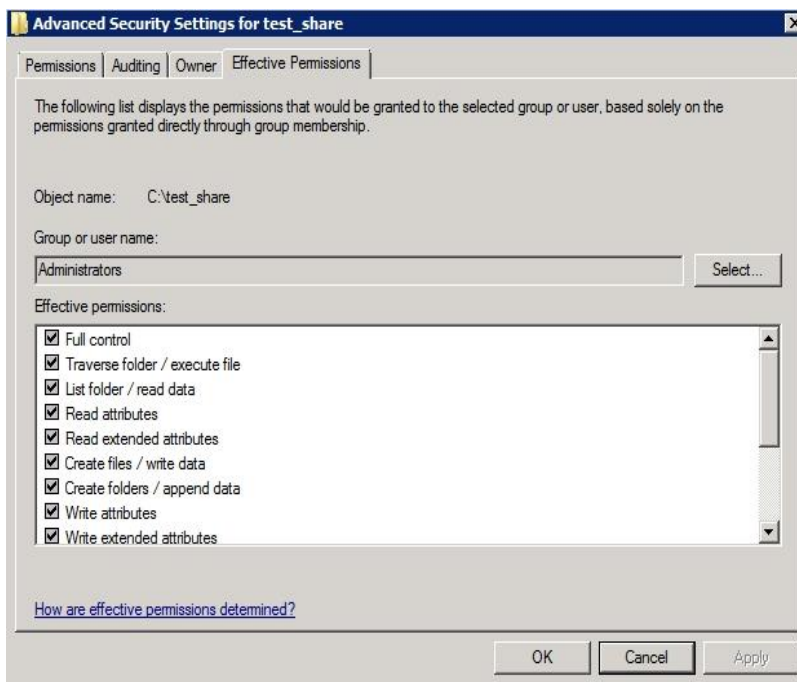
Στην Εικ.8.6 αν επιλέξουμε την καρτέλα **Auditing**, έχουμε την δυνατότητα να παρακολουθήσουμε χρήστες για ενέργειες, όπως αυτές της Εικ. 8.9.

Επιπρόσθετα αν στην Εικ.8.6 επιλέξουμε **Owner**, έχουμε την δυνατότητα να πάρουμε ή να δώσουμε την ιδιοκτησία ενός αντικειμένου (Εικ. 8.10).



Εικ. 8.10. Διαχείριση ιδιοκτησίας αντικειμένου.

Τέλος, η καρτέλα **effective permissions** (Εικ. 8.11) παρουσιάζει τα συνολικά δικαιώματα που έχει κάποιος χρήστης ή ομάδα στο συγκεκριμένο αντικείμενο.



Εικ. 8.11. Effective permissions διαχειριστή.

8.4.3 Share and Storage management.

Ένας οδηγός, ο οποίος ονομάζεται **Provision a Shared Folder Wizard** (Παροχή Κοινόχρηστου Φακέλου), βοηθά να διαμοιραστούν τα περιεχόμενα φακέλων και τόμων του server στο δίκτυο και βρίσκεται στο **Share and Storage management**.

Ειδικότερα με τον οδηγό μπορούμε:

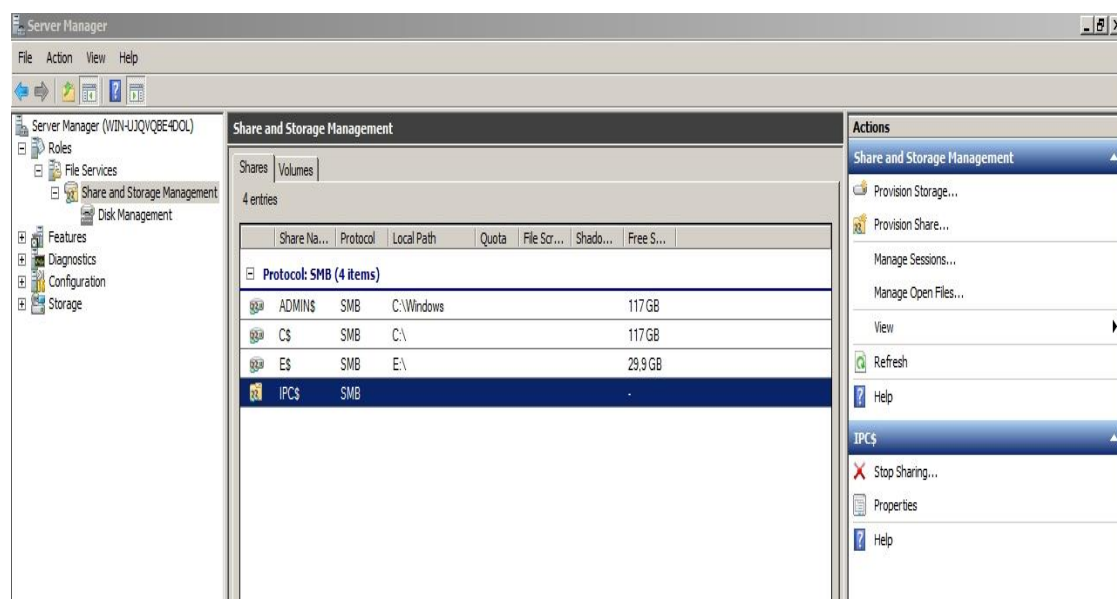
- Να ορίσουμε συγκεκριμένο φάκελο ή τόμο (Volume) τον οποίο θέλουμε να διαμοιράσουμε (Share), καθώς και να δημιουργήσουμε ένα καινούργιο φάκελο για κοινή χρήση.
- Να καθορίσουμε το **network sharing protocol** (SMB,NFS) που θα χρησιμοποιήσουμε για την κοινή χρήση των πόρων.
- Να αλλάξουμε τα NTFS permissions για τους φακέλους ή τόμους που θα διαμοιραστούν.
- Να καθορισθούν shared δικαιώματα πρόσβασης, όρια για τους χρήστες (quotas), και offline access σε αρχεία στους κοινούς πόρους.
- Να κάνουμε **publish** τον κοινό πόρο μέσω Distribute File System (DFS) namespace.
- Αν έχει καθορισθεί σαν πρωτόκολλο δικτύου το Network File System (NFS), μπορούμε να καθορίσουμε NFS δικαιώματα πρόσβασης.

Ταυτόχρονα υπάρχει η δυνατότητα να παρακολουθούμε και να τροποποιούμε σημαντικά σημεία σε νέους και υφιστάμενους κοινόχρηστους πόρους όπως:

- Να σταματάμε άμεσα την κοινή χρήση φακέλου ή τόμου.
- Να αλλάζουμε τα τοπικά NTFS δικαιώματα.
- Να αλλάζουμε τα shared access permissions, την offline διαθεσιμότητα και άλλες ιδιότητες των κοινοχρήστων πόρων.
- Να παρακολουθούμε ποιος χρήστης χρησιμοποιεί ποιόν φάκελο ή αρχείο και να τον διακόπτουμε αν είναι απαραίτητο.

Η εγκατάσταση του **Share and Storage management** πραγματοποιείται αυτόματα την πρώτη φορά που θα κάνουμε **share** μέσω φακέλου, όπως δείξαμε πιο πάνω και όταν εγκαταστήσουμε τον ρόλο **file services (Server management→Add role→File services)**.

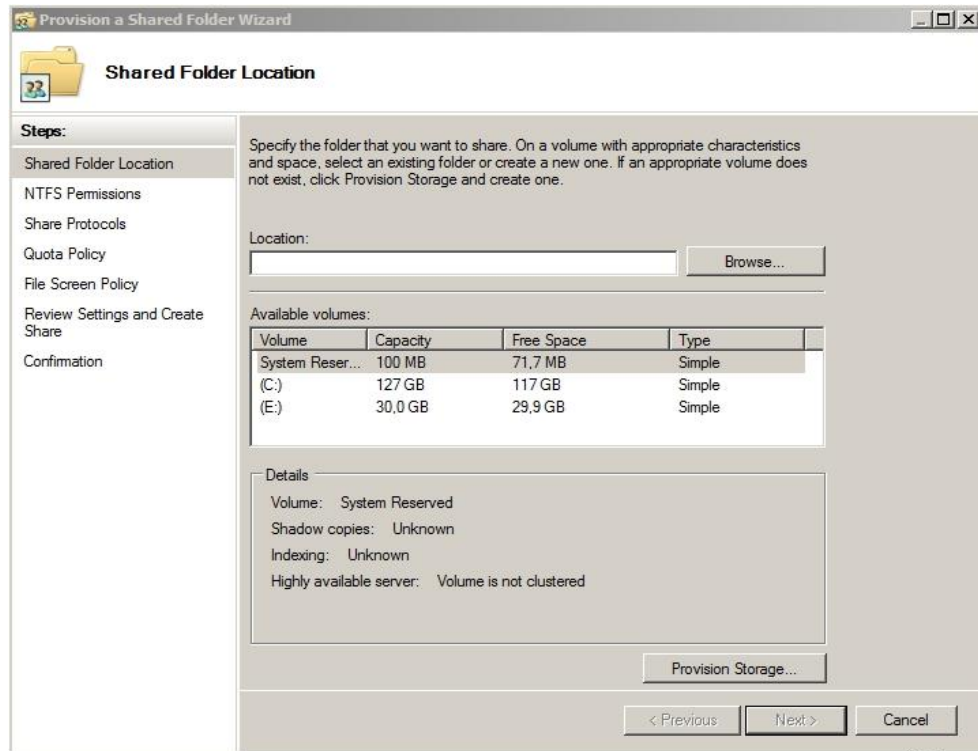
Σε κάθε περίπτωση θα δημιουργηθεί στο Start→Administrative tools η επιλογή Share and Storage management, που μας οδηγεί στην Εικ.8.12, μέσω της οποίας γίνεται η διαχείριση των κοινοχρήστων πόρων.



Εικ. 8.12. Share and Storage management.

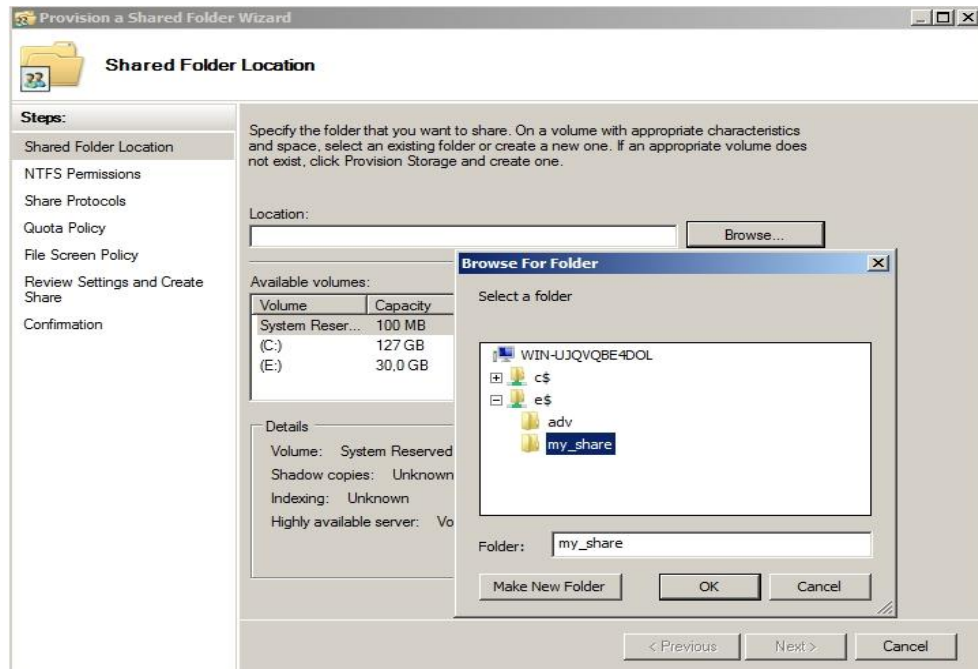
Μπορούμε να παρατηρήσουμε στο κεντρικό χώρο τα hidden shares (administrative shares) και στον ίδιο χώρο να δημιουργήσουμε, να διαχειριστούμε και να διαγράψουμε νέους κοινόχρηστους πόρους.

Για να δημιουργήσουμε έναν νέο κοινόχρηστο πόρο, επιλέγουμε δεξιά στο panel **action → Provision share** για να ξεκινήσει ο οδηγός που θα δημιουργήσει τον **shared folder**.



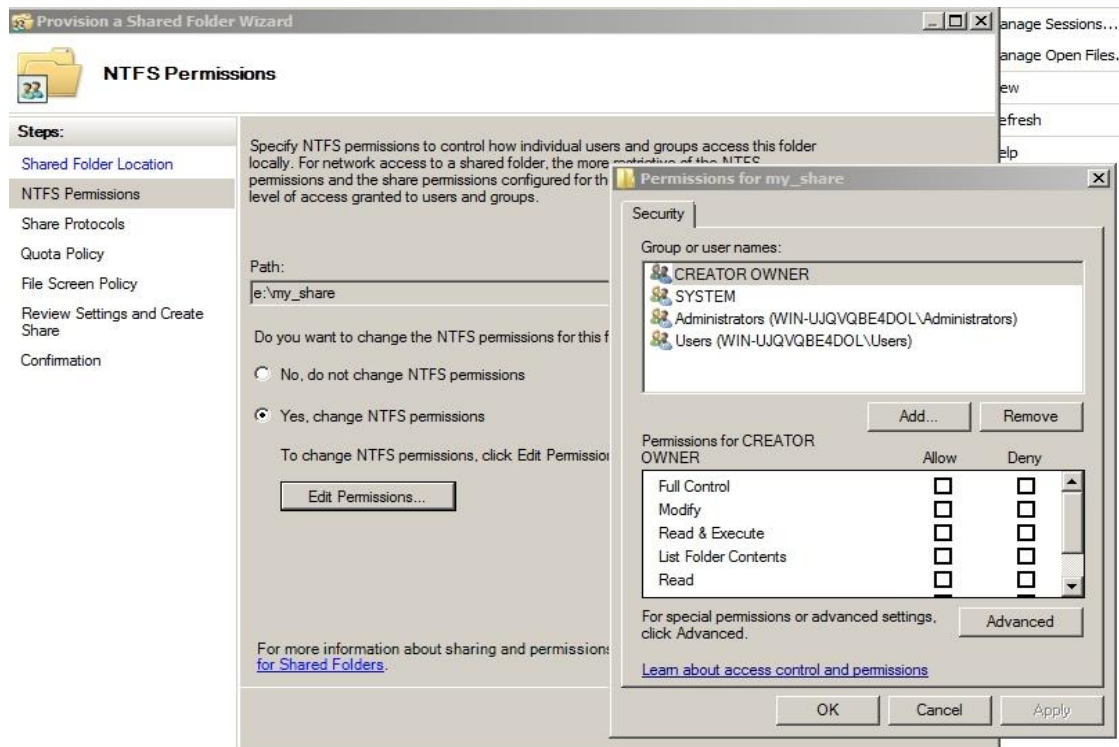
Εικ. 8.13. Provision share wizard.

Στην Εικ.8.13 επιλέγουμε **Browse** και δημιουργούμε τον φάκελο (My_share) που θέλουμε να διαμοιράζουμε (Εικ. 8.14).



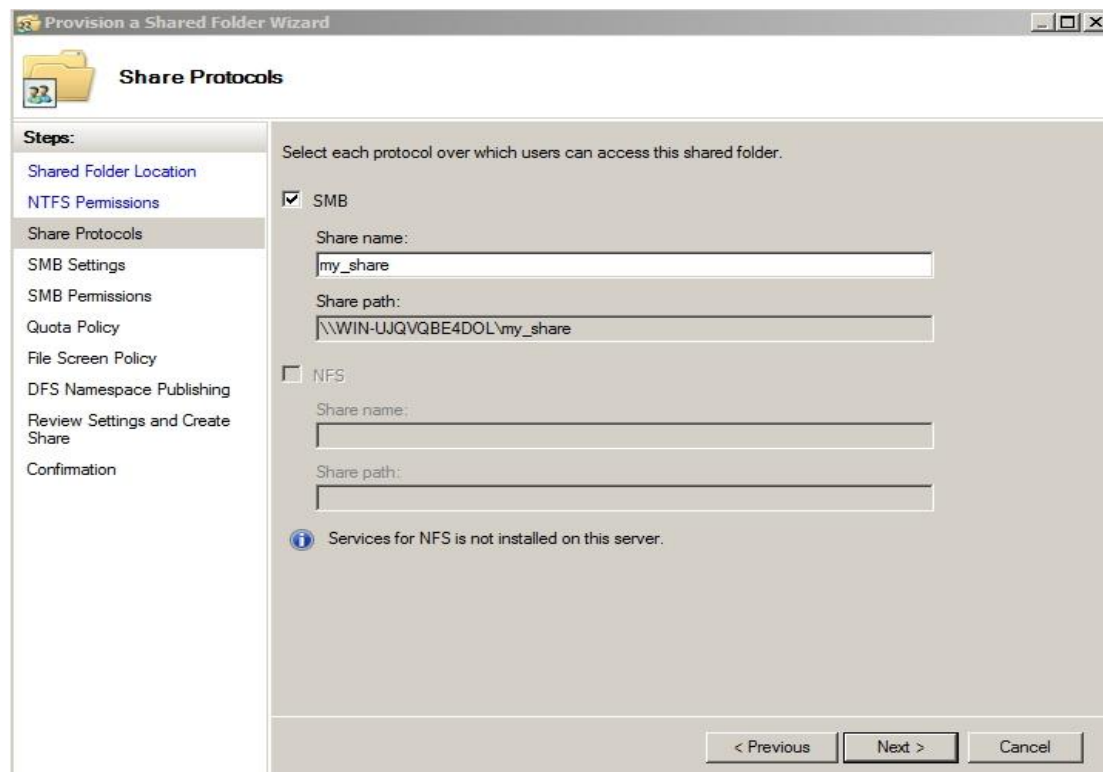
Εικ. 8.14. Provision share wizard.

Μπορούμε να αφήσουμε τα προκαθορισμένα NTFS δικαιώματα ή να τα τροποποιήσουμε ανάλογα (Εικ. 8.15).

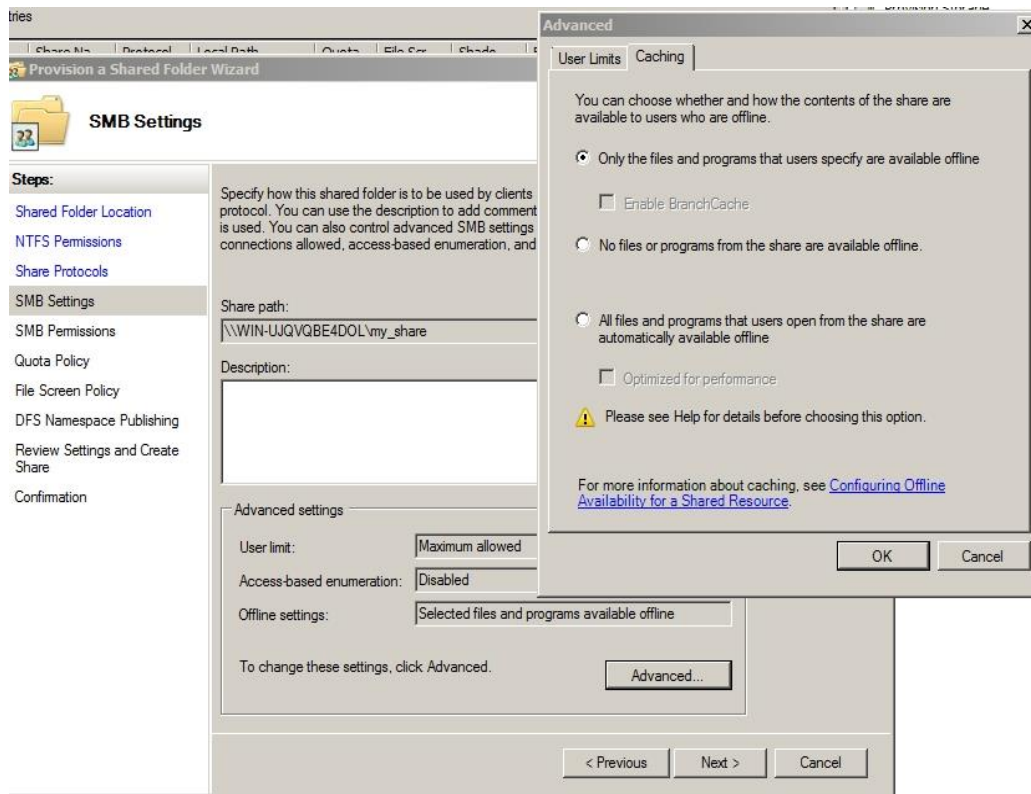


Εικ. 8.15. Provision share wizard, δικαιώματα NTFS.

Επιλέγουμε Πρωτόκολλο (Εικ. 8.16) και έχουμε την δυνατότητα ρύθμισης **user limits** (αριθμός χρηστών) και **caching**, που θα αναλύσουμε σε επόμενες ενότητες (Εικ. 8.17).

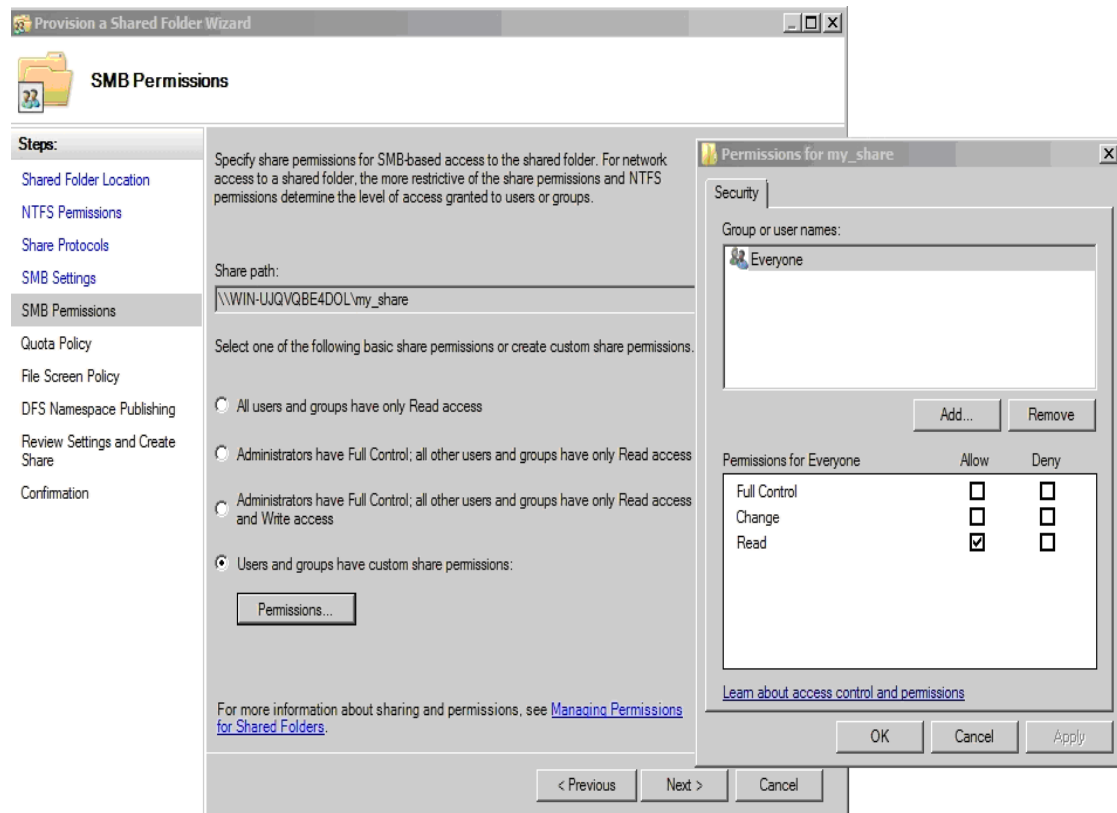


Εικ. 8.16. Provision share wizard, επιλογή πρωτοκόλλου.



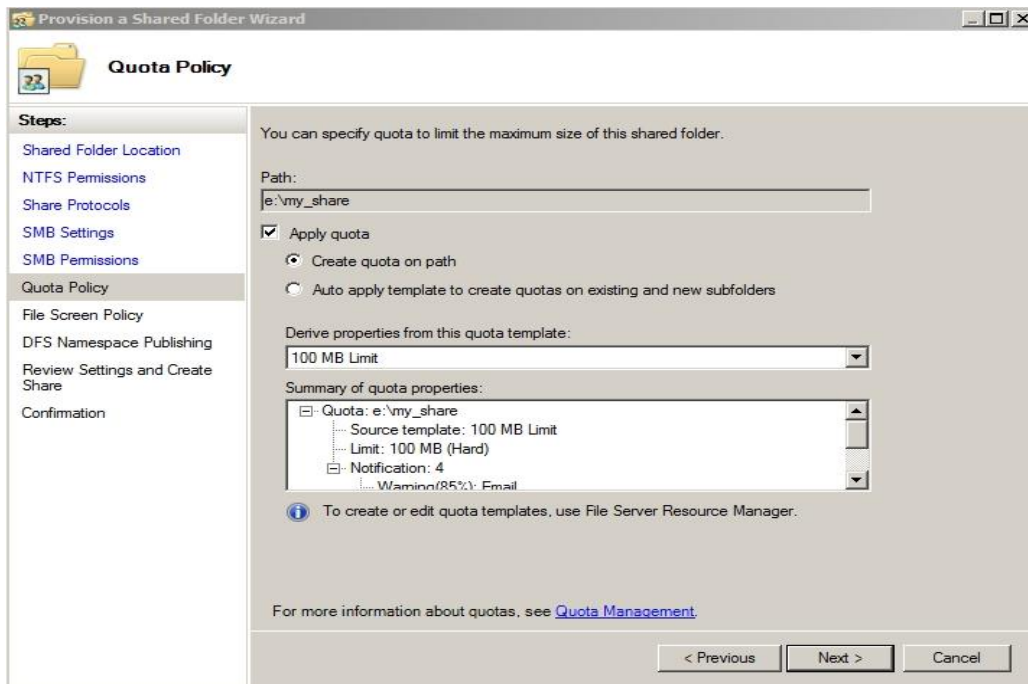
Εικ. 8.17. Provision share wizard, user limits & caching.

Μπορούμε να αφήσουμε τα προκαθορισμένα Shared δικαιώματα ή να τα τροποποιήσουμε ανάλογα (Εικ. 8.18).



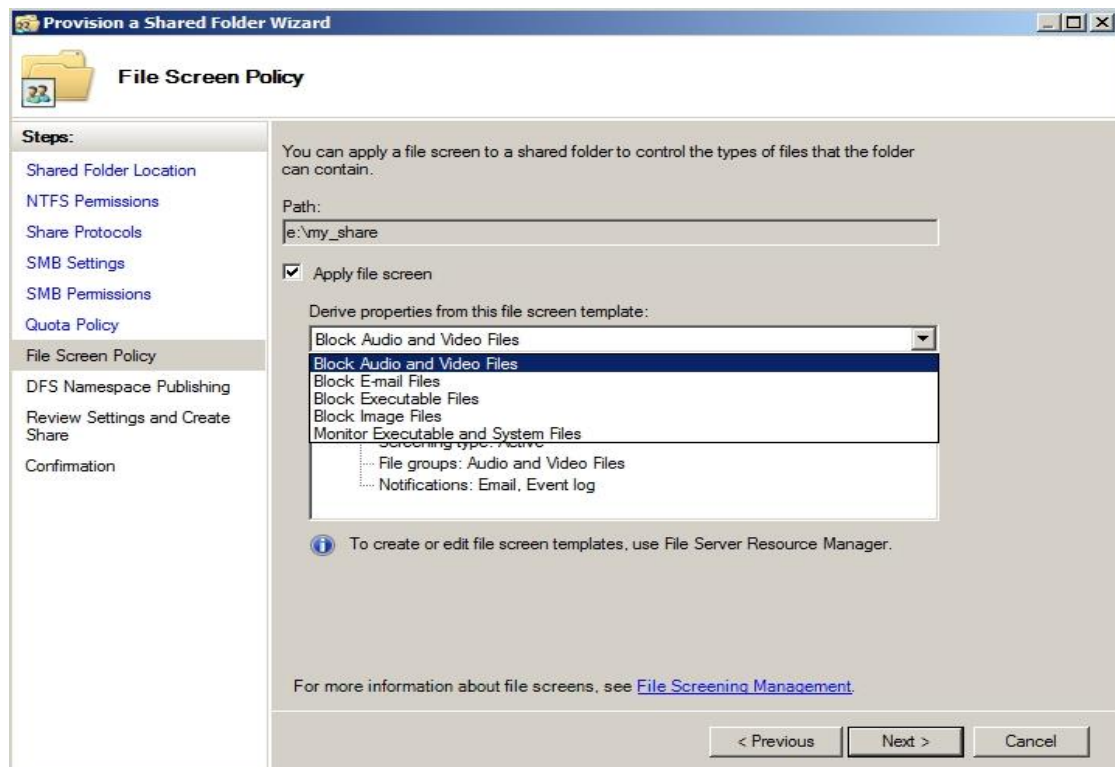
Εικ. 8.18. Provision share wizard, shared δικαιώματα.

Ακολουθούν δυνατότητες quotas (αναλύεται στην ενότητα 9) (Εικ.8.19), File screen policy (Εικ. 8.20),

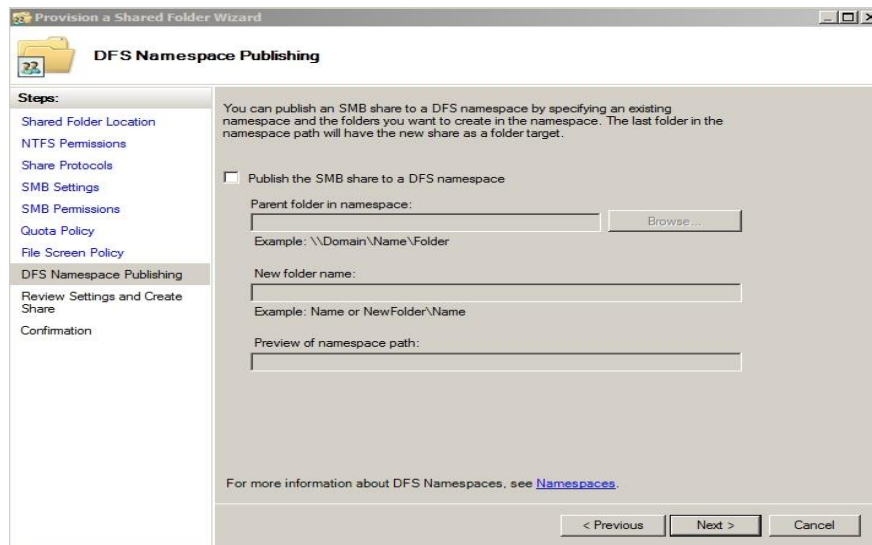


Εικ. 8.19. Provision share wizard, quotas.

η οποία μας δίνει δυνατότητες φιλτραρίσματος του φακέλου για συγκεκριμένους τύπους αρχείων και παρουσίασης του κοινόχρηστου φακέλου (Εικ. 8.21) μέσω του Distribute file system (DFS).

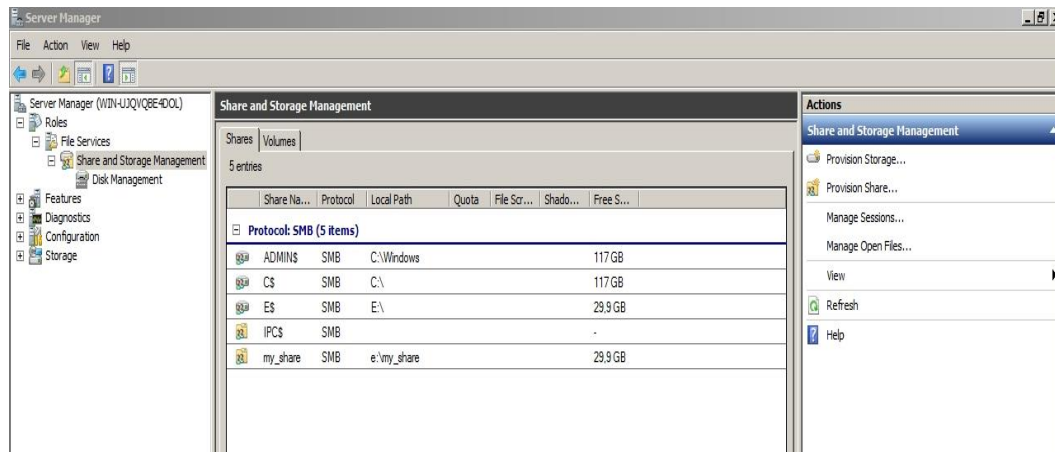


Εικ. 8.20. Provision share wizard, file screen policy.



Εικ. 8.21. Provision share wizard, DFS publishing.

Τελικά έχουμε την Εικ. 8.22, στην οποία εμφανίζεται ο κοινόχρηστος πόρος.



Εικ. 8.22. Provision share wizard, ολοκλήρωση shared folder.

Επιλέγοντας οποιονδήποτε φάκελο και κάνοντας δεξί κλικ μπορούμε, όποτε θελήσουμε, να σταματήσουμε τον διαμοιρασμό ή να τροποποιήσουμε τις ιδιότητες του φακέλου (sharing-permissions), όπως παρουσιάστηκε πιο πάνω.

Η επιλογή **Manage sessions** στο panel **Action** μας παρέχει την δυνατότητα να παρακολουθούμε ποιος χρήστης είναι συνδεδεμένος κάθε στιγμή και να διακόψουμε οποιαδήποτε σύνδεση, όποτε χρειαστεί.

Η επιλογή **Manage Open Files** στο panel **Action** παρουσιάζει τα αρχεία που έχουν προσπελαστεί και τον χρήστη που τα χειρίζεται στον κοινόχρηστο φάκελο και έχουμε την δυνατότητα να κλείσουμε όποιον απαιτείται.

Και οι δύο πιο πάνω διακοπές είναι δυνατόν να προκαλέσουν χάσιμο δεδομένων από πλευράς χρηστών.

Μέσα μόνο από το **Share and Storage management** υπάρχει η δυνατότητα να

συνδεθούμε σε άλλον Η/Υ, για να διαχειριστούμε κοινόχρηστους πόρους και αποθηκευτικά μέσα. Με δεξί κλικ στην κονσόλα στο **Share and Storage management** επιλέγουμε **Connect to another Computer**, κλικ στο another computer και γράφουμε το όνομα του server ή επιλέγουμε Browse και βρίσκουμε τον απομακρυσμένο Η/Υ. Απαραίτητες προϋποθέσεις:

- Στον τοπικό υπολογιστή πρέπει να γίνει login με domain account που να είναι μέλος της ομάδας administrators του απομακρυσμένου Η/Υ.
- Το απομακρυσμένο μηχάνημα να έχει λειτουργικό Windows Server 2008 ή νεώτερο.
- Στο firewall και των δύο υπολογιστών να έχει δοθεί άδεια στο Remote Volume Management.

8.4.4 Διαχείριση αποθηκευτικών χώρων

Ένα επιπλέον εργαλείο που παρέχεται μέσω του **Share and Storage management**, είναι η **διαχείριση αποθηκευτικών χώρων** με την ευρύτερη έννοια των τοπικών σκληρών δίσκων και αποθηκευτικών υποσυστημάτων που υποστηρίζουν Virtual Disk Service (VDS).

Με έναν αντίστοιχο οδηγό, ο οποίος ονομάζεται **Provision Storage Wizard**, μπορούμε να εκτελέσουμε όλες τις αναγκαίες εργασίες που αφορούν την διαχείριση δίσκων (Αρχικοποίηση, μορφοποίηση, δημιουργία, διαγραφή partition-volume) και που αναλυτικά θα αναπτυχθούν στην ενότητα 9.

Η ιδιαιτερότητα της συγκεκριμένης κονσόλας είναι ότι μας δίνει την δυνατότητα να δημιουργήσουμε **Logical Unit Numbers (LUNs)** για Οπτικά κανάλια (fiber channels) και iSCSI υποσυστήματα δίσκων που ενώνονται στο Server. Ταυτόχρονα μπορούμε να δημιουργήσουμε τομείς και να τους μορφοποιήσουμε ανάλογα, με διαδικασίες ανάλογες του Disk management.

Ένα LUN είναι μια λογική αναφορά σε ένα τμήμα κάποιου αποθηκευτικού υποσυστήματος και διευκολύνει στην διαχείριση των αποθηκευτικών πόρων, διότι χρησιμοποιούνται σαν λογικοί προσδιοριστές, στους οποίους μπορούμε να αναθέσουμε δικαιώματα πρόσβασης και ελέγχου.

8.4.5 Shadow copies of Share folders

Shadow copies κοινόχρηστων φακέλων είναι μία δυνατότητα, που παρέχεται στον windows server 2008 και νεώτερο, με την οποία παρέχονται «point in time»

αντίγραφα των αρχείων που βρίσκονται μέσα στους κοινόχρηστους πόρους ενός file server.

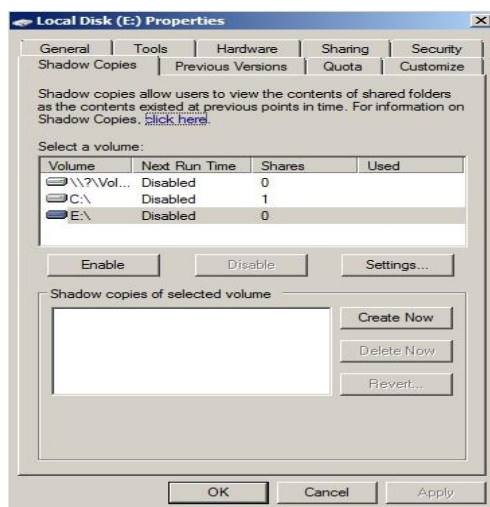
Ο χρήστης, δηλαδή, έχει την δυνατότητα να «δει» κοινόχρηστα αρχεία και φακέλους όπως ήταν κάποια στιγμή στο παρελθόν και να επαναφέρει κάποια που διαγράφηκαν κατά λάθος ή αυτά που έγιναν «overwrite» καθώς και να συγκρίνει αρχεία με προηγούμενη έκδοση τους την στιγμή που «γραφεί».

Ορισμένα επιπρόσθετα χαρακτηριστικά που πρέπει να λαμβάνονται υπόψη είναι:

- Όταν επαναφέρεται ένα αρχείο, τα δικαιώματα που είχε δεν αλλάζουν.
- Όταν επαναφέρεται αρχείο, που διαγράφηκε κατά λάθος, τα δικαιώματά του θα γίνουν ίδια με τα προεπιλεγμένα του φακέλου όπου τοποθετείται.
- Τα Shadow copies δεν αντικαθιστούν το backup.
- Όταν ο αποθηκευτικός χώρος των shadow copies περιορίζεται, τότε αυτόματα διαγράφεται για εξοικονόμηση χώρου το παλαιότερο shadow copy και δεν είναι δυνατόν να το επαναφέρουμε.
- Μέχρι 64 shadow copies μπορούν να αποθηκευτούν και μετά διαγράφεται το παλαιότερο.
- Το shadow copy δεν μπορούμε να το επεξεργαστούμε, απλά μόνο να το «διαβάσουμε» (Read only).
- Το shadow copy δημιουργείται ανά τόμο και δεν μπορούμε να ορίσουμε ποια αρχεία θέλουμε να αντιγράφονται και ποια όχι.

Για να ενεργοποιήσουμε τα shadow copies μπορούμε με:

- Start → Administrative tools → Computer Management → Share folders → All tasks → Configure Shadow Copies ή

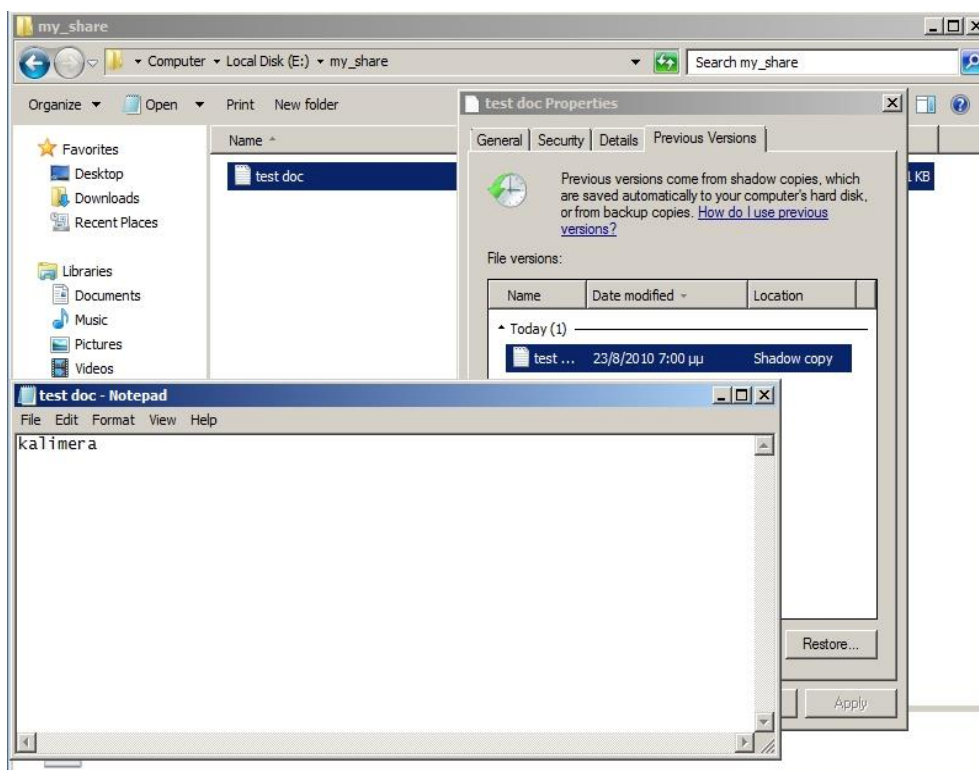


Εικ. 8.23. Shadow copies.

- My computer, οποιοδήποτε drive δεξί κλικ, properties καρτέλα shadow copies.

Εμφανίζεται η Εικ. 8.23, στην οποία μπορούμε να επιλέξουμε τον τόμο που θέλουμε και να κάνουμε **enable**. Σαν προεπιλογή αυτόματα θα δημιουργείται κάθε μέρα ένα shadow copy και αν θέλουμε να επέμβουμε στις ρυθμίσεις επιλέγουμε **settings** και τροποποιούμε ανάλογα.

Στην Εικ. 8.24 θέλουμε να δούμε πως ήταν το αρχείο test σε προηγούμενη κατάσταση. Κάνουμε στο όνομα δεξί κλικ, properties, previous versions και εμφανίζεται η λίστα με τα shadow copies. Διαλέγουμε αυτό που επιθυμούμε και έχουμε δυνατότητες open, copy σε κάποιο σημείο και restore στην φυσική του θέση.



Εικ. 8.24. Shadow copy έλεγχος προηγούμενου αρχείου.

8.5 Offline caching

Είναι η δυνατότητα να ρυθμίσουμε αν και πώς τα αρχεία και οι φάκελοι που βρίσκονται σε έναν κοινόχρηστο φάκελο, θα είναι διαθέσιμα στους χρήστες, όταν δεν θα υπάρχει επικοινωνία, για οποιονδήποτε λόγο, με τον φάκελο.

Οι χρήστες είναι δυνατόν να «δουλεύουν» με τον κοινόχρηστο φάκελο, ακόμα και όταν αυτός δεν είναι διαθέσιμος, λόγω του offline caching, δηλαδή, της δυνατότητας να αποθηκεύονται στον τοπικό δίσκο του χρήστη σε προκαθορισμένο χώρο (local cache) αντίγραφα των κοινόχρηστων αρχείων. Όταν διακοπεί η σύνδεση, ο χρήστης

εργάζεται τοπικά και οι αλλαγές μεταφέρονται αυτόματα όταν αποκατασταθεί η σύνδεση.

Με την δημιουργία κοινοχρήστου φακέλου, αυτόματα επιτρέπεται το offline caching. Αυτό, όμως, σημαίνει ότι δεδομένα που αποθηκεύονται σε έναν ασφαλισμένο κοινόχρηστο χώρο, βρίσκονται ταυτόχρονα και αποθηκευμένα τοπικά στην cache ενός μη ασφαλούς Η/Υ. Για τον λόγο αυτό προτείνεται να μην επιτρέπεται στους χρήστες να υποθηκεύουν offline.

Στην εικόνα 8.17 συναντήσαμε την φόρμα διαχείρισης του offline caching αλλά μπορούμε να έχουμε πρόσβαση και από τον κοινόχρηστο φάκελο, δεξί κλικ properties, καρτέλα sharing, advanced sharing και κλικ στο caching όπου εμφανίζεται η Εικ. 8.25.

Οι δυνατές επιλογές είναι:

- Μόνο τα προγράμματα και τα αρχεία που καθορίζει ο χρήστης, να είναι διαθέσιμα offline.
- Τίποτα να μην είναι διαθέσιμο offline.
- Όλα τα αρχεία και τα προγράμματα που «ανοίγει» ο χρήστης στον κοινόχρηστο φάκελο να είναι διαθέσιμα offline.



Εικ. 8.25. Offline Caching.

- **Optimize for performance:** Αν επιλεγεί, εκτελέσιμα αρχεία που βρίσκονται στον κοινόχρηστο φάκελο και εκτελούνται μια φορά από τον χρήστη, αυτόματα γίνονται cached στον Η/Υ του χρήστη και την επόμενη φορά που θα επιλέξει ο χρήστης να τα

εκτελέσει από τον κοινό φάκελο, αυτόματα θα φορτωθούν από την τοπική cache μειώνοντας τον φόρτο στον server και το δίκτυο.

- **Enable Branch Cache:** Δυνατότητα που καθιστά έναν H/Y σε ένα υποκατάστημα (Branch office) να τοποθετεί στην cache του αρχεία από τον κοινόχρηστο φάκελο και στην συνέχεια να τα διαμοιράζει στους υπολοίπους υπολογιστές του καταστήματος με ασφάλεια.

8.6 Υλοποίηση και διαχείριση εκτυπώσεων

Σε υπολογιστή με Windows Server 2008 και νεώτερο, μπορούμε να κάνουμε κοινή χρήση των εκτυπωτών στο δίκτυο, να εκτελούμε κεντρικά εκτυπώσεις και να διαχειριζόμαστε εργασίες εκτυπώσεων χρησιμοποιώντας το Print Management snap-in σε mmc.

Η κονσόλα Print Management μας βοηθά να παρακολουθούμε τις ουρές εκτύπωσης και να λαμβάνουμε ενημερωτικά μηνύματα, όταν μια ουρά σταματήσει την εξυπηρέτηση των εκτυπώσεων. Επίσης παρέχει τη δυνατότητα να μεταφέρουμε (migrate) υπάρχοντες print servers και να υλοποιούμε συνδέσεις εκτυπωτών με Group Policy (GPO).

8.6.1 Εγκατάσταση και κοινή χρήση εκτυπωτών

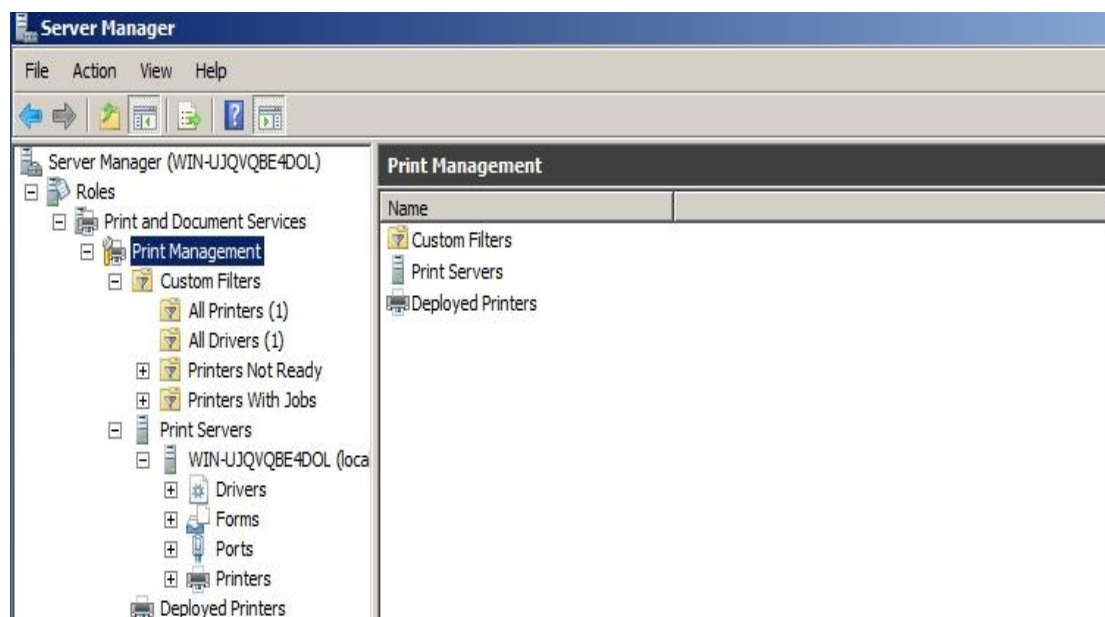
Στον Windows Server 2008 υπάρχει ένας ρόλος για να διαμοιράζουμε κοινόχρηστους εκτυπωτές στο δίκτυο, να εγκαθιστούμε print servers και κεντρικούς εκτυπωτές, ο οποίος ονομάζεται **Print and Document Service Role**. Ο ίδιος ρόλος διαχειρίζεται και scanners.

Η εγκατάσταση του ρόλου πραγματοποιείται από **το Start → Administrative Tools → Server Manager → Roles → Add role** και ακολουθώντας τον οδηγό επιλέγουμε **Print and Document Service** και μετά εμφανίζονται τα services:

- **Print Server Role Service:** Εγκαθιστά το Print management snap-in, με το οποίο, διαχειριζόμαστε πολλούς δικτυακούς printers ή print server και μπορούμε να μεταφέρουμε printers προς και από άλλους windows print servers.
- **LPD Service Role Service:** Εγκαθιστά και ξεκινά το TCP/IP Print Server service, το οποίο δίνει την δυνατότητα σε υπολογιστές με λειτουργικό UNIX-based ή και άλλους που χρησιμοποιούν Line Printer Remote (LPR) service, να εκτυπώνουν σε κοινόχρηστους εκτυπωτές μέσω του Server.
- **Internet Printing Role Service:** Δημιουργεί ένα Web site που φιλοξενείται από το Internet Information Service (IIS). Μέσω του Site οι χρήστες διαχειρίζονται

εκτυπωτικές εργασίες στον server, ενώ ταυτόχρονα μπορούν να ενώνονται σε κοινόχρηστους εκτυπωτές χρησιμοποιώντας το Internet Printing Protocol (IPP) σε συνδυασμό με Internet Printing Client.

- **Distribute Scan Server Role Service:** Εγκαθιστά το Scan Management snap-in, με το οποίο μπορούμε να παρακολουθούμε πολλαπλούς δικτυακούς scanners, να ρυθμίζουμε Scan servers, να εκτελούμε διεργασίες σάρωσης εγγράφων και να τα δρομολογούμε μέσω δικτύου.



Εικ. 8.26. Διαχείριση Εκτυπώσεων.

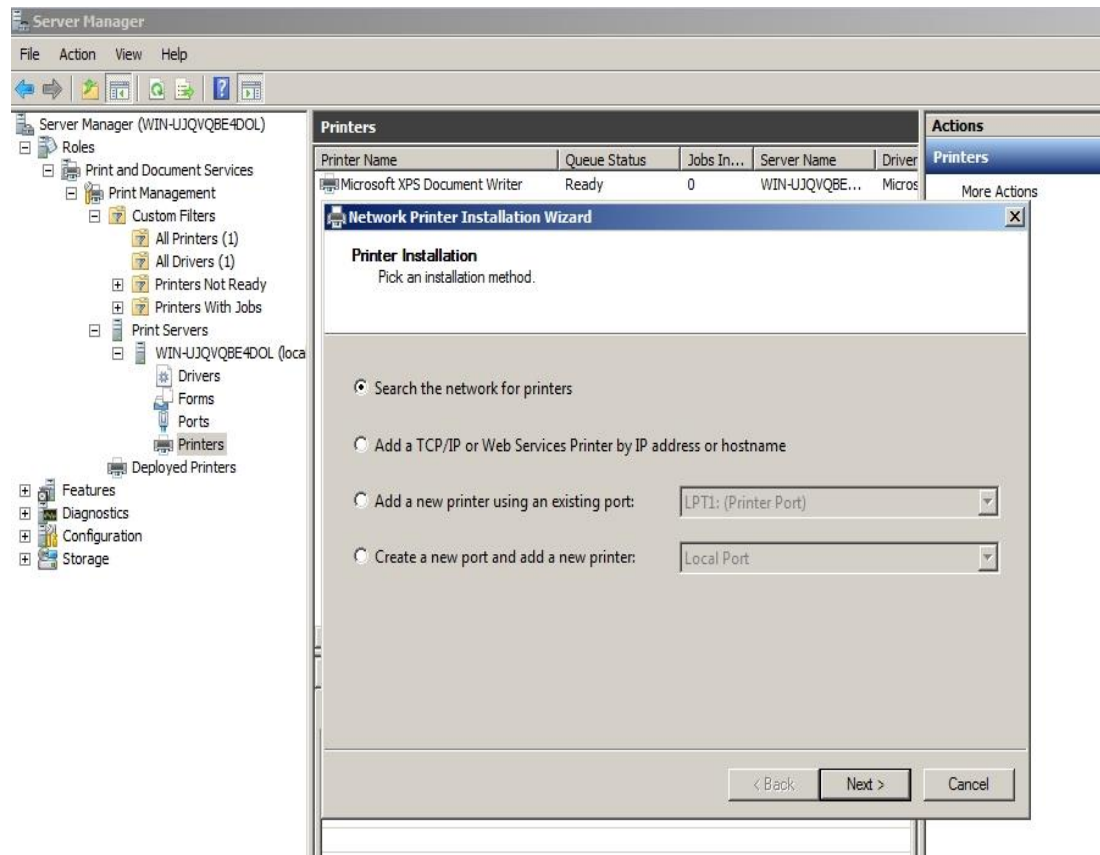
Διαλέγουμε Print server και ολοκληρώνουμε την εγκατάσταση του ρόλου. Κάτω από το δένδρο των ρόλων έχει εγκατασταθεί το **Print and Document Service**, στο οποίο βρίσκεται ο print management (Εικ. 8.26).

Είναι προκαθορισμένο ο print management να διαχειρίζεται τον τοπικό υπολογιστή. Μέσω της κονσόλας υπάρχει δυνατότητα να διαχειριζόμαστε και παρακολουθούμε οποιοδήποτε print server στο δίκτυο αρκεί να τρέχει Windows 2000 και νεώτερο και το προσθέσουμε στο δένδρο με την εξής διαδικασία: Print Management, δεξί κλικ, add/remove servers → specify print server → όνομα ή browse → Add to List → ok (Αφαίρεση με την ίδια διαδικασία και remove αντί για add).

Για όλες τις ρυθμίσεις πρέπει απαραίτητα να ανήκουμε στην ομάδα των administrators ή να έχουμε δικαιώματα Manage Server.

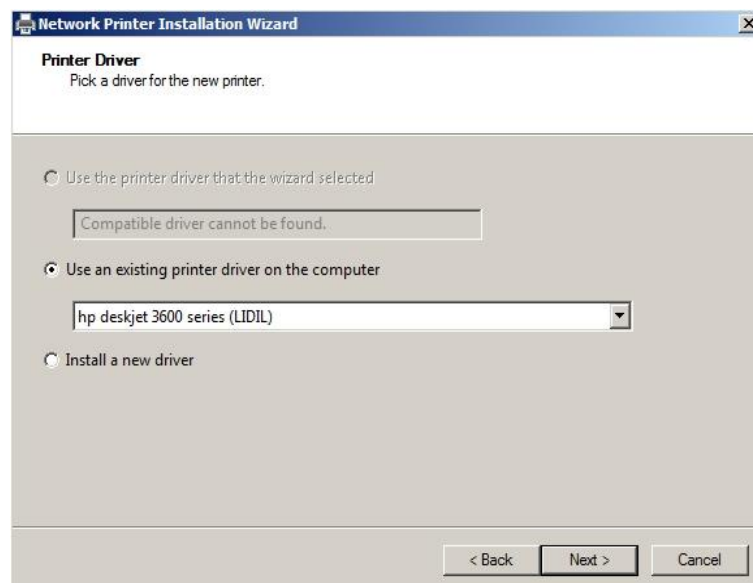
Μπορούμε να εγκαταστήσουμε εκτυπωτές μέσω IP ή hostname αλλά και αυτόματα να βρούμε στο δίκτυο εκτυπωτές, να εγκατασταθούν οι αντίστοιχοι drivers, να ρυθμιστούν οι ουρές και να γίνουν κοινόχρηστοι.

Στο Print Management, print servers, printers, δεξί κλικ, add printer εμφανίζεται ο οδηγός της εικόνας 8.27.



Εικ. 8.27. Προσθήκη εκτυπωτών.

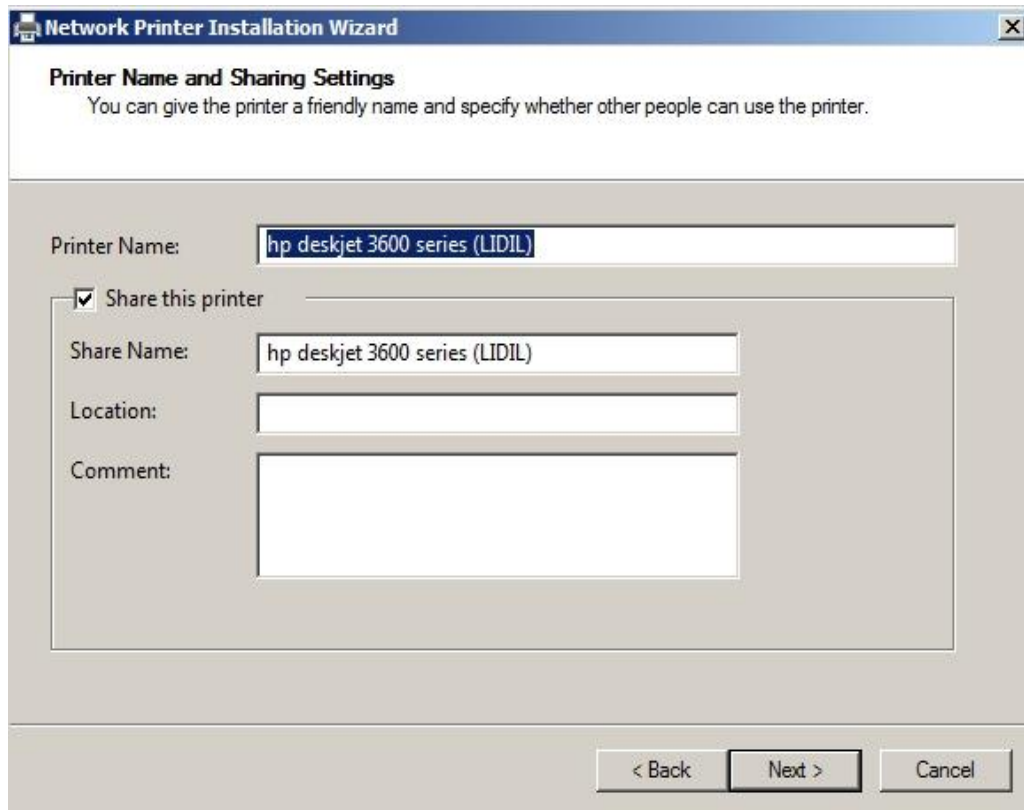
Υπάρχει η δυνατότητα της αυτόματης αναζήτησης, TCP, Web service printer, local port printer αλλά και να δημιουργήσουμε νέα port για νέο εκτυπωτή. Ακολουθεί



Εικ. 8.28. Προσθήκη οδηγών.

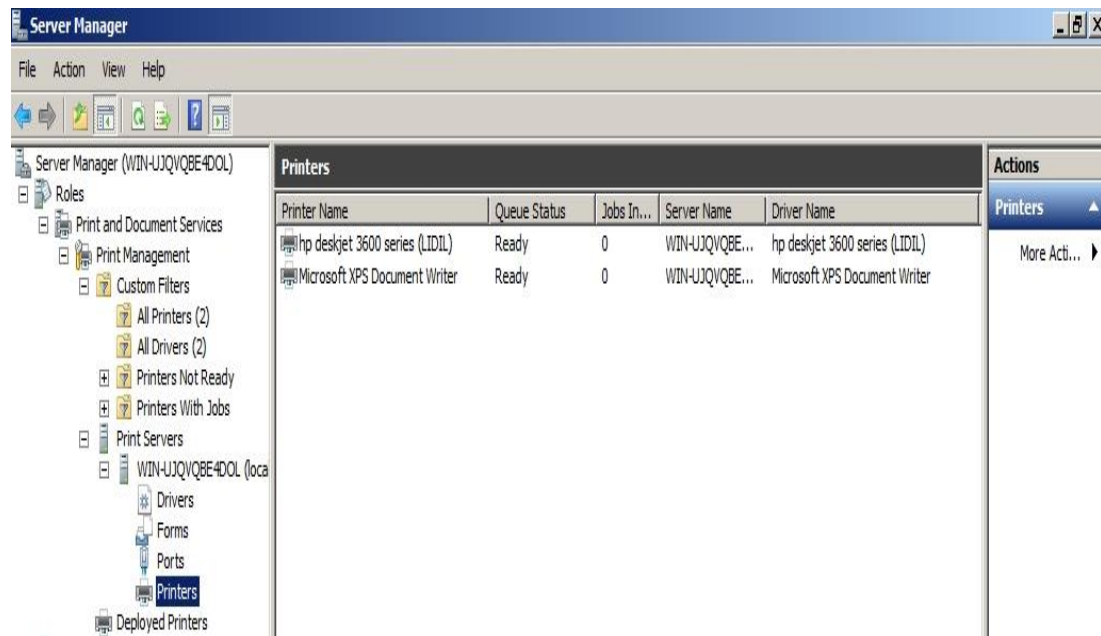
εγκατάσταση των αντίστοιχων οδηγών (Εικ. 8.28), ενώ στην αμέσως επόμενη εικόνα

8.29, μας δίνεται η δυνατότητα να κάνουμε κοινόχρηστο τον εκτυπωτή με ό,τι όνομα επιλέξουμε.



Εικ. 8.29. Επιλογή κοινής χρήσης.

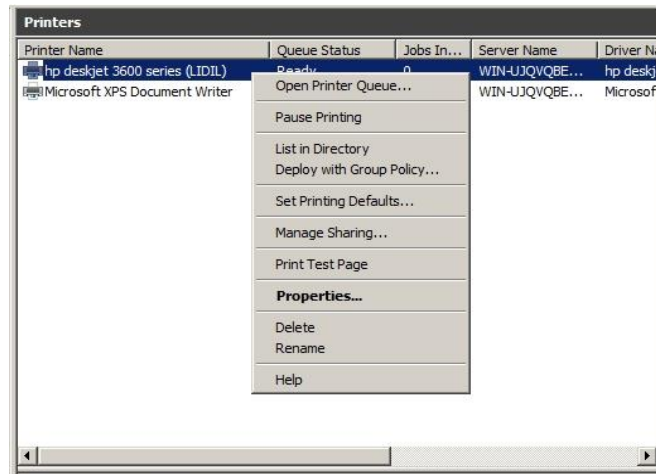
Στην Εικ. 8.30 φαίνεται ο νέος εκτυπωτής (HP 3600) που μόλις εγκαταστήσαμε.



Εικ. 8.30. Εγκατεστημένοι εκτυπωτές.

8.6.2 Διαχείριση πρόσβασης στους εκτυπωτές

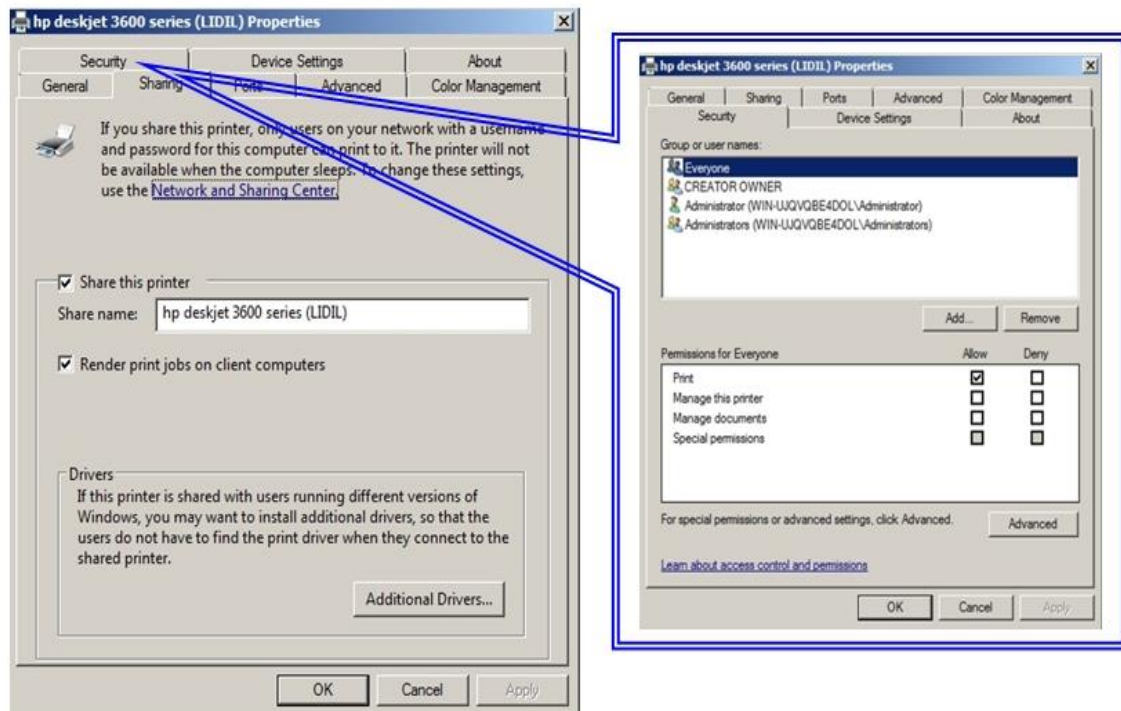
Η όλη διαχείριση μετά την εγκατάσταση των εκτυπωτών καθίσταται απλή. Με δεξί



Εικ. 8.31. Διαχείριση πρόσβασης στους εκτυπωτές.

κλικ στον εκτυπωτή, στον οποίο θέλουμε να καθορίσουμε την πρόσβαση, εμφανίζεται η Εικ. 8.31. Εκεί μπορούμε:

- Open printer queue: Βλέπουμε και διαχειριζόμαστε τις εκτυπώσεις στην ουρά.
- Pause printing: Σταμάτημα εκτυπώσεων.
- List in Directory: Εμφανίζεται στην αναζήτηση στο active directory.
- Deploy with GPO: Διανομή μέσω κατάλληλου ρυθμισμένου GPO.
- Set printers Default: Καθορίζουμε προκαθορισμένα χαρακτηριστικά.
- Manage Sharing: Μπορούμε να ενεργοποιούμε - απενεργοποιούμε το sharing και μέσω της καρτέλας security να ορίζουμε ποιοι θα έχουν πρόσβαση (Εικ. 8.32).



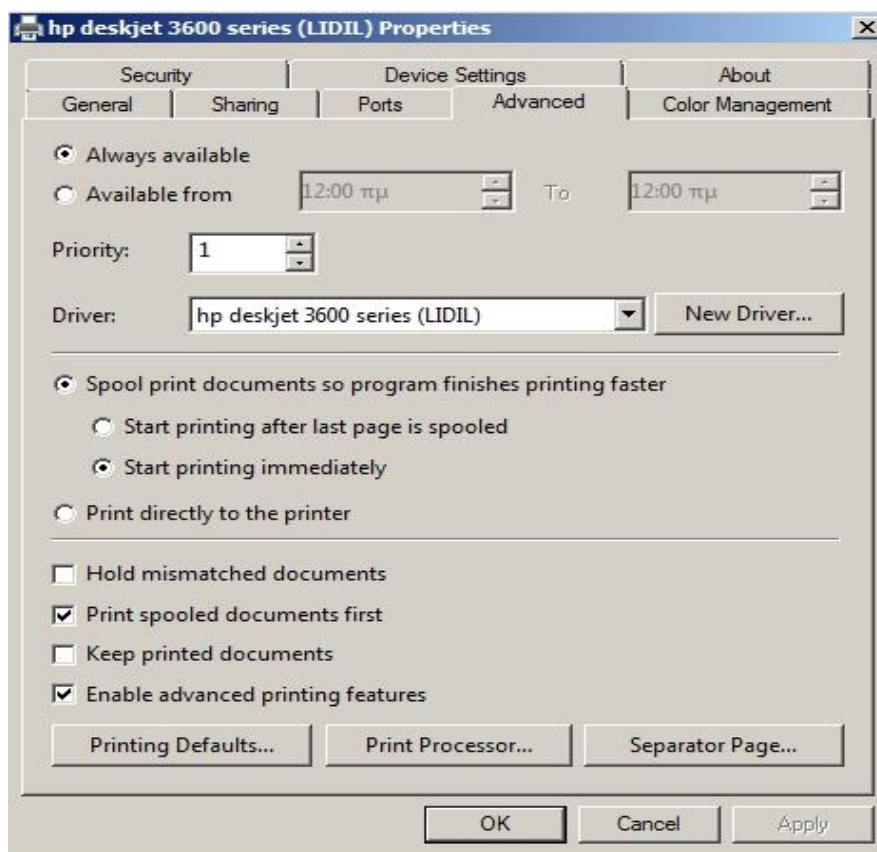
Εικ. 8.32. Διαχείριση Sharing και Security.

8.6.3 Προτεραιότητες εκτυπώσεων – Printer Spooler

Στην εικόνα 8.33 και στην καρτέλα advanced μπορούμε να ορίσουμε προτεραιότητες εκτυπώσεων.

Στο πεδίο priority ορίζουμε προτεραιότητα με το 1 να είναι η χαμηλότερη και το 99 η υψηλότερη.

Μπορούμε τώρα να κάνουμε και δεύτερο ή περισσότερα αντίγραφα ενός εκτυπωτή με add printer και αφού τους δώσουμε διαφορετική προτεραιότητα να τους διαθέσουμε σε διαφορετικούς χρήστες.

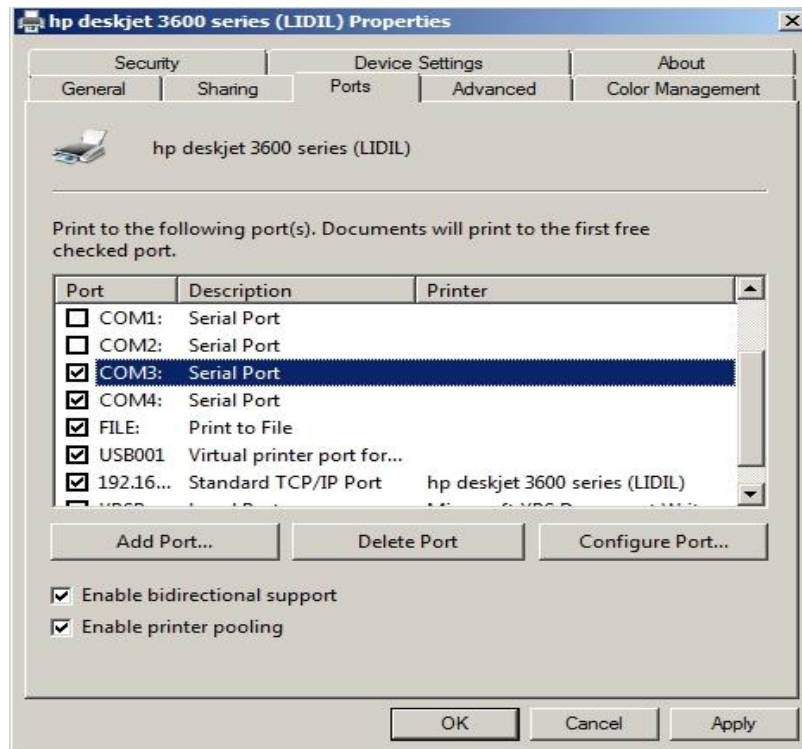


Εικ. 8.33. Printer Priority.

Οι χρήστες θα εκτυπώνουν τώρα ανάλογα με την προτεραιότητά τους (Υψηλότερη πρώτα από την χαμηλότερη)

Μια άλλη δυνατότητα που μας προσφέρεται (Εικ. 8.34), είναι το printing pooling με το οποίο διανέμουμε τις εξόδους εκτύπωσης μέσω ενός συνόλου από διάφορους εκτυπωτές. Το βασικότερο πλεονέκτημα που κερδίζουμε είναι το ότι εκτυπώνουμε σε δύο ή περισσότερους, φθηνότερους εκτυπωτές, αντί για έναν ακριβότερο όπως και το ότι υπάρχει backup εκτυπωτής σε περίπτωση που κάποιος εκτυπωτής χαλάσει.

Επιλέγοντας Enable printer pooling έχουμε την δυνατότητα να χρησιμοποιήσουμε και άλλα ports με αντίστοιχους εκτυπωτές.



Εικ. 8.34. Printer pooling.

Αν όλοι οι εκτυπωτές είναι του ίδιου τύπου, τότε όλα είναι εύκολα. Αν είναι διαφορετικοί, τότε ίσως θα έχουμε πρόβλημα με τον τύπο των οδηγών που θα χρησιμοποιήσουμε. Γενικά χρησιμοποιούμε εκτυπωτές του ίδιου κατασκευαστή, διότι υπάρχει driver backwards compatibility και αν χρησιμοποιήσουμε σαν βασικό τον «παλαιότερο» οδηγό θα λειτουργήσουν και οι νεότεροι εκτυπωτές.

ΔΙΣΚΟΙ & ΑΠΟΘΗΚΕΥΣΗ ΔΕΔΟΜΕΝΩΝ

9.1 Εισαγωγή

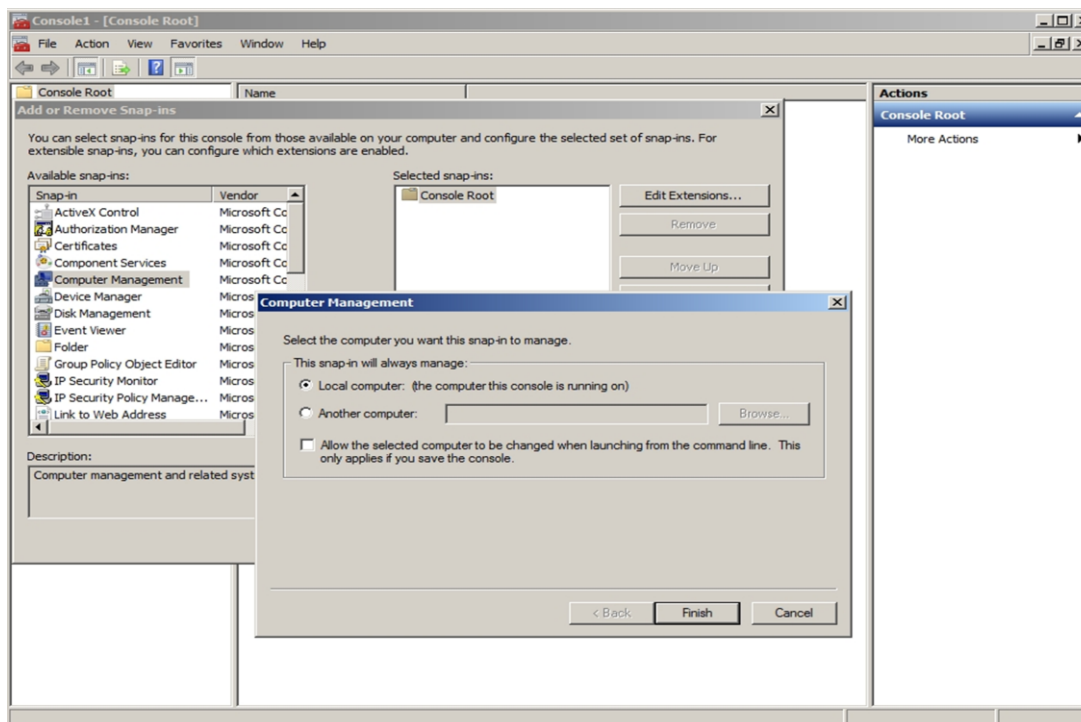
Οι επιθυμητές γνώσεις και δεξιότητες που θα αποκτήσουν οι επιμορφωμένοι στην ενότητα Δίσκοι & Αποθήκευση Δεδομένων, θα τους καταστήσουν ικανούς να :

- Αναγνωρίζουν έννοιες (Volumes, partitions) και να υλοποιούν εργασίες σχετικές με τους δίσκους (Hard Disks) σε έναν Server 2008, όπως μετατροπές basic to dynamic disks.
- Εκτελούν εργασίες διαχείρισης σε τόμους, όπως κρυπτογράφηση, συμπίεση, quotas.
- Γνωρίζουν και υλοποιούν τις διάφορες υλοποιήσεις RAID, όπως striped volume (0), mirrored volume (1), striped with parity (5).

9.2 Διαχείριση Δίσκων (Disks Management)

Το εργαλείο που χρησιμοποιείται από το σύστημα για την διαχείριση των δίσκων ονομάζεται **Disk Management** και είναι προσβάσιμο από διάφορα σημεία ενός server 2008 και ειδικότερα:

- Start --> Administrative tools --> Server Manager --> Storage --> Disk Management, όπου έχουμε άμεση πρόσβαση στους δίσκους του συγκεκριμένου συστήματος.



Εικ. 9.1. Computer Management σε mmc.

- Start --> Run, γράφουμε mmc και πατάμε ok. Στην κονσόλα που εμφανίζεται επιλέγουμε File --> Add/Remove Snap-in --> Computer Management και Add, όπου εμφανίζεται η δυνατότητα να ενωθούμε τοπικά ή απομακρυσμένα (remotely) στους δίσκους κάποιου H/Y (Εικ 9.1).

Με το Disk management του Windows Server 2008 R2 έχουμε την δυνατότητα χωρίς επανεκκίνηση ή ενόχληση των χρηστών να:

- Αρχικοποιούμε δίσκους (Initialize Disks)
- Διαχειριζόμαστε δίσκους (Create, modify, delete partitions, volumes)
- Μορφοποιούμε δίσκους (Format disks)
- Δημιουργούμε basic, spanned ή striped partitions, με ένα απλό δεξί κλικ, κατευθείαν από το μενού.
- Μετατρέπουμε MBR σε GUID (GPT)
- Μεγαλώνουμε και μικραίνουμε partitions μέσα από τα windows.

9.2.1 Βασικοί Ορισμοί

Master Boot Record (MBR)

MBR ή **partition sector** είναι ο BOOT τομέας ενός σκληρού δίσκου ό οποίος περιέχει το partition table και το σημείο που το BIOS δίνει την σκυτάλη για να εκκινήσει (μέσω μηχανισμών bootstrapping) το λειτουργικό σύστημα. Δεν βρίσκεται σε partition αλλά είναι στην αρχή των partitions. Έχει περιορισμούς στα primary partitions (έως 4) και στην μέγιστη χωρητικότητα (<2TB).

GUID Partition Table.

Το GUID Partition Table (GPT) αποτελεί το σύγχρονο τύπο για το partition table σε έναν φυσικό δίσκο. Είναι μέρος της τυποποίησης EFI (Extensible Firmware Interface) και ξεπερνά τους περιορισμούς που έχει το MBR. Συγκεκριμένα υποστηρίζει μέχρι 128 primary partitions και δίσκους χωρητικότητας >2TB.

Βασικός δίσκος (Basic disk).

Κάθε δίσκος είναι εξ ορισμού basic. Χωρίζεται σε ένα ή περισσότερα διαμερίσματα (partitions) με ένα λογικό δίσκο (logical drive) στο πρωτεύον διαμέρισμα και έναν ή περισσότερους λογικούς δίσκους στα εκτεταμένα διαμερίσματα (extended partitions). Ο βασικός δίσκος δεν υποστηρίζει τις περισσότερες προηγμένες λειτουργίες της διαχείρισης δίσκων αλλά μπορεί να μετατραπεί, υπό προϋποθέσεις, σε δυναμικό.

Δυναμικός δίσκος (Dynamic disk).

Σε αυτόν δημιουργούνται τόμοι (volumes) και αποτελεί τη βάση για την εφαρμογή

νέων τεχνολογιών (προηγμένες λειτουργίες) χρησιμοποίησης και εκμετάλλευσης, περισσότερων του ενός, δίσκων (Mirroring, Striped, RAID). Μπορεί να μετατραπεί, υπό προϋποθέσεις, σε Βασικό.

Τόμος (Volume): Μονάδα χώρου που αποτελείται από ένα ή περισσότερα τμήματα ενός ή περισσότερων δυναμικών δίσκων.

Απλός τόμος (Simple volume): Το αντίστοιχο ενός διαμερίσματος (partition). Μπορεί να συνδεθεί (mount) σε ένα ή περισσότερα σημεία σύνδεσης (mount points).

RAID (Redundant Array of Independent Disks): Τεχνολογία που επιτρέπει τη χρήση πολλών σκληρών δίσκων σε συστοιχία επιτυγχάνοντας μεγάλη χωρητικότητα, ανοχή σε λάθη και αυξημένη απόδοση. Αναλόγως επιπέδου (π.χ. RAID-0, RAID-1, RAID-5), καθορίζεται και ανάλογος τρόπος λειτουργίας.

Spanned Volume: Λογικός δίσκος, τα τμήματα του οποίου βρίσκονται σε διαφορετικούς φυσικούς δίσκους. Δεν προσφέρει ανοχή σε λάθη, απλά επιτρέπει την καλύτερη εκμετάλλευση των φυσικών δίσκων.

Striped volume: Είναι μια τεχνική (RAID-0) τυχαίου διαχωρισμού δεδομένων σε δύο ή περισσότερους δίσκους χωρίς πλεονασματικές πληροφορίες (redundancy). Δεν προσφέρει ανοχή σε σφάλματα (fault tolerance).

Mirror volume: Ζεύγος δυναμικών δίσκων που περιέχουν τα ίδια δεδομένα (RAID-1) και παρουσιάζονται ως μία ενότητα. Προσφέρει ανοχή σε σφάλματα (fault tolerance).

RAID-5 volume: Λογικός δίσκος, τμήματα του οποίου βρίσκονται σε διαφορετικούς φυσικούς δίσκους. Προσφέρει εξαιρετικό ρυθμό μεταγωγής δεδομένων κατά την ανάγνωση από το λογικό δίσκο και ανοχή σε λάθη. Απαιτείται ελάχιστος αριθμός 3 δίσκων για να υλοποιηθεί και προσφέρει ανοχή σε σφάλματα (fault tolerance).

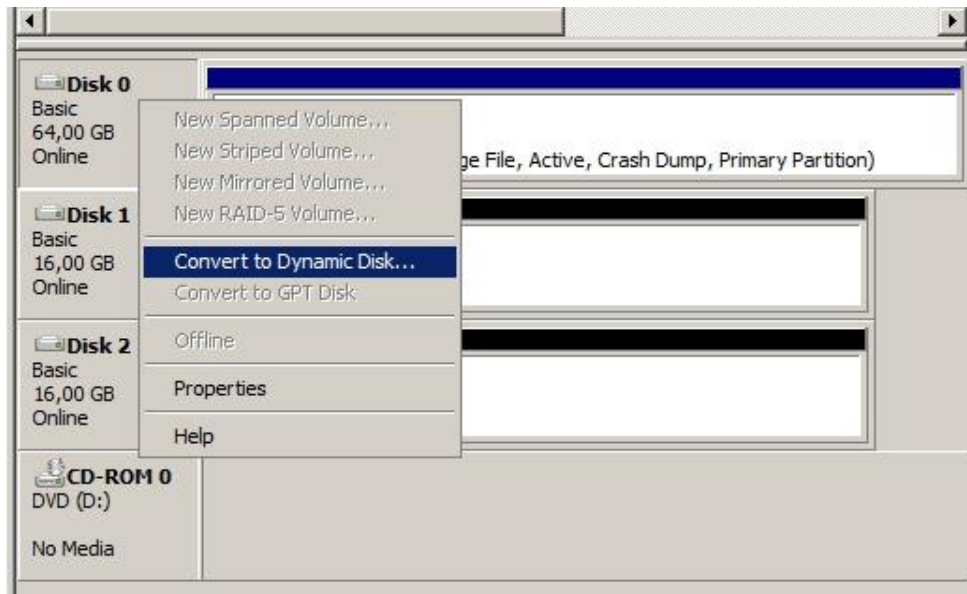
9.2.2 Μετατροπές Δίσκων

Το Disk Management επιτρέπει την μετατροπή μεταξύ των διαφόρων τύπων (MBR, GPT, Basic or Dynamic) των partitions, ώστε να χρησιμοποιείται ο καταλληλότερος για τις εφαρμογές μας.

Παρόλα αυτά, όμως, υπάρχουν οι παρακάτω περιορισμοί:

- **MBR:** Μπορεί να μετατραπεί σε GPT, αρκεί ο δίσκος να μην έχει volumes. Μπορεί να μετατραπεί σε Dynamic, αλλά υπάρχει πιθανότητα να μην κάνει Boot.
- **GPT:** Μπορεί να μετατραπεί σε MBR, αρκεί ο δίσκος να μην έχει volumes. Μπορεί να μετατραπεί σε Dynamic, αλλά υπάρχει πιθανότητα να μην κάνει Boot.

- Basic σε Dynamic: Μετατρέπεται άμεσα έχοντας ή μη δεδομένα. Αρκεί ένα δεξί κλικ και convert to dynamic disk (Εικόνα 9.2). **ΠΡΟΣΟΧΗ όχι μετατροπή σε Multi Boot συστήματα**, διότι κατά την μετατροπή δεν θα ξεκινήσει από άλλο λειτουργικό πλην αυτού που πραγματοποιήθηκε η μετατροπή.



Εικ. 9.2 Μετατροπή basic σε dynamic disk.

- Dynamic σε Basic: Πραγματοποιείται μόνο αν ο δίσκος δεν περιέχει volumes ή δεδομένα. Εφόσον χρειαζόμαστε αυτά που έχει ο δίσκος, πριν την διαγραφή τους παίρνουμε backup και μετά την μετατροπή του δίσκου, κάνουμε restore.
- Οι δυναμικοί δίσκοι δεν υποστηρίζονται σε portable computers, removable disks, USB ή Fire wire (IEEE1394) disks και shared SCSI Buses.
- Δεν έχει νόημα η μετατροπή ενός μόνο δίσκου σε δυναμικό, διότι για να εκμεταλλευτούμε τις προηγμένες δυνατότητες, απαιτούνται δύο ή περισσότεροι δίσκοι.

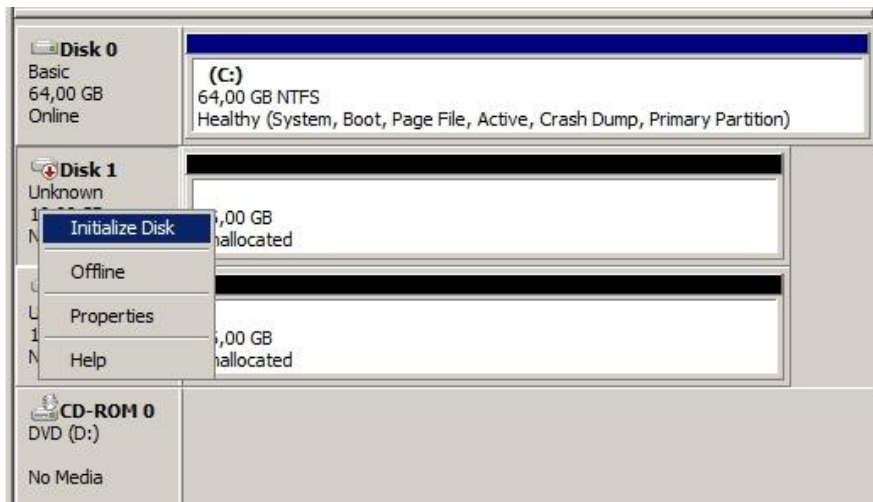
9.2.3 Online, offline status

Το Disk management παρουσιάζει την κατάσταση online ή offline των δίσκων. Στον server 2008 όλοι οι νεοτοποθετούμενοι δίσκοι τίθενται online με read και write access εκτός αν βρίσκονται σε shared bus (SCSI, iSCSI, Serial Attached SCSI, Fiber channel) που τίθενται την πρώτη φορά offline.

Για να αρχικοποιηθεί ένας δίσκος πρέπει να είναι online.

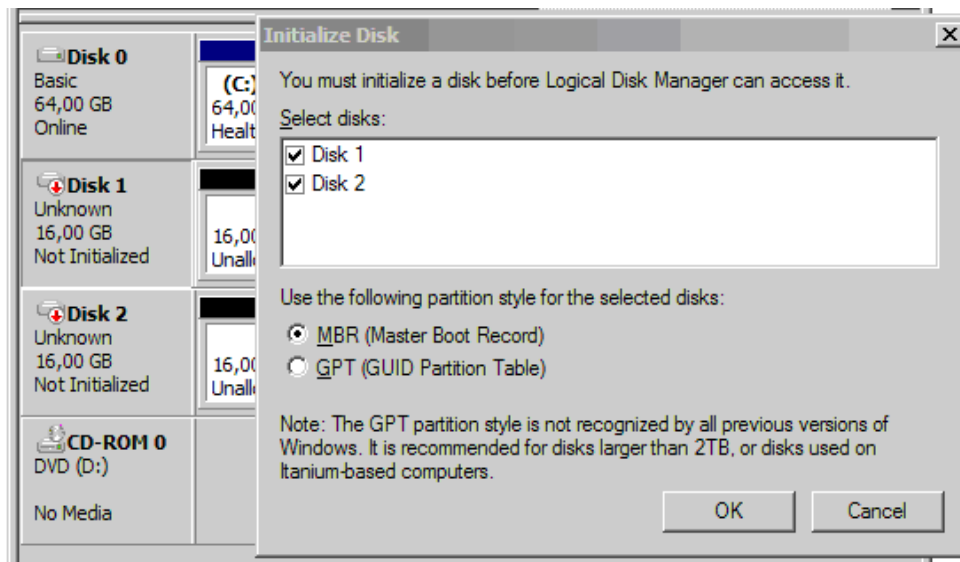
9.2.4 Initializing (Αρχικοποίηση)

Για να μπορεί κάποιος δίσκος να χρησιμοποιηθεί πρέπει να γίνει online και κάνοντας δεξί κλικ στο όνομα του δίσκου (Disk 1, Εικ. 9.3) να αρχικοποιηθεί.



Εικ. 9.3. Αρχικοποίηση Δίσκου (Initializing)

Εμφανίζεται η εικόνα 9.4 η οποία μας ενημερώνει ότι πρέπει να κάνουμε Initializing και μας προτρέπει να διαλέξουμε το style του partition (MBR, GPT).



Εικ. 9.4. Αρχικοποίηση Δίσκου (Initializing)

Ιδιαίτερη **ΠΡΟΣΟΧΗ** ότι το GPT δεν αναγνωρίζεται από παλαιότερα Windows.

Δίσκος που αρχικοποιείται αυτόματα γίνεται Basic και MBR.

Όλες οι ενέργειες πραγματοποιούνται κατελάχιστον από τον Administrator ή Backup Operator.

9.2.5 Μεταφορά δίσκου σε άλλο H/Y

Αν ο δίσκος που πρόκειται να μεταφερθεί είναι basic τότε θα πάρει το επόμενο ελεύθερο γράμμα στον νέο H/Y.

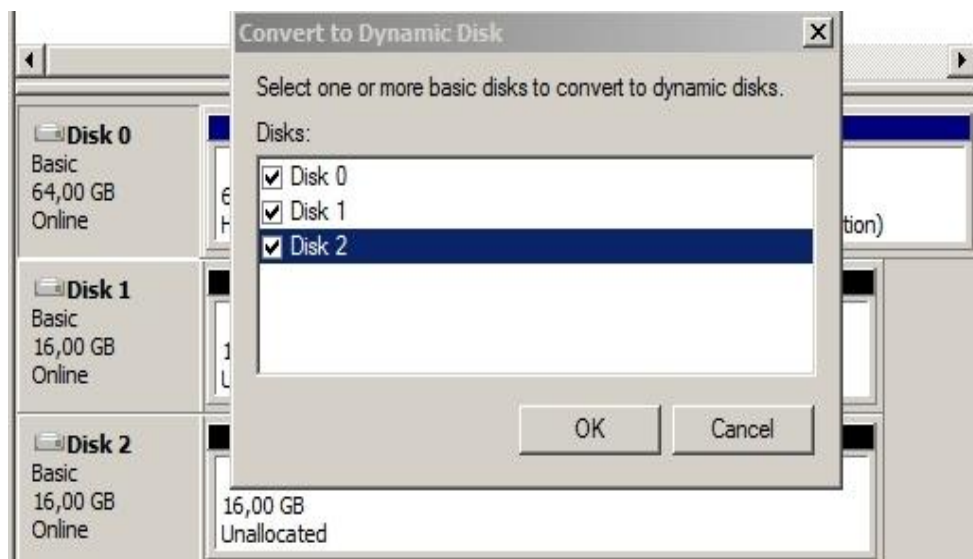
Οι dynamic δίσκοι κρατούν το γράμμα που είχαν στον προηγούμενο υπολογιστή. Αν δεν είχαν δεν παίρνουν αυτόματα νέο γράμμα. Αν το γράμμα που είχαν χρησιμοποιείται ήδη, τότε παίρνουν το αμέσως επόμενο διαθέσιμο.

Αν μεταφέρονται spanned, mirrored, striped ή Raid-5 δίσκοι απαιτείται να μετακινείται ολόκληρο το σετ των δίσκων, αλλιώς δεν θα γίνουν online και δεν θα είναι προσβάσιμοι παρά μόνο αν διαγραφούν.

Αν μεταφέρουμε ένα GPT δίσκο, που περιέχει λειτουργικό windows, σε ένα νέο x86 ή x64 H/Y, θα έχετε την δυνατότητα πρόσβασης στα δεδομένα, αλλά το σύστημα δεν θα κάνει boot.

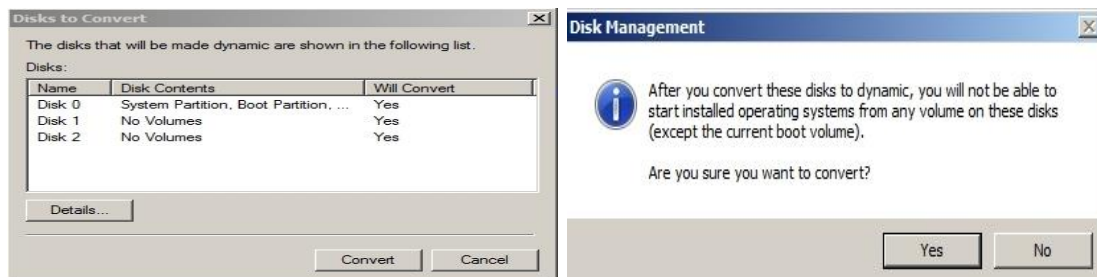
9.2.6 Basic σε Dynamic

Κάθε νέος δίσκος είναι basic και εφόσον είναι αναγκαίο να μετατραπεί σε dynamic, αφού λάβουμε υπόψη τους προαναφερθέντες περιορισμούς, από την εικόνα 9.2 οδηγούμαστε στην Εικ. 9.5.



Εικ. 9.5. Μετατροπή Βασικού δίσκου σε Δυναμικό

Εδώ υπάρχει η δυνατότητα να μετατρέψουμε ταυτόχρονα περισσότερους του ενός δίσκους.



Εικ. 9.6

Μετατροπή Βασικού δίσκου σε Δυναμικό

Εικ. 9.7

Με τις Εικ 9.6 και 9.7 επιβεβαιώνουμε την επιλογή μας, αφού μας υπενθυμίζεται το θέμα με την boot volume.

Κατά την μετατροπή δεν χάνονται υπάρχοντα δεδομένα.

9.2.7 Dynamic σε Basic

Κρατάμε backup όλων των δεδομένων του δίσκου και μετά στο disk management κάνουμε δεξί κλικ και διαγράφουμε κάθε volume του δίσκου.

Αφού διαγραφούν τα πάντα από τον δίσκο με δεξί κλικ στο όνομα του δίσκου πατάμε Convert to basic.

9.2.8 Χειρισμός Χαμένου ή εκτός λειτουργίας Δυναμικού δίσκου

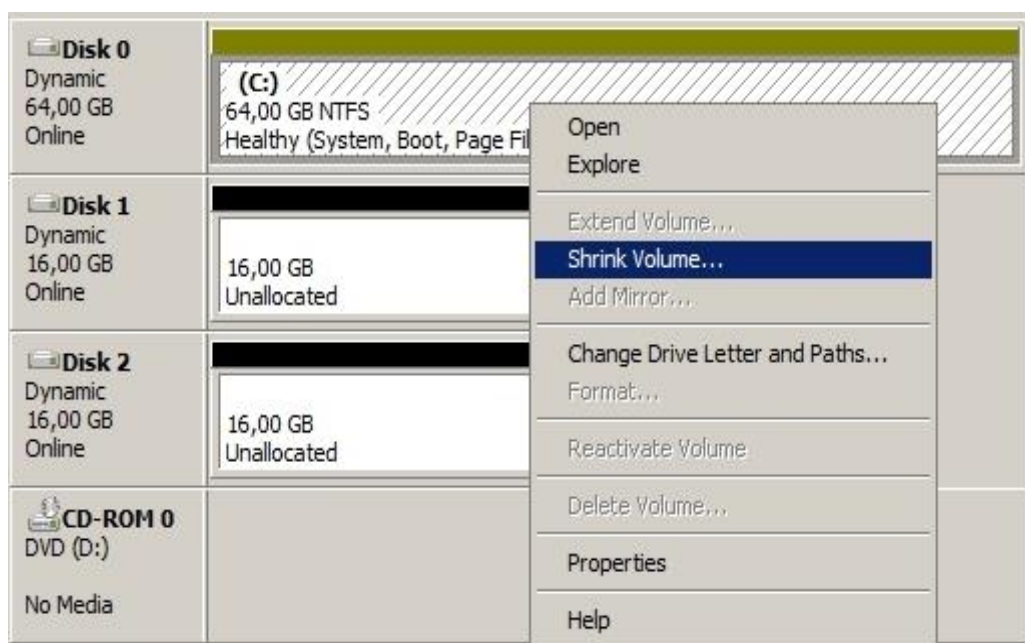
Ένας δυναμικός δίσκος είναι δυνατόν να χαθεί (missing), όταν διακοπεί απότομα η λειτουργία του, εάν γίνει διακοπή ρεύματος ή αποσυνδεθεί ξαφνικά. Μπορεί να γίνει offline (εκτός λειτουργίας), όταν διακοπεί απότομα η λειτουργία του, αν περιοδικά δεν είναι διαθέσιμος ή αν προσπαθήσουμε να τον κάνουμε import και αυτό αποτύχει.

Το missing και το offline είναι χαρακτηριστικά των δυναμικών δίσκων και εφόσον έχουμε minimum δικαιώματα administrator ή backup operator, μπορούμε να τους επανενεργοποιήσουμε.

Αρκεί ένα δεξί κλικ στο όνομα του δίσκου, εκεί που βρίσκεται το εικονίδιο λάθους και κλικ **reactivate disk**.

9.2.9 Shrink (Συρρίκνωση) τόμου

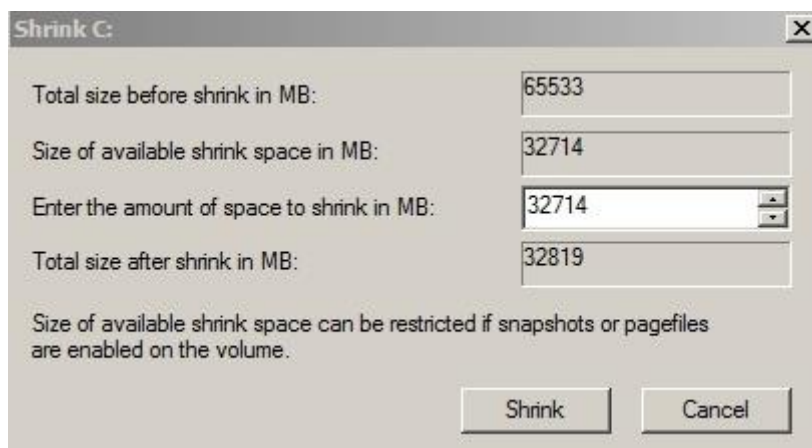
Κάθε τόμος έχει την δυνατότητα να συρρικνωθεί ασχέτως αν είναι primary ή logical partition ή volume, προκειμένου να εξοικονομηθεί χώρος για κάποια άλλη χρήση. Το shrink γίνεται με δεξί κλικ και ανάλογη επιλογή (Εικ. 9.8) σε οποιοδήποτε τμήμα του δίσκου.



Εικ. 9.8. Συρρίκνωση χώρου δίσκου

Αφού πραγματοποιηθεί αυτόματη έρευνα για το αν το συγκεκριμένο partition μπορεί να συρρικνωθεί εμφανίζεται η εικόνα 9.9 με πρόταση για το μέγιστο δυνατό χώρο που μπορούμε να εξασφαλίσουμε.

Δεν είναι απαραίτητο να χρησιμοποιήσουμε ολόκληρο το χώρο, αλλά δεν μπορούμε μέσα από το disk management να εκμεταλλευτούμε παραπάνω.



Εικ. 9.9. Μέγιστη δυνατή συρρίκνωση χώρου δίσκου.

Αν χρειάζομαστε παραπάνω υπάρχουν εργαλεία άλλων εταιρειών που το κάνουν αυτό.

9.2.10 Χειρισμός Βασικού δίσκου

Ο βασικός δίσκος αν είναι τύπου MBR, θα έχει χωρητικότητα μικρότερη των 2 TB και διαθέτει:

- Ένα ή δύο ή τρία ή τέσσερα primary partitions
- Ένα primary partition και Extended με ένα η περισσότερα logical drives
- Δύο primary partitions και Extended με ένα η περισσότερα logical drives
- Τρία primary partitions και Extended με ένα η περισσότερα logical drives

Αν ο βασικός δίσκος είναι τύπου GPT, μπορεί να έχει χωρητικότητα πολύ μεγαλύτερη των 2 TB και να διαθέτει έως 128 primary partitions.

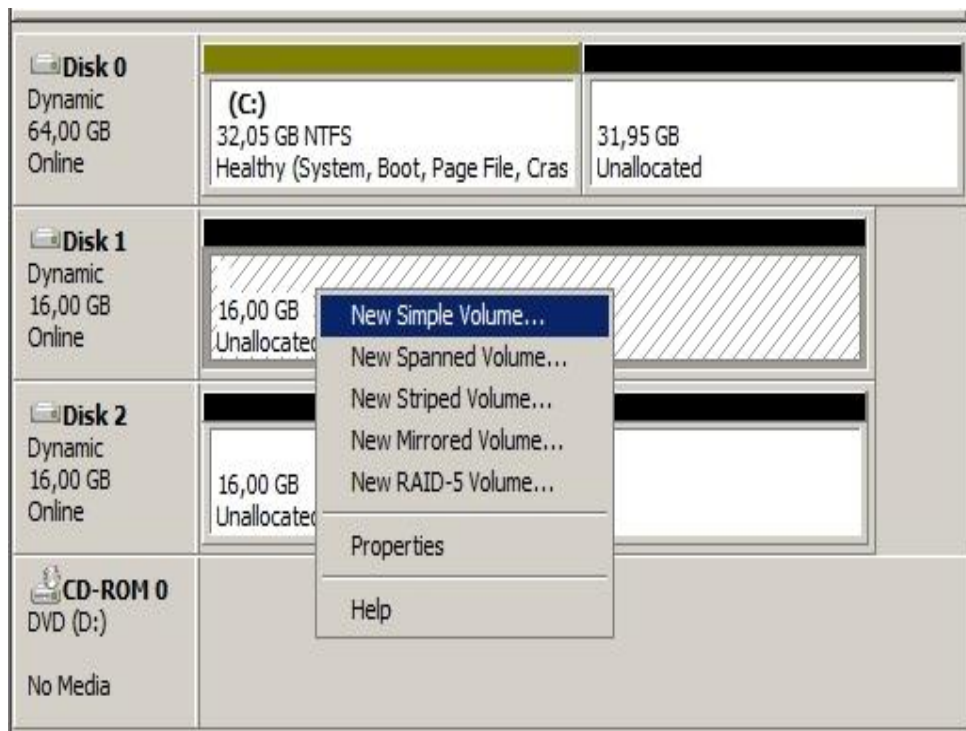
Με ένα απλό δεξί κλικ στον ελεύθερο χώρο του δίσκου ακολουθώντας τον οδηγό εύκολα και γρήγορα μοιράζουμε τον δίσκο.

9.2.11 Χειρισμός Δυναμικού δίσκου

Ένας δυναμικός δίσκος χωρίζεται σε ένα ή περισσότερα volumes. Κάθε volume αναλόγως του τρόπου που έχει διαμορφωθεί είναι δυνατόν να είναι μια αυτόνομη περιοχή του δίσκου ή συνεργαζόμενες περιοχές του ιδίου ή περισσότερων δίσκων. Θα πρέπει να διαθέτουμε δικαιώματα τουλάχιστον administrator ή backup operator για οποιαδήποτε διαμόρφωση.

9.2.12 Simple Volume

Για να δημιουργήσουμε μια Simple Volume κάνουμε δεξί κλικ σε μη διαμορφωμένο χώρο του δυναμικού δίσκου (Εικ. 9.10).



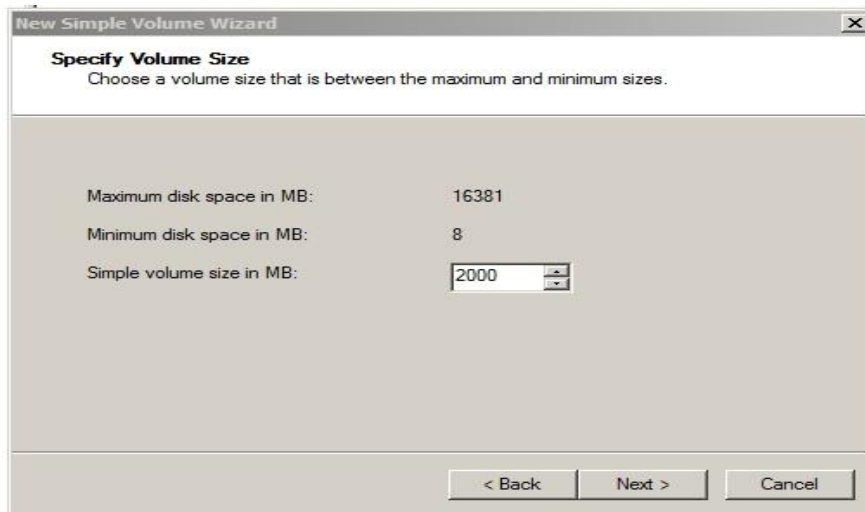
Εικ. 9.10. Νέα Simple Volume.

Ακολουθεί ένας οδηγός που μας κατευθύνει στην δημιουργία του Simple Volume (Εικ. 9.11).



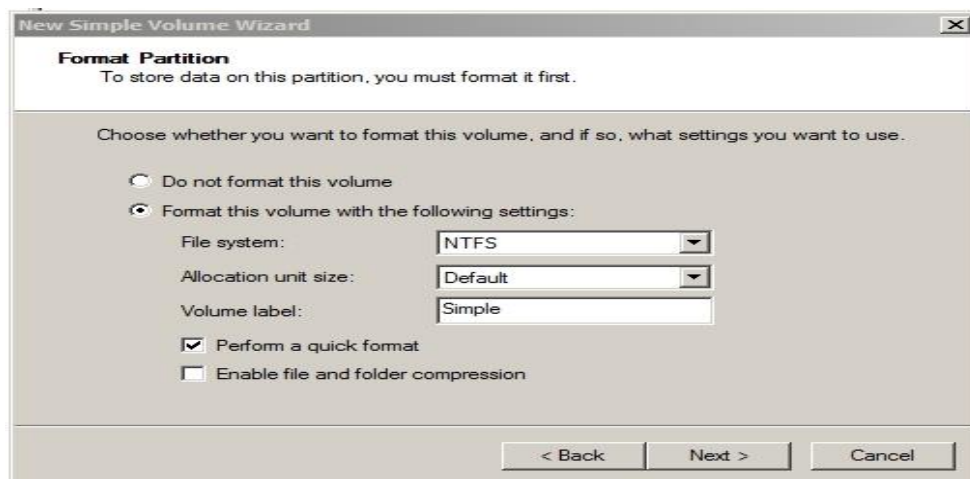
Εικ. 9.11. Οδηγός για Simple Volume

Αφού ορίσουμε το γράμμα που αντιστοιχεί στο τμήμα, καθορίζουμε το μέγεθος σε MB (Εικ. 9.12).



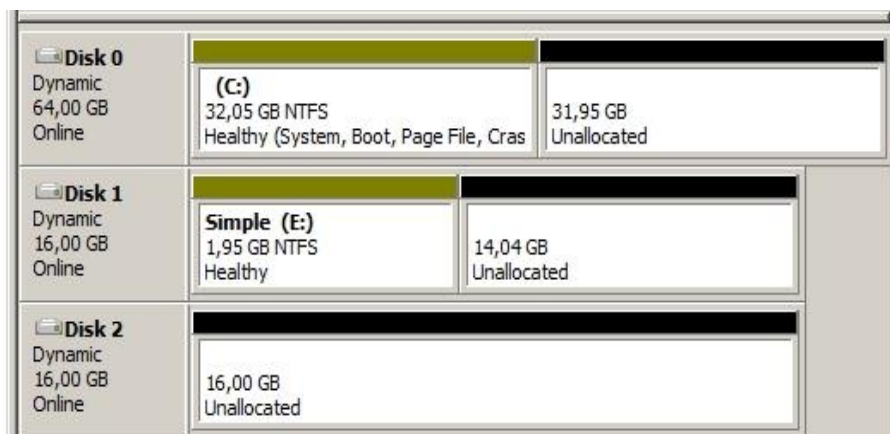
Εικ. 9.12. Καθορισμός μεγέθους Simple Volume

Στην εικόνα 9.13 ορίζουμε το format.



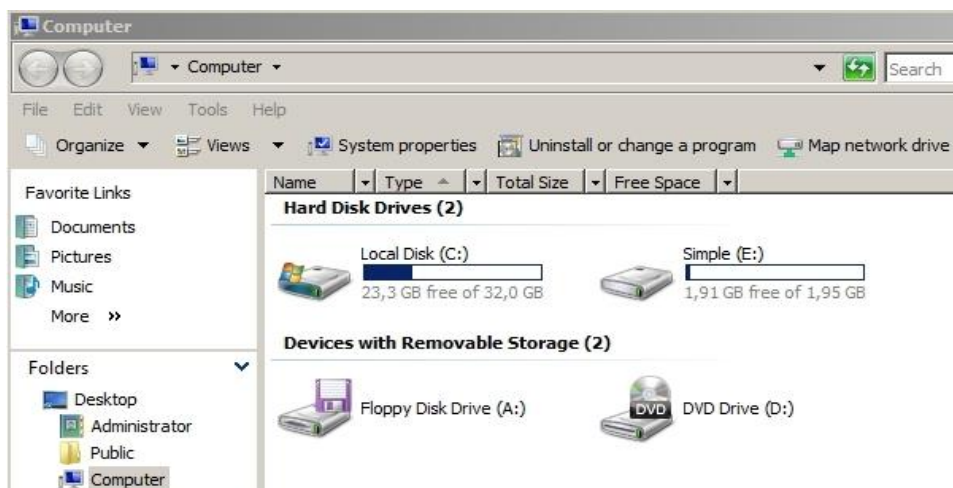
Εικ. 9.13. Καθορισμός Format Simple Volume

Και τέλος δημιουργείται το Simple Volume (Εικ. 9.14).



Εικ. 9.14. Ολοκλήρωση δημιουργίας Simple Volume.

Στην εικόνα 9.15 φαίνεται το volume (E:) και η χωρητικότητα που ορίσαμε πιο πάνω.



Εικ. 9.15. Εμφάνιση Simple Volume στον Explorer.

Για να διαγράψουμε ένα Simple Volume στο disk management, κάνουμε δεξί κλικ επάνω σε αυτό και επιλέγουμε delete.

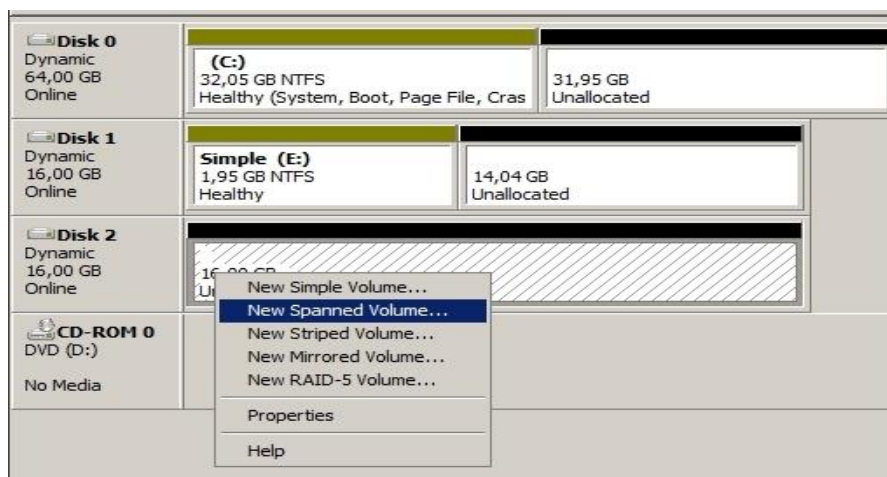
9.2.13 Spanned Volume

Η Spanned Volume αποτελείται από χώρους σε έναν ή περισσότερους δίσκους. Αν μια simple volume δεν είναι system ή boot volume είναι δυνατόν να επεκταθεί και σε άλλους δίσκους φτιάχνοντας Spanned Volume.

Μπορούμε να επεκτείνουμε μια Spanned Volume μέχρι και σε 32 δυναμικούς δίσκους εκμεταλλευόμενοι στο μέγιστο, ολόκληρο το διαθέσιμο αποθηκευτικό χώρο. Δεν είναι fault tolerant και για τον λόγο αυτό οποιοδήποτε κομμάτι και αν χαθεί χάνεται και το σύνολο.

Στον Explorer εμφανίζεται, όπως θα δούμε παρακάτω, σαν ένας ενιαίος χώρος.

Για να δημιουργήσουμε μια Spanned Volume κάνουμε δεξί κλικ σε μη διαμορφωμένο χώρο του δυναμικού δίσκου (Εικ. 9.16).



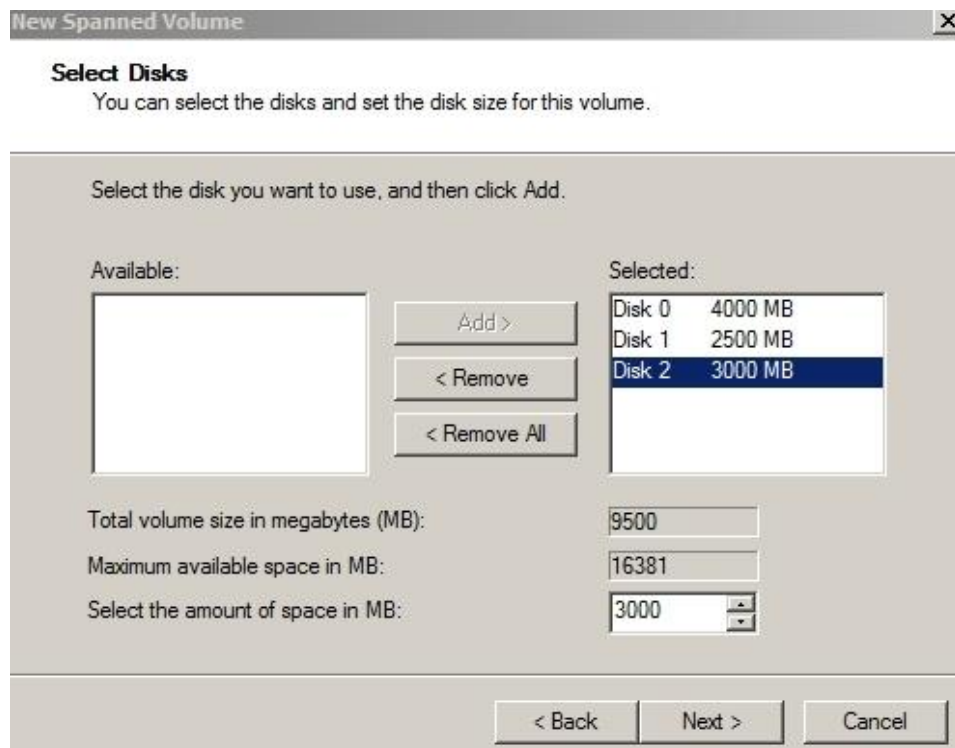
Εικ. 9.16. Νέα Spanned Volume.

Ακολουθεί ένας οδηγός που μας κατευθύνει στην δημιουργία του Spanned Volume (Εικ. 9.17).



Εικ. 9.17. Οδηγός για Spanned Volume.

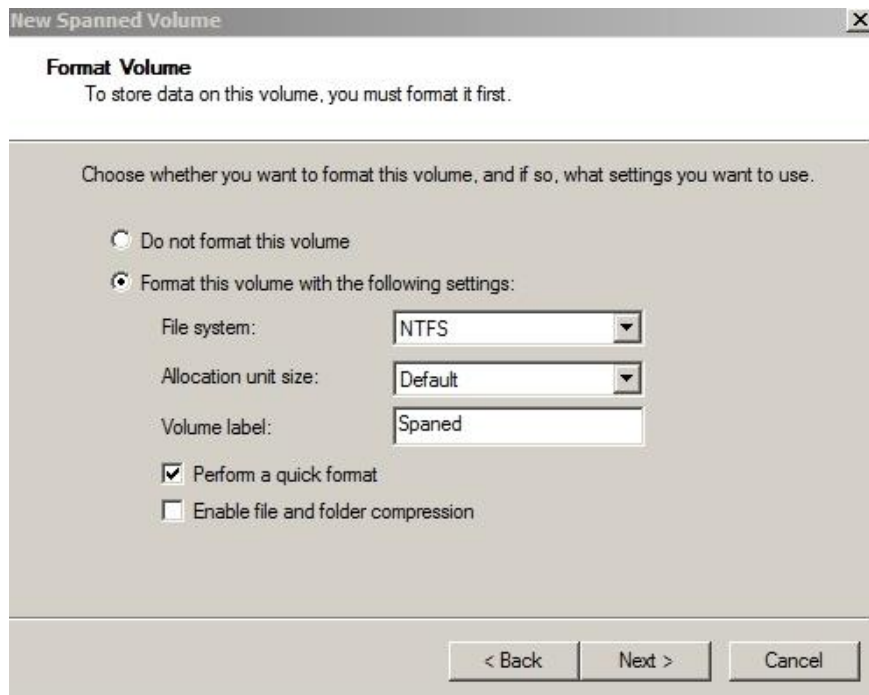
Αφού ορίσουμε το γράμμα που αντιστοιχεί στο τμήμα, καθορίζουμε το μέγεθος σε MB (Εικ. 9.18).



Εικ. 9.18. Καθορισμός μεγέθους Spanned Volume

Ποια χωρητικότητα, από ποιόν δίσκο και σε πόσους δίσκους αποτελεί αποκλειστικά δική μας επιλογή.

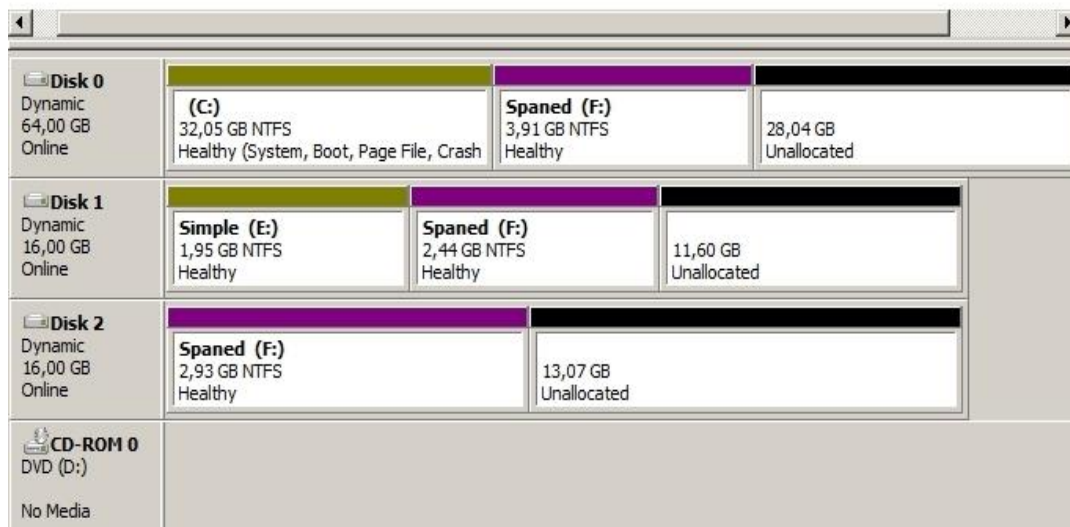
Στην εικόνα 9.19 ορίζουμε το format του spanned volume.



Εικ. 9.19. Καθορισμός Format Spanned Volume.

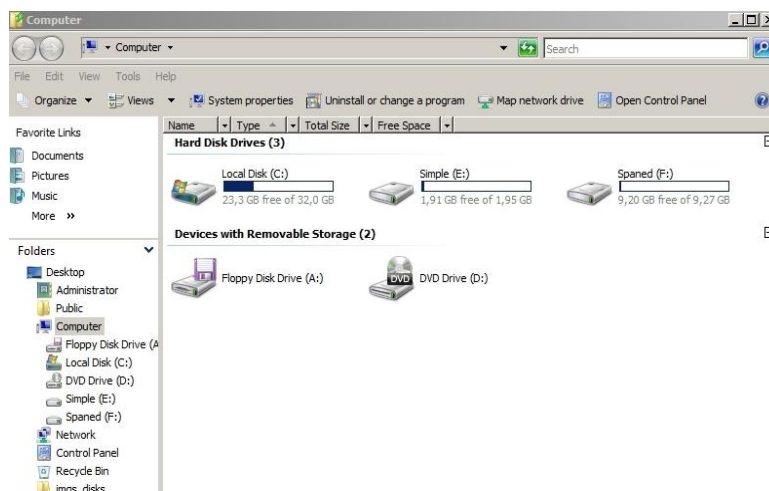
Και τέλος δημιουργείται το Spanned Volume (Εικ. 9.20) το οποίο αποτελείται από τμήματα των disk0,1 και 2.

Disk Management Volume List + Graphical View								
Volume	Layout	Type	File ...	Status	Capacity	Free Space	% Free	Fault Tolerance
(C:)	Simple	Dynamic	NTFS	Healthy (System, Boot, Page File, Cra...	32,05 GB	23,33 GB	73 %	No
Simple (E:)	Simple	Dynamic	NTFS	Healthy	1,95 GB	1,92 GB	98 %	No
Spanned (F:)	Spanned	Dynamic	NTFS	Healthy	9,28 GB	9,20 GB	99 %	No



Εικ. 9.20. Ολοκλήρωση δημιουργίας Spanned Volume.

Όπως παρατηρείται στην Εικ. 9.21 η spanned volume (F:) εμφανίζεται σαν ένα volume με άθροισμα την χωρητικότητα των επιμέρους τμημάτων.



Εικ. 9.21. Εμφάνιση Spanned Volume στον Explorer.

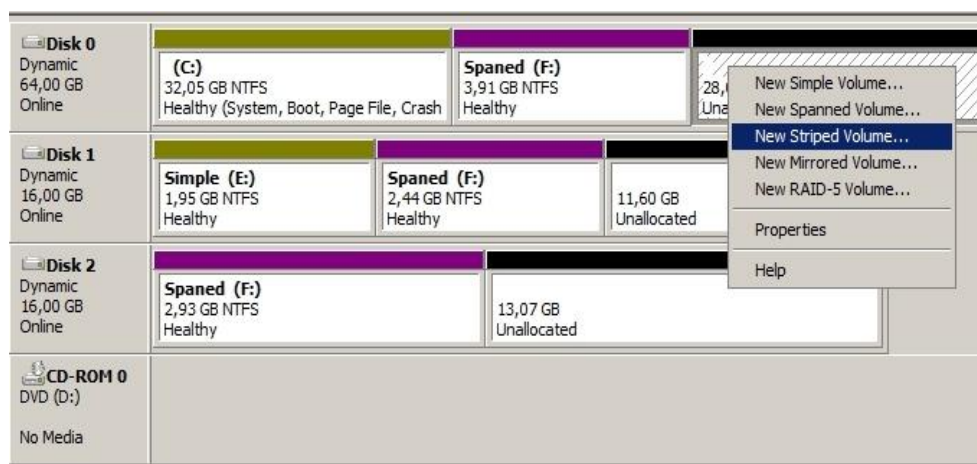
Για να διαγράψουμε ένα **Spanned Volume** στο disk management κάνουμε δεξί κλικ επάνω σε οποιοδήποτε τμήμα του και επιλέγουμε delete. Διαγράφεται όλος ο τόμος.

9.2.13.1 Striped Volume

Μία Striped Volume είναι ένας δυναμικός τόμος που αποθηκεύει δεδομένα σε stripes (λωρίδες ή ρίγες) σε δύο ή περισσότερους φυσικούς δίσκους. Τα δεδομένα αποθηκεύονται διαδοχικά και ομοιόμορφα σε stripes στους δίσκους.

Ο τύπος αυτός έχει την καλύτερη απόδοση σε σχέση με τα άλλα volumes στα Windows, αλλά δεν παρέχει fault tolerant. Αν κάποιο striped volume χαλάσει, χάνεται ολόκληρος ο τόμος.

Οι striped volumes δεν επεκτείνονται και μπορούν να δημιουργηθούν μέχρι και σε 32 δυναμικούς δίσκους.



Εικ. 9.22. Νέα Striped Volume.

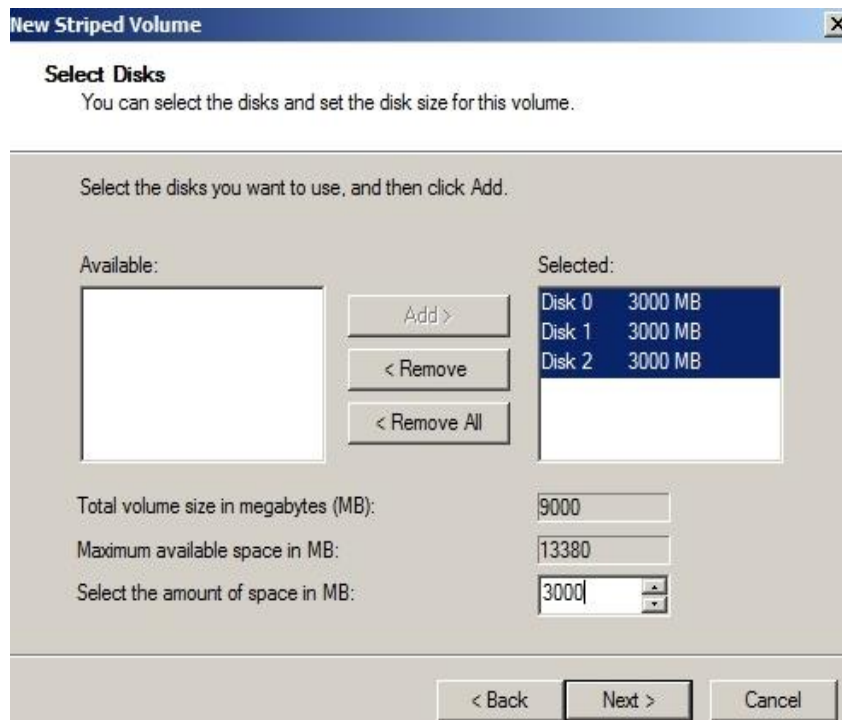
Για να δημιουργήσουμε μια Striped Volume κάνουμε δεξί κλικ σε μη διαμορφωμένο χώρο του δυναμικού δίσκου (Εικ. 9.22).

Ακολουθεί ένας οδηγός που μας κατευθύνει στην δημιουργία του Striped Volume (Εικ. 9.23).



Εικ. 9.23. Οδηγός για Striped Volume.

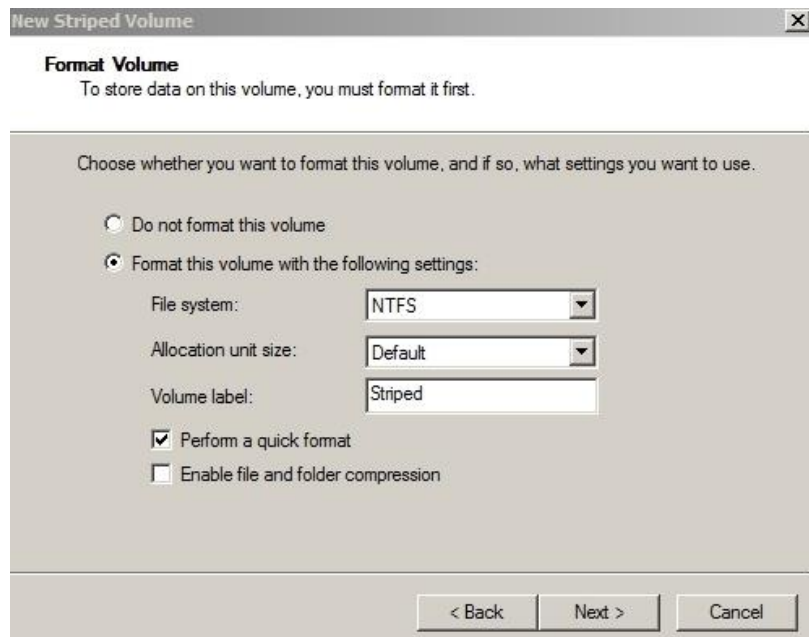
Αφού ορίσουμε το γράμμα που αντιστοιχεί στο τμήμα, καθορίζουμε το μέγεθος σε MB (Εικ. 9.24).



Εικ. 9.24. Καθορισμός μεγέθους Striped Volume.

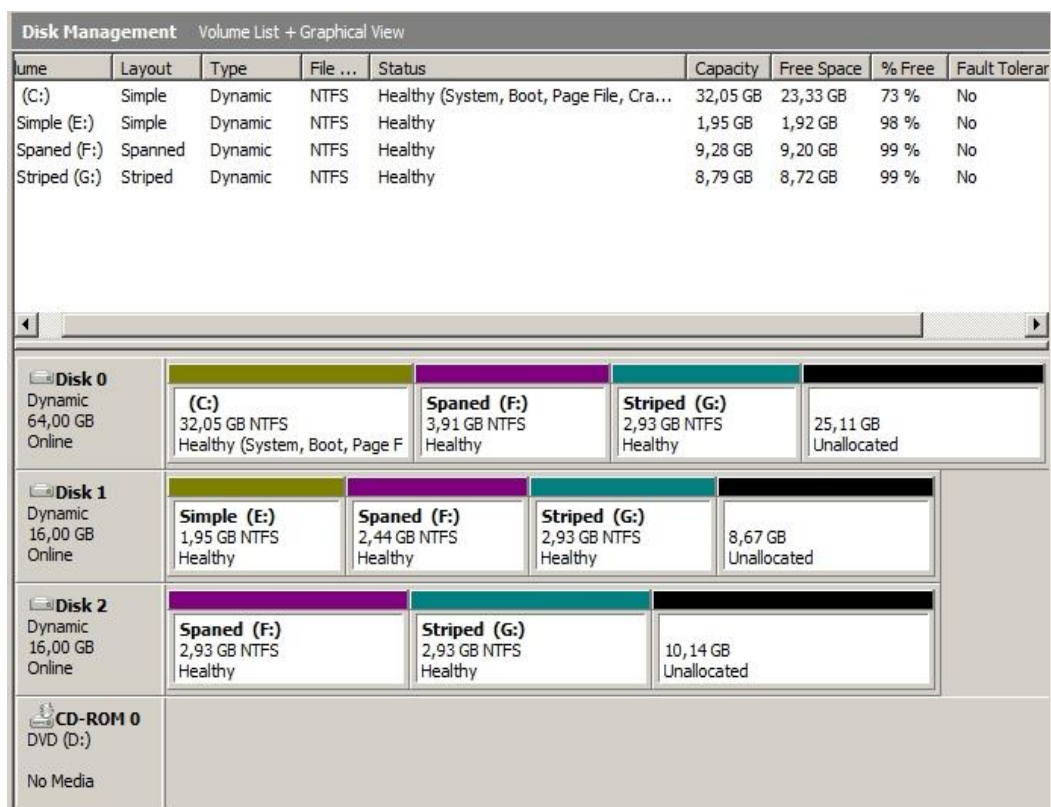
Όπως παρατηρείται, ο αριθμός των MB πρέπει να είναι ακριβώς ο ίδιος σε όλα τα stripes.

Στην εικόνα 9.25 ορίζουμε το format του spanned volume.



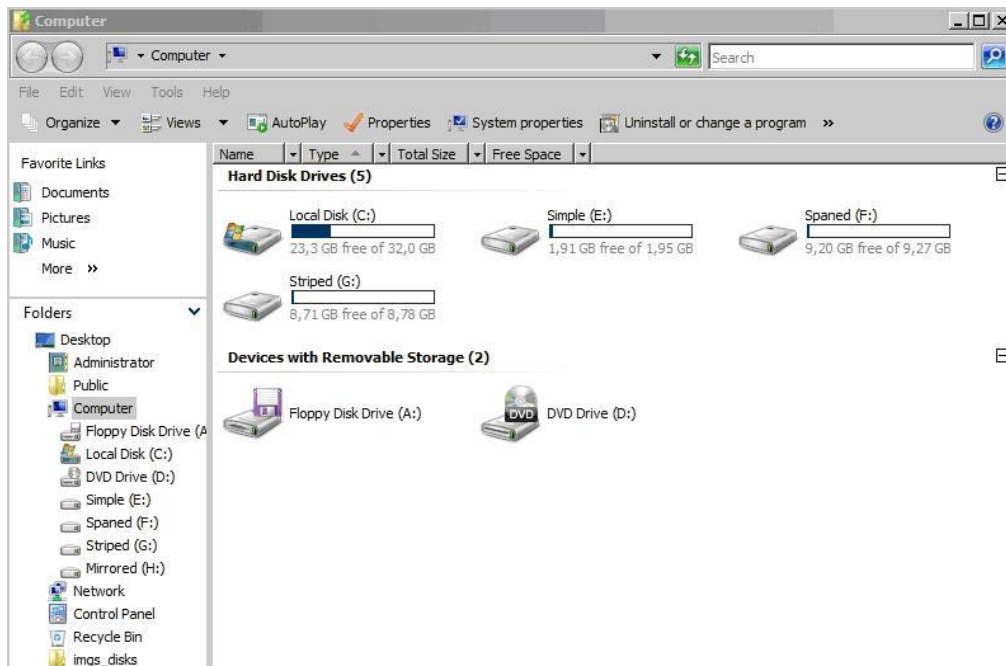
Εικ. 9.25. Καθορισμός Format Striped Volume.

Και τέλος δημιουργείται το Spanned Volume (Εικ. 9.26), το οποίο αποτελείται από τμήματα των disk0,1 και 2.



Εικ. 9.26. Ολοκλήρωση δημιουργίας Striped Volume.

Στην Εικ. 9.27 η striped volume (G:) εμφανίζεται σαν ένα volume με άθροισμα την χωρητικότητα των επιμέρους τμημάτων.

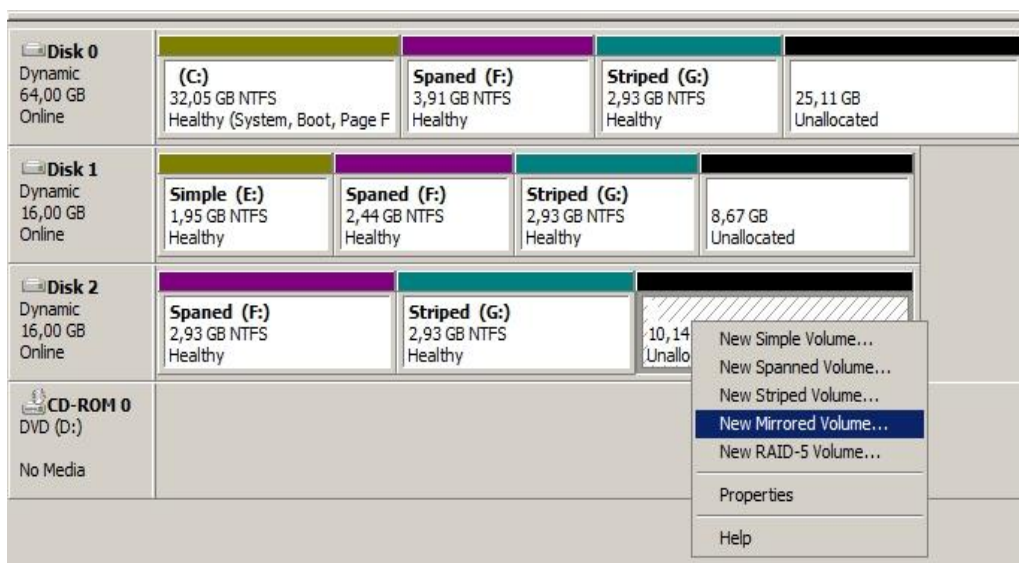


Εικ. 9.27. Εμφάνιση Striped Volume στον Explorer.

Για να διαγράψουμε ένα **Striped Volume** στο disk management, κάνουμε δεξί κλικ επάνω σε οποιοδήποτε τμήμα του και επιλέγουμε delete. Διαγράφεται όλος ο τόμος.

9.2.13.2 Mirrored Volume

Η δημιουργία Mirrored Volume (κατόπτρου) μας βοηθά να αποκτήσουμε fault tolerant. Δημιουργείται ακριβές αντίγραφο ενός τόμου και άρα σε περίπτωση που χαλάσει ο τόμος δεν χάθηκε τίποτα. Εμπλέκει δύο δυναμικούς τόμους της ίδιας χωρητικότητας αλλά με το 50% άμεσα εκμεταλλεύσιμη.



Εικ. 9.28. Νέο Mirrored Volume.

Έχει χαμηλότερη απόδοση από το striped volume, αφού τα δεδομένα γράφονται δύο φορές, αλλά μας εξασφαλίζει τα δεδομένα.

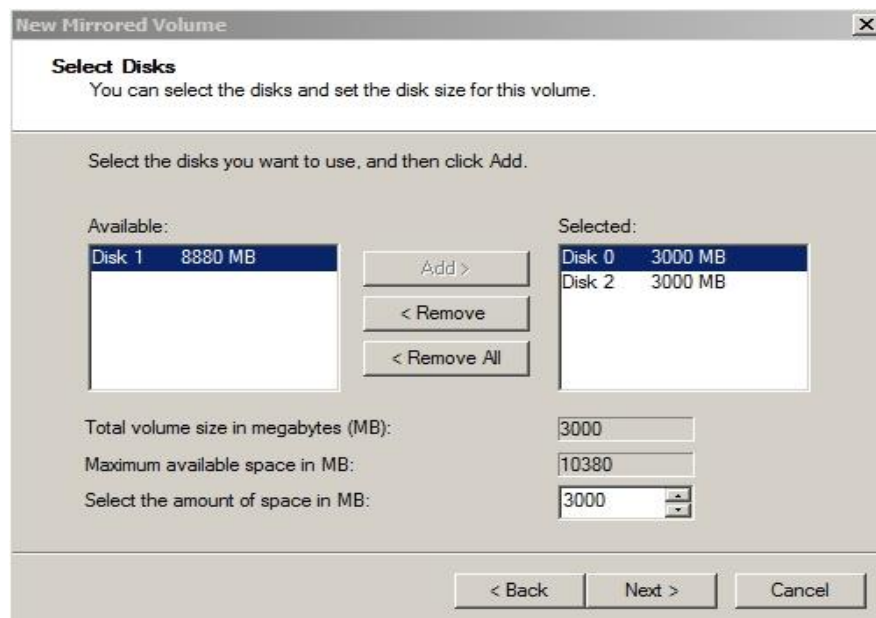
Για να δημιουργήσουμε ένα Mirrored Volume κάνουμε δεξί κλικ σε μη διαμορφωμένο χώρο του δυναμικού δίσκου (Εικ. 9.28).

Ακολουθεί ένας οδηγός που μας κατευθύνει στην δημιουργία του Mirrored Volume (Εικ. 9.29).



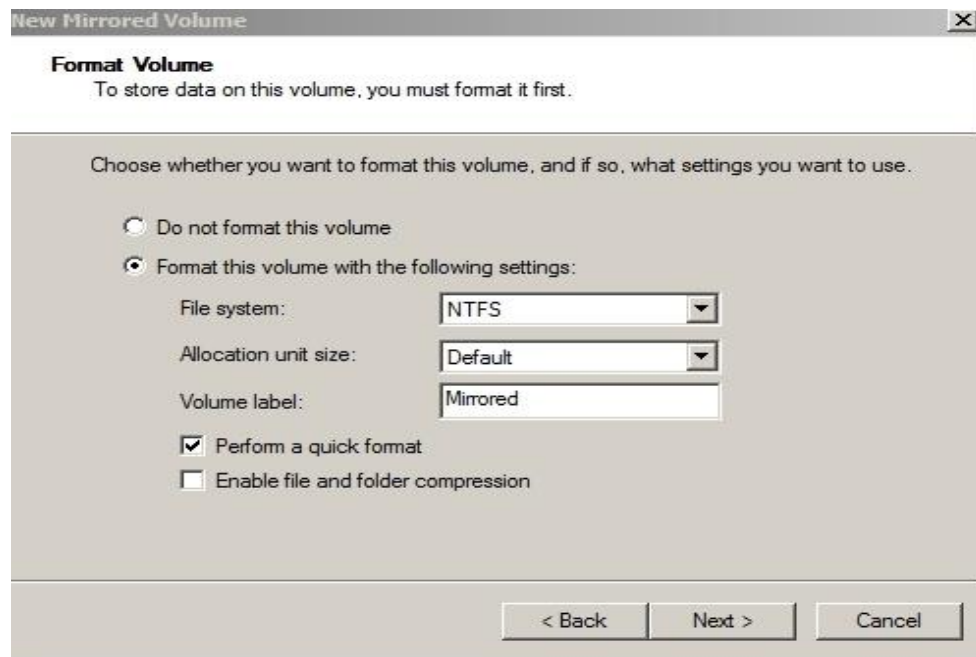
Εικ. 9.29. Οδηγός για Mirrored Volume.

Αφού ορίσουμε το γράμμα που αντιστοιχεί στο τμήμα, καθορίζουμε το μέγεθος σε MB (Εικ. 9.30).



Εικ. 9.30. Καθορισμός μεγέθους Mirrored Volume.

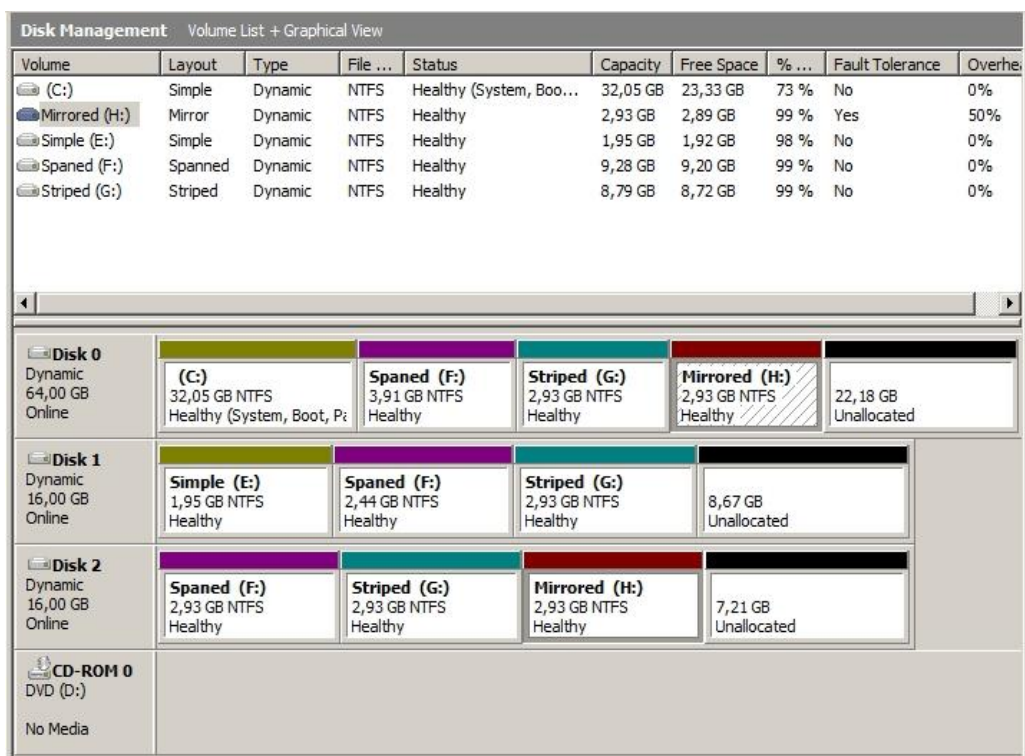
Όπως παρατηρείται, ο αριθμός των MB πρέπει να είναι ακριβώς ο ίδιος και στους δύο δίσκους.



Εικ. 9.31. Καθορισμός Format Mirrored Volume.

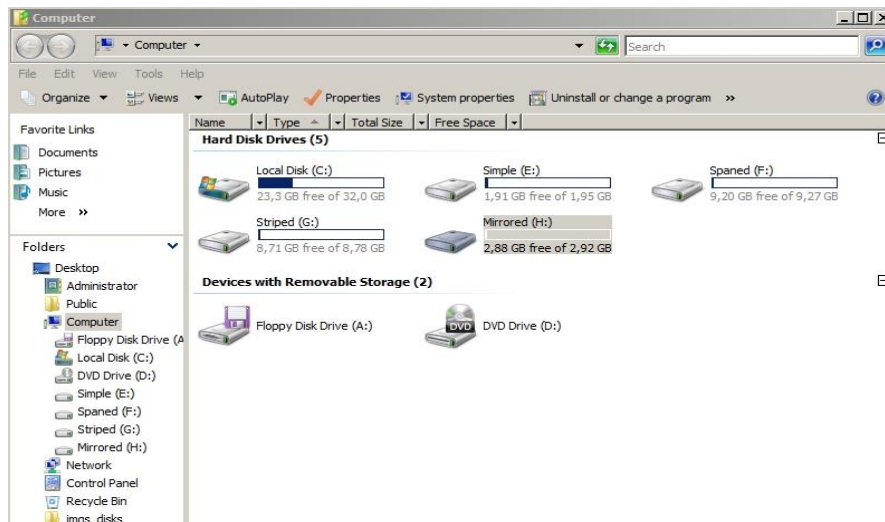
Στην εικόνα 9.31 ορίζουμε το format του Mirrored Volume.

Και τέλος δημιουργείται το Mirrored Volume (Εικ. 9.32), το οποίο αποτελείται από τμήματα των disk 0 και 2.



Εικ. 9.32. Ολοκλήρωση δημιουργίας Mirrored Volume.

Στην Εικ. 9.33 η Mirrored Volume (H:) εμφανίζεται σαν ένα volume με χωρητικότητα το 50% του αθροίσματος των τμημάτων.



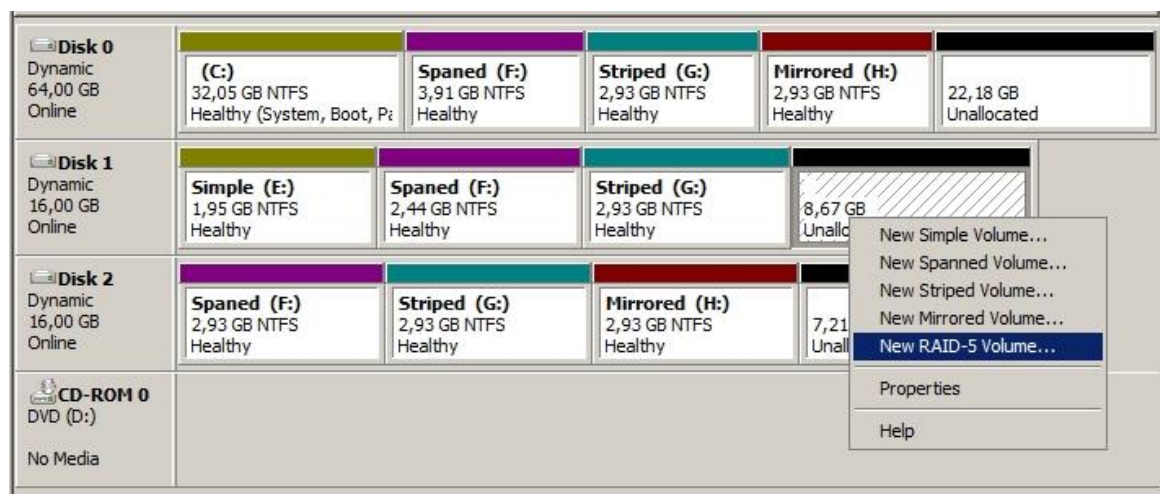
Εικ. 9.33. Εμφάνιση Mirrored Volume στον Explorer.

Για να διαγράψουμε ένα **Mirrored Volume** στο disk management, κάνουμε δεξί κλικ επάνω σε οποιοδήποτε τμήμα του και επιλέγουμε remove mirror. Ο άλλος τόμος μένει ανέπαφος.

9.2.13.3 Raid-5 Volume

Απαιτεί 3 τουλάχιστον δίσκους. Συνδυάζει ταχύτητα μοιράζοντας τα δεδομένα στους δίσκους που το απαρτίζουν και ασφάλεια, διότι κάθε φορά που μοιράζονται τα δεδομένα (στους 2 δίσκους), εκτελείται μια λογική πράξη (XOR) μεταξύ αυτών. Το αποτέλεσμα γράφεται στον 3ο δίσκο και αν ένας δίσκος «χτυπήσει» τα δεδομένα του αναπαράγονται αυτόματα. Διαθέτει κατανεμημένη parity σε διαφορετικό δίσκο κάθε φορά που εξασφαλίζει την αποκατάσταση του τόμου μετά την αντικατάσταση του χαλασμένου δίσκου.

Για να δημιουργήσουμε ένα Raid-5 volume, κάνουμε δεξί κλικ σε μη διαμορφωμένο χώρο του δυναμικού δίσκου (Εικ. 9.34).



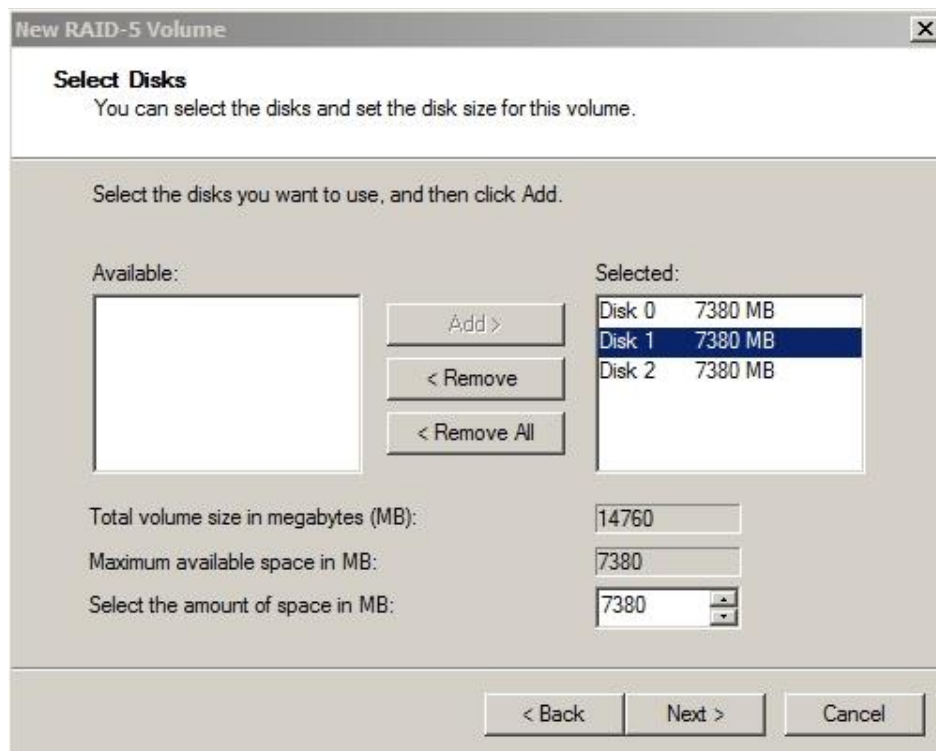
Εικ. 9.34. Νέο Raid-5 Volume.

Ακολουθεί ένας οδηγός που μας κατευθύνει στην δημιουργία του Raid-5 Volume (Εικ. 9.35).



Εικ. 9.35. Οδηγός για Raid-5 Volume.

Αφού ορίσουμε το γράμμα που αντιστοιχεί στο τμήμα, καθορίζουμε το μέγεθος σε MB (Εικ. 9.36). Παρατηρούμε ότι ο αποθηκευτικός χώρος σε κάθε δίσκο πρέπει να είναι ίδιος και αναπροσαρμόζεται αυτόματα σε οποιοδήποτε δίσκο και αν τον ορίσουμε.



Εικ. 9.36. Καθορισμός μεγέθους Raid-5 Volume.

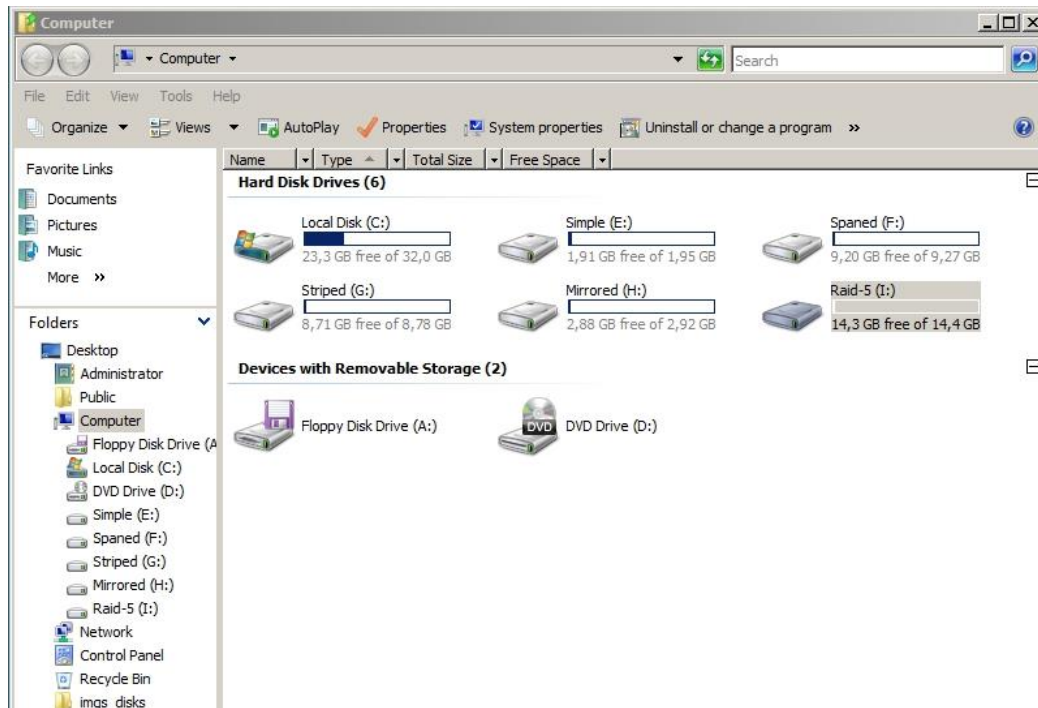
Αφού ορίσουμε το format, δημιουργείται το Raid-5 Volume (Εικ. 9.37), το οποίο αποτελείται από τμήματα των disk 0,1 και 2.

Disk Management Volume List + Graphical View									
Volume	Layout	Type	File ...	Status	Capacity	Free Space	% ...	Fault Tolerance	Overhe
(C:)	Simple	Dynamic	NTFS	Healthy (System, Boo...	32,05 GB	23,33 GB	73 %	No	0%
Mirrored (H:)	Mirror	Dynamic	NTFS	Healthy	2,93 GB	2,89 GB	99 %	Yes	50%
Raid-5 (I:)	RAID-5	Dynamic	NTFS	Healthy	14,41 GB	14,33 GB	99 %	Yes	33%
Simple (E:)	Simple	Dynamic	NTFS	Healthy	1,95 GB	1,92 GB	98 %	No	0%
Spanned (F:)	Spanned	Dynamic	NTFS	Healthy	9,28 GB	9,20 GB	99 %	No	0%
Striped (G:)	Striped	Dynamic	NTFS	Healthy	8,79 GB	8,72 GB	99 %	No	0%

Disk 0 Dynamic 64,00 GB Online	(C:) 32,05 GB NTFS Healthy (System, Boc	Spanned (F:) 3,91 GB NTFS Healthy	Striped (G:) 2,93 GB NTFS Healthy	Mirrored (H:) 2,93 GB NTFS Healthy	Raid-5 (I:) 7,21 GB NTFS Healthy	14,97 GB Unallocated
Disk 1 Dynamic 16,00 GB Online	Simple (E:) 1,95 GB NTFS Healthy	Spanned (F:) 2,44 GB NTFS Healthy	Striped (G:) 2,93 GB NTFS Healthy	Raid-5 (I:) 7,21 GB NTFS Healthy	1,47 GB Unallocated	
Disk 2 Dynamic 16,00 GB Online	Spanned (F:) 2,93 GB NTFS Healthy	Striped (G:) 2,93 GB NTFS Healthy	Mirrored (H:) 2,93 GB NTFS Healthy	Raid-5 (I:) 7,21 GB NTFS Healthy		
CD-ROM 0 DVD (D:) No Media						

Εικ. 9.37. Ολοκλήρωση δημιουργίας Raid-5 Volume.

Στην Εικ. 9.38 η Raid-5 Volume (I:) εμφανίζεται σαν ένα volume με χωρητικότητα N-1, από N τμήματα φυσικών δυναμικών δίσκων.



Εικ. 9.38. Εμφάνιση Raid-5 Volume στον Explorer.

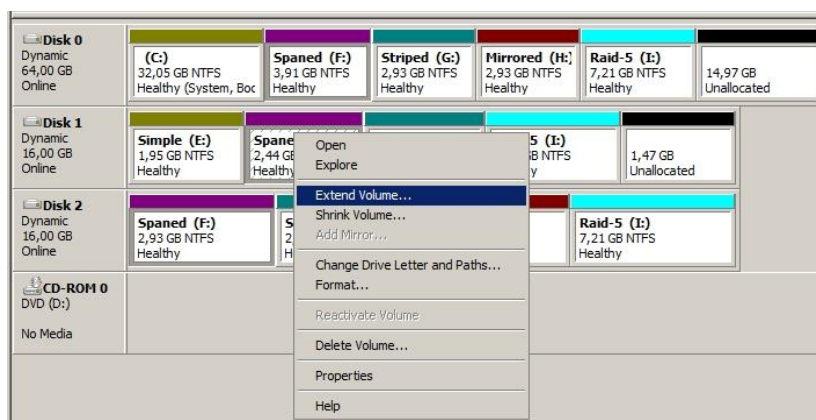
Για να διαγράψουμε ένα **Raid-5 Volume** στο disk management, κάνουμε δεξί κλικ επάνω σε οποιοδήποτε τμήμα του και επιλέγουμε delete.

9.2.13.4 Extend (επέκταση) τόμου

Μπορούμε να προσθέσουμε περισσότερο χώρο σε κάποιο τόμο (Extend), οποιουδήποτε primary ή logical partition ή volume, προκειμένου να εκμεταλλευτούμε αχρησιμοποίητο γειτονικό χώρο. Απαραίτητη προϋπόθεση να έχει format NTFS και να πληρεί ορισμένες συνθήκες αναλόγως του είδους του τόμου (Boot, Primary, logical για basic ή volume για dynamic).

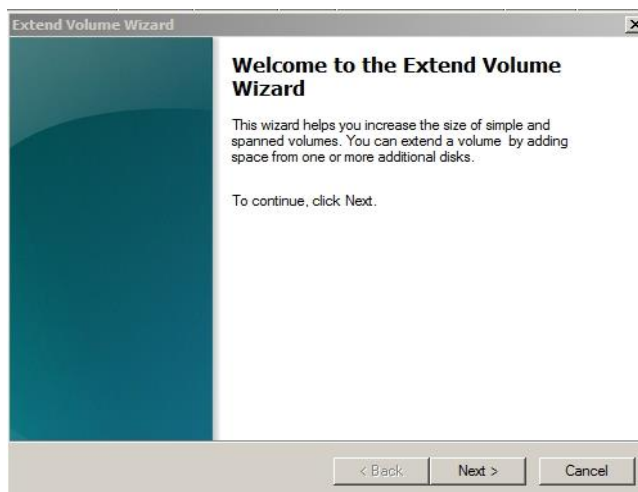
Το Extend γίνεται με δεξί κλικ και ανάλογη επιλογή (Extend volume) σε οποιοδήποτε τμήμα του δίσκου επιθυμούμε την επέκταση.

Στην εικόνα 9.37 παρατηρούμε ότι στον δίσκο 0 έχουμε ανεκμετάλλευτο χώρο 14,97 GB ενώ στον δίσκο 1 , 1,47 GB. Θα μπορούσαμε να εκμεταλλευτούμε τον χώρο αυτό κάνοντας extend στον spanned volume (F:).



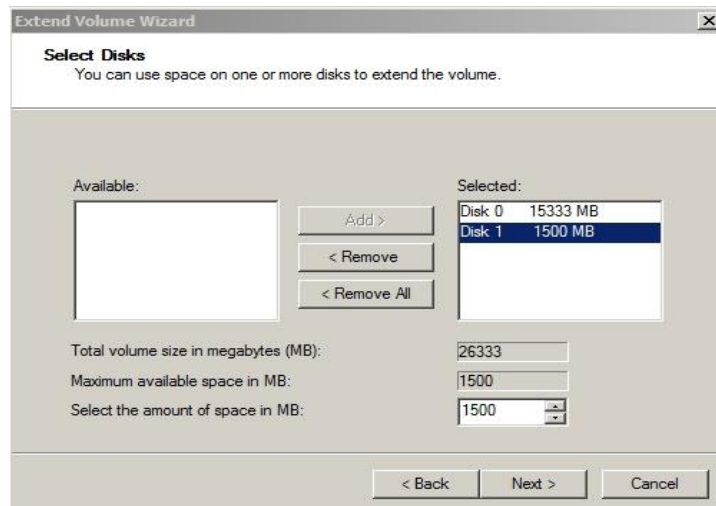
Εικ. 9.39. Extend Volume.

Σε τμήμα του (F:) κάνουμε δεξί κλικ (Εικ. 9.39) και επιλέγουμε Extend volume. Ακολουθεί ένας οδηγός που μας κατευθύνει (Εικ. 9.40).



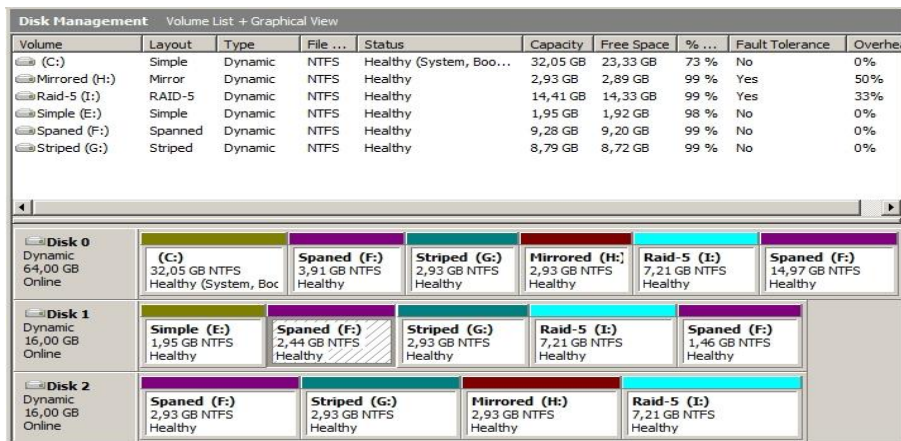
Εικ. 9.40. Οδηγός για Extend Volume.

Ορίζουμε τα τμήματα που θέλουμε να προσθέσουμε (Εικ. 9.41).

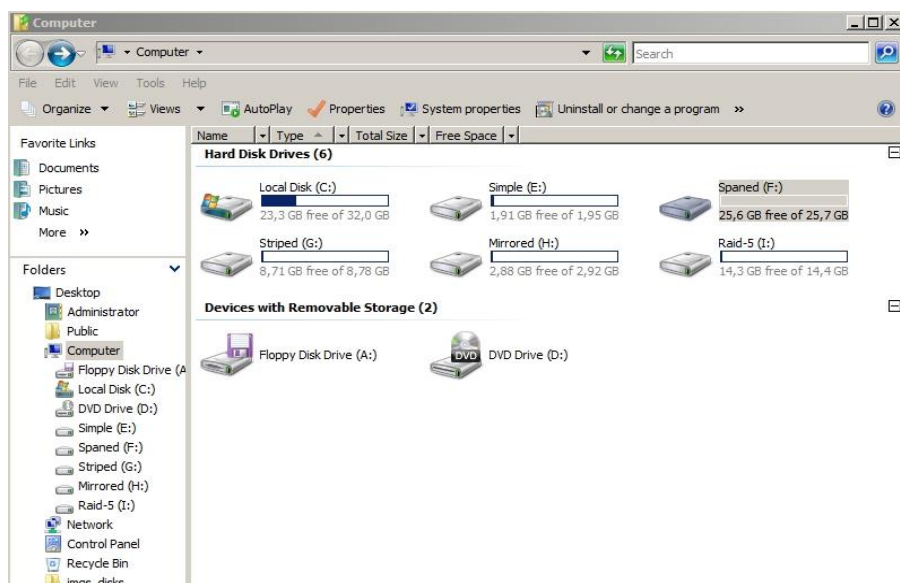


Εικ. 9.41. Καθορισμός χώρου για Extend Volume.

Στην Εικ. 9.42 φαίνονται τα τμήματα που έχουν προστεθεί.



Εικ. 9.42. Πραγματοποίηση Extend Volume στο (F:).



Εικ. 9.43. Εμφάνιση Extend Volume στο (F:) στον Explorer.

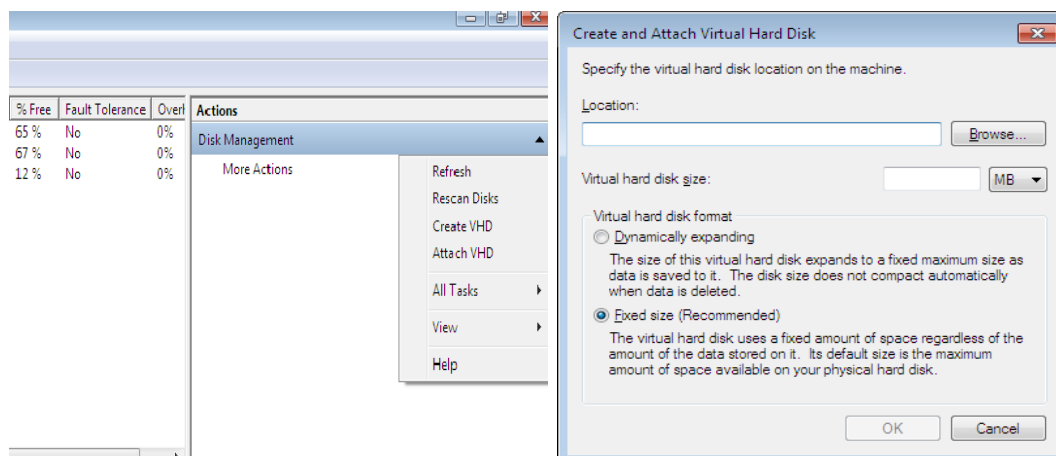
Στο (F:) έχει προστεθεί και ο επιπλέον χώρος (Εικ. 9.43).

9.2.13.5 Επιπρόσθετες δυνατότητες Disk Management

Από την έκδοση Windows Server 2008 R2 το disk management παρέχει την δυνατότητα δημιουργίας, σύνδεσης (attach) και αποσύνδεσης (detach) Virtual Hard Disks (VHDs).

Όταν γίνει attach ένας VHD, μπορούμε να τον διαχειριζόμαστε σαν φυσικό δίσκο που παρουσιάζεται στον explorer και συναναστρεφόμαστε με αυτόν. Με το detach αναιρούνται, αντίστοιχα, αυτές οι δυνατότητες.

Για να δημιουργηθεί ένας VHD, στο μενού **Action** επιλέγουμε **Create VHD**. Στο **Create and Attach Virtual Hard Disk** δηλώνουμε την διαδρομή στον H/Y, που επιθυμούμε να αποθηκευτεί ο εικονικός δίσκος, καθώς και το μέγεθος που θα έχει. Στο **Virtual hard disk format** επιλέγουμε **Dynamically expanding** ή **Fixed size** και πατάμε **OK**.



Εικ. 9.44 Επιπρόσθετες δυνατότητες Disk Management

Θα πρέπει να γνωρίζουμε όμως ότι:

- Η διαδρομή του VHD δεν μπορεί να είναι στο φάκελο των Windows.
- Το ελάχιστο μέγεθος του εικονικού δίσκου να είναι 3 MB.
- Ο VHD να είναι μόνο Basic.
- Αν χρησιμοποιήσουμε Fixed size, θα χρειαστεί αρκετή ώρα η αρχικοποίηση του (Initializing).

9.2.14 Σύνδεση φακέλου (Mount point folder path) σε Drive

Υπάρχει η δυνατότητα στο disk management να αναθέσουμε, αντί για ένα γράμμα σε κάποιο partition ή volume, ένα φάκελο, έτσι ώστε όταν ανοίγουμε τον φάκελο αυτό να ανοίγει ο τόμος. Η ανάθεση μπορεί να γίνει μόνο σε άδειο φάκελο σε οτιδήποτε τύπο δίσκου.

Στο Disk Manager κάνουμε δεξί κλικ στο partition που θα αναθέσουμε τον φάκελο και επιλέγουμε **Change Drive Letter and Paths**. Επιλέγουμε **Add, Mount in the following empty NTFS folder** και **Browse**, βρίσκοντας τον φάκελο που επιθυμούμε.

9.2.15 Απομακρυσμένη διαχείριση δίσκων

Για να διαχειριστούμε δίσκους που βρίσκονται σε άλλο H/Y μέσω του disk management, θα πρέπει ο απομακρυσμένος H/Y να υποστηρίζει Virtual Disk Service (VDS).

Αν δεν υποστηρίζει VDS, τότε η διαχείριση μπορεί να πραγματοποιηθεί μόνο με Remote Desktop Connection.

Και οι δύο υπολογιστές θα πρέπει να βρίσκονται στο ίδιο Domain.

Επιπρόσθετα θα πρέπει να ρυθμιστεί και το Firewall και στους δύο H/Y για να γίνει η διαχείριση. Ανάλογα με το λειτουργικό σύστημα είναι αναγκαίες οι παρακάτω ρυθμίσεις στο Firewall:

- Enable Remote Volume Management exception.
- Enable the File and Print Sharing exception.
- Enable the following exceptions:
 - ✓ TCP port 135
 - ✓ Vds.exe

9.3 Διαχείριση Αποθήκευσης Δεδομένων

Για την διαχείριση της αποθήκευσης των δεδομένων σε ό,τι αφορά την εξασφάλιση τους, την εξοικονόμηση χώρου και τους περιορισμούς σε συγκεκριμένο χώρο, στον Server 2008 υπάρχουν σε πιο εξελιγμένη μορφή οι τεχνολογίες Encrypting File System (EFS), File Compression και Quota.

9.3.1 EFS File Encryption

Encrypting File System (EFS) είναι μια τεχνολογία κρυπτογράφησης που χρησιμοποιείται για την κρυπτογράφηση αρχείων αποθηκευμένων σε NTFS τομείς.

Τα κρυπτογραφημένα αρχεία δεν μπορούν να χρησιμοποιηθούν από κανένα χρήστη, εκτός αν διαθέτει πρόσβαση στο κλειδί που απαιτείται για την αποκρυπτογράφηση.

Το EFS υποστηρίζει γνωστούς αλγορίθμους, όπως Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA), elliptic curve cryptography (ECC), smart card-based encryption και διαθέτει πρόσθετες δυνατότητες.

Η αρχιτεκτονική του EFS, ιδιαίτερα στα windows Server 2008 R2 και windows 7, έχει αλλάξει για να συνεργάζεται με την ECC και να συμμορφώνεται έτσι με την

Suite B των κρυπτογραφικών απαιτήσεων που έχουν καθοριστεί από το National Security Agency για την προστασία διαβαθμισμένων πληροφοριών.

Η προεπιλεγμένη πολιτική για το EFS public key επιτρέπει την δημιουργία αυτό-υπογραφόμενου (self signed) πιστοποιητικού, όταν δεν είναι διαθέσιμη κάποια certification authority (CA).

Ένα 256-bit key χρησιμοποιείται σαν προεπιλογή για ECC certificates και δύναται να αυξηθεί σε 384 ή 512 - bit ECC.

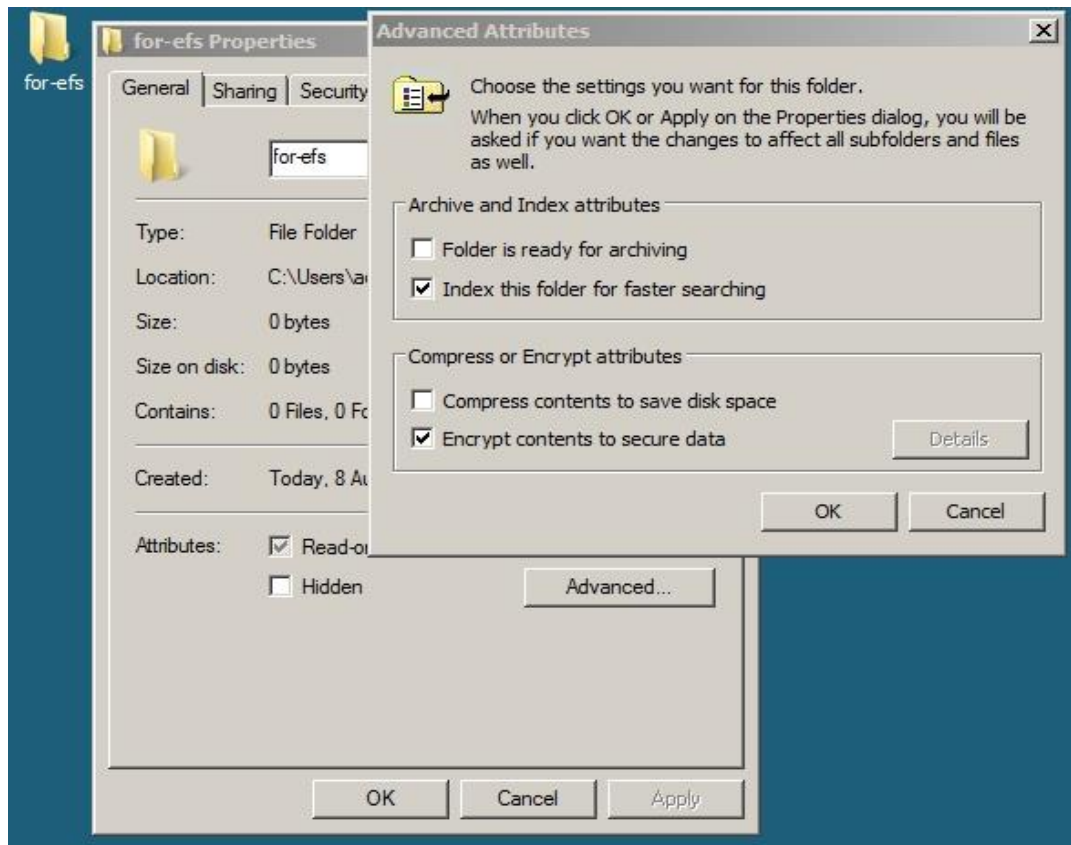
Οι ρυθμίσεις για το EFS βρίσκονται στο **Local Computer Policy Security Settings\Public Key Policies\Encrypting File System**.

Αν τα κρυπτογραφημένα αρχεία μετακινηθούν στον ίδιο Η/Υ, παραμένουν κρυπτογραφημένα.

Αν σε έναν κρυπτογραφημένο φάκελο προσθέσουμε αρχεία, αυτά κρυπτογραφούνται αυτόματα.

Δεν χρειάζεται αποκρυπτογράφηση των αρχείων για να χρησιμοποιηθούν, αφού αυτόματα το κάνει το λειτουργικό σύστημα και με ασφάλεια.

Αν χαθεί το προσωπικό κλειδί του χρήστη, υπάρχει δυνατότητα επαναφοράς μέσω του EFS recovery agent.



Εικ. 9.45. Encrypting File System.

Το EFS δεν κρυπτογραφεί δεδομένα που στέλνονται μέσω δικτύου, αφού έχει σχεδιαστεί για την προστασία των αποθηκευμένων δεδομένων. Όταν το κρυπτογραφημένο αρχείο στέλνεται μέσω δικτύου, πρώτα αποκρυπτογραφείται και στέλνεται σε «ανοιχτή» μορφή με ό,τι κινδύνους αυτό συνεπάγεται. Για κρυπτογράφηση κατά την διαβίβαση μπορεί να χρησιμοποιηθεί σε συνδυασμό με IPSec, L2TP τεχνολογίες.

Για να χρησιμοποιήσουμε EFS απλά κάνουμε σε έναν φάκελο δεξί κλικ ιδιότητες, advanced και επιλέγουμε Encrypt contents to secure data (Εικ. 9.45).

Αν στον φάκελο υπάρχουν φάκελοι και αρχεία, τότε εμφανίζεται η Εικ. 9.46 και επιλέγουμε ανάλογα.

Ο κρυπτογραφημένος φάκελος αλλάζει χρώμα.



Εικ. 9.46. Encrypting File System, επιλογές.

Αν θέλουμε να καταργηθεί η κρυπτογράφηση, κάνουμε δεξί κλικ ιδιότητες στον φάκελο advanced και αποεπιλέγουμε το Encrypt contents to secure data και OK .

9.3.2 Συμπίεση Αρχείων (File compression)

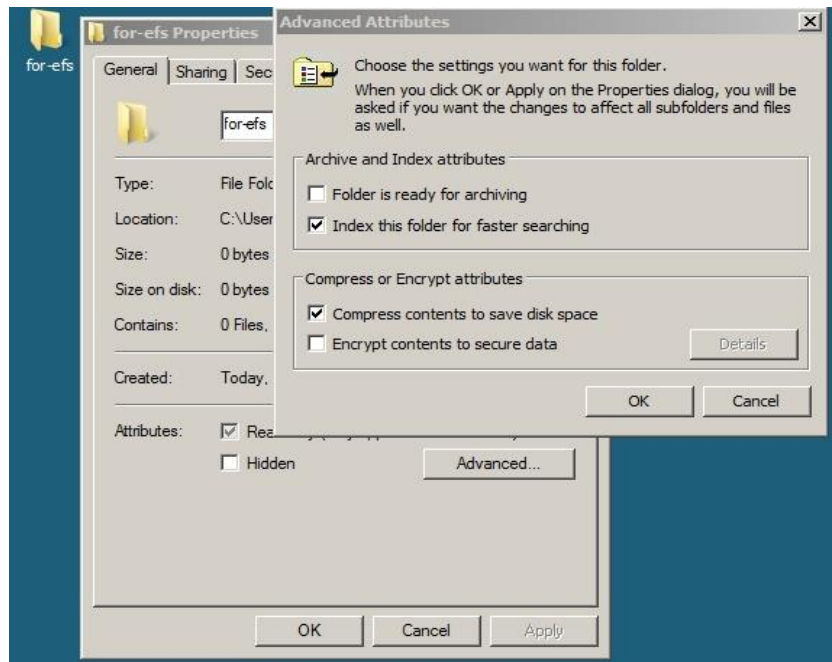
Συμπίεση κάνουμε για να εξοικονομήσουμε χώρο. Οι φάκελοι και τα αρχεία σε ένα NTFS volume μπορεί να είναι συμπιεσμένα ή ασυμπιεστά.

Όταν τα συμπιεσμένα αρχεία αντιγράφονται ή μετακινούνται σε έναν άλλο φάκελο στον ίδιο H/Y, το NTFS αποσυμπιέζει τα αρχεία , τα αντιγράφει ή τα μετακινεί στην νέα θέση και τα επανασυμπιέζει.

Η ίδια συμπεριφορά (αποσυμπίεση) πραγματοποιείται και κατά την μετακίνηση ή αντιγραφή του αρχείου μέσω δικτύου, γεγονός που δεν εξοικονομεί bandwidth.

Ένας φάκελος μπορεί να είναι συμπιεσμένος και όλα η κάποια από τα αρχεία που εμπεριέχει να μην είναι.

Για να συμπίεσουμε ένα φάκελο κάνουμε δεξί κλικ, properties, Advanced, επιλέγουμε Compress contents to save disk space και OK (Εικ. 9.47).



Εικ. 9.47. File compression.

Αν στον φάκελο υπάρχουν φάκελοι και αρχεία τότε εμφανίζεται η Εικ. 9.48 και επιλέγουμε ανάλογα.



Εικ. 9.48. File compression, επιλογές.

Αν θέλουμε να καταργηθεί η συμπίεση, κάνουμε δεξί κλικ ιδιότητες στον φάκελο advanced και αποεπιλέγουμε το Compress contents to save disk space και OK.

9.3.3 Quotas

Disk Quota, είναι ένας περιορισμός που τίθεται από τον διαχειριστή, με τον οποίο καθορίζει πόσο αποθηκευτικό χώρο θα χρησιμοποιήσει ένας χρήστης σε έναν δίσκο πέραν του οποίου δεν μπορεί να επεκταθεί. Η λειτουργικότητα της χρησιμοποίησης

Disk Quota έγκειται στον καθορισμό ορίων σε λογικά πλαίσια ανά μονάδα δίσκου και ανά χρήστη.

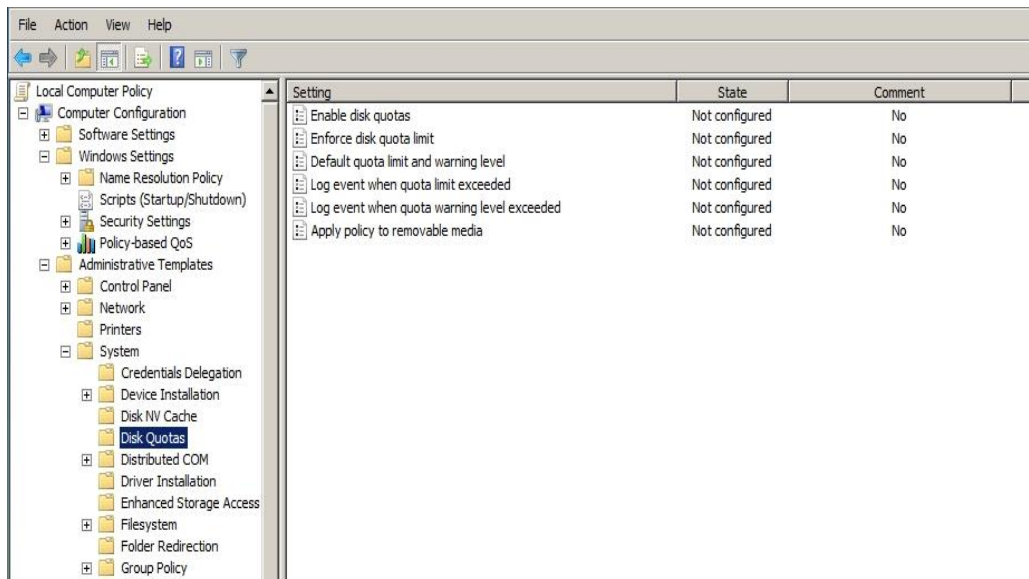
Για να λειτουργήσει είναι αναγκαία η χρησιμοποίηση NTFS και μπορεί να περιορίσει όλους τους χρήστες πλην των διαχειριστών.

Υπάρχουν δύο βασικοί τύποι Disk Quota.

Ο πρώτος που είναι γνωστός σαν usage quota ή block quota περιορίζει το σύνολο του δίσκου που μπορεί να χρησιμοποιηθεί, ενώ ο δεύτερος, γνωστός σαν file quota ή inode quota, περιορίζει τον αριθμό των αρχείων και των φακέλων που μπορούν να δημιουργηθούν.

Επιπροσθέτως οι διαχειριστές καθορίζουν ένα soft quota, το οποίο είναι ένα προειδοποιητικό επίπεδο που ενημερώνει τους χρήστες ότι πλησιάζουν το όριο τους, το οποίο βρίσκεται σε χαμηλότερο επίπεδο από το μέγιστο επιτρεπτό όριο χρησιμοποίησης ή hard quota. Υπάρχει ακόμα ένα επίπεδο «ανεκτικότητας» το grace interval, με το οποίο καθορίζεται στους χρήστες προσωρινά, αν είναι απαραίτητο, να ξεπερνούν τα quotas τους.

Το disk quota προτείνεται να καθορισθεί μέσω πολιτικής ασφαλείας (GPO), Εικ. 9.49, για καλύτερη διαχείριση.



Εικ. 9.49. Disk Quotas σε GPO.

9.3.3.1 Disk Quotas σε τοπική μονάδα δίσκου

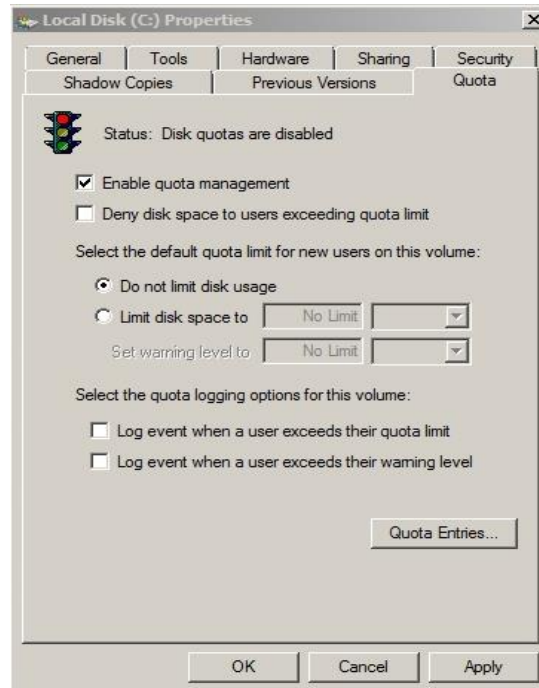
Για να χρησιμοποιήσουμε disk quota σε μια τοπική μονάδα δίσκου, πρέπει να την ενεργοποιήσουμε και να την ρυθμίσουμε κατάλληλα.

Στην μονάδα δίσκου πατάμε δεξί κλικ, properties, quota και εμφανίζεται η Εικ. 9.50.

Επιλέγοντας το Enable quota management ενεργοποιείται η διαδικασία.

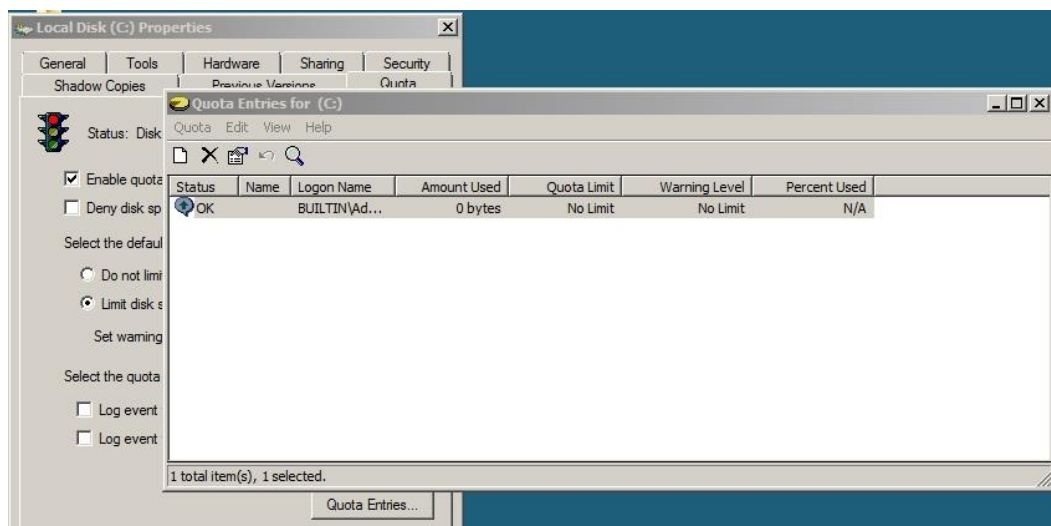
Αν επιλέξουμε Deny disk space to users exceeding quota limits, επιβάλλεται απαγόρευση υπερβάσης ορίου και απενεργοποιείται η «ανεκτικότητα».

Limit disk space to καθορίζει το χώρο χρησιμοποίησης, ενώ το set warning level to, το όριο που θα προειδοποιεί τον χρήστη ότι πλησιάζει την υπέρβαση.



Εικ. 9.50. Disk Quotas σε τοπική μονάδα δίσκου.

Η επιλογή Select the quota logging option for this volume αφορά ανάλογα με την πιο κάτω επιλογή την ενεργοποίηση καταγραφής σε log files συμβάντων σχετικά με το πότε ο χρήστης ξεπερνά τα όρια και πότε ξεπερνά τα επίπεδα προειδοποίησης.



Εικ. 9.51. Disk Quotas σε τοπική μονάδα δίσκου για χρήστες.

Τα όρια που έχουμε ορίσει αν στην προηγούμενη διαδικασία επιλέγαμε OK, αφορούν όλους τους χρήστες πλην των διαχειριστών.

Μπορούμε να επιλέξουμε ξεχωριστές καταχωρήσεις για κάθε χρήστη, αν στην Εικ. 9.50 επιλέξουμε Quota entries.

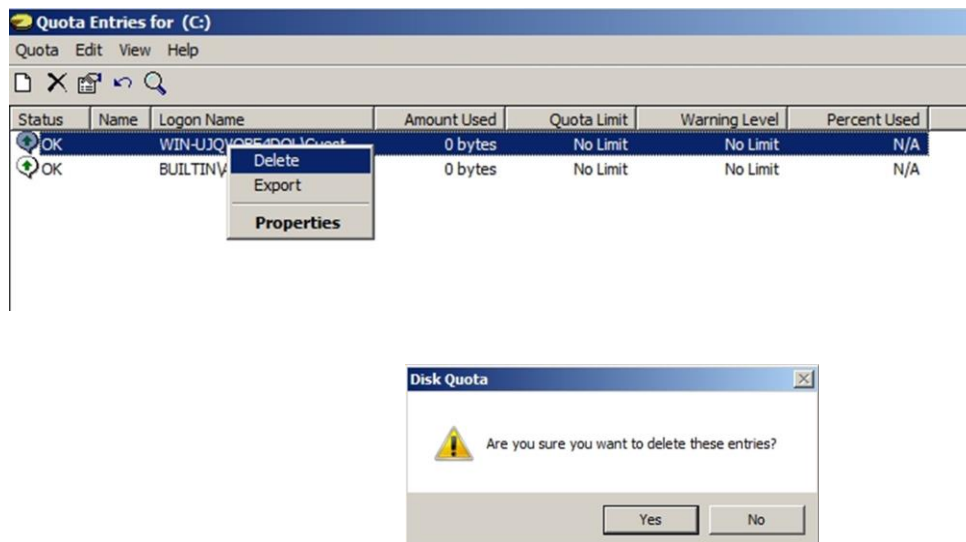
Στην Εικ. 9.51 μπορούμε να καταλάβουμε γιατί δεν υπάρχει όριο στο διαχειριστές αφού δηλώνεται ότι δεν θα έχουν όρια.

Ανάλογα αν επιλέξουμε Quota → New quota entry, αφού επιλέξουμε χρήστη, τότε μπορούμε να τον έχουμε χωρίς όρια ή να ορίσουμε συγκεκριμένα όρια (Εικ. 9.52).



Εικ. 9.52. Disk Quotas σε τοπική μονάδα δίσκου για χρήστες.

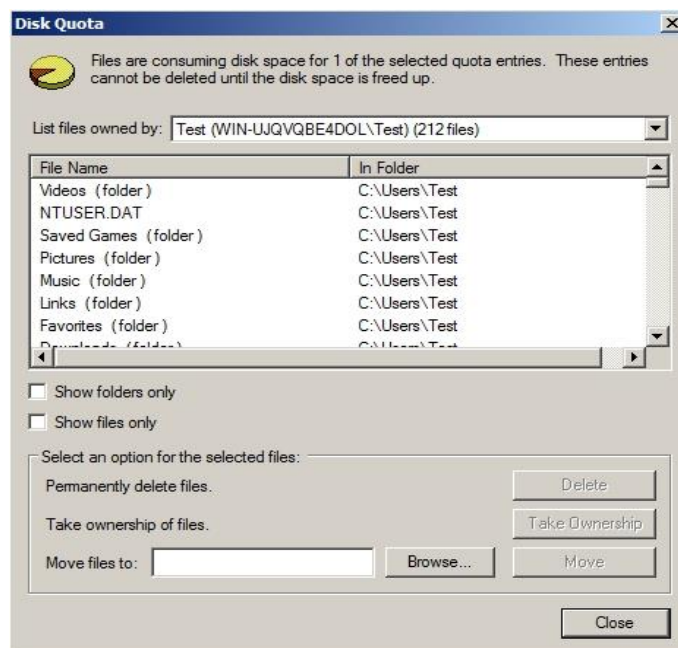
Αν θέλουμε να διαγράψουμε κάποιον χρήστη, με δεξί κλικ, delete (Εικ. 9.53) εμφανίζεται μια επιβεβαίωση και με YES διαγράφεται.



Εικ. 9.53. Disk Quotas σε τοπική μονάδα δίσκου διαγραφή χρήστη.

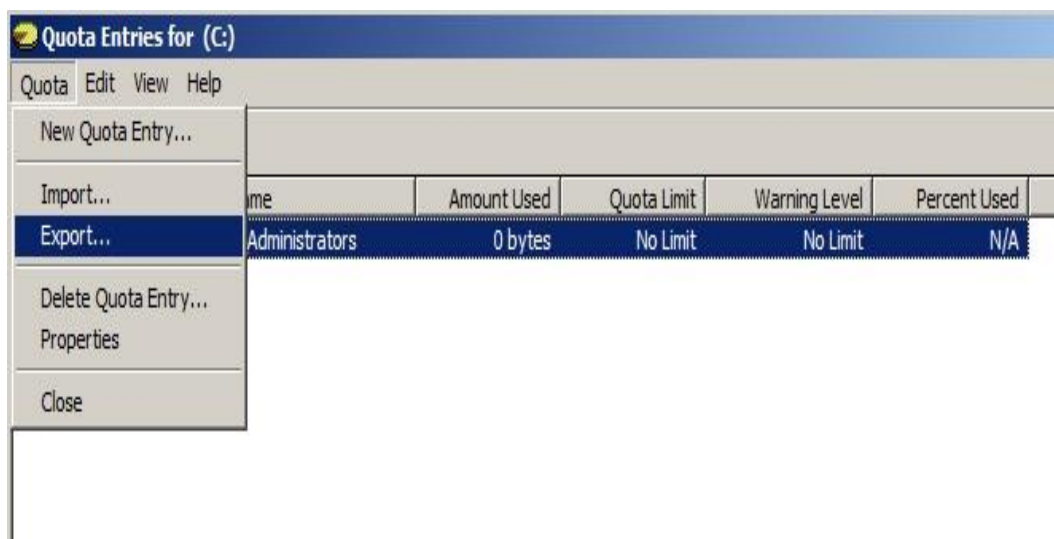
Αν ο χρήστης είχε δημιουργήσει αρχεία και φακέλους τότε κατά την διαγραφή εμφανίζεται η Εικ. 9.54. Εμφανίζεται οτιδήποτε έχει δημιουργηθεί και μπορούμε να

τα διαγράψουμε οριστικά, να αναλάβουμε το Ownership ή να μετακινήσουμε τα δεδομένα σε άλλο χώρο.



Εικ. 9.54. Disk Quotas σε τοπική μονάδα δίσκου διαγραφή χρήστη με αρχεία.

Αν θέλουμε για οποιονδήποτε λόγο να μεταφέρουμε ήδη ορισμένα σε άλλο δίσκο ή να τα εξασφαλίσουμε σαν backup τότε από το Quota → export (Εικ. 9.55) εξάγουμε τα δεδομένα σε ένα αρχείο και αν θέλουμε να τα επαναφέρουμε οπουδήποτε επιλέγοντας Import, τοποθετούνται στον νέο χώρο.

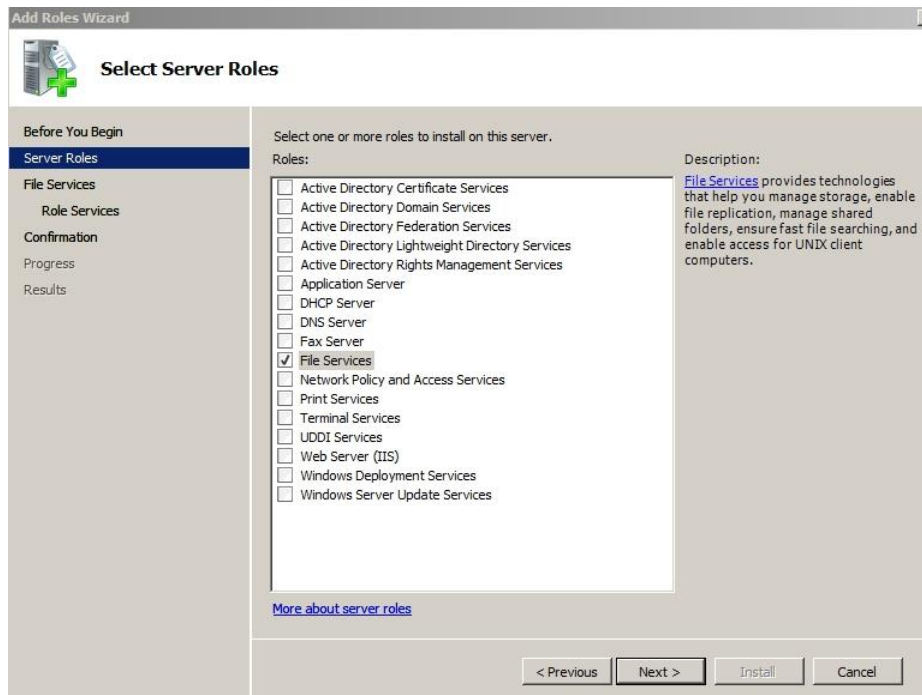


Εικ. 9.55. Disk Quotas, Import-Export ρυθμίσεις.

9.3.3.2 Quotas σε φάκελο

Η δυνατότητα Quotas σε αρχεία και φακέλους υπάρχει από τα windows server 2003 R2 και στον Sever 2008 εξελίχθηκε.

Για να χρησιμοποιηθεί, θα πρέπει να ενεργοποιηθεί μέσα από τον ρόλο του file service στον Server manager η επιλογή file server resource manager.

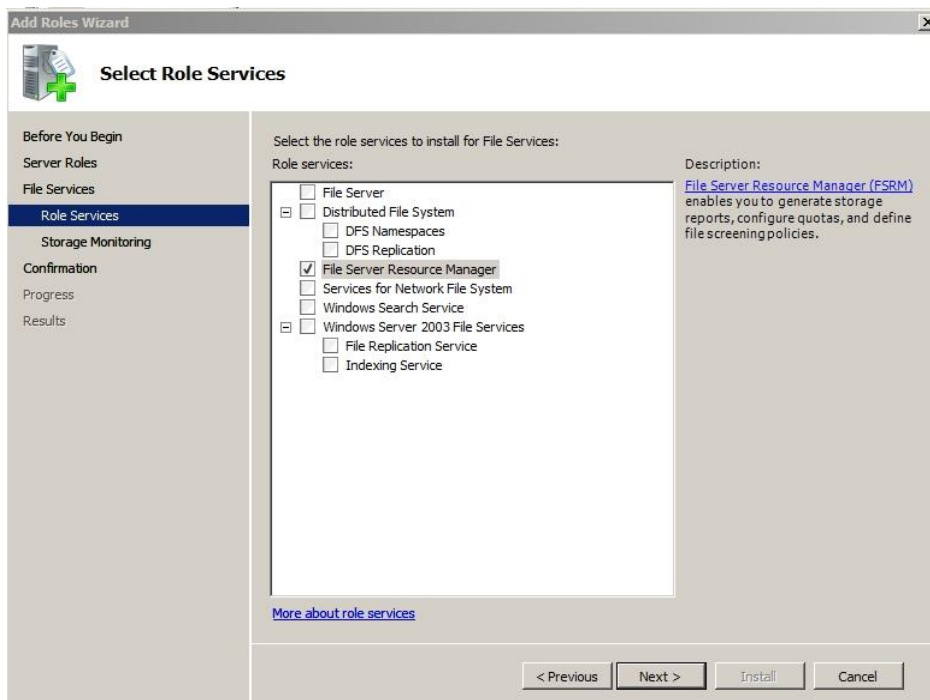


Εικ. 9.56. Προσθήκη ρόλου στον Server Manager.

Ειδικότερα στον Start → Administrative Tools → Server Manager → Roles → Add Roles αρχίζει ο οδηγός και επιλέγω File Services (Εικ. 9.56) και Next.

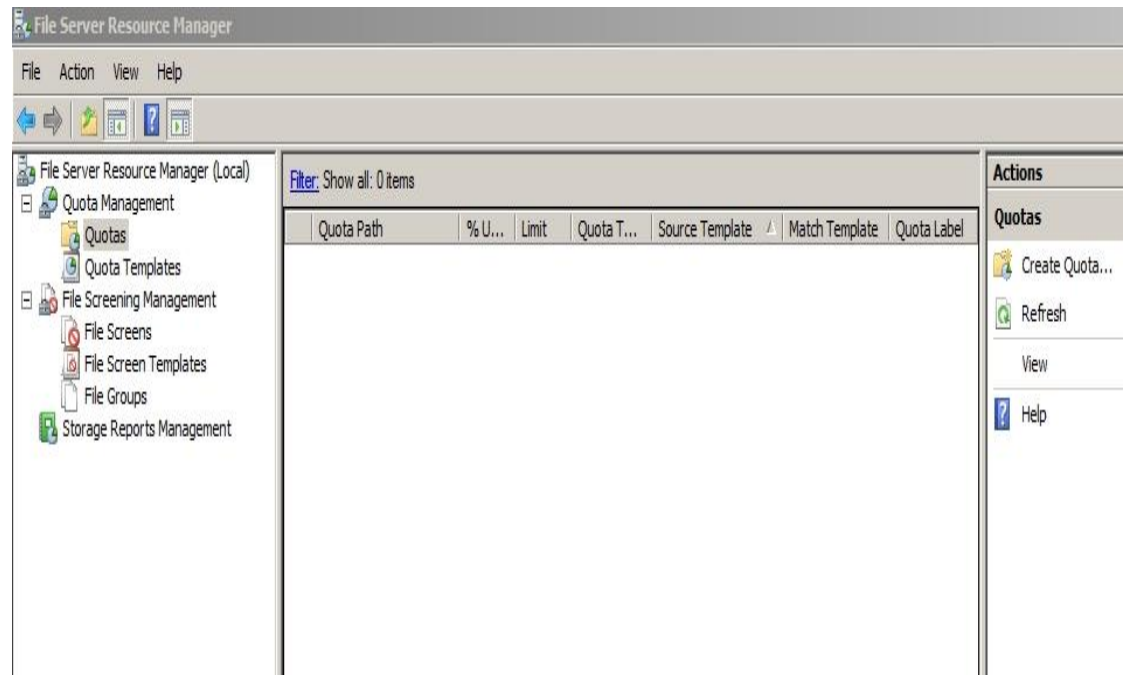
Επιλέγουμε file server resource manager και Next (Εικ. 9.57).

Ολοκληρώνουμε τον οδηγό και εγκαθίσταται ο file server resource manager.



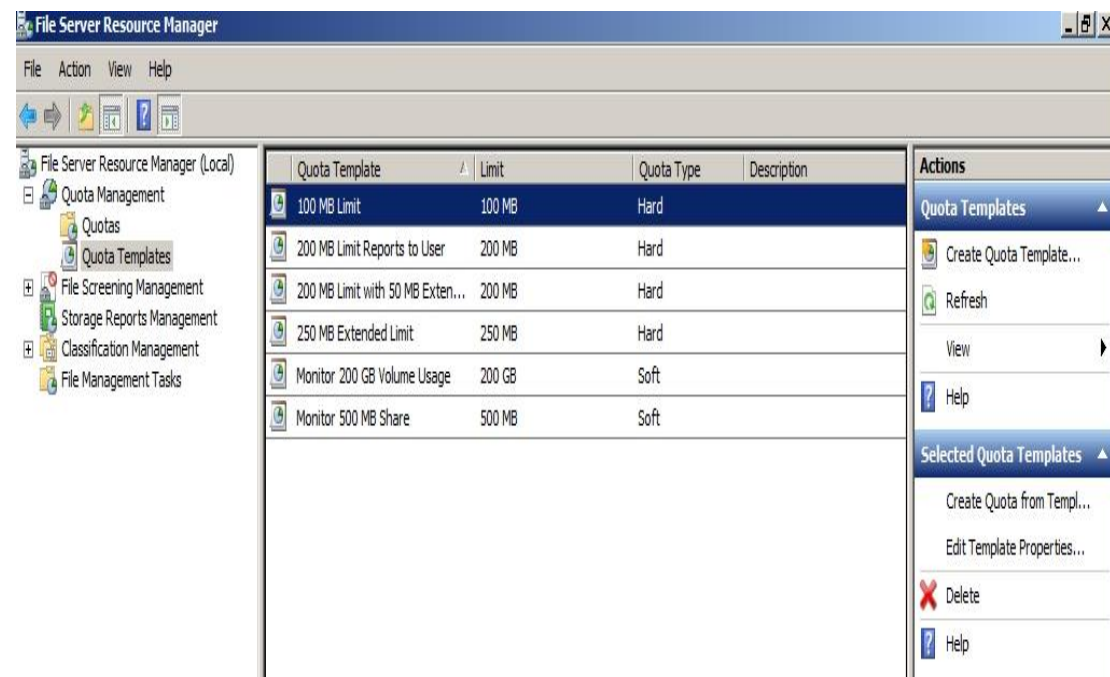
Εικ. 9.57. Προσθήκη ρόλου file server resource manager στον Server Manager.

Από **Start** → **Administrative Tools** → **File server resource manager** εμφανίζεται η κονσόλα διαχείρισης (Εικ. 9.58).



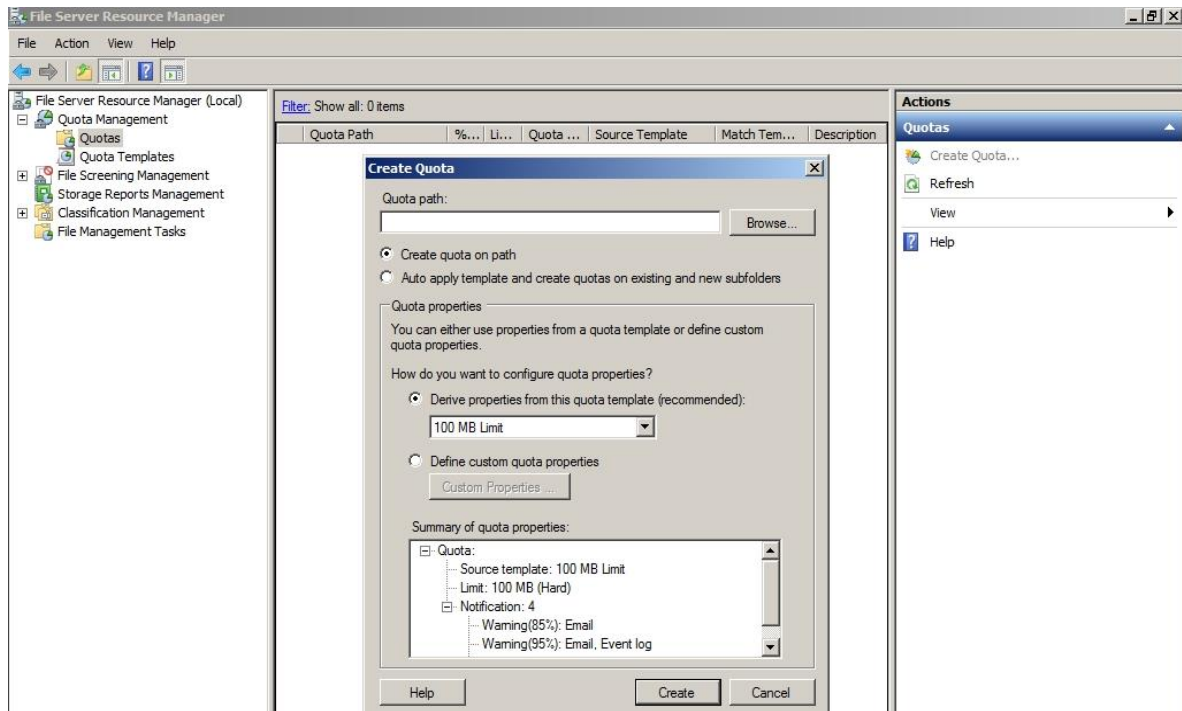
Εικ. 9.58. File server resource manager console.

Επιλέγοντας **Quota templates** εμφανίζονται προκαθορισμένες ρυθμίσεις (Εικ. 9.59), οι οποίες μας βοηθούν στην συνέχεια. Υπάρχει και η δυνατότητα να ορίσουμε δικά μας πρότυπα από το **Actions** → **Create Quota Template**.



Εικ. 9.59. Quota templates.

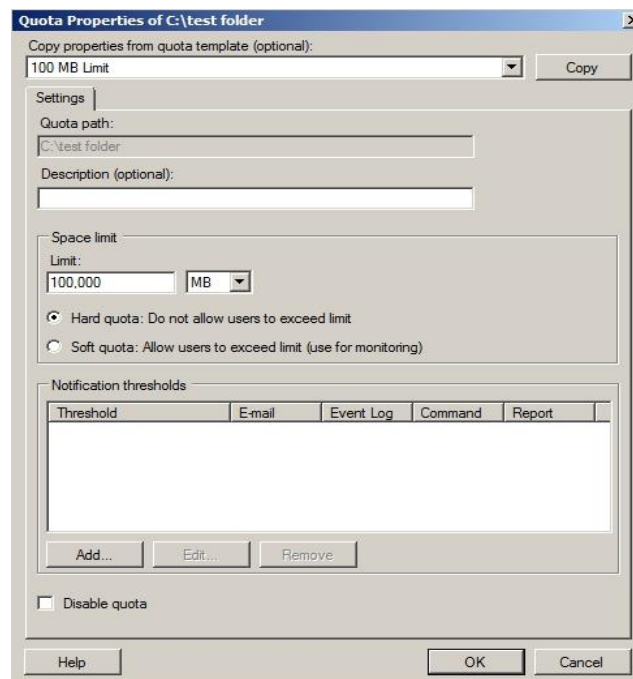
Για να δημιουργήσουμε quota για ένα φάκελο επιλέγουμε **quota management** → **Quotas** → **Actions** → **Create Quota** και εμφανίζεται η Εικ. 9.60.



Εικ. 9.60. Quota φακέλου.

Επιλέγουμε **Browse** και ορίζουμε τον φάκελο που επιθυμούμε.

Η επιλογή **create quota on path** δίνει την δυνατότητα επιλογής **Template**. Η επιλογή **Auto apply template and create quotas on existing and new subfolders** δεν επιτρέπει το **Define custom properties**.

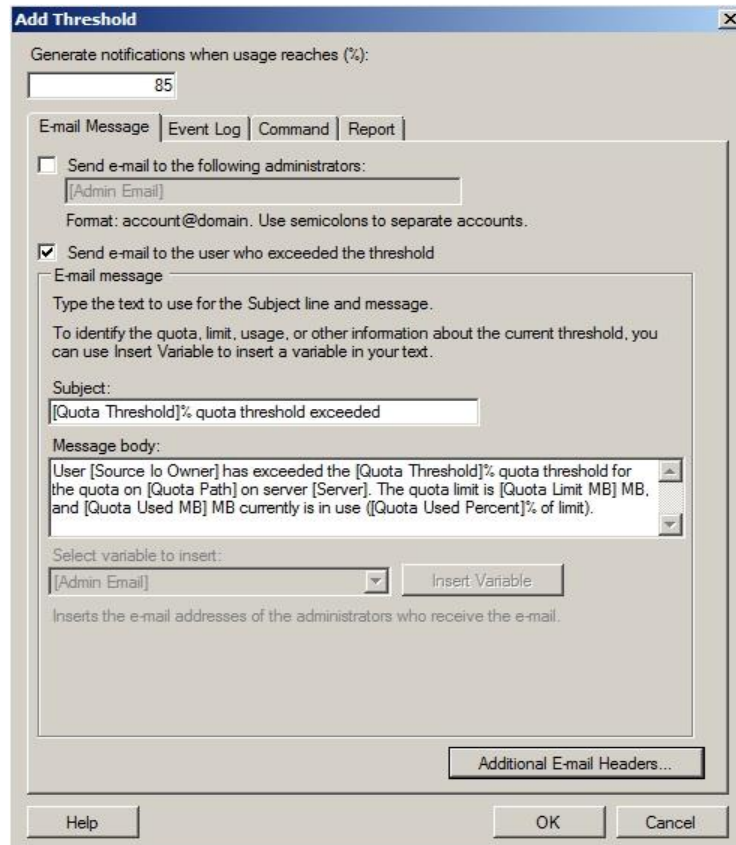


Εικ. 9.61. Quota φακέλου Custom.

Για κάθε επιλογή φαίνονται στο **Summary of quota properties** οι αντίστοιχες επιλογές.

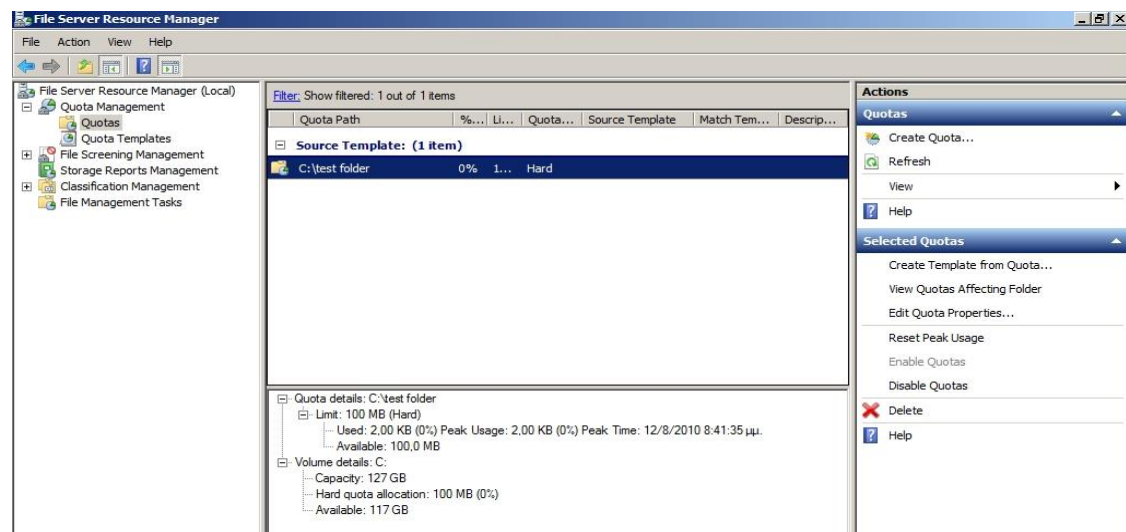
Επιλέγουμε **create quota on path** και **Define custom properties** και πατάμε **Custom properties**.

Εμφανίζεται η Εικ. 9.61 με επιλογές ανάλογες του disk quota, με περισσότερες, όμως, επιλογές ειδοποίησης που εμφανίζονται αν επιλέξουμε **Add** στο **Notification Thresholds** στην Εικ. 9.62.



Εικ. 9.62. Add Threshold.

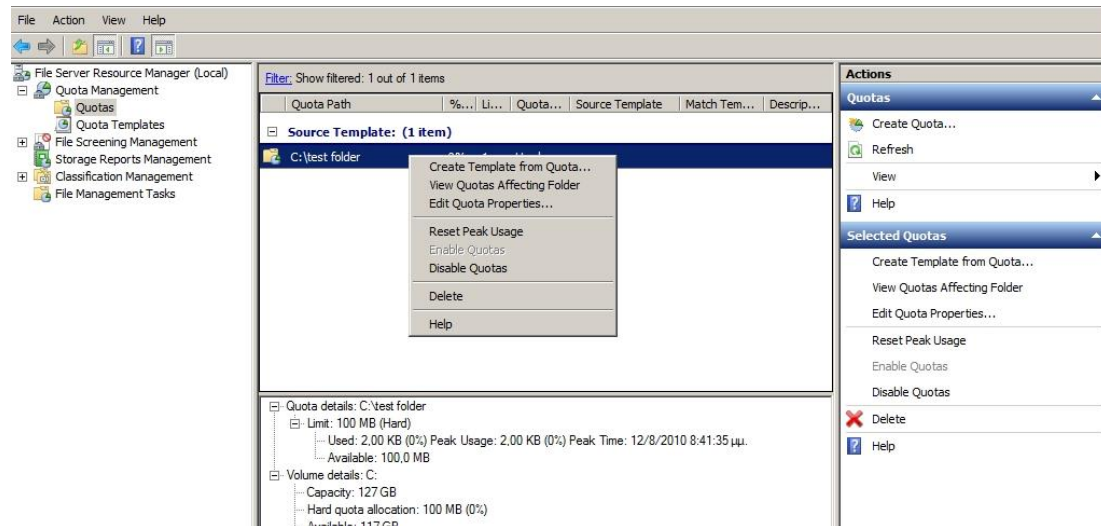
Επιλέγοντας cancel, επιστρέφουμε στην προηγούμενη φόρμα και OK.



Εικ. 9.63. Εμφάνιση των δημιουργημένων Quotas.

Στη συνέχεια **create** και έχουμε επιλογή να αποθηκευτεί σαν πρότυπο η ρύθμιση μας ή απλά να την δημιουργήσουμε.

Στην Εικ. 9.63 παρουσιάζονται τα δημιουργημένα quotas. Με δεξί κλικ σε κάποιο από αυτά παρουσιάζεται το μενού της Εικ. 9.64 με επιλογές που βρίσκονται και στο Action Panel δεξιά.



Εικ. 9.64. Διαχείριση Quotas.

Μπορούμε να δημιουργήσουμε πρότυπο, να δούμε τους φακέλους που επηρεάζονται, να διαμορφώσουμε τις ιδιότητες να επανακινήσουμε το Peak Usage, να απενεργοποιήσουμε και επαναενεργοποιήσουμε το quota και τέλος να το διαγράψουμε.

DISASTER RECOVERY

10.1 Εισαγωγή

Οι επιθυμητές γνώσεις και δεξιότητες που θα αποκτήσουν οι επιμορφωμένοι στην ενότητα Disaster Recovery, θα τους καταστήσουν ικανούς να :

- Περιγράφουν την αναγκαιότητα και τις στρατηγικές τήρησης αντιγράφων ασφαλείας.
- Δημιουργούν backups και να ανακτούν δεδομένα από αυτά στην αρχική ή σε εναλλακτική θέση.
- Λαμβάνουν αντίγραφο ασφαλείας της κατάστασης του συστήματος (System State) και άρα και του Active Directory.
- Χρησιμοποιούν εργαλεία και τεχνικές για επαναφορά σε περίπτωση ολικής αστοχίας του συστήματος.

10.2 Disaster Recovery

Γενικά σαν Disaster Recovery ορίζονται οι διαδικασίες, πολιτικές και άλλες σχετικές προπαρασκευαστικές ενέργειες, που λαμβάνονται για την επαναφορά ή την συνέχιση λειτουργίας της τεχνολογικής υποδομής ενός οργανισμού μετά από μια φυσική ή προκληθείσα από άνθρωπο, καταστροφή.

Για τον σκοπό αυτό είναι απαραίτητο να χρησιμοποιούμε τα κατάλληλα εργαλεία και να υπάρχει ένα σχέδιο βάση του οποίου θα είναι δυνατή η επαναφορά, εφόσον απαιτηθεί.

10.3 Βασικοί Ορισμοί

Backup: «Αντίγραφο ασφαλείας».

Restore: Επαναφορά «Αντιγράφου ασφαλείας».

Full Server backup: Περιλαμβάνει όλους τους τόμους προκειμένου να μπορούμε να κάνουμε επαναφορά σε ολόκληρο τον Server. Μπορούμε να κάνουμε επαναφορά σε όλους τους τύπους Restore συμπεριλαμβανομένων των system state και «bare metal».

Critical volumes: Αντίγραφο κατάλληλο για επαναφορά λειτουργικού συστήματος, κατάλληλο για «bare metal» επαναφορά.

System State Backup: Είναι αντίγραφο μιας συλλογής με κρίσιμα δεδομένα και περιλαμβάνει:

- System Registry

- COM + Database component object model
- Certificate Services
- Active Directory
- SysVol
- IIS Metabase

Bare Metal: «Άδειο (Κενό) μηχάνημα».

Individual Volumes Backup: Αντίγραφο τόμων για επαναφορά αρχείων, φακέλων, εφαρμογών και δεδομένων που βρίσκονται σε αυτούς.

Folder or Files Backup: Αντίγραφα ανεξαρτήτων αρχείων η φακέλων.

Incremental Backup: Backup με διαφορές από κανονικό backup (αν είναι το προηγούμενο) ή από προηγούμενο Incremental Backup.

Differential Backup: Backup με διαφορές πάντα από το κανονικό backup.

10.4 Windows Server Backup

Το Windows Server Backup είναι ένα εργαλείο που διατίθεται με τα Windows Server 2008 και Windows Server 2008 R2. Δεν είναι διαθέσιμο στις επιλογές εγκατάστασης του Server Core, αλλά μπορεί να χρησιμοποιηθεί μέσω της εντολής **Wbadmin** και **Power shell cmdlets** ή μέσω απομακρυσμένης διαχείρισης.

Διαθέτει οδηγούς και άλλα εργαλεία που μας δίνουν την δυνατότητα να δημιουργούμε «backups» και άλλες εργασίες επαναφοράς για τον server στον οποίο εγκαθίσταται. Στα Windows Server 2008 R2 έχει αναβαθμιστεί.

Η προηγούμενη έκδοση Server Backup, που ήταν διαθέσιμη στα Windows Server 2003 και παλαιότερα (Ntbackup.exe), έχει αφαιρεθεί.

Αποτελείται από ένα Microsoft Management Console (mmc) snap-in, ένα command-line tool και Power shell cmdlets καθιστώντας το σαν μια ολοκληρωμένη λύση για τις καθημερινές backup-recovery ανάγκες.

Έχει δυνατότητες:

- Backup ολόκληρου του Server, συγκεκριμένων τόμων(volumes) και στο 2008 R2, του system state, συγκεκριμένων αρχείων και φακέλων, καθώς και Backup για χρησιμοποίηση σε «bare metal» (κενό) μηχάνημα.
- Επαναφορά (recovery) τόμων, φακέλων, αρχείων και στο 2008 R2 συγκεκριμένων εφαρμογών, του system state και σε περιπτώσεις καταστροφής του δίσκου, «bare metal» επαναφορά.
- Δημιουργεί και διαχειρίζεται backup για τον συγκεκριμένο ή και για

απομακρυσμένο H/Y, ενώ μπορεί να προγραμματισθεί η λειτουργία μέσω αυτομάτων διαδικασιών.

- Εξαιρέσεις αρχείων που δεν θα περιλαμβάνονται στο backup βάσει τύπου ή path.
- Αυτόματη διαχείριση full και incremental backups, γιατί σαν προεπιλογή δημιουργεί incremental backup, το οποίο συμπεριφέρεται σαν Full backup. Μπορούμε δηλαδή, να επαναφέρουμε οποιοδήποτε αρχείο ή φάκελο, ενώ το backup καταλαμβάνει τον χώρο ενός incremental backup.
- Δεν χρειάζεται την συγκατάθεση του χρήστη για να διαγράψει παλαιότερα backups, αλλά τα διαγράφει αυτόματα, για να ελευθερώσει χώρο για καινούργια backups.
- Αποθηκεύει backups σε απομακρυσμένο κοινόχρηστο φάκελο (συντηρώντας μόνο ένα backup) και σε virtual hard disks.

Για να χρησιμοποιήσουμε το Windows Server Backup, θα πρέπει να είμαστε μέλη της ομάδας των Administrators ή των Backup operators.

Θα πρέπει να γνωρίζουμε ότι:

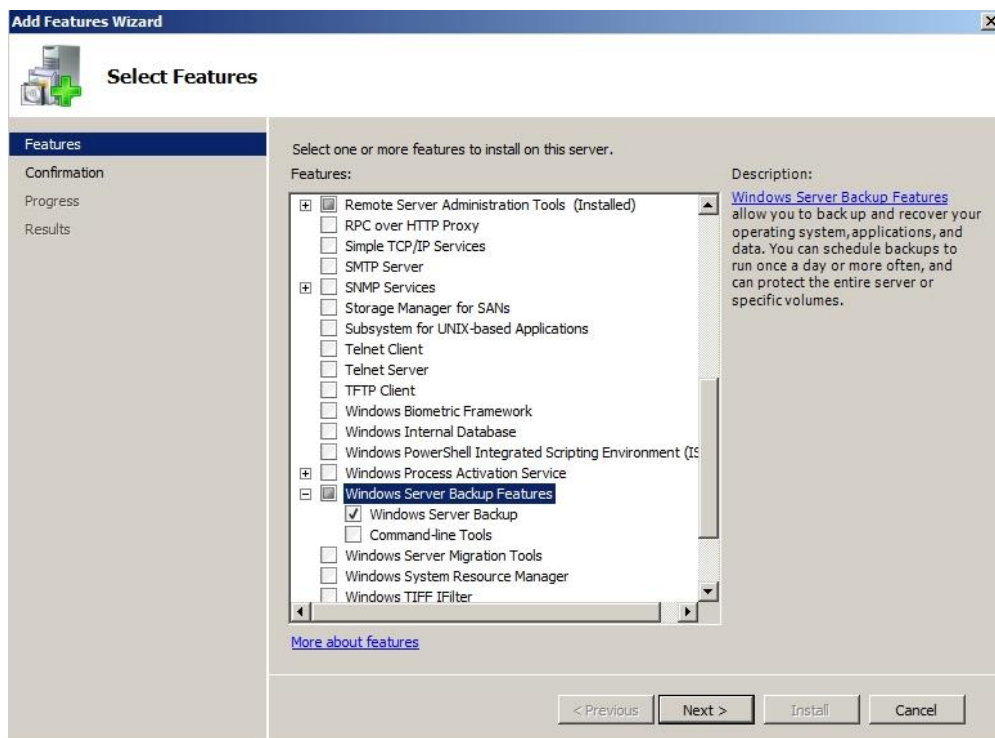
- Οι κυρίες διαδικασίες backup και restore πρέπει να πραγματοποιούνται μεταξύ υπολογιστών που διαθέτουν την ίδια έκδοση Server 2008 ή Server 2008 R2 ενώ οι υπόλοιπες μπορούν σε οποιαδήποτε έκδοση.
- Δεν μπορούμε να χρησιμοποιήσουμε backup από Server 2008 για να επαναφέρουμε system state υπολογιστή που τρέχει Server 2008 R2, διότι στην επαναφορά system state η full επαναφορά συστήματος πρέπει να χρησιμοποιείται backup από την ίδια έκδοση των windows που επαναφέρουμε.
- Δεν υποστηρίζει backup από ή προς και αποθήκευση του σε clustered shared folders.
- Μπορούμε να πάρουμε backup ενός virtual machine μέσα από Windows Server Backup που «τρέχει» σε virtual machine.
- Όταν γίνεται upgrade σε Windows Server 2008 Backup, δεν μεταφέρονται ρυθμίσεις από προηγούμενα backups και πρέπει να επαναρυθμιστούν.
- Δεν μπορούμε να κάνουμε restore σε backup που πραγματοποιήθηκε με το Ntbackup αλλά υπάρχει μια έκδοση του Ntbackup για server 2008 μέσω της οποίας, αφού εγκατασταθεί, πραγματοποιείται επαναφορά χωρίς δυνατότητα δημιουργίας νέου.
- Μόνο NTFS τόμοι γίνονται backup.

- Δεν γίνεται backup σε αρχεία ή φακέλους σε τόμους μεγαλύτερους από 2TB.
- Δεν μπορούμε να αποθηκεύουμε σε tapes, ενώ αποθηκεύουμε σε εξωτερικούς και εσωτερικούς δίσκους, removable media (CD, DVD) και κοινόχρηστους φακέλους.

10.4.1 Προπαρασκευαστικές εργασίες

Πριν προχωρήσουμε στην εγκατάσταση και περιγραφή της κονσόλας είναι αναγκαίο να καθορισθούν κρίσιμα σημεία δημιουργίας, διαχείρισης και αποθήκευσης των backups.

- Τι θέλουμε; αυτοματοποιημένο, προγραμματισμένο ή με δικό μας χειρισμό (manual) Backup;
- Τι θα κάνουμε Backup;
- Θα χρειαστούμε «Full» backup;
- Πόσες φορές την μέρα, την εβδομάδα, τον χρόνο και ποιες ώρες πρέπει να κάνουμε Backup;
- Τι θα χρησιμοποιούμε σαν αποθηκευτικό χώρο; δίσκο, τόμο, πολλαπλούς δίσκους ή κοινοχρήστους φακέλους και οπτικούς δίσκους;
- Χρησιμοποιούμε Bitlocker Drive Encryption για την προστασία στο server, ώστε και ο αποθηκευτικός χώρος να διαθέτει την ίδια προστασία;



Εικ. 10.1. Add Windows Server Backup features.

- Είναι τα δεδομένα που θα κρατήσουμε Backup περισσότερα από 2TB και αν ναι πως θα τα κατανείμουμε προκειμένου να ξεπεράσουμε τον αντίστοιχο περιορισμό; Αφού καταγραφούν οι απαντήσεις θα πρέπει να εγκαταστήσουμε το Windows Server Backup διότι δεν είναι ενεργοποιημένο μετά την εγκατάσταση των Windows Server 2008.

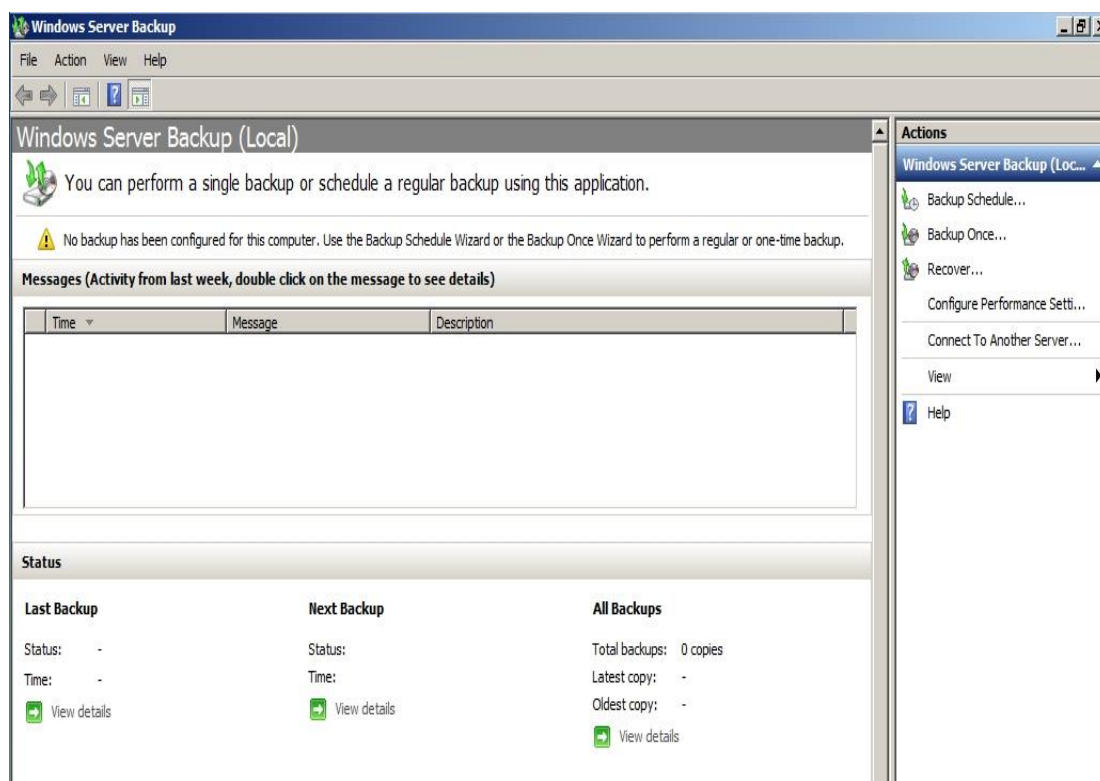
Αποτελεί **Feature** και για να το εγκαταστήσουμε ακολουθούμε:

Start→Administrative tools→Server Manager, στο αριστερό panel επιλέγουμε **Add feature** και οδηγούμαστε στην Εικ. 10.1.

Επιλέγουμε Windows Server Backup και next για να ολοκληρωθεί η εγκατάσταση.

Μετά την ολοκλήρωση έχουμε πρόσβαση από:

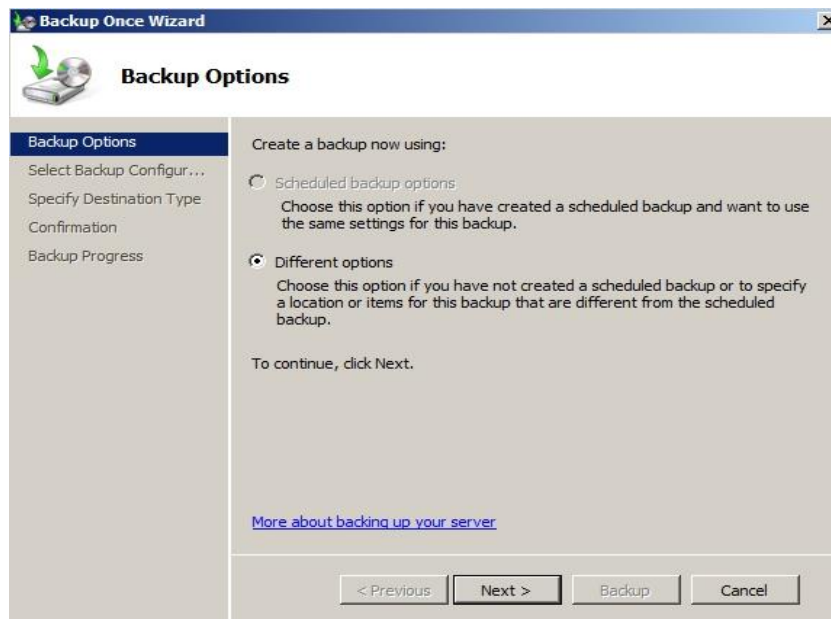
- Start→Administrative tools→Server manager→ Storage→Windows Server Backup** και
- Start→Administrative tools→ Windows Server Backup** όπου παρουσιάζεται η Εικ. 10.2 με την Κονσόλα διαχείρισης Windows Server Backup.



Εικ. 10.2. Κονσόλα διαχείρισης Windows Server Backup.

Παρατηρούμε το κεντρικό panel, όπου βλέπουμε τα Backups που έχουν ληφθεί, το status με πληροφορίες για το τελευταίο Backup, το επόμενο προγραμματισμένο και όλα τα Backups.

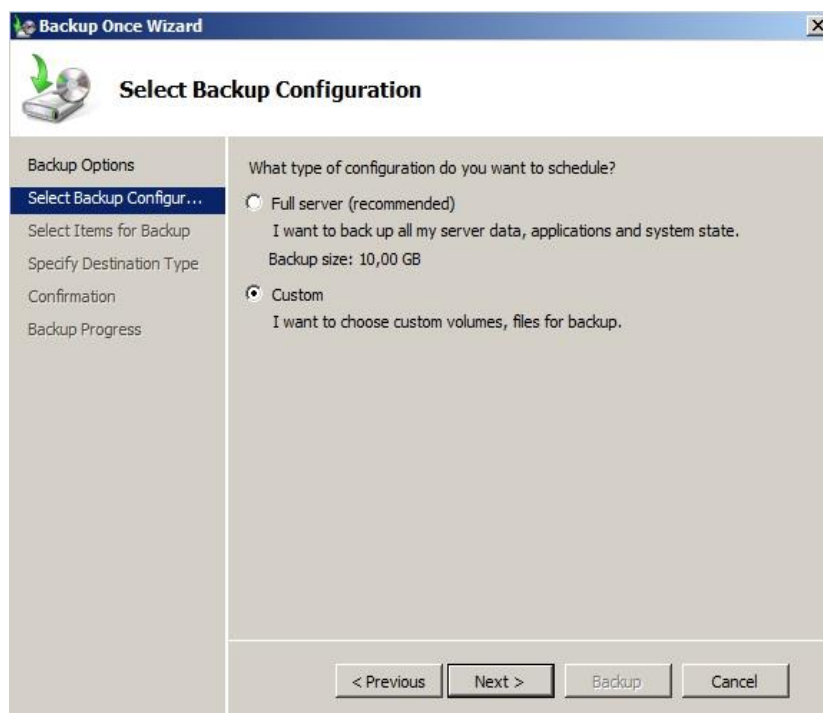
Δεξιά στο Action panel υπάρχουν οδηγοί για οποιονδήποτε τύπο Backup – Recovery.



Εικ. 10.3. Οδηγός Backup Once.

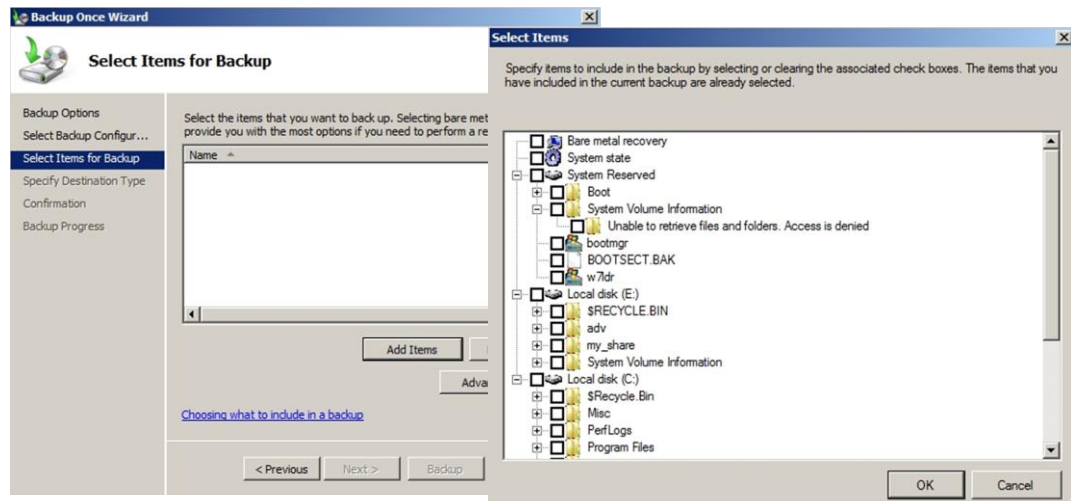
10.4.2 Δημιουργία Αντιγράφων Ασφαλείας Δεδομένων (Backup)

Μέσω της επιλογής Backup Once οδηγούμαστε να ξεκινήσουμε το πρώτο μας backup ή τα επόμενα manual backups, Εικ. 10.3. Παρουσιάζεται ο Wizard 2008 R2 προκειμένου να κατανοήσουμε τις επιπρόσθετες δυνατότητες που παρέχονται σε σχέση με το 2008 backup.



Εικ. 10.4. Οδηγός Backup Once.

Επιλέγουμε full ή custom (Εικ. 10.4) και Next, **ενώ** αν έχουμε 2008 R2, πατάμε **Add Items**, προκειμένου να παρουσιαστεί η Εικ. 10.5,

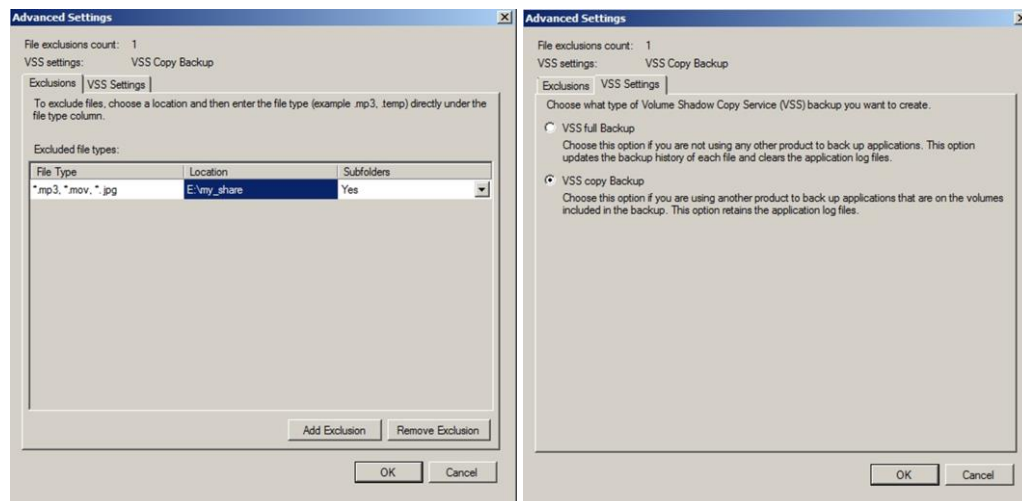


Εικ. 10.5. Επιλογή για Backup.

στην οποία μπορούμε να επιλέξουμε:

- Bare Metal και αυτόματα θα επιλεγούν τα αναγκαία.
- System State, μόνο για το System State.
- Τόμους, αρχεία φακέλους, και επιλέγουμε OK.

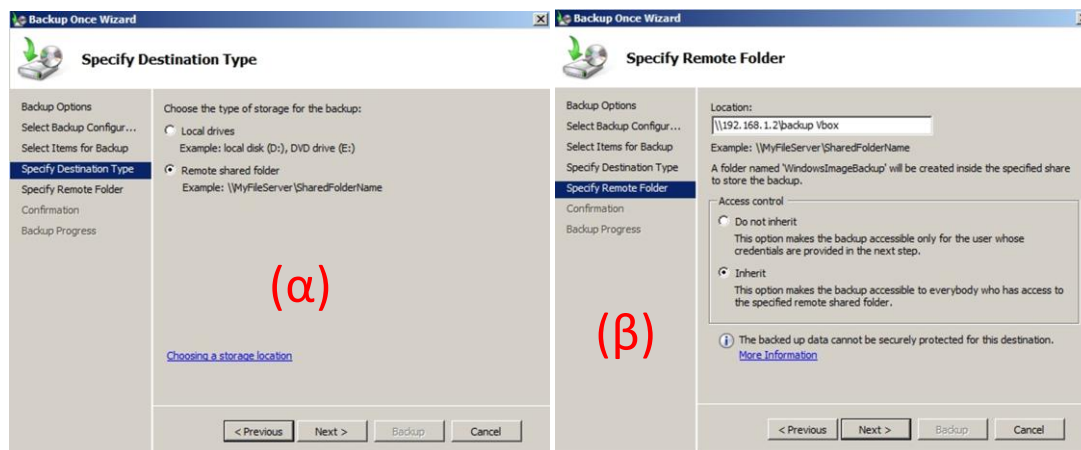
Πατώντας Advanced εμφανίζεται η Εικ. 10.6, που περιέχει δύο καρτέλες. Την Exclusions,



Εικ. 10.6. Επιλογή Advanced.

με την οποία εξαιρούμε τύπους αρχείων από συγκεκριμένους φακέλους και την Volume Shadow copy Service (VSS) settings, με την οποία καθορίζουμε το είδος του VSS.

- VSS full backup, αν δεν χρησιμοποιούμε άλλο πρόγραμμα για backup εφαρμογών, προκειμένου να ενημερώνει το backup ιστορικό κάθε αρχείου και να καθαρίζει τα Log files.
- VSS copy backup, όταν χρησιμοποιούμε άλλο πρόγραμμα για backup εφαρμογών που βρίσκονται στον backup τόμο, για να παραμένουν τα log files των εφαρμογών.

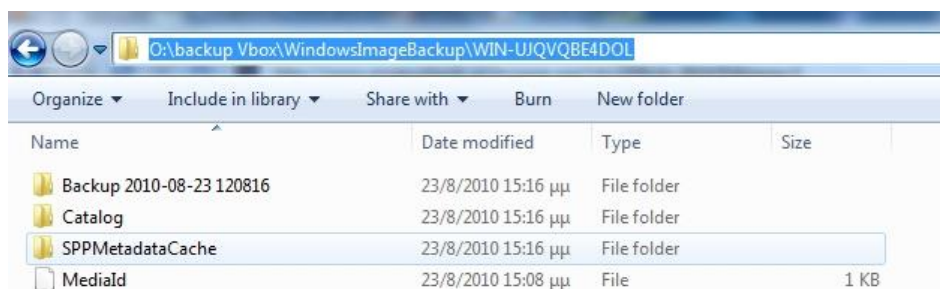


Εικ. 10.7. Επιλογή Αποθηκευτικού χώρου.

Μετά το next, εμφανίζεται η Εικ. 10.7 (α) για επιλογή του αποθηκευτικού χώρου, διαλέγουμε για παράδειγμα **remote share folder** → next στην Εικ. 10.7 (β) δίνουμε την διαδρομή του κοινόχρηστου φακέλου και επιλέγουμε αν θέλουμε να διατηρηθεί ή όχι η κληρονομικότητα στον φάκελο.

Θα ρωτηθούμε για κωδικό και password προκειμένου να υπάρχει πρόσβαση στον κοινόχρηστο φάκελο και σε περίπτωση ορθής καταχώρησης ξεκινά η διαδικασία λήψης του backup.

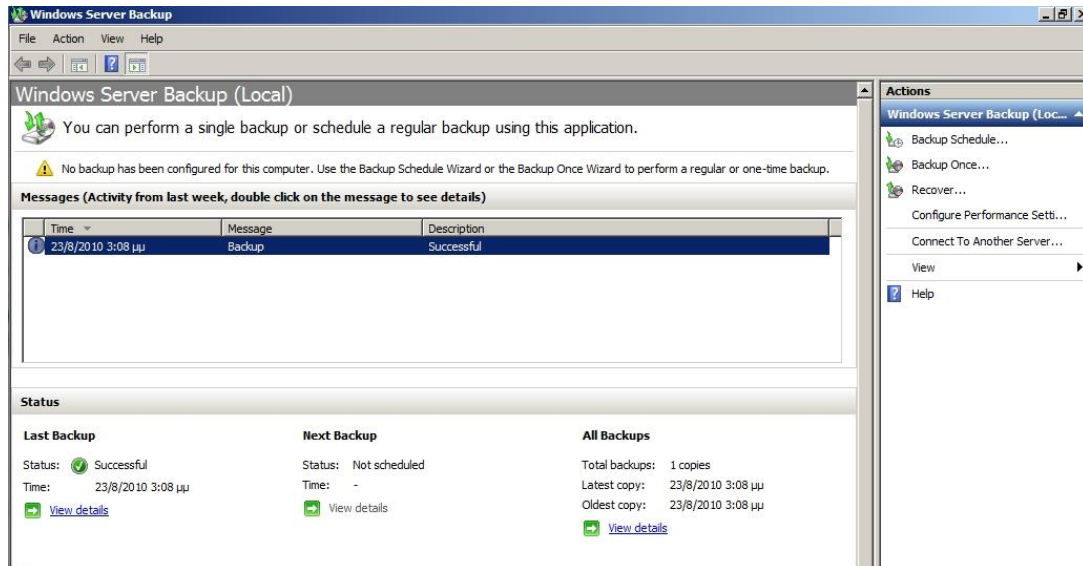
Όταν ολοκληρωθεί η διαδικασία στη Εικ. 10.8 παρουσιάζεται η δομή του κοινόχρηστου καταλόγου όπου τοποθετήθηκε το backup, που δημιουργήθηκε αυτόματα.



Εικ. 10.8. Ο κοινόχρηστος φάκελος με το backup.

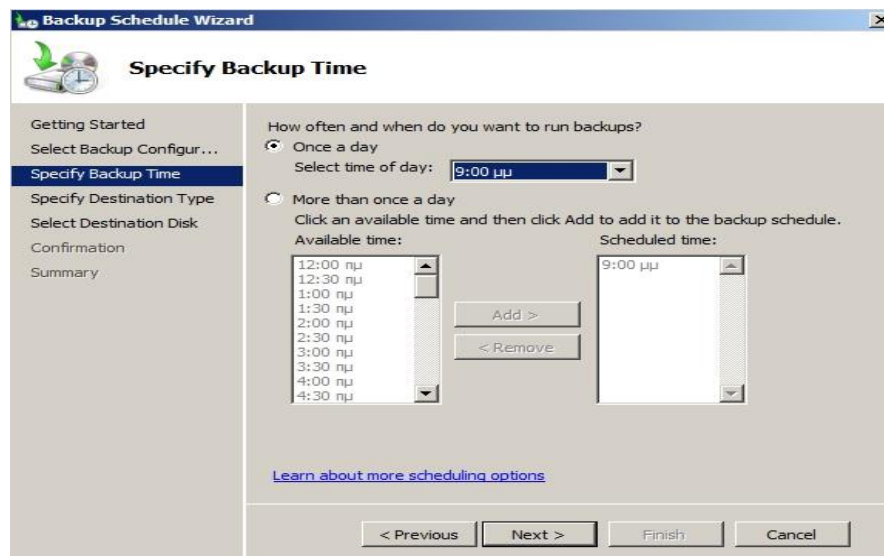
Ο φάκελος **Catalog** περιέχει λεπτομέρειες για το backup και εφόσον καταστραφεί, εμφανίζεται οδηγός που μπορεί να τον επαναφέρει.

Στην Εικόνα 10.9 παρουσιάζεται η κονσόλα διαχείρισης μετά την ολοκλήρωση του backup.



Εικ. 10.9. Η κονσόλα διαχείρισης μετά την ολοκλήρωση του backup.

10.4.3 Χρονοπρογραμματισμός Εργασιών Backup

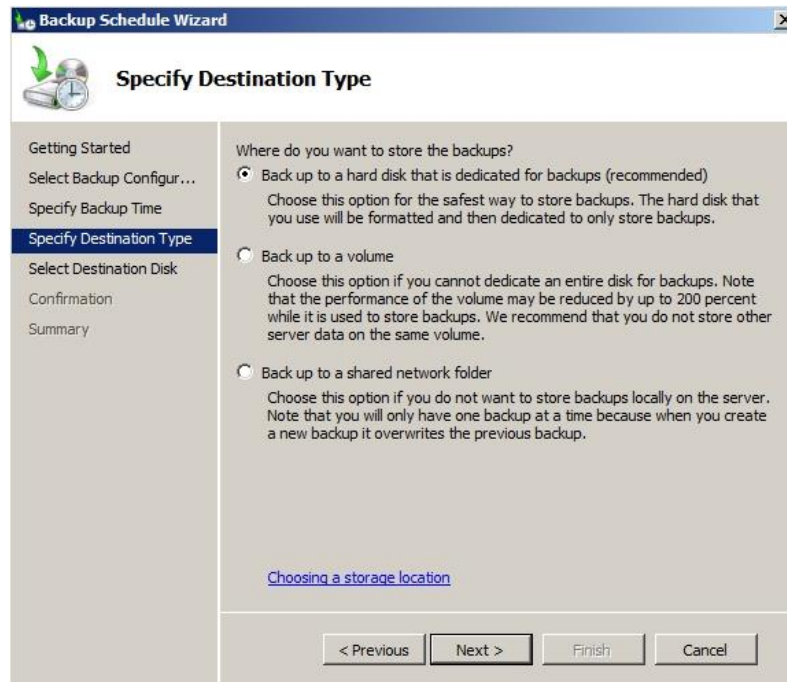


Εικ. 10.10. Χρονοπρογραμματισμός Backup.

Με το **backup schedule** έχουμε την δυνατότητα να χρονοπρογραμματίσουμε τις διαδικασίες για οπότε θέλουμε, ώστε να ενεργούνται αυτόματα. Ταυτόχρονα μπορούμε να επεμβαίνουμε και να επαναρυθμίζουμε τους χρονοπρογραμματισμούς.

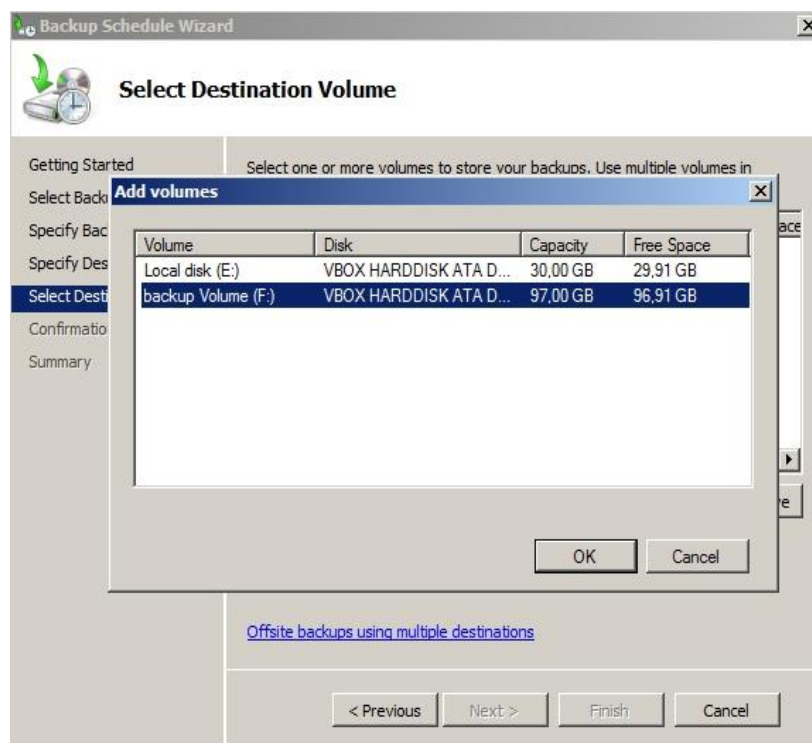
Επιλέγοντας στο Action panel **backup schedule**, ξεκινά ένας οδηγός και αφού ερωτηθούμε αν θέλουμε full ή custom backup, διαλέγουμε full και εμφανίζεται η εικόνα 10.10 (Αν επιλέξουμε custom ακολουθούμε επιλογές όπως πιο πάνω).

Εδώ επιλέγουμε τον χρόνο και την ή τις φορές που θέλουμε να εκτελείται το backup και οδηγούμαστε στην Εικ.10.11 για να διαλέξουμε τον χώρο αποθήκευσης.



Εικ. 10.11. Αποθήκευση Backup.

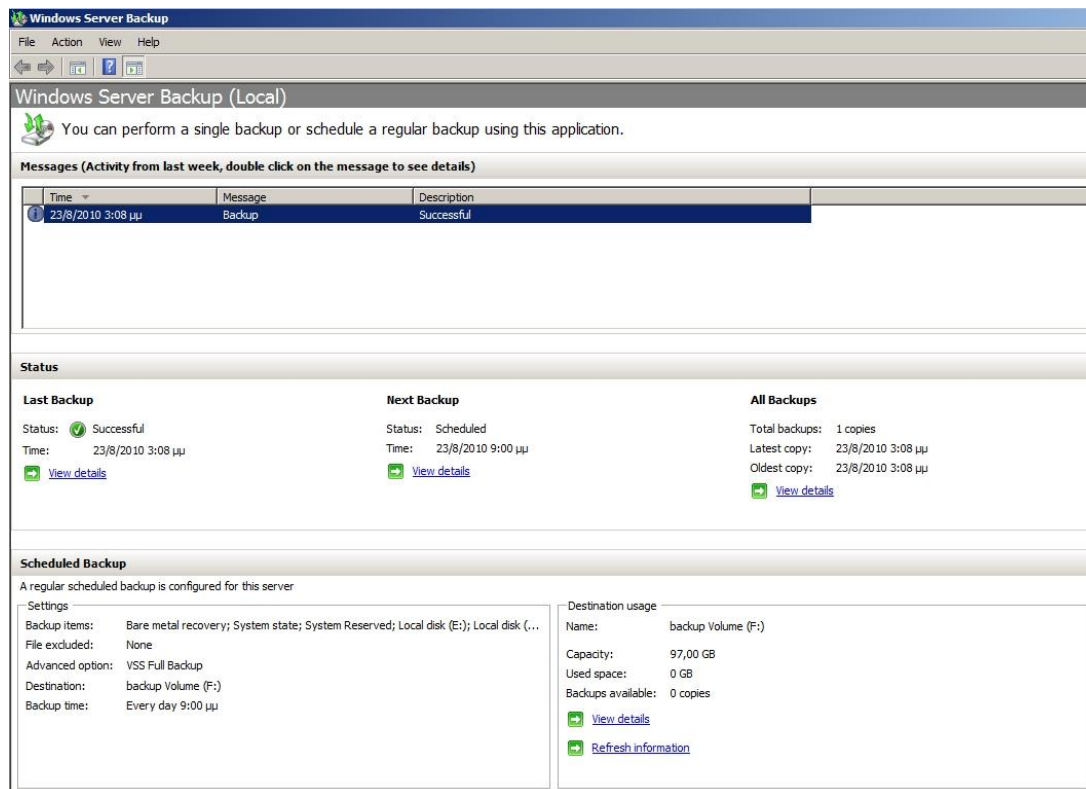
Επιλέγοντας dedicated disk→next διαλέγουμε από τους υπάρχοντες δίσκους (Εικ. 10.12) έχοντας υπόψη ότι ο δίσκος θα μορφοποιηθεί και θα χρησιμοποιείται μόνο για Backups.



Εικ. 10.12. Αποθήκευση Backup.

Επιλέγουμε Οκ και next και αφού παρουσιαστεί μια περίληψη του τι επιλέξαμε, ολοκληρώνεται ο προγραμματισμός.

Ξεκινώντας ξανά τον οδηγό και εφόσον έχει δημιουργηθεί κάποιος χρονοπρογραμματισμός, υπάρχει επιλογή edit.



Εικ. 10.13. Κονσόλα διαχείρισης με προγραμματισμό Backup.

Στην Εικ. 10.13 παρουσιάζεται η Κονσόλα διαχείρισης με προγραμματισμό Backup, όπου και φαίνεται ο επόμενος προγραμματισμός και στοιχεία του Schedule backup.

Για την δημιουργία **Αντιγράφων Ασφαλείας Συστήματος** και **Active Directory Backup** μπορούμε να χρησιμοποιήσουμε οποιαδήποτε μέθοδο (manual ή schedule), αρκεί να επιλέξουμε το **system state**.

10.4.4 Ανάκτηση δεδομένων από Αντίγραφο Ασφαλείας (Restore)

Για να προβούμε σε ανάκτηση δεδομένων από ένα αντίγραφο ασφαλείας, μας παρέχονται οι παρακάτω οδηγοί:

- Recovery Wizard στο Windows Server Backup για επαναφορά αρχείων, φακέλων, εφαρμογών, τόμων και του system state.
- Catalog Recovery Wizard στο Windows Server Backup, το οποίο επαναφέρει το αρχείο Catalog με τις λεπτομέρειες για τα backup και εμφανίζεται, όταν καταστραφεί το αρχείο catalog.

- Windows Recovery Environment και ένα backup δημιουργημένο στο Windows Server Backup. Το περιβάλλον αυτό μπορεί να χρησιμοποιηθεί μέσα από Windows Server 2008 R2 ή από ένα Windows Setup Disk και βοηθά στην επαναφορά λειτουργικού συστήματος, όπως και στην επαναφορά Full Server.
- Επαναφορά γίνεται και μέσω των εντολών **Wbadmin start recovery**, **Wbadmin start systemstaterecovery** και **Wbadmin restore catalog**.

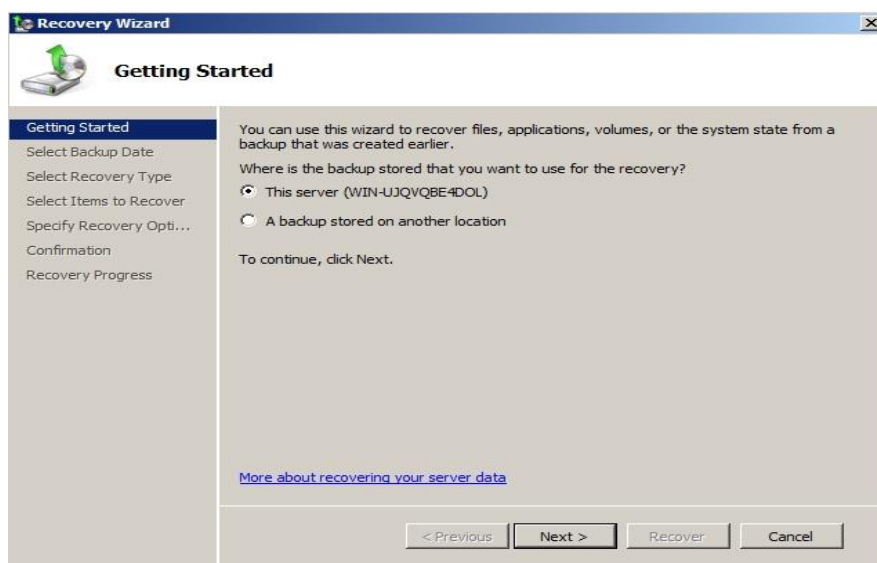
Στην περίπτωση επαναφοράς από το Windows Server Backup θα πρέπει να έχουμε καθορίσει:

- Τι θέλουμε να επαναφέρουμε;
- Το είδος του backup που θα χρειαστεί;
- Από ποια τοποθεσία θα γίνει το restore;

Σε περίπτωση επαναφοράς από το Windows Recovery Environment και ενός backup δημιουργημένου στο Windows Server Backup θα πρέπει να έχουμε ένα δίσκο εγκατάστασης Windows ή το περιβάλλον να μπορεί να «τρέχει» από τον δίσκο και να καθορίσουμε:

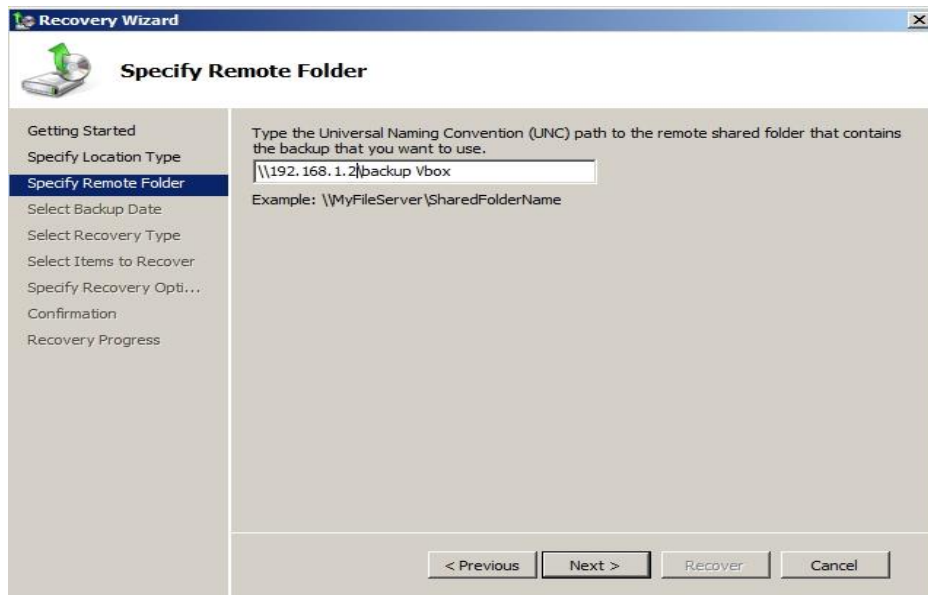
- Το Backup από το οποίο θα επαναφέρουμε;
- Που θα επαναφέρουμε; Στο ίδιο μηχάνημα ή σε άλλο;
- Έχει τον κατάλληλο χώρο για αυτά που θα επαναφέρουμε;
- Τι θα επαναφέρουμε; Critical volumes ή full server;

Αφού καταγραφούν οι απαιτήσεις μας ξεκινάμε την διαδικασία restore μέσα από τον Windows Server Backup (Παρακάτω θα δούμε πώς γίνεται restore από το Windows Recovery Environment), επιλέγοντας **Action → Restore**.



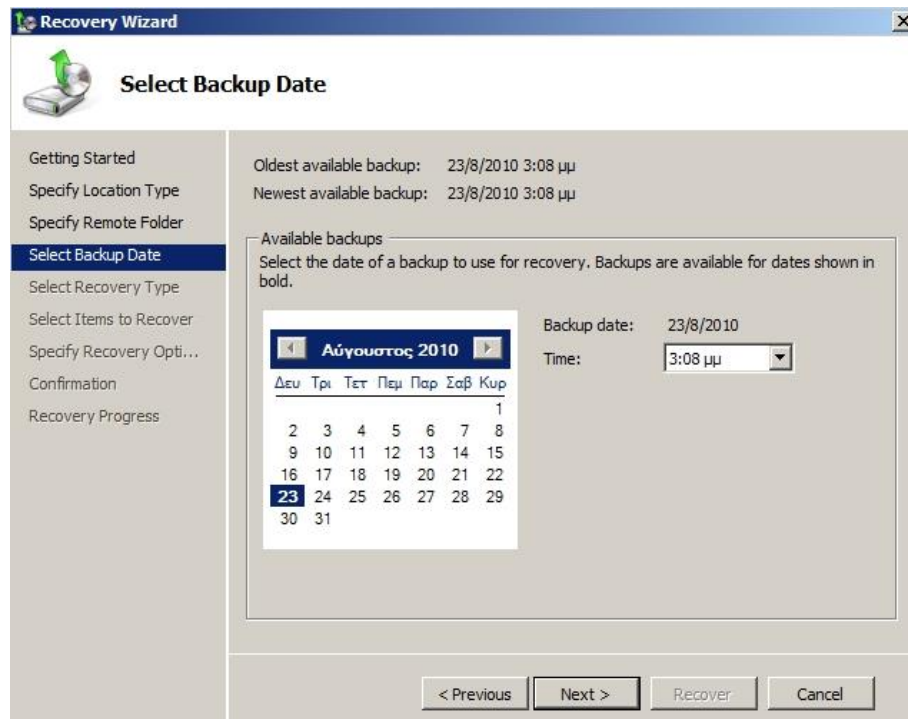
Εικ. 10.14. Restore από την κονσόλα Windows Server Backup.

Ξεκινά ο οδηγός και παρουσιάζεται η Εικ. 10.14, η οποία ζητά να ορίσουμε που βρίσκεται το αρχείο Backup, που θα χρησιμοποιήσουμε. Επιλέγουμε **a backup stored**



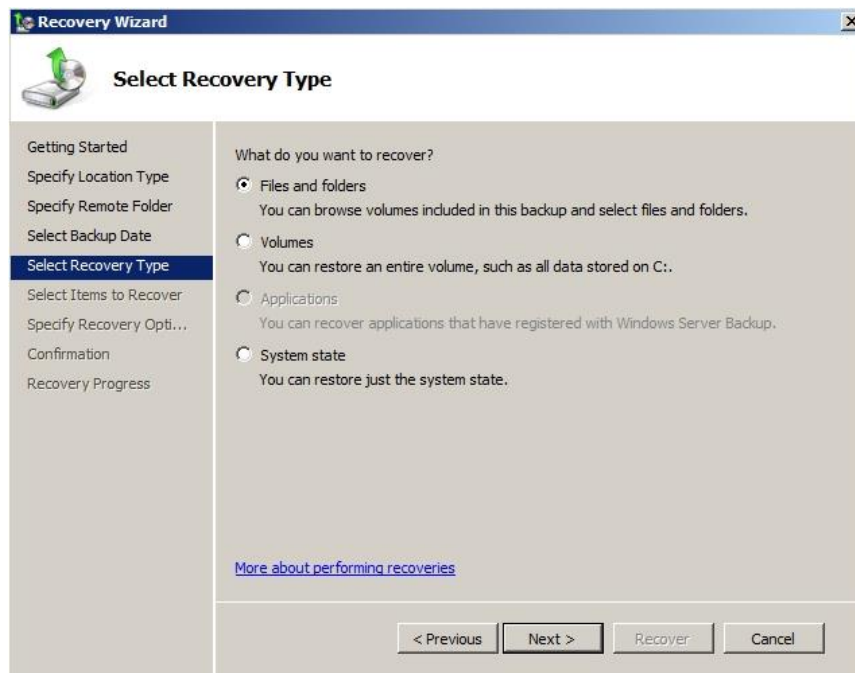
Εικ. 10.15. Restore από τον κοινόχρηστο φάκελο.

on another location και στην Εικ. 10.15 δίνουμε την διαδρομή του κοινόχρηστου φακέλου που χρησιμοποιήσαμε για το Backup.



Εικ. 10.16. Επιλογή Backup βάση ημέρας και ώρας.

Στην Εικ. 10.16 και εφόσον υπάρχουν αρκετά backups, επιλέγουμε ανάλογα με την ημέρα και την ώρα το κατάλληλο.

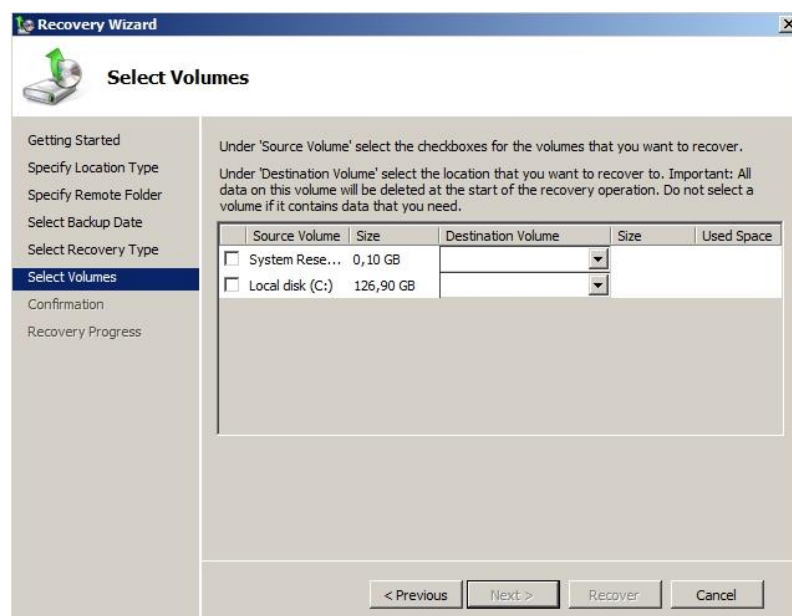


Εικ. 10.17. Επιλογή από full Backup.

Αν ήταν full backup ή «bare metal» εμφανίζεται η Εικ. 10.17 για να επιλέξουμε.

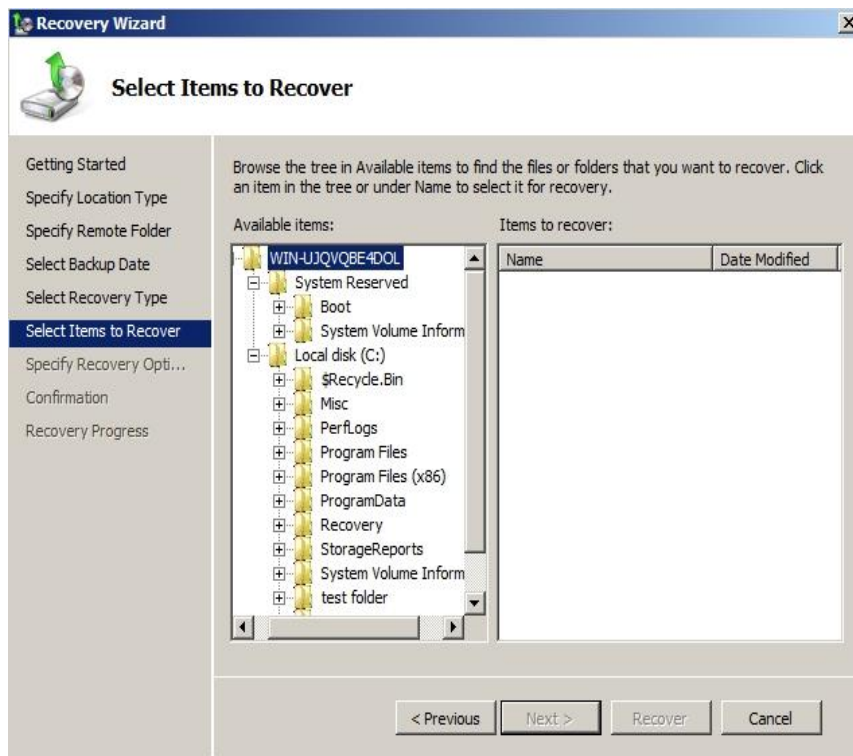
Για επαναφορά system state ακολουθεί δυνατότητα επιλογής για το που θα γίνει το backup. Στην original location ή σε alternate location. Επιλέγουμε ανάλογα και ολοκληρώνεται το restore (απαιτεί reboot).

Για επαναφορά τόμου ακολουθεί η Εικ. 10.18, για να διαλέξουμε source και destination, που επιθυμούμε την επαναφορά. Προειδοποιούμε ότι πρόκειται να διαγραφούν τα προηγούμενα περιεχόμενα του τόμου και ολοκληρώνεται η διαδικασία.



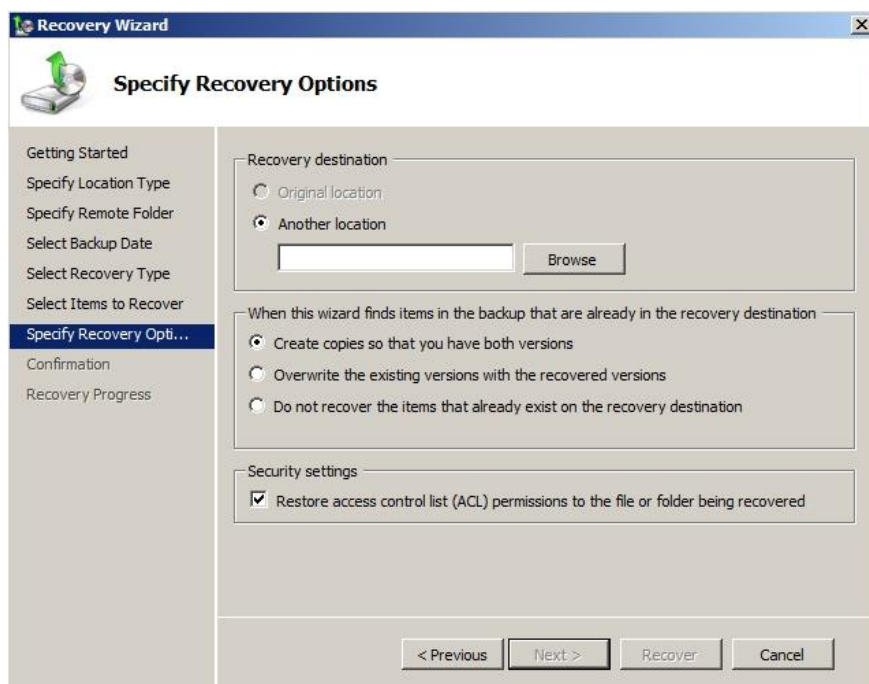
Εικ. 10.18. Επιλογή επαναφοράς τόμου.

Για επαναφορά αρχείων και φακέλων μετά την επιλογή, ακολουθεί η Εικ. 10.19.



Εικ. 10.19. Επιλογή επαναφοράς αρχείων και φακέλων.

Επιλέγουμε και με next εμφανίζεται η Εικ. 10.20, στην οποία ορίζουμε τον χώρο που θα πραγματοποιηθεί η επαναφορά, αν θα γίνει overwrite υπάρχον αρχείο ή θα γραφεί και το αντίγραφο, ώστε να υπάρχουν και τα δύο ή δεν θα αντιγραφεί το αρχείο, αν ήδη υπάρχει το ίδιο (αρχείο) στον φάκελο επαναφοράς.



Εικ. 10.20. Επιλογές επαναφοράς αρχείων και φακέλων.

Ταυτόχρονα υπάρχει προεπιλογή επαναφοράς και των access control lists (ACL) permissions στο αρχείο ή φάκελο που επαναφέρουμε. Στην συνέχεια ολοκληρώνεται η επαναφορά.

10.4.5 Windows Recovery Environment και ένα backup δημιουργημένο στο Windows Server Backup

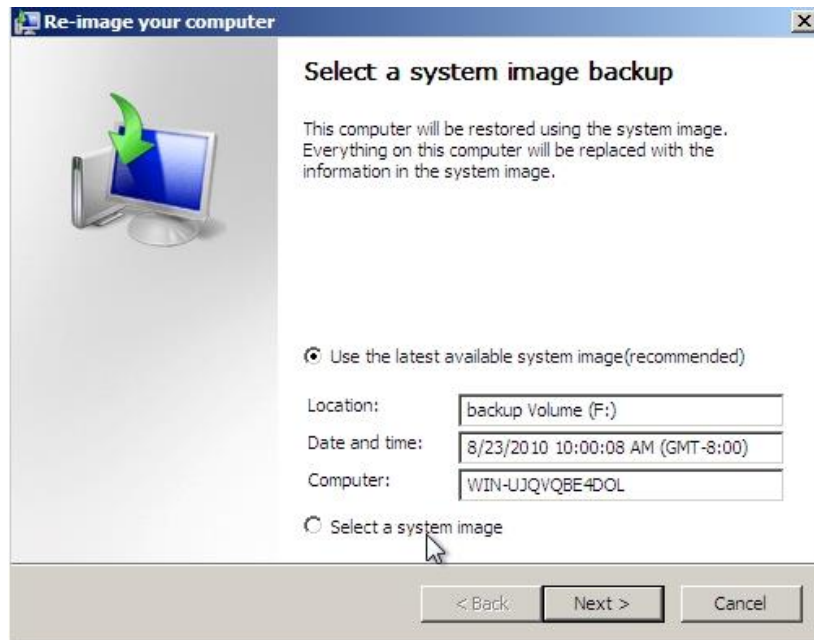
Η μέθοδος αυτή χρησιμοποιείται για επαναφορά λειτουργικού συστήματος ή ολοκλήρου του server, μετά από **Server Failure**, και απαιτεί το DVD εγκατάστασης των windows που θα κάνει το restore με προσοχή στα προαναφερθέντα περί έκδοσης των windows και ένα full ή «bare metal» backup.



Εικ. 10.21. Repair your computer με boot DVD.

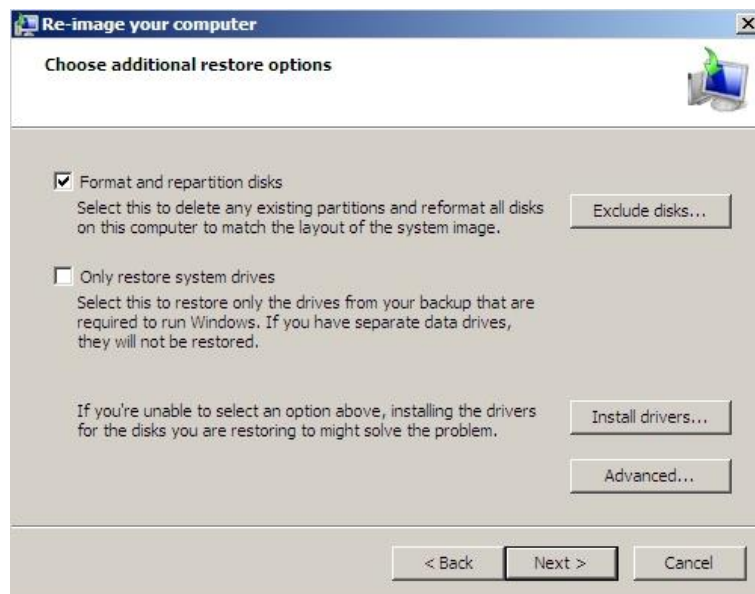
Αφού γίνει εκκίνηση από το DVD και περάσουμε την εικόνα της γλώσσας (βάζουμε Greece στο Time and currency format), με next εμφανίζεται η Εικ. 10.21, στην οποία διαλέγουμε Repair your computer.

Το setup ψάχνει στον δίσκο για εγκαταστάσεις windows και δίνει αποτελέσματα στην σελίδα system recovery. Επιλέγουμε System image recovery και εμφανίζεται η Εικ. 10.22



Εικ. 10.22. Επιλογή system image backup.

Διαλέγουμε το latest available (recommended) ή επιλέγουμε select a system image για να διαλέξουμε κάποιο άλλο.



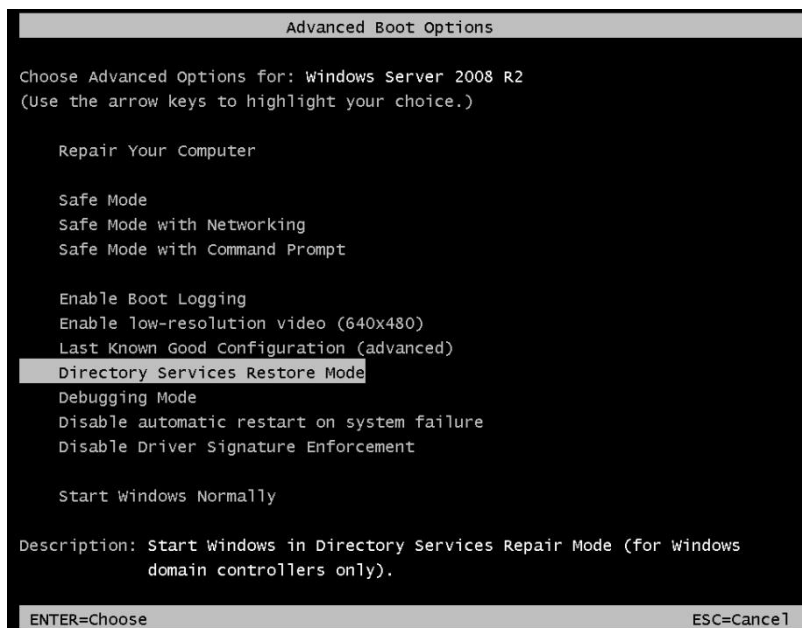
Εικ. 10.23. Επιπρόσθετες επιλογές.

Μετά τις προσθετές επιλογές (Εικ. 10.23) ξεκινά η διαδικασία και ολοκληρώνεται με reboot.

10.4.6 Active directory Restore

Το Active directory αποτελεί μέρος του system state και εφόσον κάνουμε restore to system state, όπως είδαμε ότι γίνεται πιο πάνω μέσα από τον Windows Server Backup.

Η ίδια διαδικασία ακολουθείται, αν την στιγμή της εκκίνησης του Server πατήσουμε F8 για να παρουσιαστεί η εικόνα 10.24.



Εικ. 10.24. Directory services restore mode.

Επιλέγουμε Directory services restore mode και enter.

Συνδεόμαστε σαν Administrator, ξεκινάμε το πρόγραμμα Backup και κάνουμε επαναφορά του System State.

Μετά την επανεκκίνηση ξεκινά και το active directory.

10.4.7 Shadow copies

Τα Shadow copies δεν αντικαθιστούν το backup, αλλά χρησιμοποιούνται σαν τεχνολογία στο Windows Server Backup για βελτιστοποίηση της απόδοσης.

Ανάλυση, δημιουργία, παραμετροποίηση των **Shadow copies** παρουσιάστηκε στην ενότητα 8.4.5.

10.4.8 Μέθοδοι και εργαλεία disaster recovery

Εκτός από το Wbadmin, που χρησιμοποιείται για διαδικασίες backup, υπάρχουν αξιόλογα και πλήρη εργαλεία στο εμπόριο που χρησιμοποιούμε για disaster recovery, όπως το paragon server και το Acronis server με δυνατότητες universal restore, δηλαδή, επαναφορά και σε μηχάνημα διαφορετικό από αυτό που λήφθηκε το backup.

Ταυτόχρονα υπάρχουν αντίστοιχα εργαλεία που μπορούν να μετατρέψουν το φυσικό μηχάνημα σε εικονικό προσφέροντας ευκολίες γρήγορης επαναλειτουργίας των συστημάτων σε ελάχιστο χρόνο και χωρίς την ύπαρξη φυσικού μηχανήματος.

ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΔΙΑΧΕΙΡΙΣΗ

11.1 Εισαγωγή

Οι επιθυμητές γνώσεις και δεξιότητες που θα αποκτήσουν οι επιμορφωμένοι στην ενότητα Απομακρυσμένη Διαχείριση, θα τους καταστήσουν ικανούς να :

- Δημιουργούν, αποθηκεύουν, τροποποιούν MMCs με απλά και πολλαπλά snap-ins.
- Χρησιμοποιούν MMCs για τη διαχείριση απομακρυσμένου υπολογιστή.
- Ενεργοποιούν και ρυθμίζουν το Remote Desktop for Administration.
- Συνδέονται σε απομακρυσμένο υπολογιστή με Remote Desktop.
- Εγκαθιστούν και να χρησιμοποιούν το εργαλείο RSAT για απομακρυσμένη διαχείριση εξυπηρετητών 2008 και νεώτερους.

11.2 Βασικοί Ορισμοί

Microsoft Management Console (**MMC**): Κονσόλα απομακρυσμένης Διαχείρισης.

Remote Server Administration Tool (**RSAT**): Εργαλεία απομακρυσμένης διαχείρισης Server

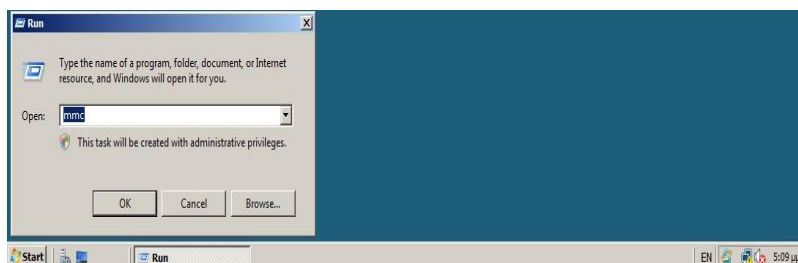
11.3 Απομακρυσμένη Διαχείριση

Με την Απομακρυσμένη Διαχείριση έχουμε την δυνατότητα να διαχειριζόμαστε Servers και Clients από οποιοδήποτε σημείο εντός ή εκτός του εσωτερικού δικτύου, της υπηρεσίας, της πόλης ή του κράτους, εφόσον είμαστε «δικτυωμένοι».

Η απομακρυσμένη διαχείριση δίνει την δυνατότητα πλήρους, ελέγχου τοπικής λειτουργίας μιας συσκευής από οποιαδήποτε απόσταση.

11.3.1 Χρήση Κονσόλας Διαχείρισης της Microsoft (MMC)

Τα Εργαλεία Διαχείρισης της Microsoft λέγονται snap-ins και η MMC είναι η πλατφόρμα στην οποία αυτά τα snap-ins λειτουργούν.



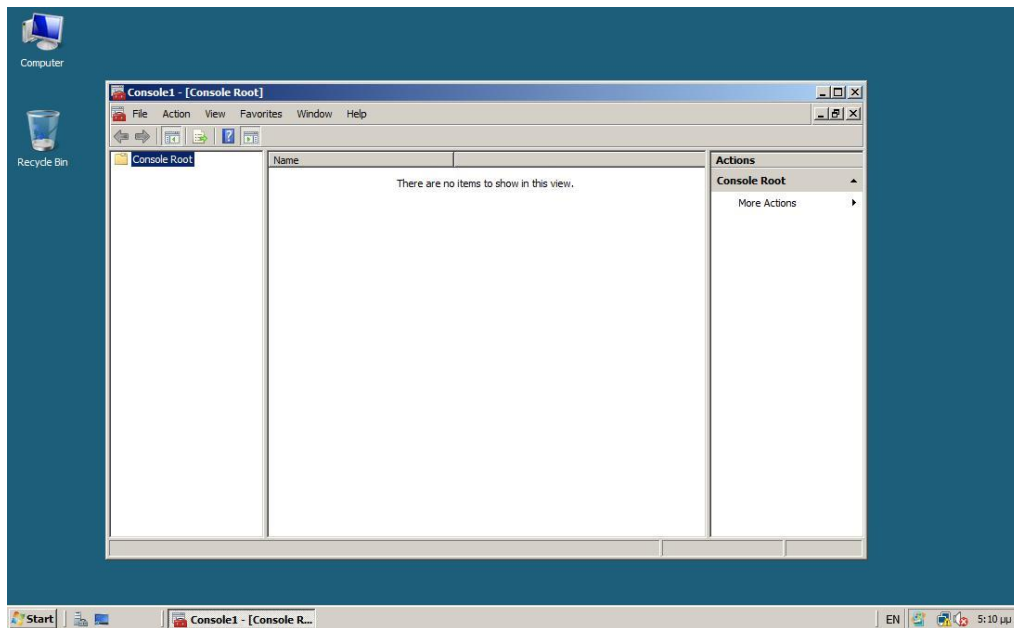
Εικ. 11.1 Εκκίνηση μίας MMC

Καθένα από Links που παρουσιάζονται στο Start → Administrative tools, αλλά και στα περισσότερα άλλα Links, αποτελεί και ένα διαμορφωμένο MMC. Συνεπώς μπορούμε να κατασκευάζουμε και τροποποιούμε mmc's ανάλογα με τις απαιτήσεις.

Για το άνοιγμα μίας MMC δίνουμε mmc στο πλαίσιο διαλόγου (Εικ. 11.1) Start → Run

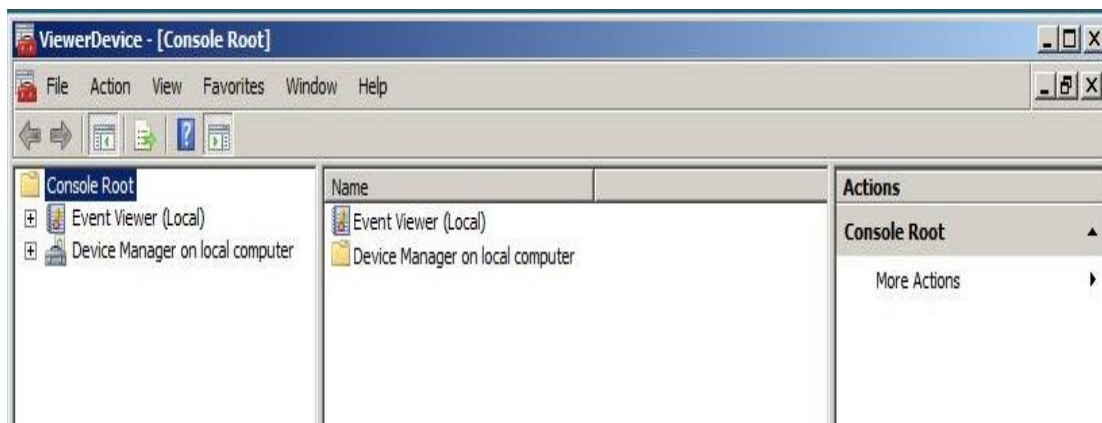
Η Εικ. 11.2 δείχνει μία κενή MMC. Αποτελείται από τρία τμήματα (panes): το console tree pane (λέγεται και scope pane), το details pane και το actions pane.

Το container Console Root θα περιέχει όλα τα snap-ins που θα επιλέξουμε για την κονσόλα μας.



Εικ. 11.2. Κενή MMC

Το παράθυρο μίας κονσόλας διαθέτει γραμμή μενού (menu), γραμμή εργαλείων (toolbar) και περιεχόμενα στα details και actions panes. Τα περιεχόμενα αυτά μπορεί να διαφέρουν ανάλογα με τα snap-ins που έχουμε επιλέξει. Η Εικ. 11.3 δείχνει μία ολοκληρωμένη MMC με όνομα ViewerDevice.msc με τα snap-ins Event Viewer (Local) και Device Manager on local computer.



Εικ. 11.3. Ολοκληρωμένη MMC.

Εξερευνώντας τα μενού και τις εντολές της Κονσόλας μπορούμε συνοπτικά να καθορίσουμε και να διαχειριστούμε τις παρακάτω επιλογές:

File: Δημιουργία νέας κενής κονσόλας, άνοιγμα υπάρχουσας κονσόλας, προσθαφαίρεση συμπληρωματικών προγραμμάτων (snap-ins), επιλογές για την αποθήκευση της κονσόλας (και κύρια το console mode), λίστα με τις κονσόλες που έχουν πρόσφατα ανοιχθεί και έξοδος.

Action: Ποικίλει ανάλογα με το επιλεγμένο snap-in, αλλά τυπικά περιλαμβάνει επιλογές import / export, ρυθμίσεων και βοήθειας για το επιλεγμένο snap-in.

View: Ποικίλει ανάλογα με το επιλεγμένο snap-in, αλλά τυπικά περιλαμβάνει επιλογές για το customization γενικών χαρακτηριστικών προβολής της κονσόλας.

Favorites: Επιτρέπει τη διαχείριση αποθηκευμένων MMCs.

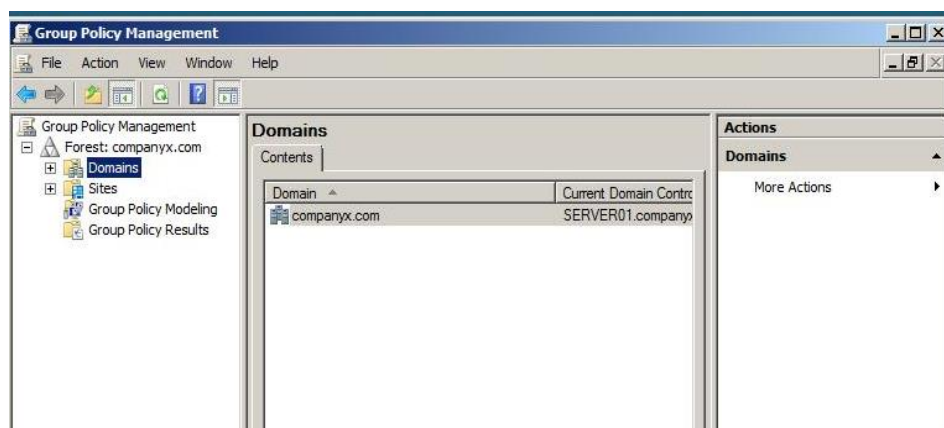
Window: Επιτρέπει τη διαχείριση της θέσης των δευτερευόντων παραθύρων (child windows) της MMC.

Help: Γενικό μενού βοήθειας.

11.3.1.1 Stand-Alone και Extension snap-ins

Τα snap-ins προσθέτουν λειτουργίες σε μία κονσόλα διαχείρισης και διακρίνονται σε δύο είδη:

- Τα **stand-alone** snap-ins που παρέχονται έτοιμα από τους δημιουργούς ενός προγράμματος ή εργαλείου. Για παράδειγμα, η Group Policy Management Console (Εικ. 11.4) περιέχει μία συλλογή από snap-ins για τη δημιουργία και εφαρμογή πολιτικών σε έναν τομέα.



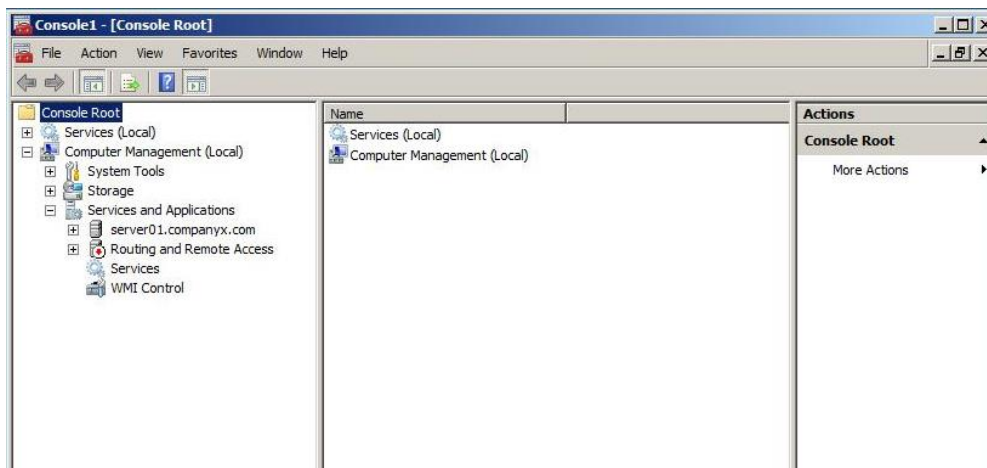
Εικ. 11.4. Group Policy Management Console.

- Τα **extension** (επεκτάσεις) snap-ins που λειτουργούν μαζί με, ένα ή περισσότερα, stand-alone snap-ins.

Προσθέτοντας ένα extension ο Windows Server 2008 το τοποθετεί στη σωστή θέση κάτω από το stand-alone snap-in.

Υπάρχουν snap-ins που λειτουργούν είτε ως stand-alone, είτε επεκτείνουν τις λειτουργίες ενός άλλου snap-in.

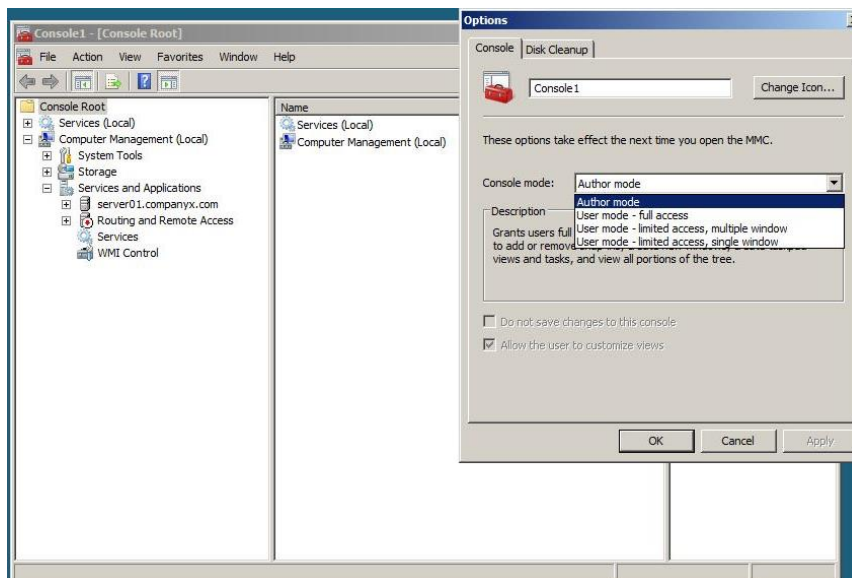
Στην Εικ. 11.5 το snap-in Services λειτουργεί και ως ανεξάρτητο (stand-alone) και ως επέκταση (extension) μέσα στο Computer Management.



Εικ. 11.5. Stand-alone και extension snap-in.

11.3.1.2 Επιλογές Κονσόλας (Console Options)

Το πλαίσιο διαλόγου Options (από το μενού File) καθορίζει τη λειτουργία της MMC ως προς τους κόμβους. Από το console tree pane μπορούν να ανοίξουν τα snap-ins, όπου μπορούν να προστεθούν και τα παράθυρα που δύναται να δημιουργηθούν.



Εικ. 11.6. MMC modes.

Μία κονσόλα μπορεί να αποθηκευθεί (Εικ. 11.6) σε Author mode (προεπιλογή) ή σε κάποιο User mode.

Όταν η κονσόλα αποθηκεύεται σε Author mode, επιτρέπεται πλήρης πρόσβαση σε όλες τις λειτουργίες της MMC, δηλαδή:

- Προσθαφαίρεση snap-ins.
- Δημιουργία παραθύρων.
- Δημιουργία Taskpad Views (από το μενού Action).
- Δημιουργία προσαρμοσμένων προβολών.
- Αποθήκευση των αλλαγών στην κονσόλα.

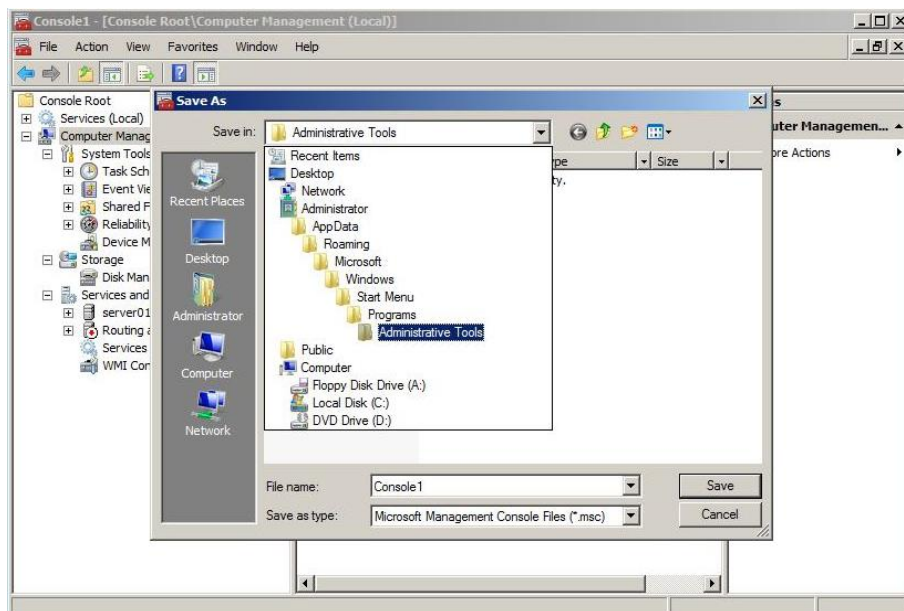
Όταν δημιουργείται μία κονσόλα για διανομή, τότε ενδείκνυται να την αποθηκεύετε σε έναν User mode, όπως παρακάτω:

Full Access: Επιτρέπει στους χρήστες να χρησιμοποιούν όλα τα snap-ins, να ανοίγουν παράθυρα και να έχουν πρόσβαση σε όλα τα τμήματα της MMC.

Limited Access, Multiple Window: Δεν επιτρέπει στους χρήστες να ανοίγουν νέο παράθυρο ή να έχουν πρόσβαση σε όλα τα τμήματα της MMC, αλλά επιτρέπει την προβολή πολλαπλών παραθύρων.

Limited Access, Single Window: Δεν επιτρέπει στους χρήστες να ανοίγουν νέο παράθυρο ή να έχουν πρόσβαση σε όλα τα τμήματα της MMC και επιτρέπει την προβολή ενός μόνο παραθύρου μέσα στην MMC.

Στην Εικ. 11.7 φαίνεται ο προεπιλεγμένος φάκελος για την αποθήκευση των MMCs, που είναι το Administrative Tools μέσα στο προφίλ του χρήστη.

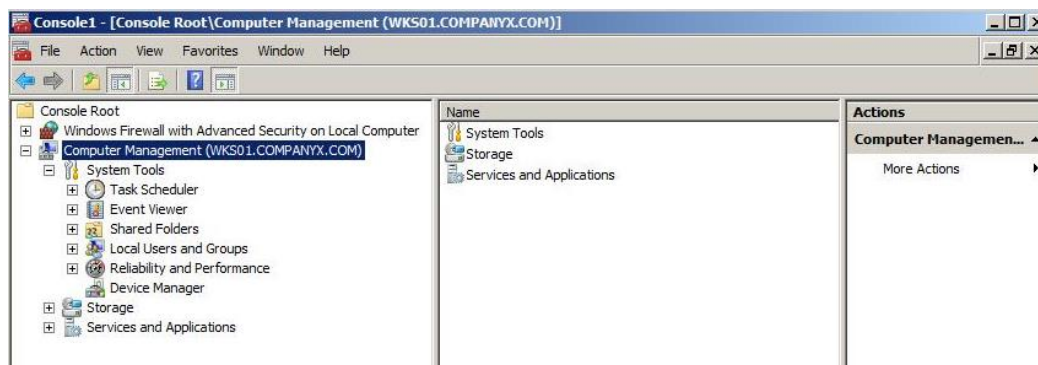


Εικ. 11.7. Αποθήκευση MMC.

11.3.1.3 Χρήση Απομακρυσμένης Διαχείρισης Υπολογιστών

Μία MMC μπορεί να περιέχει snap-ins, που να 'δείχνουν' σε έναν απομακρυσμένο υπολογιστή. Αυτό μπορεί να γίνει είτε με την προσθήκη του snap-in στην κονσόλα είτε με δεξί κλικ σε εγκατεστημένο snap-in και Connect to another computer. Στην

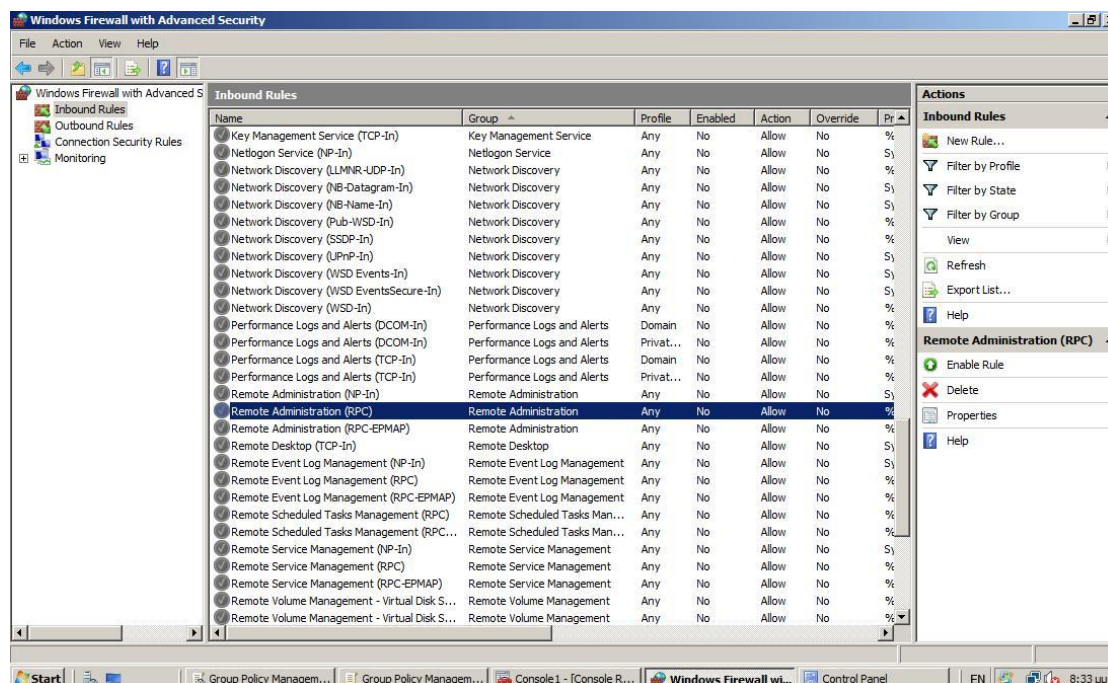
Εικ. 11.8 φαίνεται ότι το snap-in Computer Management χρησιμοποιείται για την απομακρυσμένη διαχείριση του member σταθμού εργασίας WKS01.



Εικ. 11.8. Snap-in για διαχείριση απομακρυσμένου υπολογιστή.

Για τη σύνδεση με ένα απομακρυσμένο σύστημα και τη διαχείρισή του με χρήση MMC η κονσόλα θα πρέπει να εκκινήσει από έναν λογαριασμό με δικαιώματα διαχειριστή στο απομακρυσμένο σύστημα.

Η απομακρυσμένη διαχείριση με χρήση MMC χρησιμοποιεί Remote Procedure Calls (PRCs) και εάν το απομακρυσμένο σύστημα έχει firewall, τότε θα πρέπει να επιτραπεί η εισερχόμενη κίνηση για τη διαχείριση. Προεπιλεγμένα, το Windows Firewall δεν επιτρέπει την εισερχόμενη RPC κίνηση. Θα πρέπει λοιπόν να ρυθμιστούν οι εξαιρέσεις για απομακρυσμένη διαχείριση.

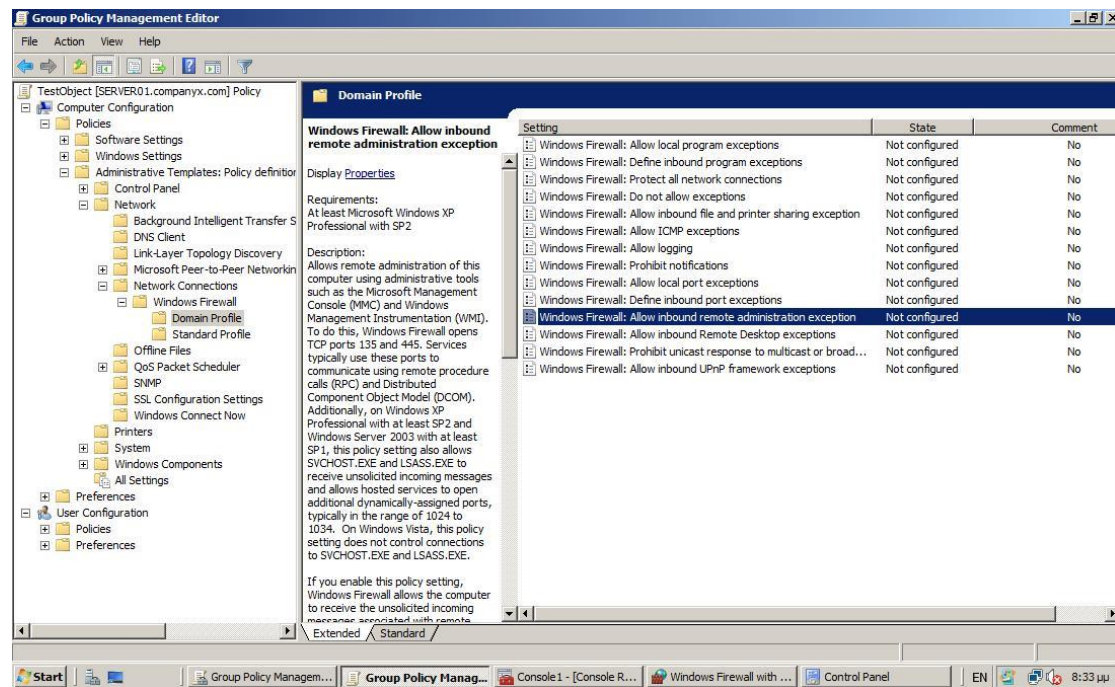


Εικ. 11.9. Windows Firewall και απομακρυσμένη διαχείριση με MMC.

Η Εικ. 11.9 δείχνει το Windows Firewall with Advanced Security (Start→Administrative tools→ Windows Firewall with Advanced Security) σε έναν

υπολογιστή Server 2008, όπου φαίνονται οι Inbound Rules για το Remote Administration.

Εάν θέλουμε η ρύθμιση αυτή να είναι policy-based για τους domain member υπολογιστές μας, τότε κάνουμε enable τη ρύθμιση Computer Configuration / Policies / Administrative Templates / Network / Network Connections / Windows Firewall / Domain Profile / Windows Firewall: Allow inbound remote administration exception, (Εικ. 11.10).



Εικ. 11.10. Group Policy Settings και απομακρυσμένη διαχείριση με MMC.

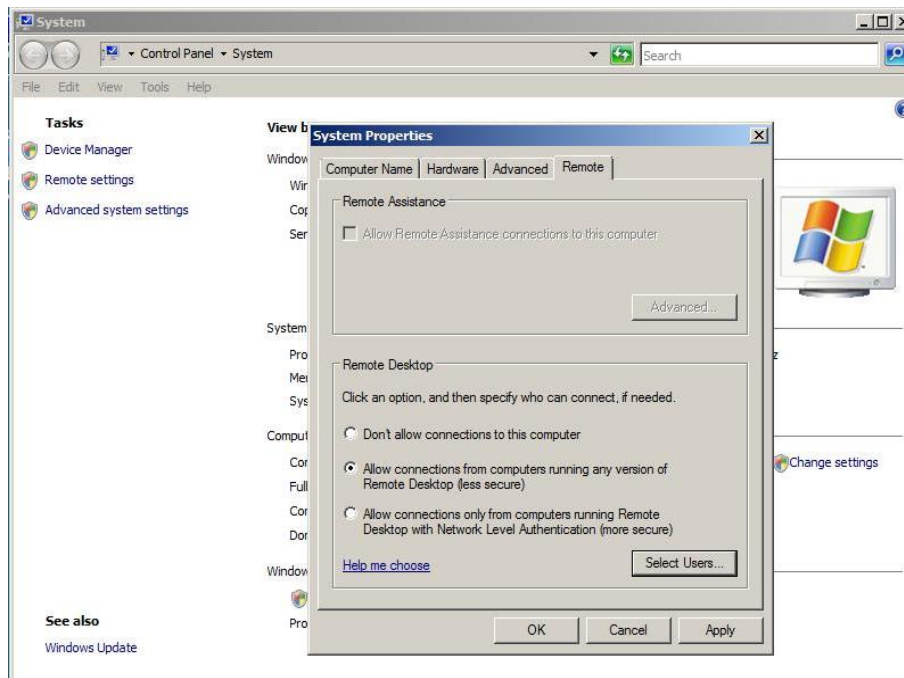
11.3.2 Χρήση Remote Desktop

Από τα Windows 2000 Server μέχρι σήμερα η λειτουργία του Remote Desktop έχει εξελιχθεί σε μία out-of-the-box δυνατότητα, ώστε με ένα μόνο κλικ ένα μηχάνημα να επιτρέπει έως και δύο ταυτόχρονες συνδέσεις για απομακρυσμένη διαχείριση. Το Remote Desktop δεν παρέχει κοινή χρήση εφαρμογών ούτε θέτει ζητήματα επιπλέον αδειοδότησης, όπως γίνεται με τον Terminal Server. Είναι μόνο μία ελαφριά και με πολύ μικρό overhead μέθοδος απομακρυσμένης πρόσβασης.

11.3.3 Ενεργοποίηση του Remote Desktop

My Computer, δεξί κλικ, properties → Remote Settings (Εικ. 11.11) δείχνει πώς ενεργοποιούνται συνδέσεις Remote Desktop σε έναν υπολογιστή.

Προεπιλεγμένα, οι Domain Controllers επιτρέπουν σύνδεση Remote Desktop μόνο σε μέλη του group των Administrators, ενώ οι member servers και στο group των Remote Desktop Users.



Εικ. 11.11. Ενεργοποίηση Remote Desktop.

Στις νέες δυνατότητες που παρουσιάζονται στο remote desktop connection server 2008 είναι οι ασφαλείς συνδέσεις που επιτυγχάνονται, εφόσον οι συνδεδεμένες συσκευές υποστηρίζουν remote desktop with Network Level Authentication (Vista και νεώτερα λειτουργικά).

11.3.4 Απαιτήσεις και Ρυθμίσεις - Remote Desktop Connection Client

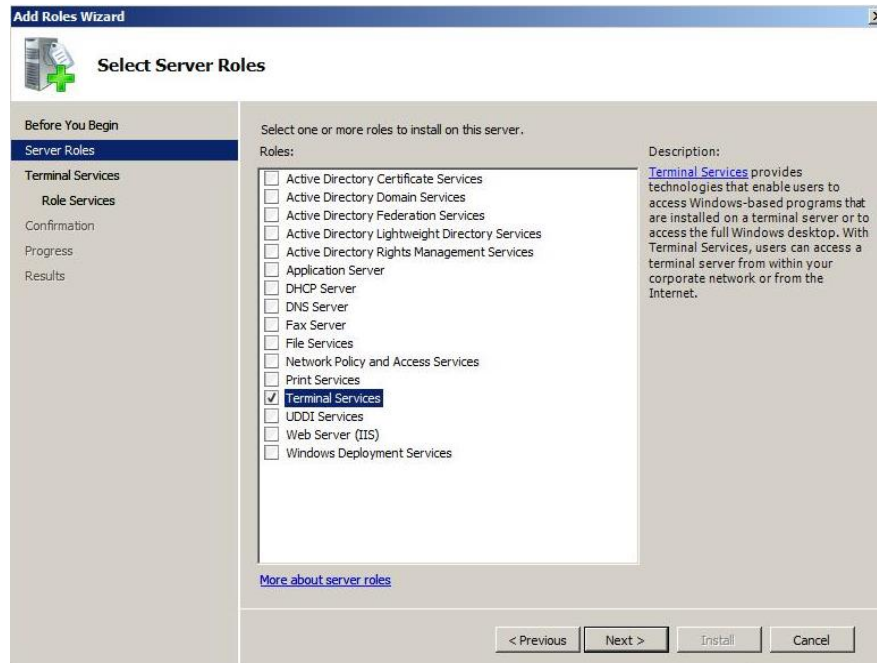
Εάν ένας υπολογιστής που δέχεται συνδέσεις Remote Desktop αντιπροσωπεύει το



Εικ. 11.12. Remote Desktop Connection Client.

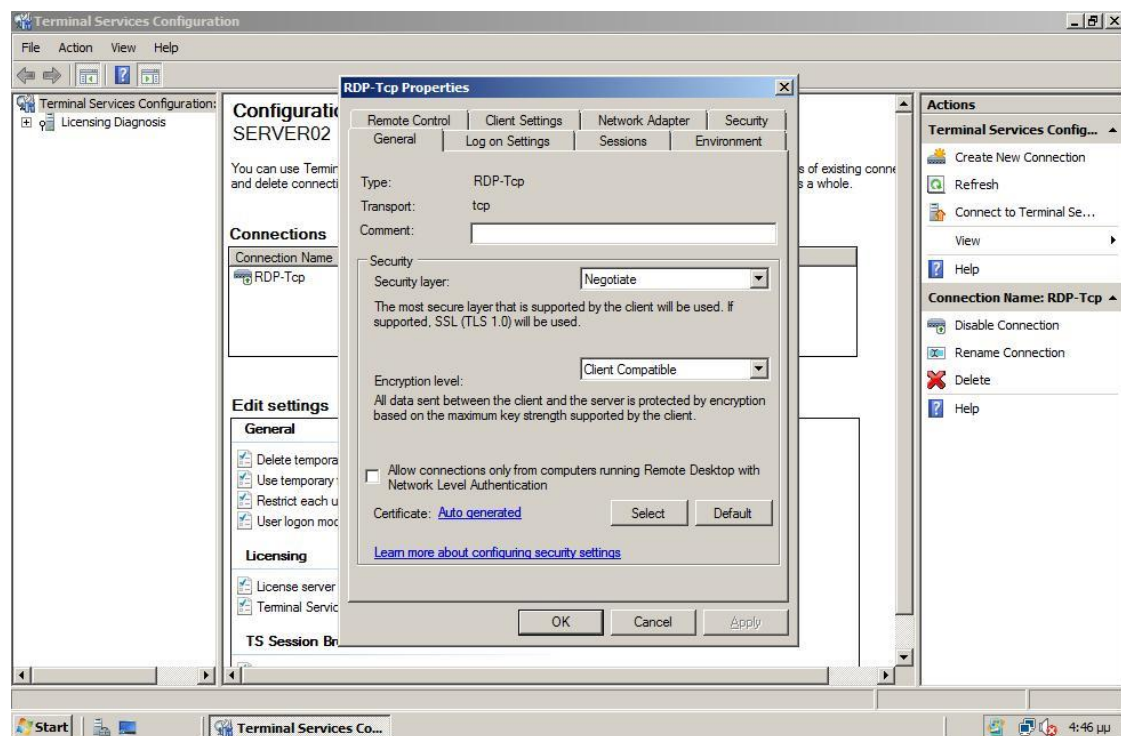
server-side, τότε το client-side είναι το πρόγραμμα Remote Desktop Connection.

Από **Start→Run** και **mstsc.exe** ή **Start→All Programs → Accessories→Remote Desktop Connection** ενεργοποιείται η φόρμα που φαίνεται στην Εικ.11.12 δηλ., ένα Remote Desktop Connection Client προς έναν απλό member server.



Εικ. 11.13. Εγκατάσταση Terminal Services.

Για να μελετήσουμε τις ρυθμίσεις του Remote Desktop από τη μεριά του server, εγκαθιστούμε Terminal Services με τον Add Roles Wizard (Εικ. 11.13.).



Εικ. 11.14. Ρυθμίσεις Remote Desktop από τη μεριά του server.

Οι ρυθμίσεις από τη μεριά του server, γίνονται με το πλαίσιο διαλόγου RDP-TCP Properties (Εικ.11.14) του Terminal Services Configuration snap-in, ενώ από τη μεριά του client, με τον Remote Desktop Connection Client.

Σε περίπτωση αντικρουόμενων ρυθμίσεων υπερισχύουν αυτές του server.

Οι σημαντικότερες ρυθμίσεις και για τις δύο πλευρές είναι οι παρακάτω:

Client

General: Απομακρυσμένος υπολογιστής (DNS όνομα ή IP διεύθυνση), username, επιλογές αποθήκευσης.

Display: Επιλογές προβολής του παραθύρου του Remote Desktop client.

Local Resources: Ερμηνεία συνδυασμών πλήκτρων στον απομακρυσμένο υπολογιστή, διαθεσιμότητα πόρων όπως, τοπικοί δίσκοι, εκτυπωτές, σειριακές συνδέσεις.

Programs: Μονοπάτι και φάκελος στόχος για κάθε πρόγραμμα που θα εκκινεί με την αποκατάσταση της σύνδεσης.

Experience: Λειτουργίες απεικόνισης για την εμπειρία του χρήστη μπορούν να ενεργοποιηθούν ή όχι ανάλογα με το εύρος ζώνης της διαθέσιμης γραμμής ανάμεσα στον server και τον client.

Advanced: Θέματα πιστοποίησης ταυτότητας (authentication) και ρυθμίσεις για Terminal Services Gateway server.

Server

Logon Settings: Δυνατότητα επιλογής στατικών credentials αντί αυτών που δίνονται κάθε φορά από τον client.

Sessions: Επιλογές χρόνων λήξης και επανασυνδέσεων.

Environment: Ρυθμίσεις για την εκκίνηση προγραμμάτων που υπερισχύουν των επιλογών στον client.

Remote Control: Απομακρυσμένος έλεγχος της σύνδεσης Remote Desktop, με δυνατότητα αλληλεπίδρασης.

Client Settings: Ρυθμίσεις που υπερισχύουν αυτών του client.

Security: Χρήστες και ομάδες χρηστών με τα αντίστοιχα permissions πάνω στη σύνδεση Remote Desktop.

11.4 Remote Server Administration Tools (RSAT)

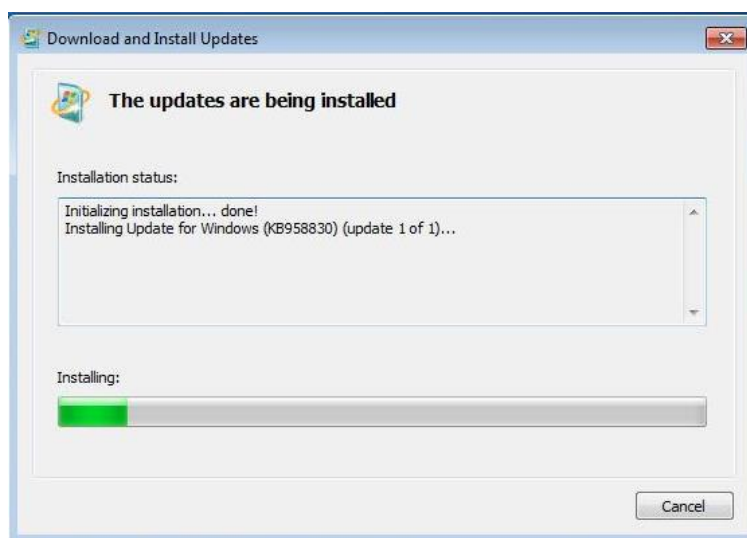
11.4.1 Τι είναι τα RSAT

Τα Remote Server Administration Tools επιτρέπουν σε έναν διαχειριστή συστημάτων

να πραγματοποιεί πληθώρα εργασιών διαχείρισης σε μηχανήματα Server 2008, απομακρυσμένα από έναν client Vista ή νεώτερο.

Τα RSAT είναι μία εξέλιξη του Server 2003 Administration Tools Pack (AdminPack).

Ο Server 2008 μπορεί να είναι είτε Core είτε πλήρους εγκατάστασης, ενώ τα RSAT μπορούν να χρησιμοποιηθούν και για την απομακρυσμένη διαχείριση Server 2003.

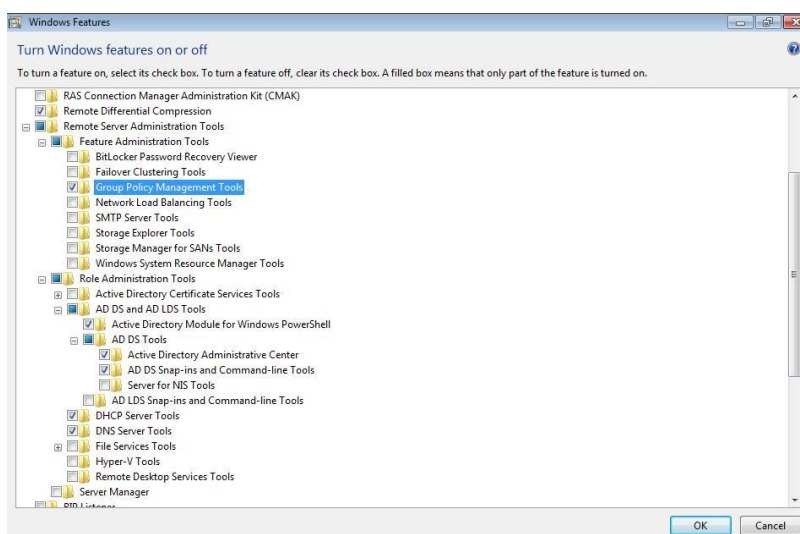


Εικ. 11.15. Εγκατάσταση RSAT update σε Windows 7 client.

11.4.2 Εγκατάσταση και χρήση των RSAT

Τα RSAT έχουν τη μορφή Microsoft Update Standalone Package και είναι «downloadable» από το internet ανάλογα με το είδος του λειτουργικού (x32,x64) καθώς και τον τύπο του (vista, win 7, Hyper-V) .

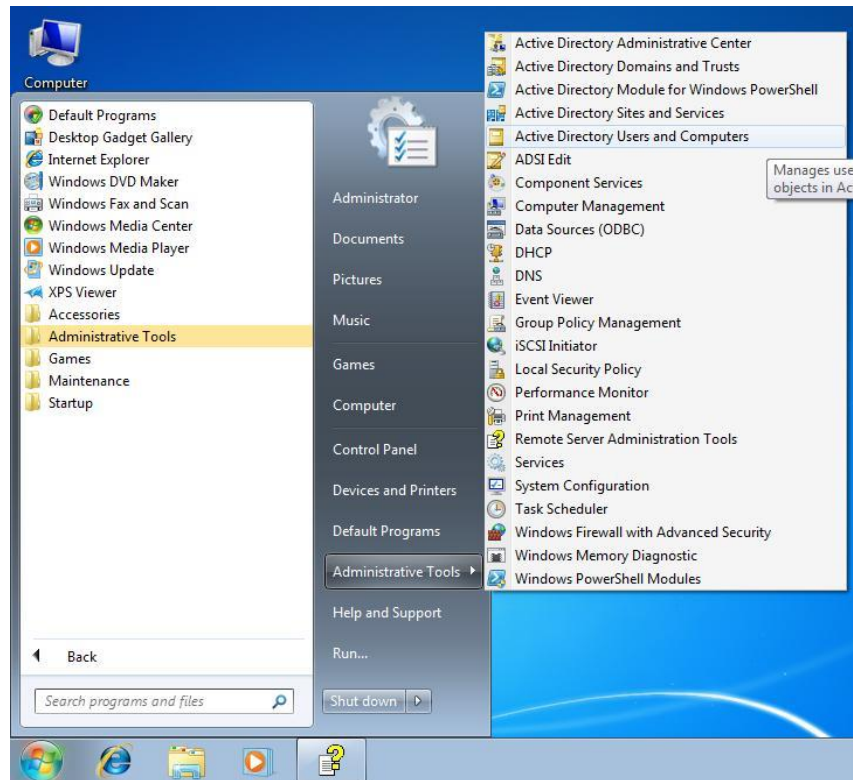
Η εγκατάσταση για λειτουργικά vista και νεώτερα γίνεται μέσω του Download and Install Updates (Εικ. 11.15).



Εικ. 11.16. Ενεργοποίηση ρόλων και λειτουργιών για τα RSAT.

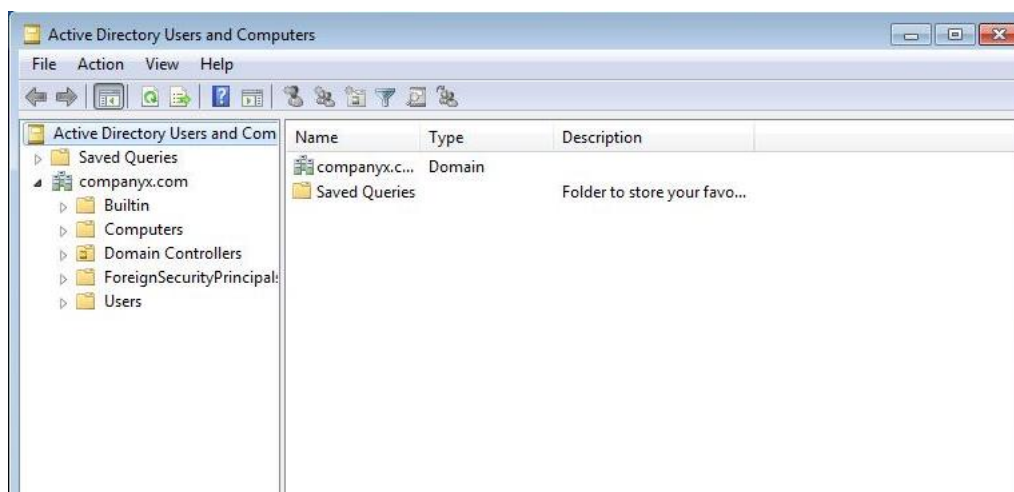
Με την ολοκλήρωση της εγκατάστασης του Update θα επιλέξουμε τους προς διαχείριση ρόλους και λειτουργίες που θα εγκατασταθούν στο σταθμό εργασίας, μέσω του παραθύρου Turn Windows features on or off (Εικ. 11.16).

Τα αντίστοιχα snap-ins έχουν εγκατασταθεί στο start menu του client μηχανήματός μας (Εικ. 11.17).



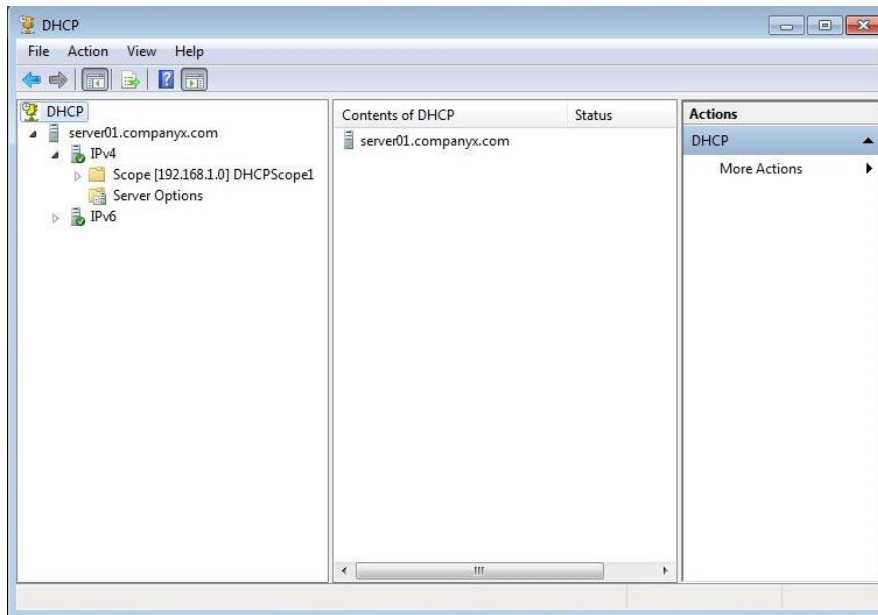
Εικ. 11.17. Snap-ins που έχουν εγκατασταθεί.

Επιλέγοντας Active directory Users and Computers έχουμε τη δυνατότητα να διαχειριστούμε τον DC σαν να είμαστε στον ίδιο τον server, ασχέτως της απόστασης που βρίσκεται ο client από αυτόν.



Εικ. 11.18. Active Directory Users & Computers από Windows 7 client.

Με την ίδια ευκολία διαχειριζόμαστε και οποιαδήποτε άλλη επιλογή, όπως την διαχείριση του DHCP Server (Εικ. 11.19) καθιστώντας τα RSAT απαραίτητα εργαλεία για κάθε διαχειριστή.



Εικ. 11.19. Διαχείριση DHCP από Windows 7 client.

ORGANIZATIONAL UNITS

12.1 Εισαγωγή

Οι επιθυμητές γνώσεις και δεξιότητες που θα αποκτήσουν οι επιμορφωμένοι στην ενότητα Organizational Units (OUs), θα τους καταστήσουν ικανούς να :

- Δημιουργούν, τροποποιούν, διαγράφουν και διαχειρίζονται OUs.
- Σχεδιάζουν την δομή πολιτικών ασφαλείας.
- Εφαρμόζουν πολιτικές ασφαλείας σε αντικείμενα του Active Directory.
- Διαχειρίζονται αντικείμενα με OUs.
- Μεταβιβάζουν των διαχειριστικό έλεγχο των OUs.

12.2 Βασικοί Ορισμοί

Organizational Unit (OU): Οργανωτική Μονάδα.

Delegation: Μεταβίβαση – εξουσιοδότηση διαχειριστικού ελέγχου.

Access Control Lists (ACLs): Λίστες ελέγχου πρόσβασης.

Group Policy Object, (GPO): Βασική μονάδα πολιτικών ασφαλείας.

12.3 Ορισμός, Βασικές έννοιες, Δομή

Μία Organizational Unit (OU) είναι ένα container, το οποίο χρησιμοποιείται για την οργάνωση και τακτοποίηση αντικειμένων μέσα σε ένα domain σε λογικές διαχειρίσιμες ομάδες.

Μία OU μπορεί να περιέχει αντικείμενα όπως λογαριασμοί χρηστών, ομάδες, υπολογιστές, εκτυπωτές, εφαρμογές, κοινοί φάκελοι, καθώς και άλλες OUs μέσα στο ίδιο domain.

Στην OU βάζουμε πολιτικές ασφαλείας, τις οποίες εφαρμόζουν τα αντικείμενα που περιέχονται σε αυτή.

Μπορούμε να «φωλιάσουμε» μία OU μέσα σε μία άλλη (nested) δημιουργώντας με τον τρόπο αυτό μία ιεραρχική δομή.

Κάθε domain έχει τη δική του δομή από OUs, η οποία είναι ανεξάρτητη από τη δομή των OUs σε κάθε άλλο domain.

Με την εγκατάσταση του AD-DS δημιουργείται αυτόματα η OU των Domain Controllers που περιέχει τον Server 2008 και στην οποία θα εγκαθίσταται αυτόματα κάθε νέος DC του domain.

Υπάρχουν τρεις σημαντικοί λόγοι για την δημιουργία OUs μέσα στο domain μας:

- Η απόδοση / μεταβίβαση διαχειριστικού ελέγχου αντικειμένων.

- Η διαχείριση της Group Policy.
- Η απόκρυψη αντικειμένων.

12.3.1 Απόδοση / Μεταβίβαση Διαχειριστικού Ελέγχου

Ένας σημαντικός λόγος για να δημιουργούμε OUs είναι η ανάθεση διαχειριστικών εργασιών, delegate administration.

Δηλαδή την απόδοση διαχειριστικών δικαιωμάτων και ευθυνών για ένα κομμάτι του τομέα (μία OU) σε χρήστη ή ομάδα.

Στο Windows Server 2008 αυτό γίνεται μέσω των δικαιωμάτων (permissions) που αποδίδονται με τις Access Control Lists (ACLs).

Μία ACL είναι ο μηχανισμός για το έλεγχο της πρόσβασης σε συγκεκριμένα κομμάτια δεδομένων με βάση τα στοιχεία ταυτότητας του χρήστη ή τη συμμετοχή του σε ομάδες.

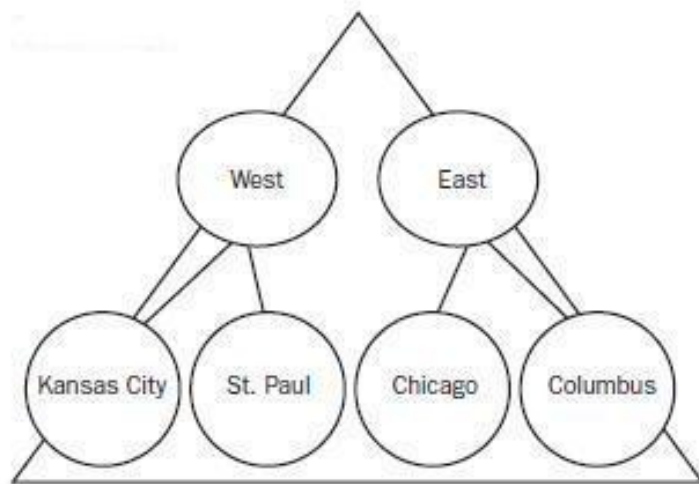
Η καταχώρηση ελέγχου πρόσβασης (Access Control Entry, ACE) προσδιορίζει ακριβώς ποιοι χρήστες ή ομάδες έχουν πρόσβαση σε μία OU, καθώς και το είδος της πρόσβασης.

Η απόδοση τέτοιων δικαιωμάτων με ACLs και ACEs είναι μία από τις σημαντικότερες εργασίες διαχείρισης του καταλόγου μας (Active Directory Objects Administration).

12.3.2 Ιεραρχία των OUs

Ο τρόπος με τον οποίο σχεδιάζεται η ιεραρχία των OUs γενικά αντανακλά τη δομή του οργανισμού μας.

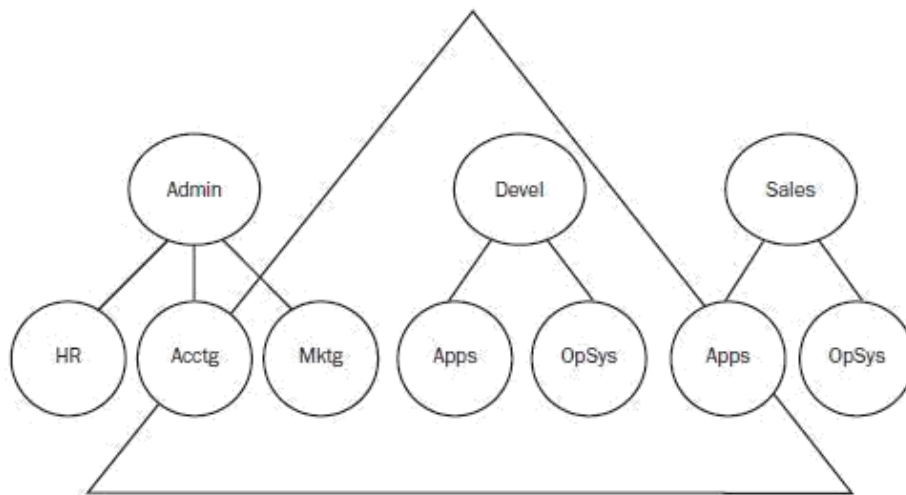
Η σχεδίαση μπορεί να βασίζεται στη γεωγραφική θέση, την εταιρική λειτουργία, το είδος του αντικειμένου ή όλα αυτά συνδυασμένα.



Εικ. 12.1. Ιεραρχία OUs με βάση τη γεωγραφική θέση.

Η Εικ. 12.1 δείχνει μία δομή βασισμένη στη γεωγραφική θέση. Ο οργανισμός εκτείνεται σε δύο λογικές περιφέρειες με τέσσερα φυσικά γραφεία. Οι περιφέρειες αντιστοιχούν στις OUs ανώτερου επιπέδου (top - level OUs) και τα γραφεία στις OUs δεύτερου επιπέδου (second - level OUs).

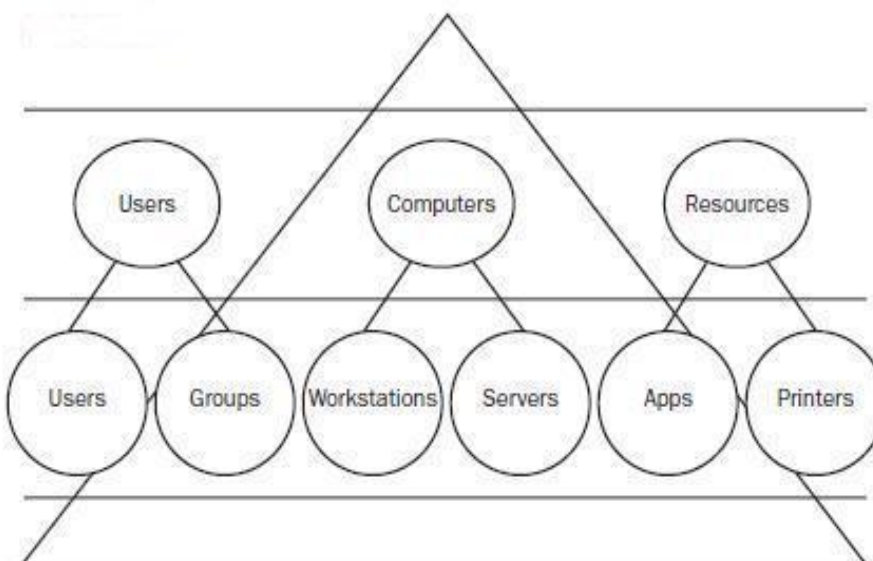
Στην Εικ. 12.2 παρουσιάζεται μία σχεδίαση, όπου η διαχείριση του domain γίνεται με βάση την εταιρική λειτουργία.



Εικ. 12.2. Ιεραρχία OUs με βάση την εταιρική λειτουργία.

Τρεις top-level OUs αντιστοιχούν στις διευθύνσεις, ενώ οι second-level OUs στα τμήματα.

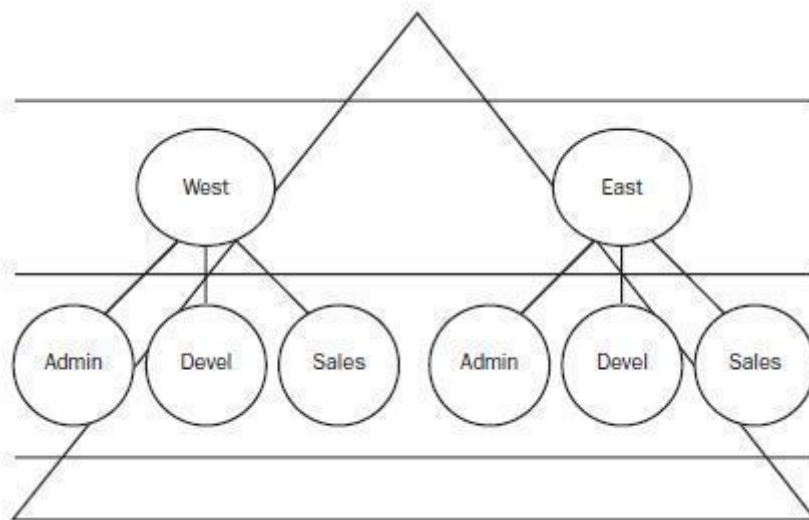
Μία σχεδίαση που βασίζεται στο είδος των προς διαχείριση αντικειμένων φαίνεται στην Εικ. 12.3. Οι top-level OUs ομαδοποιούν τους χρήστες, τους υπολογιστές και τους άλλους πόρους. Οι second-level OUs εξειδικεύουν περισσότερο το κάθε αντικείμενο.



Εικ. 12.3. Ιεραρχία ΟUs με βάση το είδος των αντικειμένων.

Η Εικ. 12. 4 δείχνει μία σχεδίαση που συνδυάζει τις παραπάνω προσεγγίσεις.

Οι top-level ΟUs αντιστοιχούν στις περιφέρειες όπου ο οργανισμός έχει γραφεία, ενώ οι second-level ΟUs αντιπροσωπεύουν τμήματα σε κάθε περιφέρεια.



Εικ. 12.4. Υβριδική ιεραρχία ΟUs.

12.3.3 Group Policy Object (GPO)

Λέγοντας Group Policy Object (GPO), εννοούμε μία συλλογή από ρυθμίσεις χρηστών και υπολογιστών που συνδέονται με μία ΟU. Οι ρυθμίσεις αυτές επηρεάζουν χρήστες και μηχανήματα με τρόπους που θα δούμε παρακάτω.

12.3.4 Δημιουργία ΟUs για την απόκρυψη αντικειμένων

Εάν η πολιτική του οργανισμού μας απαιτεί κάποια αντικείμενα να μην είναι ορατά από χρήστες ή ομάδες, τότε η λύση είναι η δημιουργία μίας ΟU με αυτά τα αντικείμενα και η σωστή στέρηση ή απόδοση δικαιωμάτων (permissions) στους συγκεκριμένους χρήστες.

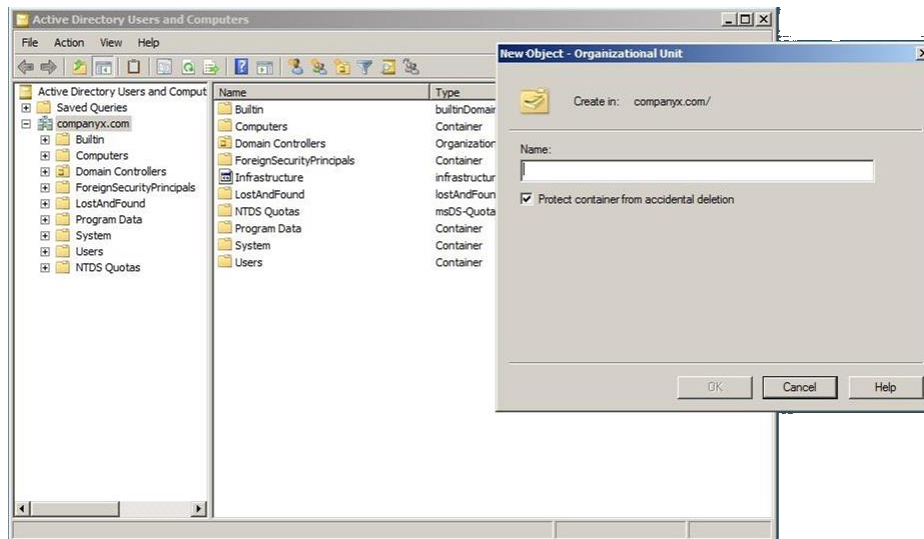
12.4 Δημιουργία και διαχείριση ΟUs

Για να δημιουργήσουμε μια ΟU, ακολουθούμε Start → Administrative Tools → Active Directory Users And Computers και δεξί κλικ στο «δένδρο» του domain, New → Organizational Unit.

Εμφανίζεται (Εικ. 12.5) το πλαίσιο διαλόγου για τη δημιουργία μίας νέας κενής ΟU μέσα στο domain μας στην οποία μπορούμε να δώσουμε κάποιο όνομα.

Προσέξτε το check box με το Protect container from accidental deletion. Μπορεί να ρυθμιστεί και αργότερα στην καρτέλα Object του παραθύρου των ιδιοτήτων του

αντικειμένου, εφόσον ενεργοποιήσουμε τα Advanced Features από το μενού View του Active Directory Users and Computers.

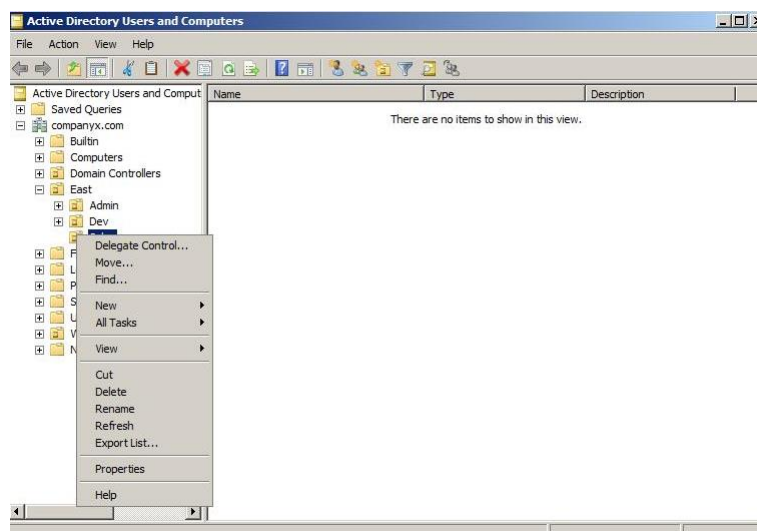


Εικ. 12.5. Δημιουργία ΟΥ.

Οι βασικές εργασίες για τη διαχείριση μίας υφιστάμενης ΟΥ, είναι οι εξής:

- Μετονομασία μίας ΟΥ.
- Μετακίνηση μίας ΟΥ.
- Διαγραφή μίας ΟΥ.
- Επεξεργασία των ιδιοτήτων μίας.
- Μετακίνηση αντικειμένων από μία ΟΥ σε μία άλλη.

Με δεξί κλικ στην ΟΥ παρουσιάζεται το menu της Εικ. 12.6.



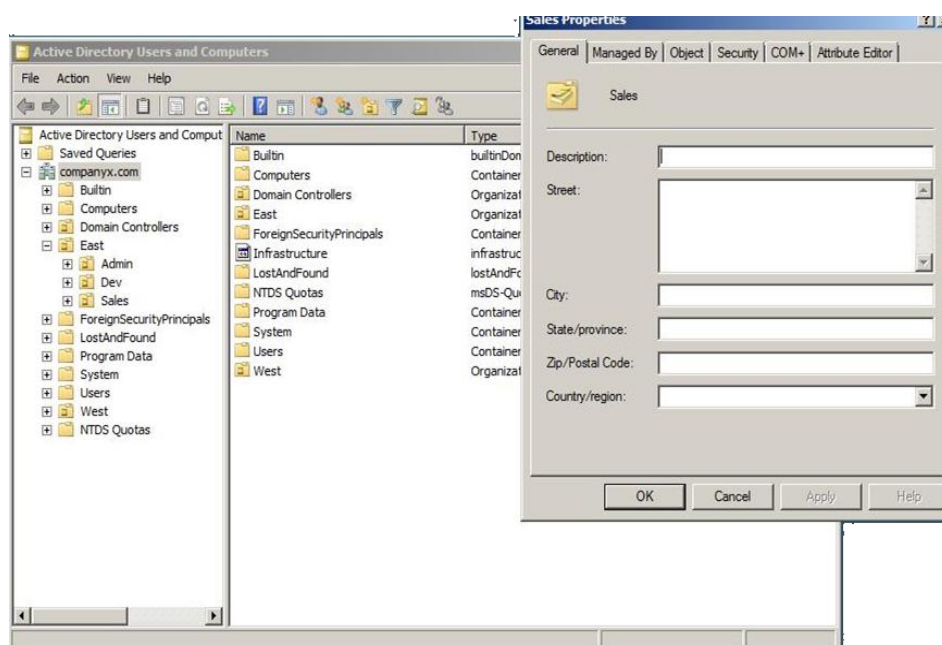
Εικ. 12. 6 Μετονομασία, μετακίνηση, διαγραφή

Στην ΟΥ Sales, που είναι second-level ΟΥ μέσα στην East, γίνονται οι εργασίες της μετονομασίας, μετακίνησης και διαγραφής της ΟΥ.

Με την εντολή Move γίνεται επίσης η μετακίνηση ενός αντικειμένου από μία ΟΥ σε άλλη.

Με drag and drop, επίσης, μετακινούνται αντικείμενα μέσα στο Active Directory Users and Computers.

Στην Εικ. 12.7 φαίνεται το πλαίσιο διαλόγου των ιδιοτήτων μίας ΟΥ, εφόσον έχουμε ενεργοποιήσει από το μενού View τα Advanced Features. Στην καρτέλα επισημαίνουμε τη ρύθμιση Protect object from accidental deletion, ενώ στην καρτέλα Security θα αναφερθούμε παρακάτω.



Εικ. 12. 7 Ιδιότητες ΟΥ

12.4.1 Διαχείριση αντικειμένων του Active Directory

Εγκαθιστώντας υπηρεσίες Active Directory στο δίκτυο δημιουργούμε τη βάση για την αναζήτηση πόρων οπουδήποτε μέσα στον οργανισμό.

Η υπηρεσία καταλόγου Active Directory αποθηκεύει πληροφορίες σχετικές με δικτυακά αντικείμενα.

Active Directory Object εννοούμε κάθε διακριτό σύνολο χαρακτηριστικών (attributes), που αναπαριστά μία συγκεκριμένη δικτυακή οντότητα.

Βασικά αντικείμενα του Active Directory και τα περιεχόμενά τους αναφέρονται παρακάτω.

Αντικείμενα

Λογαριασμός Χρήστη (User Account): Πληροφορία που επιτρέπει σε ένα χρήστη να κάνει log on σε ένα μηχάνημα Windows Server 2008.

Επαφή (Contact): Πληροφορία για ένα υποκείμενο που συνδέεται με τον οργανισμό μας.

Ομάδα (Group): Μία συλλογή από λογαριασμούς χρηστών, υπολογιστές ή άλλες ομάδες που δημιουργείται για ευκολία στη διαχείριση.

Κοινός Φάκελος (Shared Folder): Δείκτης προς έναν κοινό φάκελο σε υπολογιστή. Όταν δημιουργούμε έναν κοινό φάκελο ή βάζουμε έναν εκτυπωτή στο Active Directory στην πραγματικότητα δημιουργούμε ένα αντικείμενο-δείκτη προς τον κοινό φάκελο ή τον εκτυπωτή.

Εκτυπωτής (Printer): Ένας εκτυπωτής που έχει «δημοσιευθεί» στο Active Directory.

Υπολογιστής (Computer): Πληροφορία για ένα μηχάνημα που είναι μέλος του τομέα.

Ελεγκτές Τομέα (Domain Controllers): Πληροφορία για έναν domain controller, που περιλαμβάνει το DNS όνομα του μηχανήματος, ένα προ-Windows 2000 όνομα, την έκδοση του λειτουργικού συστήματος, τη θέση, τον υπεύθυνο για τη διαχείριση του domain controller και άλλες πληροφορίες.

Organizational Unit (OU): Περιέχει άλλα αντικείμενα, που μπορεί να είναι επίσης OUs.

Ένα αντικείμενο μπορεί να είναι είτε container είτε leaf (φύλλο).

Ένα container εμπεριέχει άλλα αντικείμενα και έχει μία θέση ενδιάμεσου κόμβου στο δένδρο.

Ένα leaf δεν μπορεί να αποθηκεύει μέσα του άλλα αντικείμενα και βρίσκεται στην άκρη του δένδρου.

12.4.2 Τροποποίηση δικαιωμάτων πρόσβασης του Active Directory

Τα Windows Server 2008 χρησιμοποιούν ένα μοντέλο ασφάλειας βασισμένο σε αντικείμενα (object- base) για την υλοποίηση του ελέγχου της πρόσβασης στο Active Directory.

Πρόκειται για ένα μοντέλο παρόμοιο με τα ήδη γνωστά σε μας από την ασφάλεια του NTFS file system.

Σε αυτή τη βάση, η πρόσβαση σε ένα αντικείμενο γίνεται με την απόδοση ή άρνηση δικαιωμάτων πάνω σε security principals.

Δικαίωμα (permission) είναι η άδεια να εκτελούμε μία λειτουργία πάνω στο αντικείμενο, η οποία αποδίδεται από τον ιδιοκτήτη (owner) του αντικειμένου.

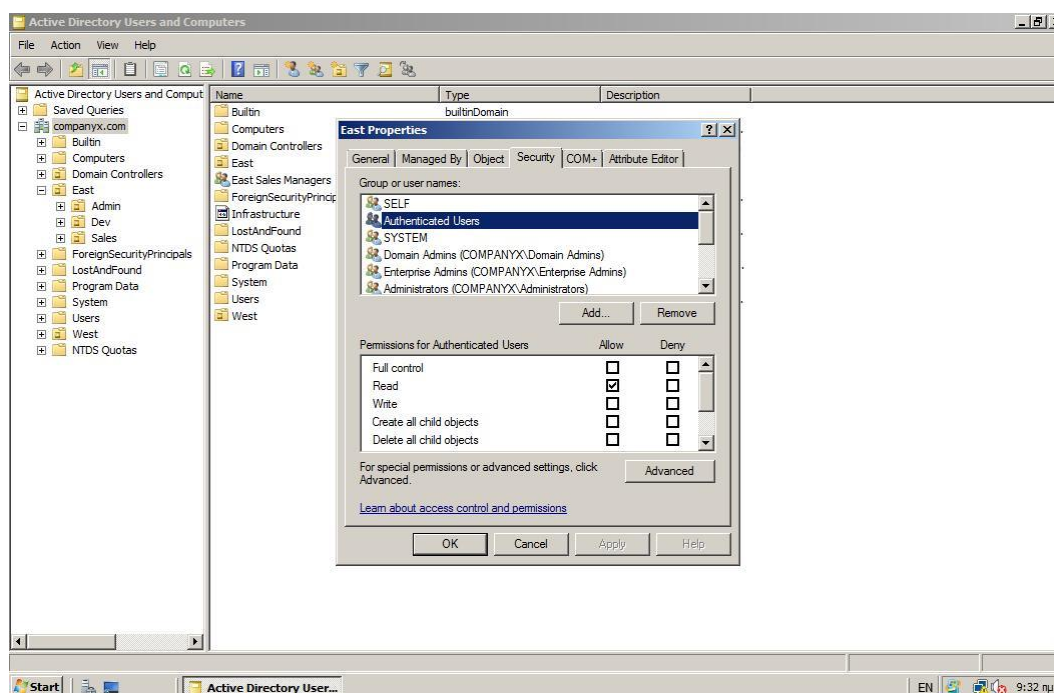
Λέγοντας security principal εννοούμε ένα χρήστη, ομάδα, υπολογιστή ή υπηρεσία στο οποίο έχει αποδοθεί ένα μοναδικό security identifier, SID.

Το SID προσδιορίζει μοναδικά το χρήστη, την ομάδα, τον υπολογιστή ή την υπηρεσία μέσα στο δίκτυο και χρησιμοποιείται για τη διαχείριση των security principals.

Μία από τις σημαντικές εργασίες του διαχειριστή είναι η απόδοση δικαιωμάτων σε security principals μέσα στο domain.

Οι OUs δε συνιστούν security principals και για αυτό δεν είναι δυνατό να αποδώσουμε δικαιώματα πρόσβασης (access permissions) σε μία OU, δηλαδή, σαν να ήταν χρήστης ή ομάδα.

Σε μία OU μπορούμε να εκτελέσουμε μεταβίβαση διαχειριστικού ελέγχου.



Εικ. 12.8. ACL σε OU.

Τα δικαιώματα πρόσβασης σε ένα αντικείμενο του Active Directory αποθηκεύονται σε έναν κατάλογο που λέγεται Access Control List (ACL).

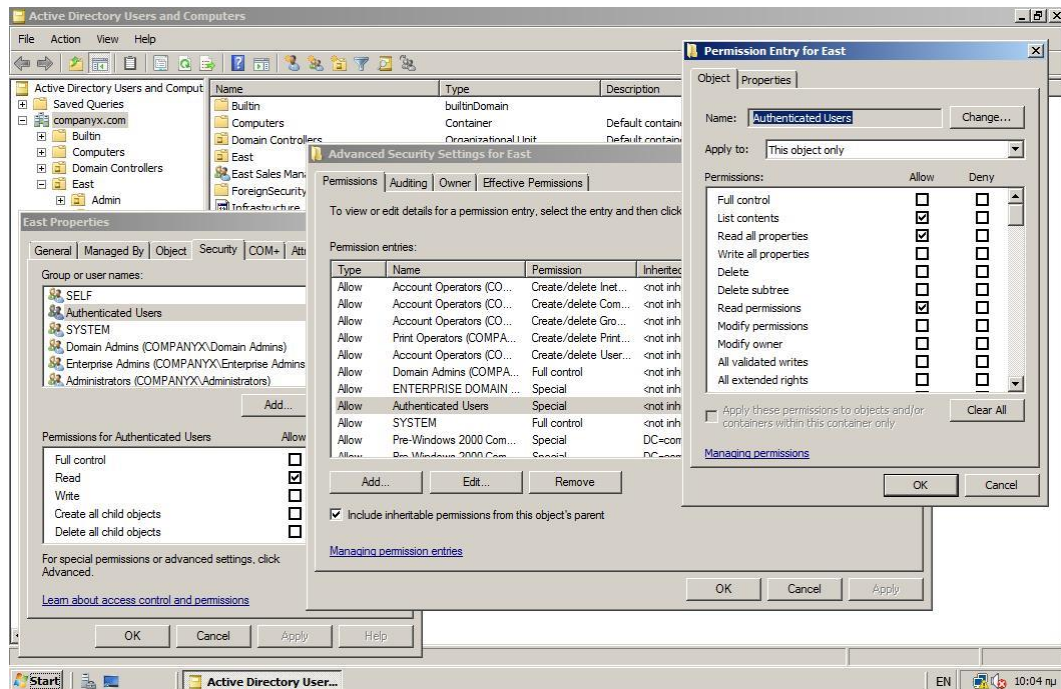
Στην Εικ. 12.8 παρουσιάζεται η καρτέλα Security του πλαισίου διαλόγου των ιδιοτήτων της OU με όνομα East. Θυμηθείτε να έχετε ενεργοποιημένο το Advanced Features από το μενού View του Active Directory Users and Computers.

Οι ρυθμίσεις στην καρτέλα Security ενός αντικειμένου συνιστούν τα standard permissions.

Τα βασικά είναι Full Control, Read και Write.

Για μία πιο λεπτομερή απόδοση δικαιωμάτων υπάρχουν τα special permissions, ή αλλιώς advanced security settings.

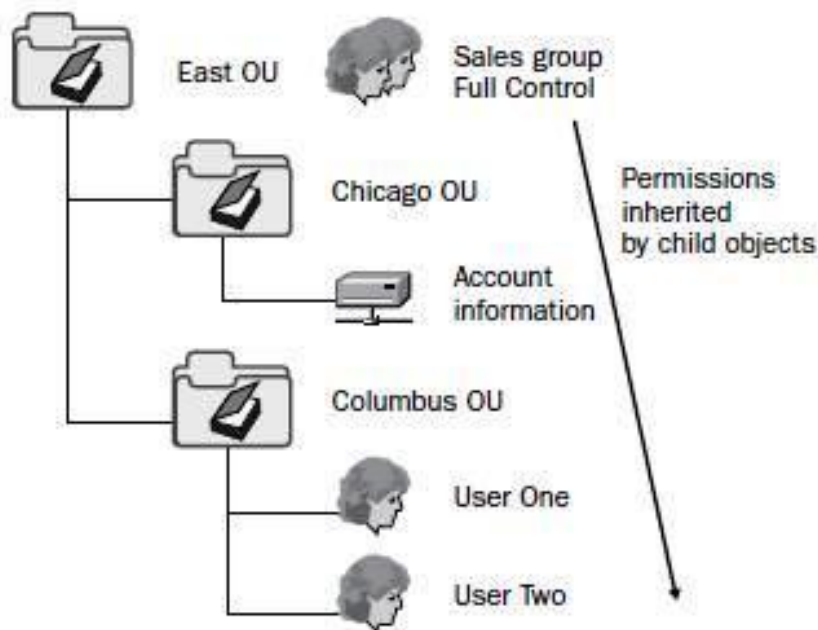
Στην Εικ. 12.9 φαίνονται τα special permissions της OU East για τους Authenticated Users.



Εικ. 12.9. Special Permissions σε OU.

Υπάρχουν δύο τρόποι για την απόδοση δικαιωμάτων σε ένα security principal:

- **Άμεσα:** Η απόδοση του permission γίνεται από τον owner του αντικείμενου.
- **Κληρονομικά (inheritance):** Τα κληροδοτημένα (inherited) permissions διαδίδονται από ένα αντικείμενο στα αντικείμενα-παιδιά του (child objects)



Εικ. 12.10 Άμεσα και inherited permissions.

Εάν δώσουμε Full Control πάνω στην OU με όνομα East στην ομάδα Sales (Εικ. 12.10), το permission αυτό (Πλήρης Έλεγχος) θα διαδοθεί προς τα κάτω για όλα τα child objects.

Τα δικαιώματα της ομάδας Sales πάνω στην East είναι άμεσα, ενώ τα δικαιώματα της Sales πάνω στην Columbus OU είναι inherited.

Η σωστή χρήση των inherited permissions διευκολύνει τη διαχείριση του domain και εξασφαλίζει μία συνέχεια (consistency) στον έλεγχο της πρόσβασης.

12.4.3 Μεταβίβαση διαχειριστικού ελέγχου OUs

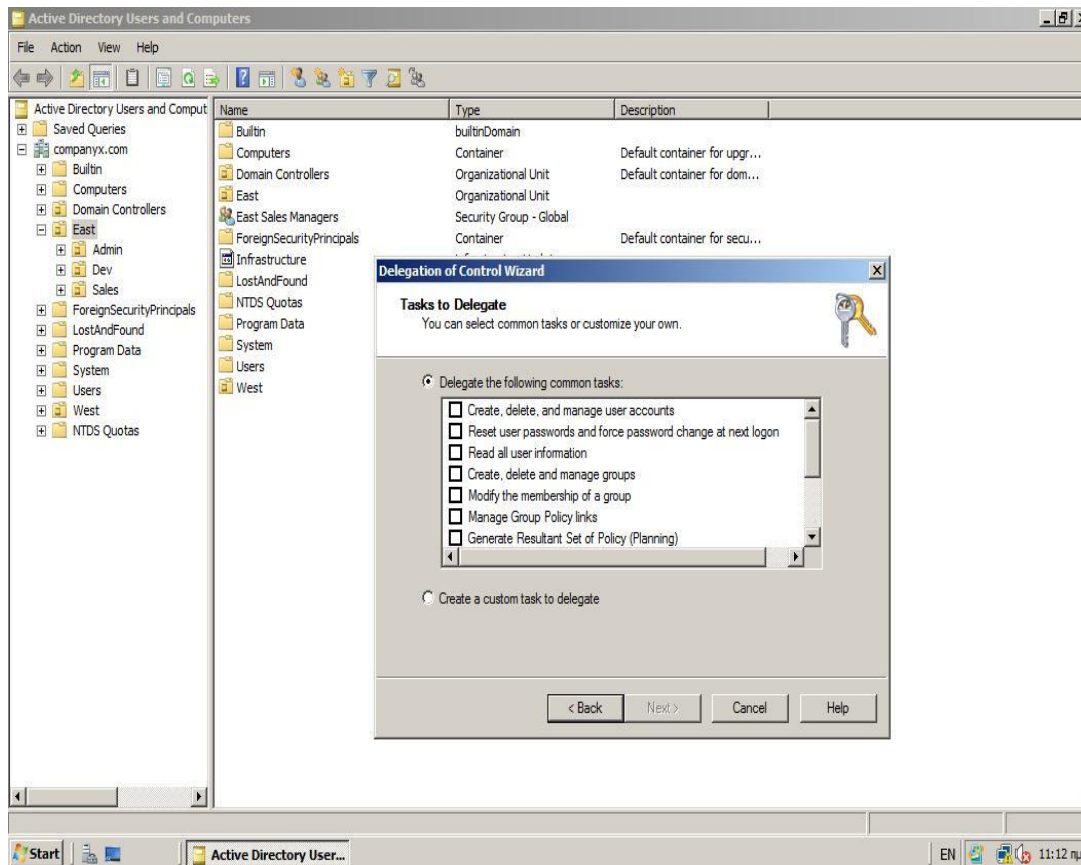
Με το λεκτικό αυτό Administrative Control Delegation εννοούμε γενικά την απόδοση δικαιωμάτων διαχειριστή για domain ή OUs σε ομάδες ή χρήστες.

Αυτό γίνεται αρχικά με χρήση του Delegation of Control Wizard.

Η εκκίνηση του Wizard γίνεται με δεξί κλικ πάνω στο προς διαχείριση αντικείμενο (OU).

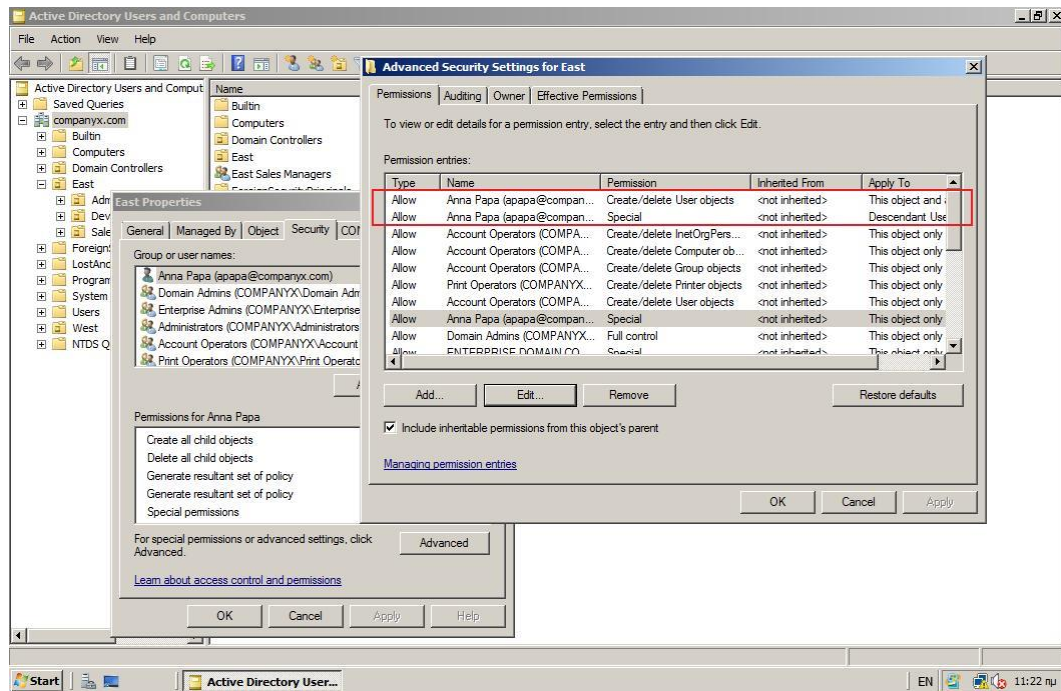
Η Εικ. 12.11 δείχνει το κρίσιμο βήμα του Οδηγού, που είναι το Tasks to Delegate.

Θα επιτρέψουμε στο χρήστη Anna Papa να εκτελεί βασικές εργασίες διαχείρισης λογαριασμών χρηστών μέσα στην OU East, οι οποίες αντιστοιχούν στα δύο πρώτα Tasks to Delegate.



Εικ. 12.11. Delegation of Control Wizard.

Για να επιβεβαιώσουμε ή να αφαιρέσουμε Delegated Permissions, χρησιμοποιούμε το Security tab και τις Advanced επιλογές, όπως φαίνεται στην Εικ. 12.12.



Εικ. 12.12. Delegated permission.

GROUP POLICY

13.1 Εισαγωγή

Οι επιθυμητές γνώσεις και δεξιότητες που θα αποκτήσουν οι επιμορφωμένοι στην ενότητα Group Policy, θα τους καταστήσουν ικανούς να :

- Δημιουργούν, τροποποιούν, διαγράφουν και διαχειρίζονται GPOs.
- Σχεδιάζουν και κατανοούν πολιτικές ασφαλείας.
- Εφαρμόζουν πολιτικές ασφαλείας σε αντικείμενα του Active Directory.
- Διαχειρίζονται αντικείμενα με GPOs.
- Αποθηκεύουν, μεταφέρουν και επανεφαρμόζουν πολιτικές σε νέα Domains.
- Εφαρμόζουν διαδικασίες επαναφοράς πολιτικών ασφαλείας μετά από καταστροφή (Disaster Recovery).

13.2 Βασικοί Ορισμοί

Group Policy: Πολιτική ασφαλείας

Group Policy Object (GPO): Αντικείμενο μέσω του οποίου καθορίζονται μία ή περισσότερες πολιτικές ασφαλείας.

Group Policy Management Console (GPMC): Εργαλείο διαχείρισης πολιτικών ασφαλείας.

Multiple Local Group Policy objects (MLGPO): Πολλαπλές τοπικές πολιτικές.

13.3 Group Policy

Με τον όρο Group Policy θεωρούμε την υποδομή εκείνη που μας δίνει τη δυνατότητα να εφαρμόζουμε συγκεκριμένες ρυθμίσεις σε αντικείμενα (objects), για να ελέγχουμε το περιβάλλον λειτουργίας και συμπεριφορά τους.

Οι ρυθμίσεις αυτές πραγματοποιούνται με τη σύνδεση Group Policy Objects (GPOs), σε Active Directory Domain Service containers: sites, domains, organizational units (OUs) και εφαρμόζονται στα αντικείμενα που εμπεριέχουν.

13.3.1 Ιεράρχηση εφαρμογής πολιτικών Ασφαλείας

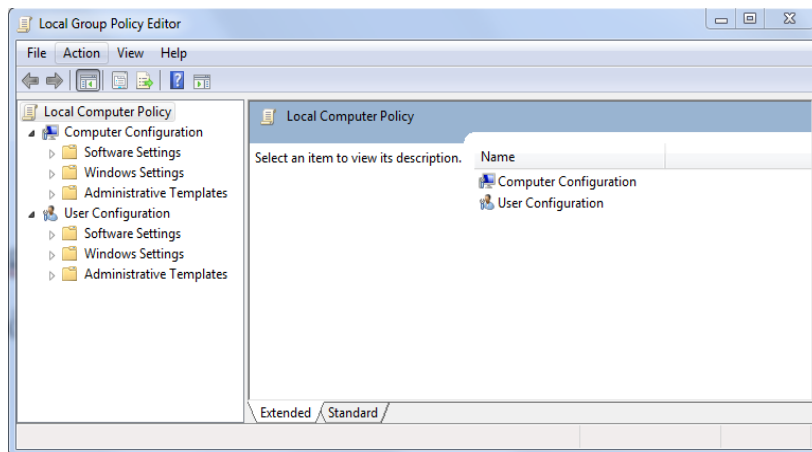
Η εφαρμογή πολιτικών ασφαλείας δεν γίνεται τυχαία, αλλά ακολουθεί μια συγκεκριμένη και σαφή ιεράρχηση βασισμένη σε προϋπάρχουσες πολιτικές, οι οποίες αλληλεπιδρούν με τις νέες, για να εξαχθεί το επιθυμητό αποτέλεσμα.

13.3.1.1 Local Security Policy

Η επαφή με το GPO προϋπάρχει, ασχέτως ύπαρξης Active Directory, διότι όλοι οι υπολογιστές διαθέτουν τη **local policy**, μέσω της οποίας εφαρμόζονται οι default

πολιτικές του λειτουργικού συστήματος, όπως κοινό αρχικά wallpaper και εικονίδια, κοινόχρηστοι χώροι κτλ.

Εκτελώντας gpedit.msc, στο Start→Run και σε οποιοδήποτε υπολογιστή με Windows αποκτάμε πρόσβαση στη local security policy.



Εικ. 13.1. Local Security Policy.

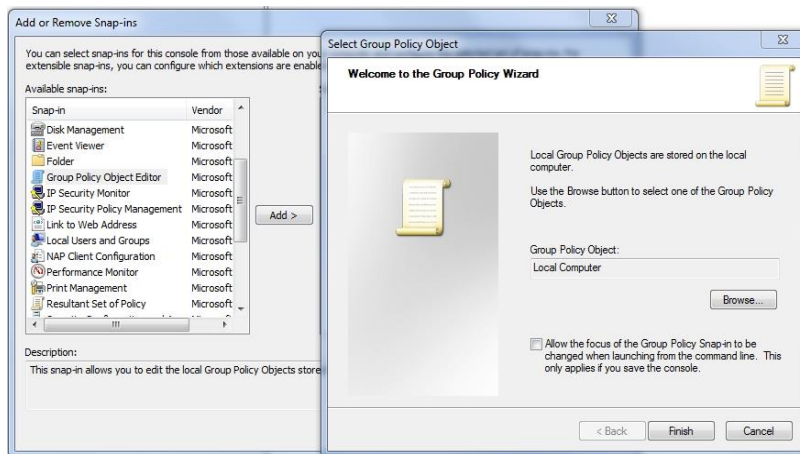
Η Εικ. 13.1 αναφέρεται σε ένα συγκεκριμένο GPO, τη local policy ενός απλού υπολογιστή.

Ο Windows Server 2008 έχει αντίστοιχη local policy, που του δίνει τις δυνατότητες που παρουσιάζονται, αμέσως μετά την εγκατάστασή του.

Επηρεάζοντας το local security policy, ανεξαρτήτως χρήστη που το χρησιμοποιεί, επηρεάζεται η συμπεριφορά ολόκληρου του υπολογιστή.

Συνεπώς, εφόσον είναι δυνατόν, προτείνεται να αποφεύγεται οποιαδήποτε τροποποίηση της local policy.

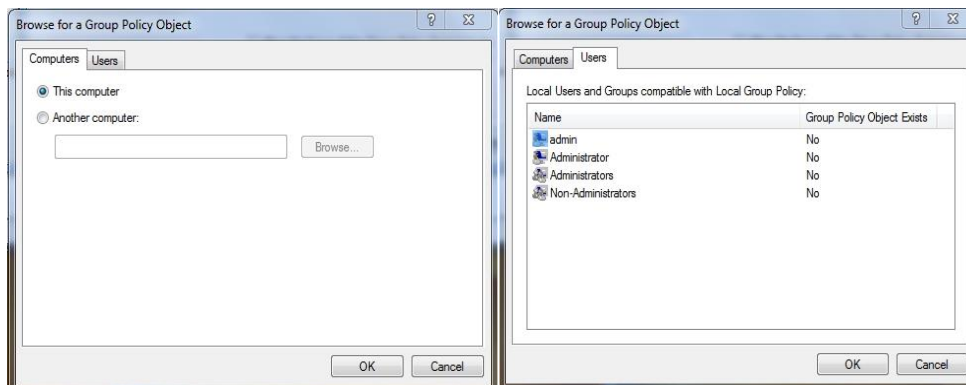
Σε vista και νεότερα λειτουργικά συστήματα υπάρχει η δυνατότητα local security policy ανά χρήστη, μέσω της οποίας τροποποιείται η default local security policy για τον συγκεκριμένο user.



Εικ. 13.2. Local Security Policy ανά User.

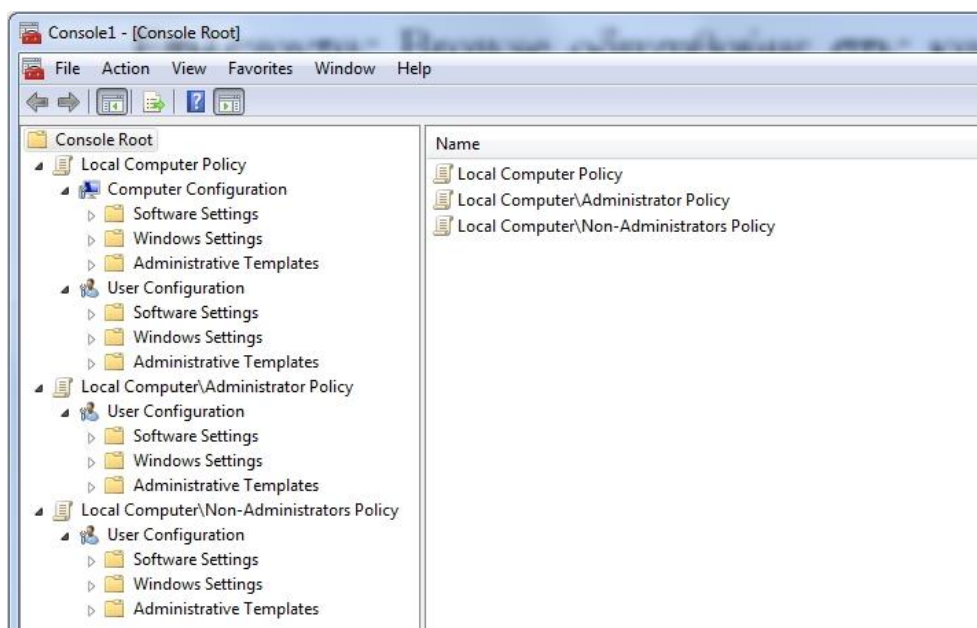
Η εμφάνιση της τοπικής πολιτικής του χρήστη γίνεται μέσα από start→Run→mmc
κονσόλα File→Add remove snap-ins → group policy editor (Εικ. 13.2).

Επιλέγοντας Browse θα οδηγηθούμε στις καρτέλες Computers και Users της Εικ. 13.3, μέσω των οποίων διαλέγουμε έναν άλλο ή το τοπικό Η/Υ αλλά και ποιοί από τους τοπικούς λογαριασμούς είναι συμβατοί με τη συγκεκριμένη πολιτική.



Εικ. 13.3. Local Security Policy ανά Computer ή User.

Διαλέγοντας ανάλογα δημιουργείται μια κονσόλα διαχείρισης για ένα ή περισσότερα επιλεγμένα αντικείμενα (Εικ. 13.4).



Εικ. 13.4. Κονσόλα διαχείρισης Local Policy Computer ή User.

Πρώτα θα εφαρμοσθεί η local policy, μετά η πολιτική των ομάδων Administrators ή Non-Administrators και τελικά η πολιτική του χρήστη.

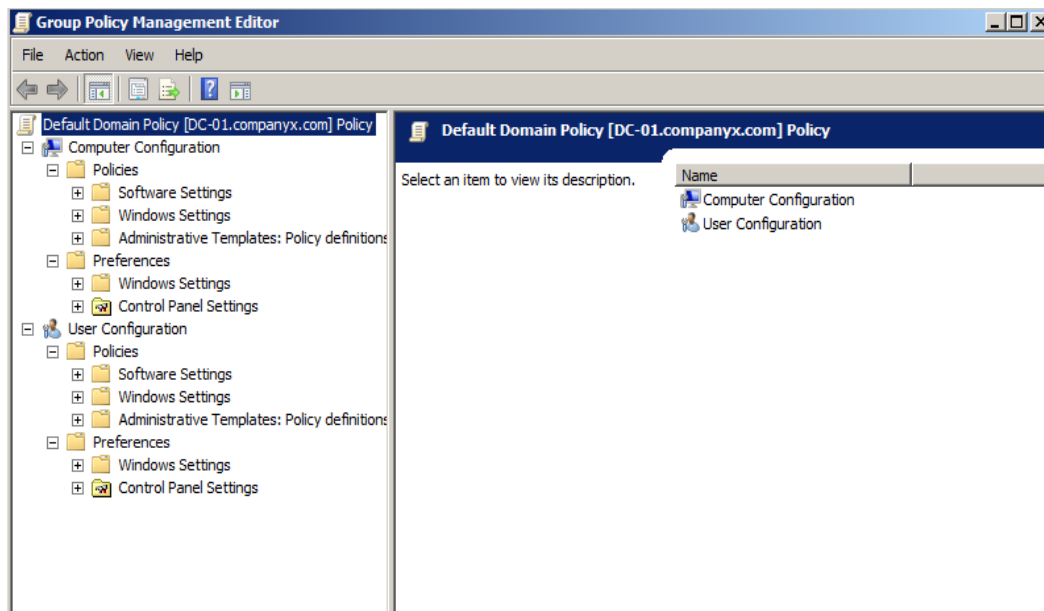
Αν οι πολιτικές κατά την εφαρμογή τους συγκρούονται με προηγούμενες στην παραπάνω ιεράρχηση, υπερισχύει η τελευταία που εκτελέστηκε.

13.3.1.2 Domain & DC policies

Αντίστοιχα με την εγκατάσταση στο server 2008 του ρόλου Active Directory Domain

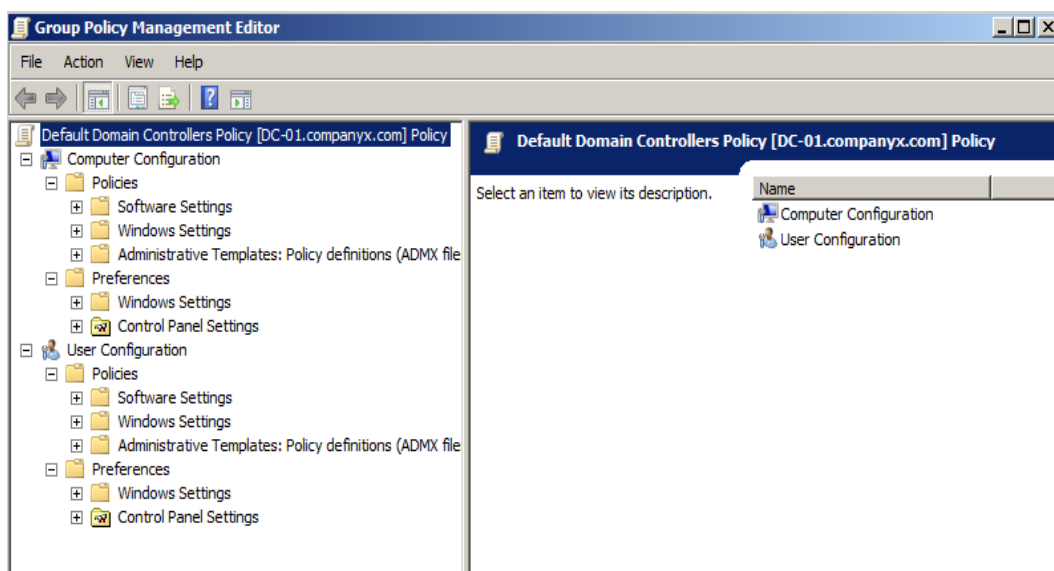
Services (AD DS) δημιουργείται η υποδομή του site (Default-First-Site-Name), στο οποίο δύναται να εφαρμοσθούν GPOs.

Ταυτόχρονα δημιουργείται η default domain policy με πολιτικές ασφαλείας εφαρμοστές σε όλα τα objects του Domain (Εικ. 13.5).



Εικ. 13.5. Default Domain Policy.

Επιπλέον δημιουργείται η Default Domain Controllers Policy με πολιτικές ασφαλείας εφαρμοστές σε όλους τους Domain Controllers του Domain (Εικ. 13.6).



Εικ. 13.6. Default Domain Controllers Policy.

Μετά από τις παραπάνω πολιτικές εφαρμόζονται οι πολιτικές που τοποθετούμε σε OUs και μετά οι πολιτικές των nested OUs.

Συνοψίζοντας οι πολιτικές εφαρμόζονται σύμφωνα με την παρακάτω σειρά με υπερισχύουσα, σε περίπτωση σύγκρουσης με τις προηγούμενες, πάντα την τελευταία.

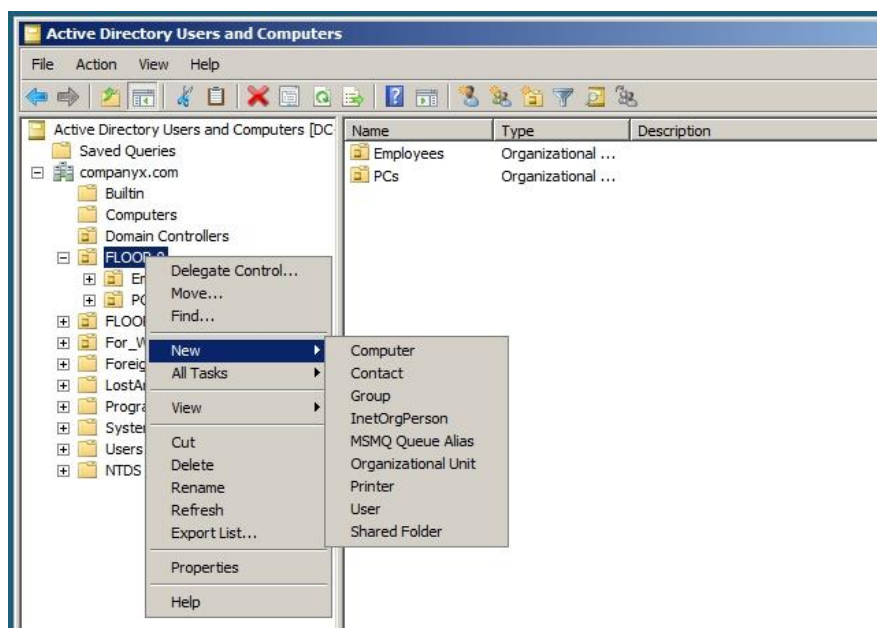
- | | | |
|-----------------|--|---------------------------|
| 1. Local Policy | | 4. Domain Controllers GPO |
| 2. Site GPO | | 5. OU GPO |
| 3. Domain GPO | | 6. Child OU GPO |

Δηλαδή, αν για παράδειγμα στη local policy υπάρχει για κάποιο αντικείμενο η πολιτική «NAI_DVD», αλλά το ίδιο αντικείμενο στο OU που βρίσκεται έχει «NO_DVD» στην ίδια θέση που συγκρούεται με την προηγούμενη πολιτική, τότε θα εφαρμόσει το «NO_DVD», διότι είναι η τελευταία σύμφωνα με την παραπάνω σειρά, που εφαρμόστηκε.

13.3.1.3 Προεπιλεγμένα εργαλεία

Με την εγκατάσταση του AD DS στο Server 2008 αυτόματα, μεταξύ άλλων, δημιουργούνται εργαλεία διαχείρισης αντικειμένων και πολιτικών ικανά να προσφέρουν «ιδανικά» αποτελέσματα ασφαλείας στο Domain.

- Στο σύνδεσμο Start → Administrative tools → Active Directory Users and Computers παρουσιάζεται η κύρια κονσόλα διαχείρισης των αντικειμένων του AD με



Εικ. 13.7. Active Directory Users and Computers.

δυνατότητες που φαίνονται κάνοντας δεξί κλικ (Εικ. 13.7) σε κάποιο OU του «δένδρου» και βασικότερη το Delegate Control.

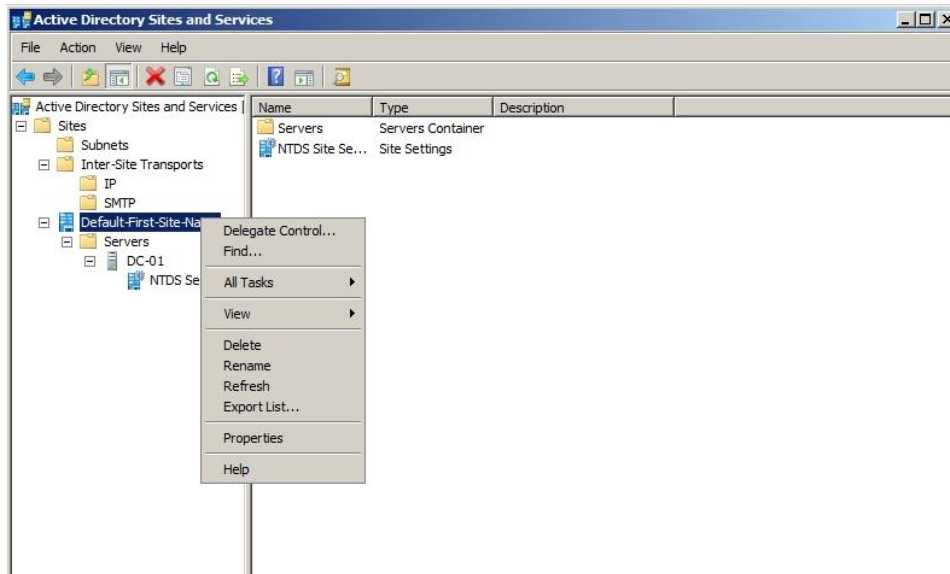
- Στο σύνδεσμο Start → Administrative tools → Active Directory Sites and Services δίνεται δυνατότητα διαχείρισης των Sites (Default-First-Site-Name) δημιουργία, τροποποίηση και διαγραφή sites και subnets.

Τα Sites στο Active Directory (AD) αναπαριστούν τη φυσική υποδομή ή την τοπολογία του δικτύου. Το AD χρησιμοποιεί αυτή την πληροφορία για να φτιάξει

την αποδοτικότερη τοπολογία για replication.

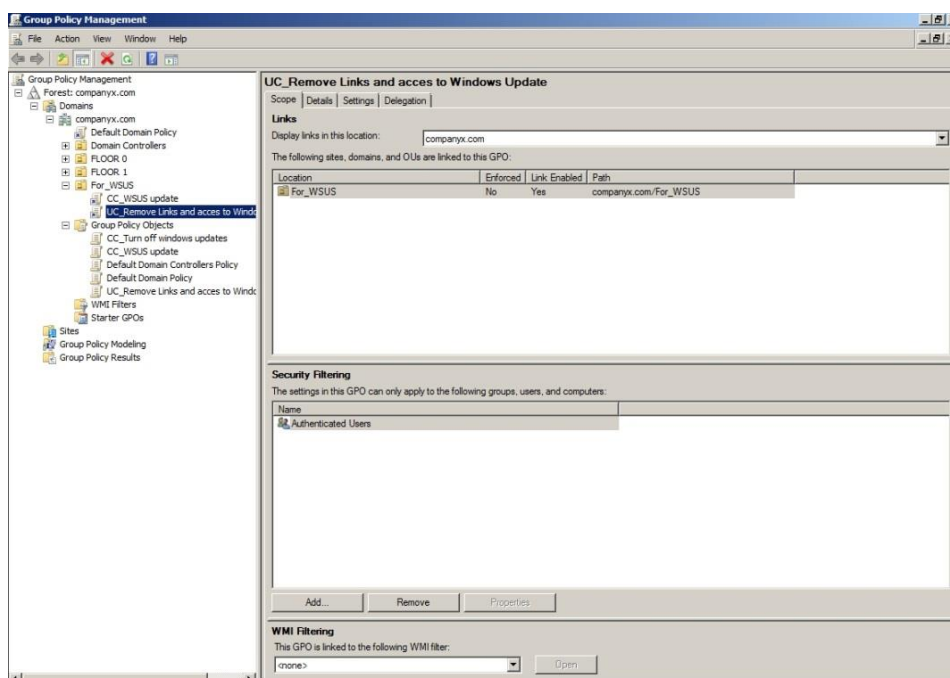
Site στην ουσία είναι ένα σύνολο από πολύ καλά συνδεδεμένα subnets που αντιπροσωπεύει τη φυσική υποδομή του δικτύου, ενώ το Domain είναι η λογική υποδομή του οργανισμού.

Όπως φαίνεται στην Εικ. 13.8, κάνοντας δεξί κλικ στο Default-First-Site-Name έχουμε τη δυνατότητα μεταβίβασης εξουσιοδότησης Delegate Control σε οποιοδήποτε αντικείμενο του AD.



Εικ. 13.8. Active Directory Sites and Services.

- Στο σύνδεσμο Start → Administrative tools → Group Policy Management

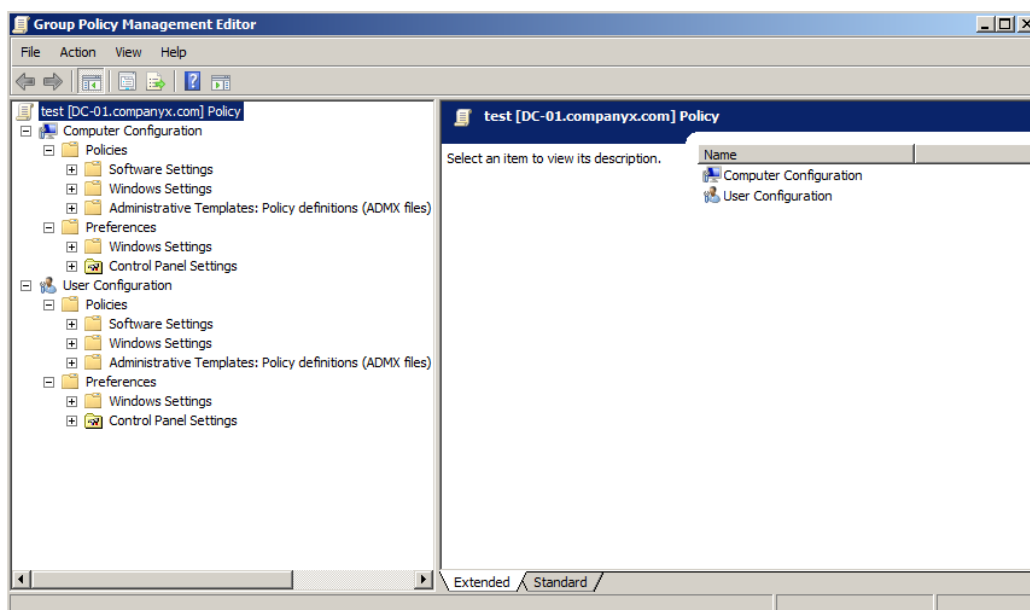


Εικ. 13.9. Group Policy Management.

ανοίγει το βασικό εργαλείο δημιουργίας και διαχείρισης των GPOs (Εικ. 13.9), το οποίο εγκαταστάθηκε αυτόματα σαν συνέπεια του AD, αλλά σαν Feature δύναται να εγκαθίσταται και standalone. Αναλυτικότερα θα αναφερθούμε παρακάτω.

13.3.1.4 Group Policy Object (GPO)

Το βασικό εργαλείο δημιουργίας πολιτικών ασφαλείας είναι το GPO, το οποίο, αφού το ρυθμίσουμε κατάλληλα, το «συνδέουμε» στο κατάλληλο container (site, domain, ΟΥ).



Εικ. 13.10. Group Policy Object (GPO).

Στην Εικ. 13.10 βλέπουμε τη δομή ενός GPO, το οποίο παρατηρούμε ότι έχει δύο βασικά χαρακτηριστικά.

Το Computer Configuration και το User Configuration.

- Ότι ρυθμίσεις γίνονται στο Computer configuration (CC), αφορούν τον υπολογιστή σαν μηχανή και οι πολιτικές εφαρμόζονται ανεξάρτητα το ποιος χρήστης το χρησιμοποιεί.

Δηλαδή, αν με μια πολιτική στο CC έχουμε απαγορεύσει τη χρησιμοποίηση DVD, οποιοσδήποτε χρήστης και να χρησιμοποιήσει τον υπολογιστή, δεν θα μπορεί να χρησιμοποιήσει DVD.

Για να εφαρμοστεί μια πολιτική CC, το client pc χρειάζεται επανεκκίνηση.

- Οι ρυθμίσεις που γίνονται στο User Configuration (UC), αφορούν τον κάθε χρήστη, ανεξαρτήτως σε ποιο μηχανήμα εργάζεται και ακολουθούν τον χρήστη σε ολόκληρο το Domain.

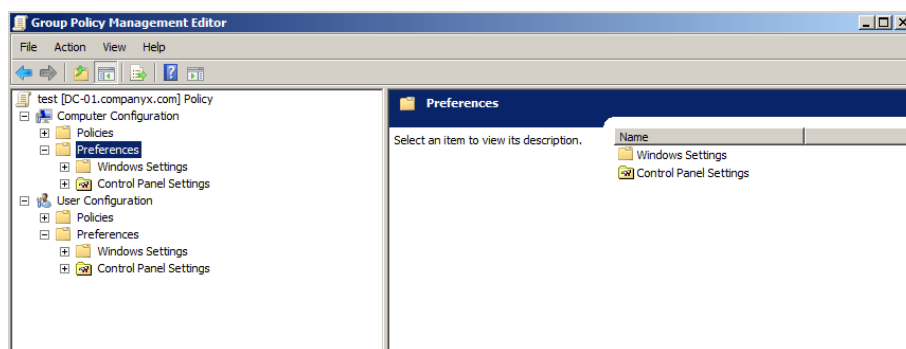
Αν, δηλαδή, στον χρήστη Α με πολιτική στο UC έχουμε καθορίσει ότι θα

χρησιμοποιεί Open Office σε οποιοδήποτε μηχάνημα και αν εργαστεί, εφόσον με άλλες πολιτικές δεν απαγορεύεται αυτή η δυνατότητα, θα έχει Open Office.

Αντίστοιχα αν σε άλλο χρήστη καθορίσθηκε στο UC ότι θα χρησιμοποιεί MS Office, αν εργαστεί στο ίδιο μηχάνημα με τον προηγούμενο, θα χρησιμοποιεί το MS office.

Η εφαρμογή των πολιτικών του UC απαιτεί να κάνει ο χρήστης logoff.

Εάν υπάρχει σύγκρουση μεταξύ ιδίων ρυθμίσεων στο CC και το UC υπερισχύει του Computer configuration.



Εικ. 13.11. GPO Preferences.

Ένα από τα χαρακτηριστικά που παρατηρούμε επιπλέον στο GPO είναι οι ρυθμίσεις preferences στο CC και UC οι οποίες δεν υπήρχαν στις προηγούμενες εκδόσεις Server (Εικ. 13.11).

Περιλαμβάνει νέα Group Policy extensions, όπως folder options, mapped drives, printers, scheduled tasks, services, και Start menu settings.

Επιπρόσθετα προσφέρει περισσότερη κάλυψη, καλύτερη στόχευση και ευκολότερη διαχείριση, ενώ οι πολιτικές εφαρμόζονται χωρίς απαραίτητα να απαγορεύεται η δυνατότητα αλλαγής τους από τοπικούς χρήστες (Local Administrators).

Με τη δυνατότητα αυτή υπάρχει ευελιξία εφαρμογής επιβεβλημένων πολιτικών που δύναται να μεταβληθούν πρόσκαιρα.

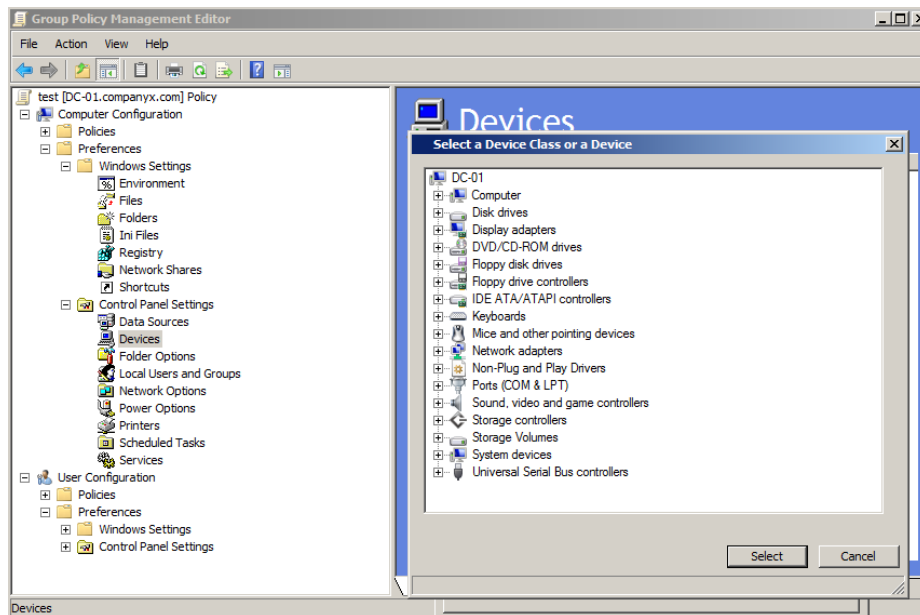
Η εκτέλεση των preferences υλοποιείται σε clients με λειτουργικό windows vista και νεώτερο, ενώ για παλαιότερα λειτουργικά απαιτείται η προεγκατάσταση του προγράμματος Client Side Extension.

Το Client Side Extension είναι διαφορετικό για κάθε έκδοση λειτουργικού και μπορούμε να το κατεβάσουμε από τη Microsoft.

Μηχάνημα που δεν έχει το Extension δεν θα εφαρμόσει πολιτικές preferences.

Η εγκατάσταση του Client Side Extension μπορεί να γίνει standalone αλλά και με GPO μέσω ενός batch file που εκτελεί εγκατάσταση στον κάθε client δικτυακά.

Για να γίνει περισσότερο κατανοητή η επιλογή preferences, παρατηρούμε την εικόνα

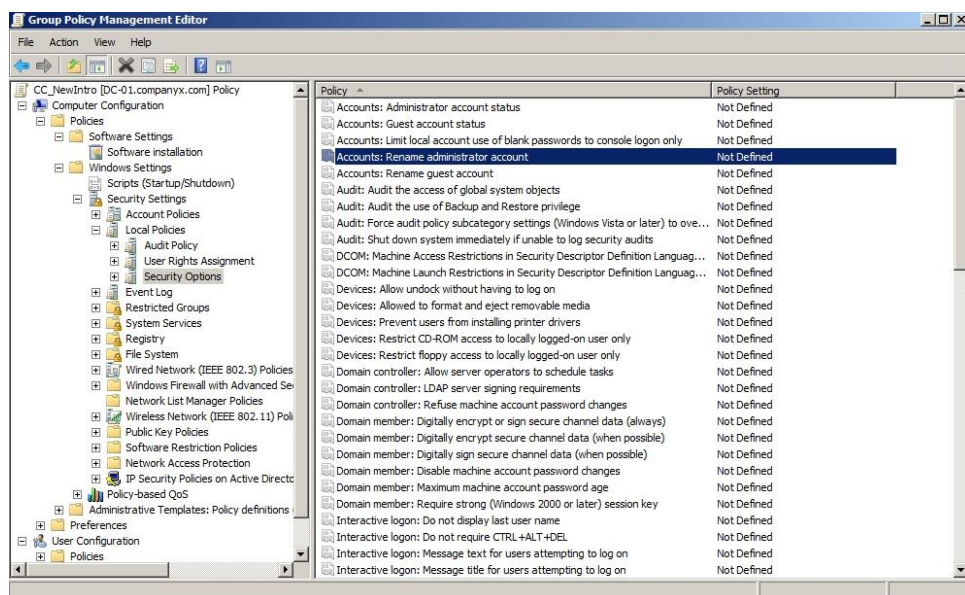


Εικ. 13.12. GPO Preferences (Devices).

Εικ. 13.12 της διαδρομής CC→Preferences→Control Panel Settings→Devices όπου με κατάλληλες επιλογές εμφανίζεται το device manager.

Όπως ένας διαχειριστής θα απενεργοποιούσε επιτόπου στον client το dvd, το ίδιο μπορεί να κάνει και τώρα μέσω του GPO.

Η διαφορά της πολιτική αυτής είναι ότι ένας τοπικός administrator, αφού ενωθεί τοπικά στο μηχάνημα σαν οποιοσδήποτε δικτυακός χρήστης, μπορεί να ενεργοποιήσει και πάλι τις επιλογές και να λειτουργεί με DVD μέχρι την επομένη επανεκκίνηση, όπου και θα εφαρμοστεί ξανά η πολιτική. Με τις policies αυτό δεν θα ήταν δυνατό.

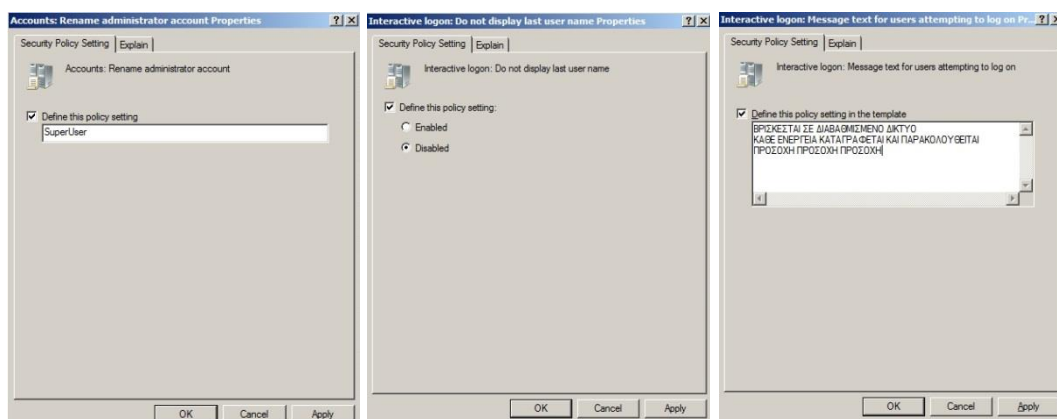


Εικ. 13.13. ρύθμιση GPO.

Οι πολιτικές στην πλειονότητα τους επηρεάζουν τη registry του υπολογιστή, εκτελούν τοπικά προγράμματα ή batch files, επηρεάζουν την εμφάνιση, την ασφάλεια, την κρυπτογράφηση, τα δίκτυα, την αποθήκευση των αρχείων, την εκτέλεση ή απαγόρευση εκτέλεσης προγραμμάτων το κρύψιμο στοιχείων και γενικά ότι μπορούμε να φανταστούμε.

Απλά χρειάζεται στο αντίστοιχο σημείο του GPO να επιλέξουμε την κατάλληλη δυνατότητα (Εικ. 13.13), η οποία θα μας οδηγήσει σε πληθώρα άλλων επιλογών.

Η ενεργοποίηση ή απενεργοποίηση της πολιτικής γίνεται με διαφόρους τρόπους, όπως το παράδειγμα της Εικ. 13.14, απαντώντας στο λεκτικό της πολιτικής.



Εικ. 13.14. αναλυτική ρύθμιση GPO.

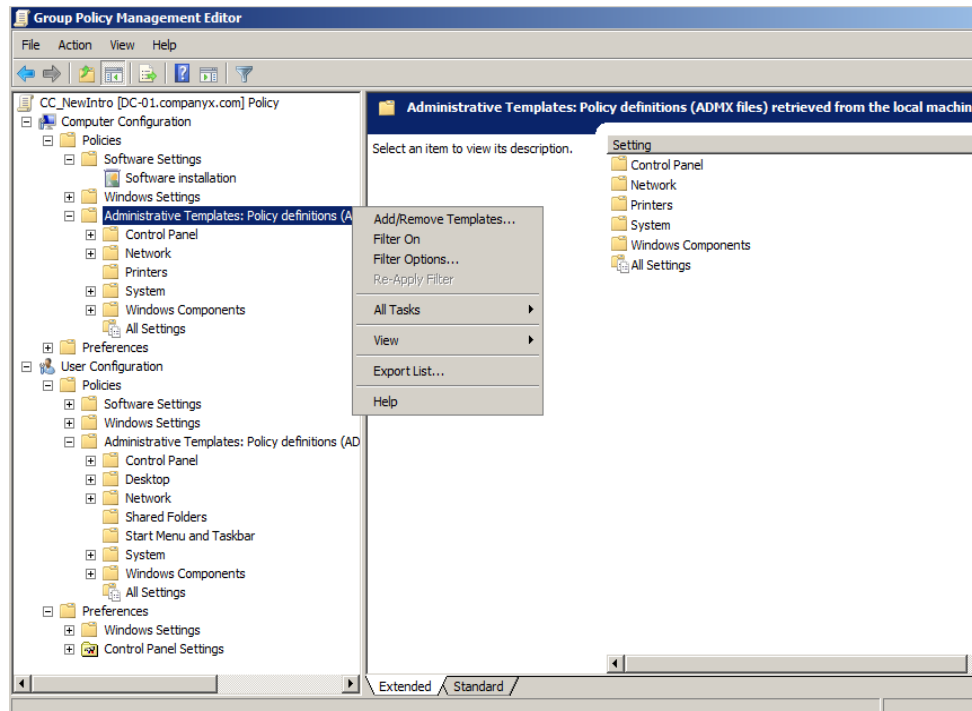
Δηλαδή, αν μια πολιτική λέει: Do not display last username με την επιλογή enable δεν θα φαίνεται το όνομα, ενώ με το disable θα φαίνεται κανονικά το τελευταίο username.



Εικ. 13.15. Ανάλυση GPO.

Στις πολιτικές υπάρχει η καρτέλα explain (Εικ. 13.15), η οποία παρέχει σχετικές πληροφορίες για το τι κάνει και πώς εφαρμόζεται η αντίστοιχη πολιτική.

Εκτός των πολιτικών που υπάρχουν default σε κάθε GPO, μπορούμε να προσθέσουμε επιπλέον πολιτικές που θα εφαρμόζονται σε συγκεκριμένα προγράμματα π.χ στο office ή θα διαχειρίζονται συγκεκριμένα εξαρτήματα.



Εικ. 13.16. Administrative Templates.

Οι πολιτικές αυτές προστίθενται στις επιλογές Administrative Templates add/remove Templates (Εικ. 13.16) και σύμφωνα με τις οδηγίες του αντίστοιχου προμηθευτή. Τα αρχεία που μπορούν να χρησιμοποιηθούν στη συγκεκριμένη διαδικασία πρέπει να έχουν τη δομή «όνομα.admx», αλλά μπορεί να χρησιμοποιηθεί και ο παλαιότερος τύπος «όνομα.adm».

13.3.1.5 Group Policy Management

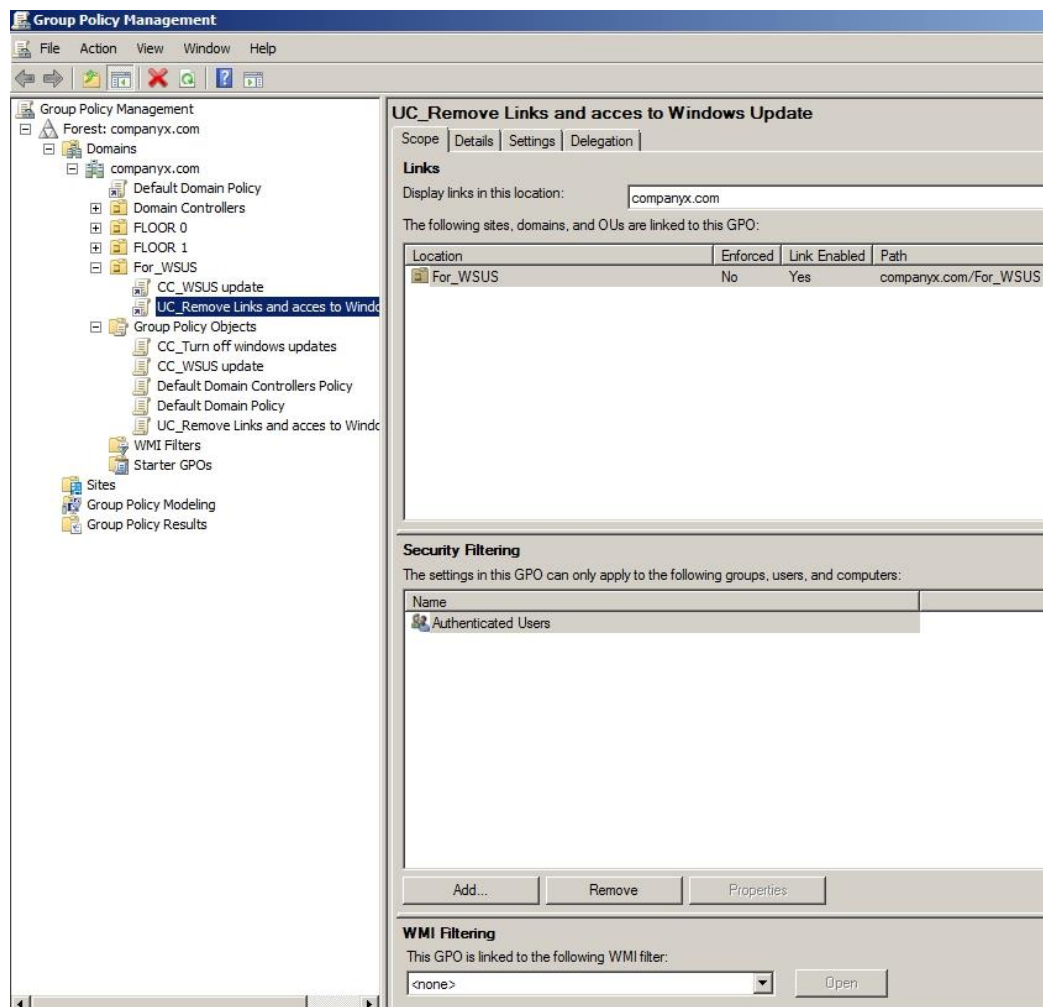
Το εργαλείο δημιουργίας και διαχείρισης πολιτικών ασφαλείας είναι το Group Policy Management, το οποίο έχει εγκατασταθεί μαζί με την εγκατάσταση του AD DS και μπορεί να εγκατασταθεί και αυτόνομα, διότι είναι feature.

Η πρόσβαση γίνεται Start → Administrative Tools → Group Policy Management, όπου εμφανίζεται η Εικ. 13.17.

Παρατηρούμε στην αριστερή πλευρά τη δομή του Forest που εμπεριέχει το domain companyx.com και ακριβώς από κάτω τα υφιστάμενα OUs, default και δημιουργημένα, στα οποία θα γίνονται link τα GPOs.

Τα GPOs γίνονται link, ώστε αν διαγράφονται από κάποιο OU, να μη διαγράφονται και από το domain ή άλλο OU.

Τα GPOs αποθηκεύονται στο container Group Policy Objects, από το οποίο δύνανται



Εικ. 13.17. Group Policy Management.

να διαγραφούν οριστικά. Επιπλέον παρατηρούμε τα παρακάτω:

WMI Filters: Τα Windows Management Instrumentation (WMI) filters επιτρέπουν τη δυναμική εκτέλεση των πολιτικών, εξαρτώμενη από τα attributes του computer που πρόκειται να εφαρμοστούν.

Αν ο υπολογιστής εκπληρώνει κάποιες προϋποθέσεις, τότε εφαρμόζεται η πολιτική. Αν όχι τότε δεν εφαρμόζεται.

Starter GPOs: Δημιουργούμε προρυθμισμένα GPOs, τα οποία μπορούμε στη συνέχεια να χρησιμοποιούμε σαν βάση για νέα GPOs.

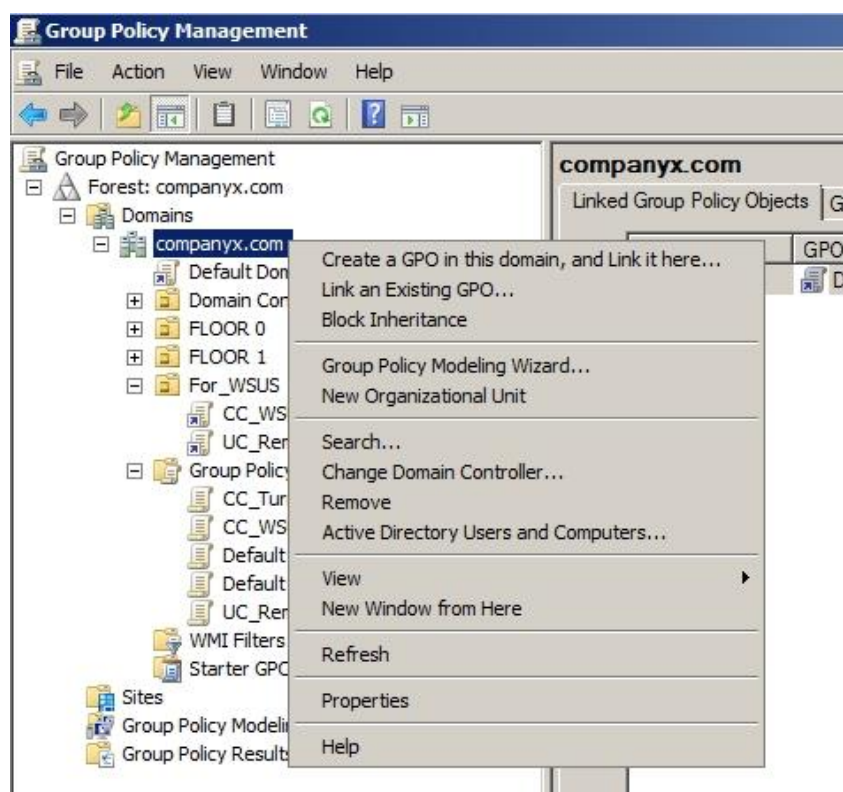
Sites: Διαλέγουμε sites και συνδέουμε GPOs.

Group Policy Modeling: Εργαλείο που επιτρέπει την προσομοίωση μιας πολιτικής που θα εφαρμοστεί σε users ή computers, πριν εφαρμοστεί στην πραγματικότητα.

Είναι γνωστό και σαν Resultant Set of Policy (RSoP).

Απαιτεί την ύπαρξη domain controller 2008 στο forest, διότι η εκτέλεση της προσομοίωσης γίνεται από ένα service που υπάρχει μόνο στο DC. Δύναται να προσομοιάσει το resultant set of policy, δηλαδή, το «συνολικό αποτέλεσμα από την εκτέλεση της πολιτικής» για όλους τους υπολογιστές του Forest.

Group Policy Results: Χρησιμοποιείται για να προσομοιάσει τις πολιτικές που τελικά θα ισχύσουν για έναν χρήστη ή υπολογιστή συγκεντρώνοντας RSoP πληροφορία από τον τελικό υπολογιστή. Σε αντίθεση με το Group Policy Modeling αποκαλύπτει τις πραγματικές ρυθμίσεις πολιτικής που θα εφαρμοστούν σε κανονικές συνθήκες στον πραγματικό υπολογιστή.



Εικ. 13.18. Επεξηγήσεις Group Policy Management.

13.3.1.6 Create, Link, Block Inheritance

Κάνοντας δεξί κλικ στο Domain ή σε οποιοδήποτε OU ή Site (Εικ. 13.18), παρουσιάζονται οι εξής επιλογές:

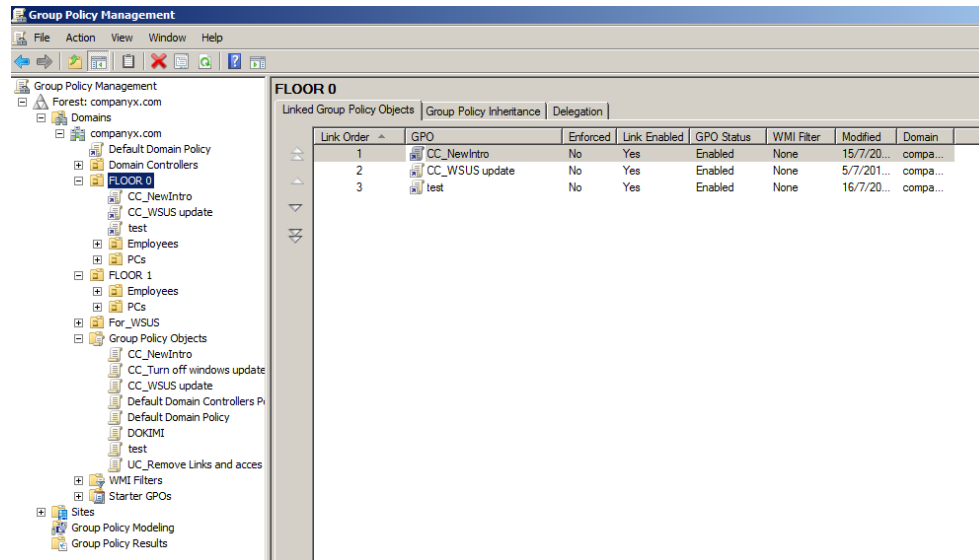
Greate a GPO in this domain and link it here ...: Δημιουργούμε μια νέα GPO στο container Group Policy Objects και την ενώνουμε άμεσα στο συγκεκριμένο container (αντίστοιχα ισχύει για sites, domains, OUs).

Link an Existing GPO: Επιλέγουμε ήδη υπάρχουσα GPO από το container Group Policy Objects και τη συνδέουμε με το συγκεκριμένο.

Block Inheritance: Διακόπτουμε την κληρονομικότητα εφαρμογής πολιτικών που «έρχονται» από προηγούμενες πολιτικές.

New Organizational Unit: Δημιουργεί απευθείας στο «δένδρο» νέο ΟΥ.

Οι υπόλοιπες επιλογές από τον ορισμό τους «φανερώνουν» τις ενέργειές τους.

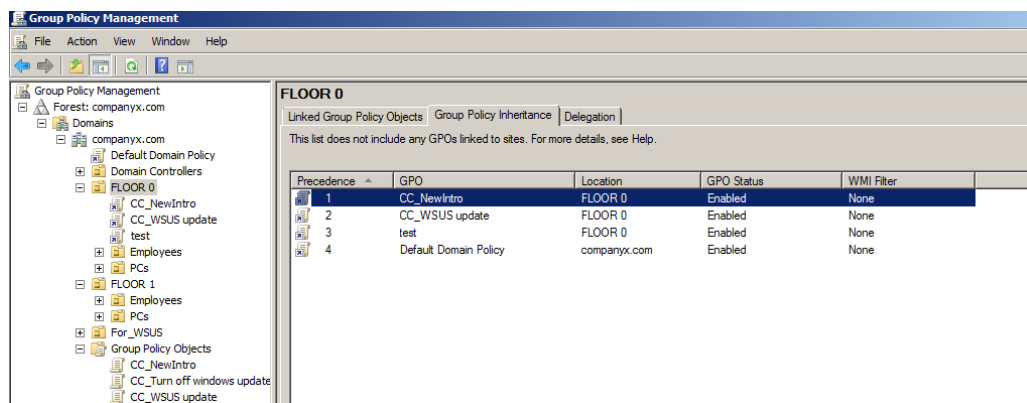


Εικ. 13.19. Περιήγηση στο Group Policy Management.

Στο δεξί panel οποιασδήποτε ΟΥ ή άλλου στοιχείου που δέχεται πολιτικές (Εικ.13.19), φαίνονται τα GPOs που έχουν συνδεθεί μέχρι στιγμής.

Σε περίπτωση που η ίδια πολιτική συναντάται σε πολλά GPOs αλληλοαναιρούμενη, τότε αγνοούνται όλες οι πολιτικές πλην της πρώτης, που συναντήθηκε κατά την αύξουσα σειρά.

Εάν επιθυμούμε κάποια πολιτική να εκτελεστεί σίγουρα τότε την ανεβάζουμε ψηλότερα χρησιμοποιώντας τα αντίστοιχα στοιχεία ελέγχου.



Εικ.

13.20. Περιήγηση στη GPMC.

Στην καρτέλα Group policy inheritance (Εικ. 13.20) φαίνονται οι πολιτικές που εφαρμόζονται άμεσα και λόγω κληρονομικότητας στο ΟΥ, FLOOR 0, ενώ στην

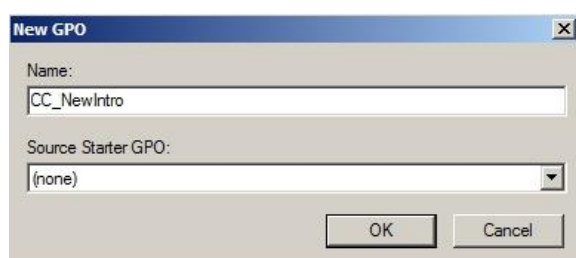
καρτέλα Delegation αναγράφονται οι εξουσιοδοτημένοι (groups, users) ανάλογα με τα permissions, για το συγκεκριμένο OU.

13.3.1.7 Δημιουργία και διαχείριση GPOs σε Domain

Για να δημιουργήσουμε μια GPO κάνουμε δεξί κλικ:

- Σε OU και Create a GPO in this domain and link it here ... ή
- Στο Group policy objects → new με την προϋπόθεση ότι θα τη συνδέσουμε μετά σε κάποια OU.

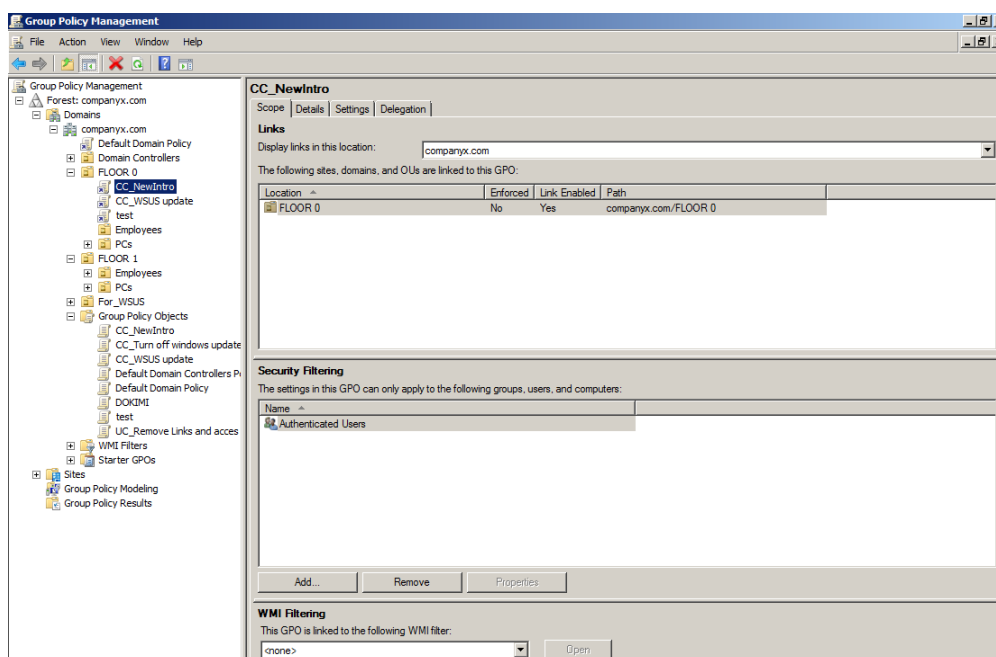
Εμφανίζεται η Εικ. 13.21, στην οποία θα πρέπει να καθορίσω ένα όνομα και να επιλέξω να χρησιμοποιήσω, εφόσον απαιτείται και αν έχω δημιουργήσει προηγουμένως, κάποια Starter GPO.



Εικ. 13.21. New GPO.

Στην ονοματολογία συνήθως χρησιμοποιούμε ονόματα που να προσδιορίζουν τι κάνει κάθε GPO, για να γίνεται εύκολα ο εντοπισμός, από κάποιο backup set.

Στο παράδειγμα της Εικ. 13.21 χρησιμοποιούμε CC (δηλώνει ότι αφορά Computer Configuration πολιτική) και NewIntro που δηλώνει κάποια νέα εισαγωγή.



Εικ. 13.22. γενικά για νέα GPO.

Αντίστοιχα αν η πολιτική αφορά user configuration, τότε μπορούμε να γράψουμε UC_FlowerWallpaper, που μας θυμίζει ότι στην πολιτική αυτή οι χρήστες έχουν «wallpaper ένα λουλούδι».

Εφόσον δημιουργήσουμε τη νέα GPO, CC_NewIntro τοποθετείται στο container group policy objects και ένα link συνδέεται με το OU, το FLOOR 0, Εικ. 13.22.

Επιλέγοντας τη CC_NewIntro βλέπουμε στο δεξί panel τις καρτέλες:

- **Scope:** α. Links: Σε τι είναι συνδεδεμένη η συγκεκριμένη πολιτική (ou,site,domain).

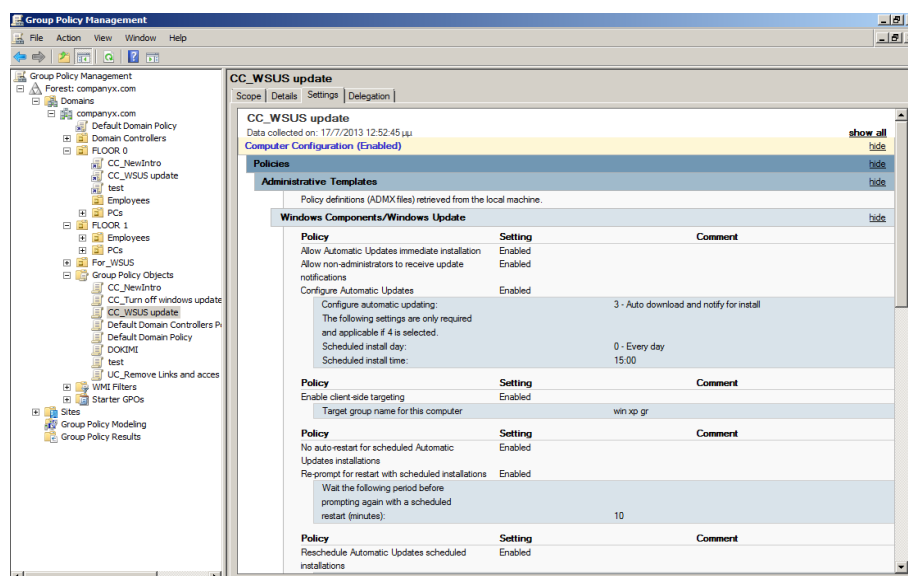
- β. Security filtering: Ποια objects εφαρμόζουν τη συγκεκριμένη πολιτική.

- γ. WMI Filtering: Αν έχουν δημιουργηθεί WMI filters μέσω του combo box μπορούμε να τα εισάγουμε και να περιορίσουμε, όπως αναφέρθηκε σε ποιο πάνω ενότητα, την εφαρμογή της πολιτικής σε υπολογιστές που έχουν συγκεκριμένα κριτήρια.

Τα WMI αρχεία είναι της μορφής «όνομα.mof» και στην ουσία είναι ένα query πάνω σε συγκεκριμένα attributes. π.χ το παρακάτω query:

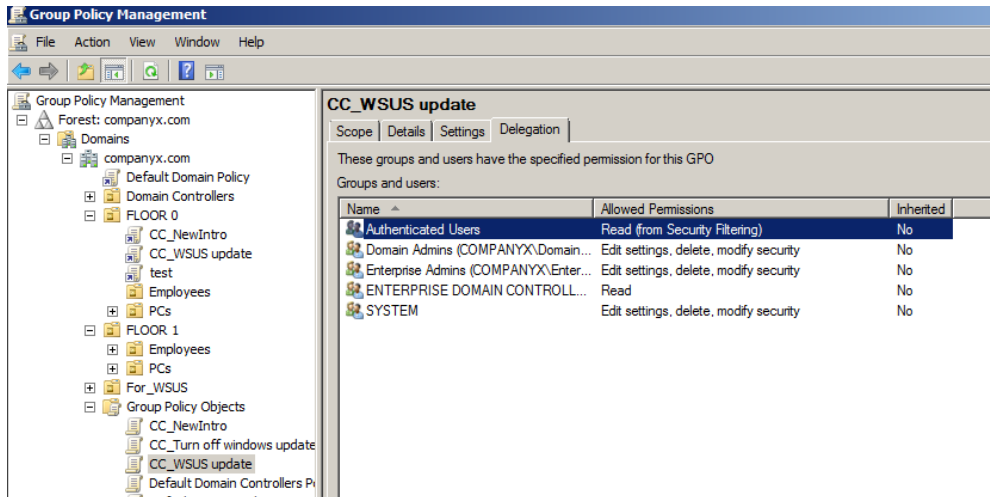
```
SELECT TotalPhysicalMemory  
FROM Win32_ComputerSystem  
WHERE TotalPhysicalMemory >= 2000000000
```

το οποίο διαλέγει τους υπολογιστές που έχουν μνήμη ≥ 2000000000 και το οποίο με κατάλληλο πρόγραμμα μετατρέπεται σε .mof και εισάγεται στο WMI filters και από εκεί σε οποιοδήποτε GPO.



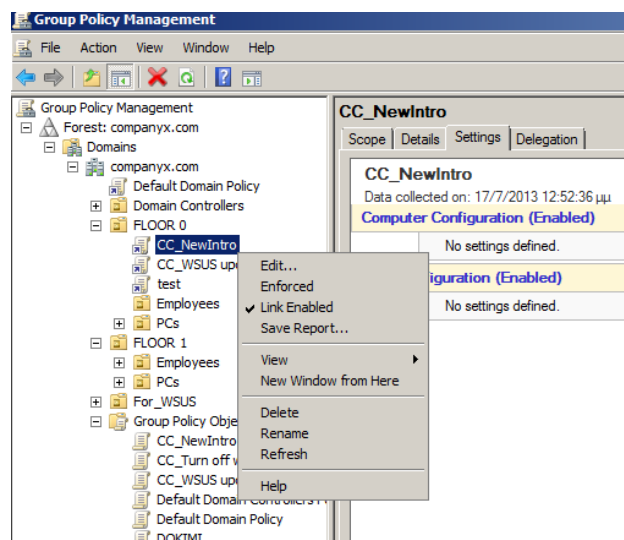
Εικ. 13.23. Settings σε GPO.

- **Details:** Στοιχεία για την πολιτική και την κατάσταση της.
- **Settings:** Μια λεπτομερής αναφορά με ποια «κλειδιά» έχουν ενεργοποιηθεί στη συγκεκριμένη GPO (Εικ. 13.23).
- **Delegation:** Ποιοι και με ποια δικαιώματα έχουν πρόσβαση στη GPO (Εικ. 13.24).



Εικ. 13.24. Delegation σε GPO.

Παραπάνω αναφέρθηκε η ιεραρχική εφαρμογή των πολιτικών που συνοψίζοντας θα μπορούσαμε να πούμε ότι, αν μια πολιτική που βρίσκεται σε ΟΥ συγκρούεται με αντίστοιχη πολιτική που έχει εκτελεστεί προηγούμενα, τότε αυτή υπερισχύει. Ενώ αν δεν υπάρχει σύγκρουση, «κληρονομικά» εφαρμόζεται σε όλο το «δένδρο» του domain.



Εικ. 13.25. Enforced σε GPO.

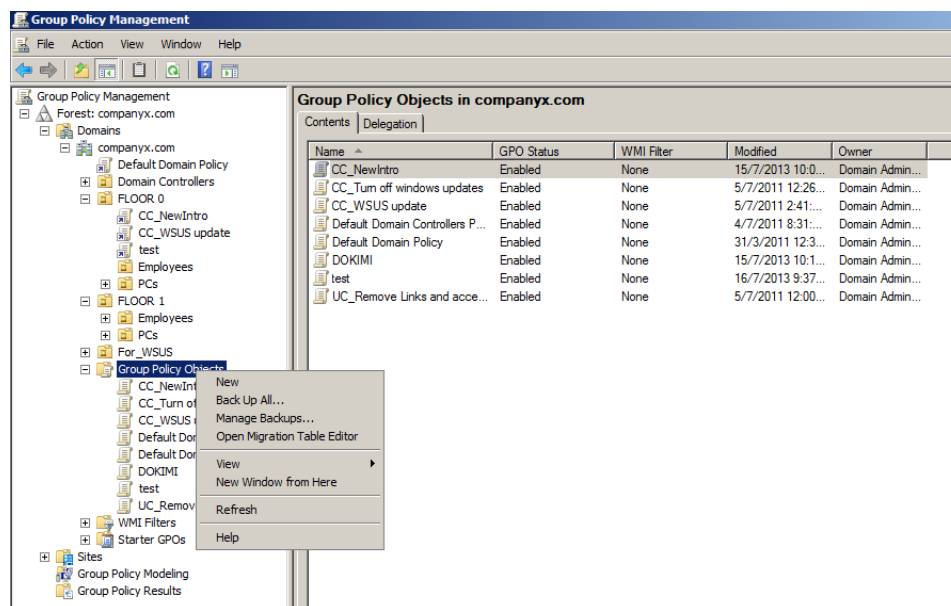
Αν, όμως, απαιτείται από κάποιο σημείο της ιεράρχησης εκτέλεσης πολιτικών να εφαρμοστεί οπωσδήποτε από εκεί και κάτω ένα συγκεκριμένο GPO, πρέπει με δεξί

κλικ στην πολιτική να επιλέξουμε enforced (Εικ. 13.25).

Από εκεί και κάτω άσχετα αν υπάρχουν «συγκρούσεις», όλα τα αντικείμενα θα εφαρμόζουν τη συγκεκριμένη πολιτική.

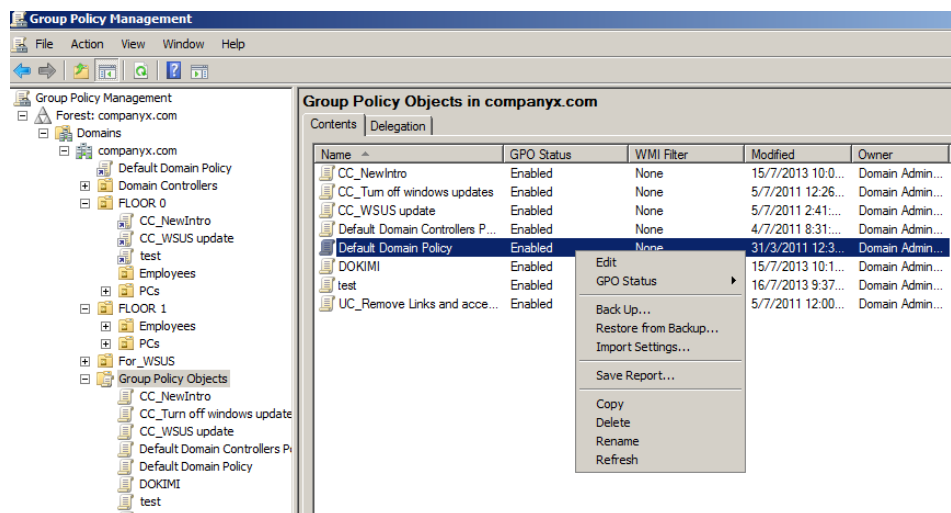
13.3.1.8 Backup, Restore GPOs

Τις πολιτικές ασφαλείας που έχουμε δημιουργήσει θέλουμε να τις «αποθηκεύσουμε» για να έχουμε disaster recovery, αλλά και να μπορούμε να τις χρησιμοποιήσουμε και σε άλλα domains.



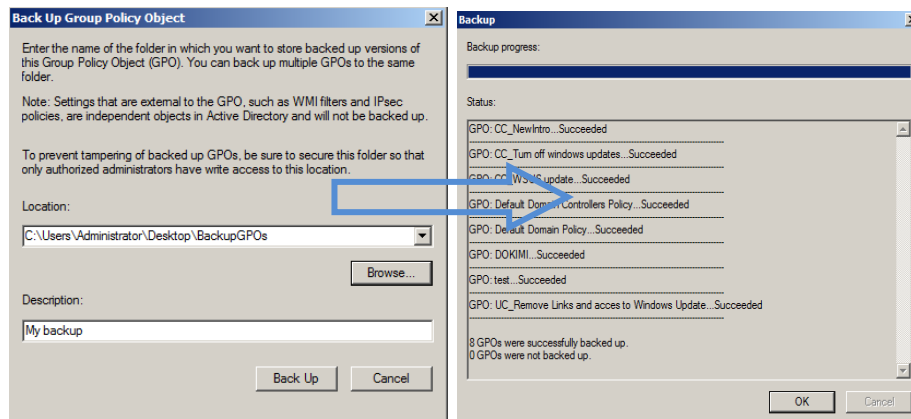
Εικ. 13.26. Backup GPOs.

Κάνουμε δεξί κλικ στο group policy objects και backup all αν θέλουμε όλες τις GPOs ή δεξί κλικ σε συγκεκριμένη GPO (Εικ. 13.27) και Backup, όπου ξεκινά ένας οδηγός

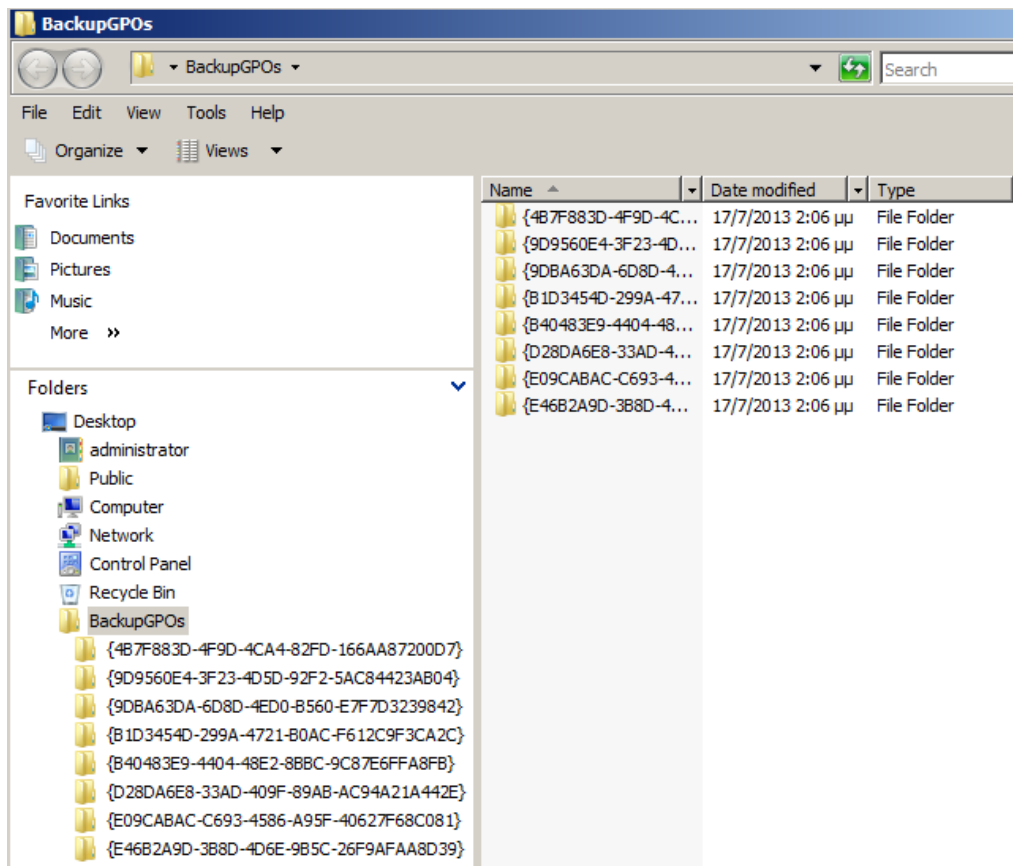


Εικ. 13.27. Individual Backup GPO.

που θα βοηθήσει στην αποθήκευση των GPOs σε συγκεκριμένο φάκελο, ενώ μπορούμε να προσθέσουμε και κάποιες πληροφορίες αναγνώρισης (Εικ. 13.28).



Εικ. 13.28. Οδηγός Backup.



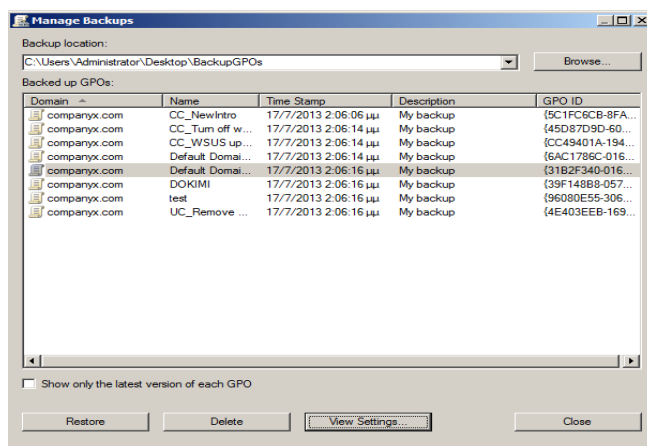
Εικ. 13.29. Φάκελος Backup.

Η Εικ. 13.29 δείχνει τη δομή των αρχείων, όπως έχουν αποθηκευτεί στο φάκελο που επιλέξαμε, από την οποία δεν μπορούμε να διαλέξουμε «εμφανώς» κάποια συγκεκριμένη GPO.

Για να εξασφαλίσουμε ότι θα λειτουργεί το backup, θα πρέπει να μεταφέρουμε το φάκελο «ως έχει».

Η διαδικασία Restore είναι απλή, αν πρόκειται για πολιτικές που θα «επαναφερθούν» στο ίδιο domain.

Δεξί κλικ στο group policy objects (Εικ. 13.26, 13.27) και managed backups ή restore from backup οδηγούμαστε στην Εικ. 13.30, όπου επιλέγουμε και επαναφέρουμε το GPO.

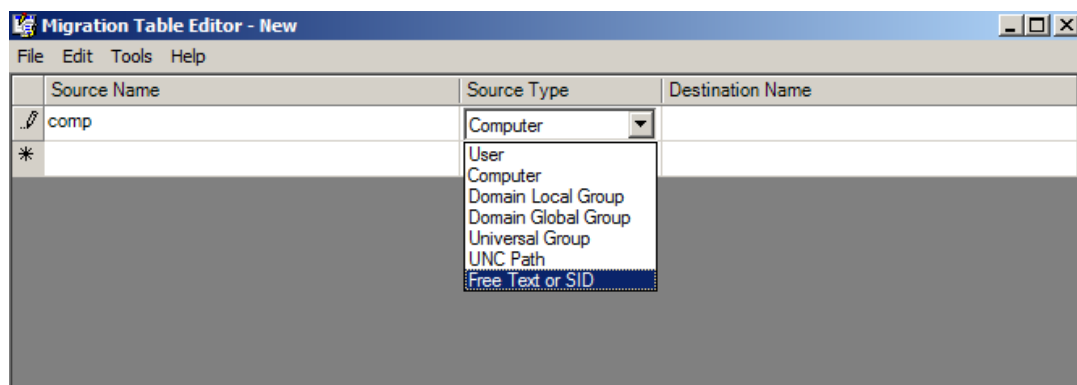


Εικ. 13.30. Restore GPOs.

Επαναφέρεται το GPO και όχι τα link που είχαμε, τα οποία θα πρέπει να επανατοποθετήσουμε, όπου απαιτούνται.

Βλέπουμε και τον ρόλο που παίζει η σωστή «ονοματολογία», διότι για το CC_NewIntro δεν θα χρειαστεί να επιλέξουμε view settings, προκειμένου να δούμε τι κάνει αφού το «όνομα» το δηλώνει.

Αν, όμως, η επαναφορά πρόκειται να γίνει σε άλλα domain, τότε θα πρέπει να επιλέξουμε (Εικ. 13.26) Open migration Table editor, για να ανοίξει η Εικ. 13.31,



Εικ. 13.31. Migration Table editor.

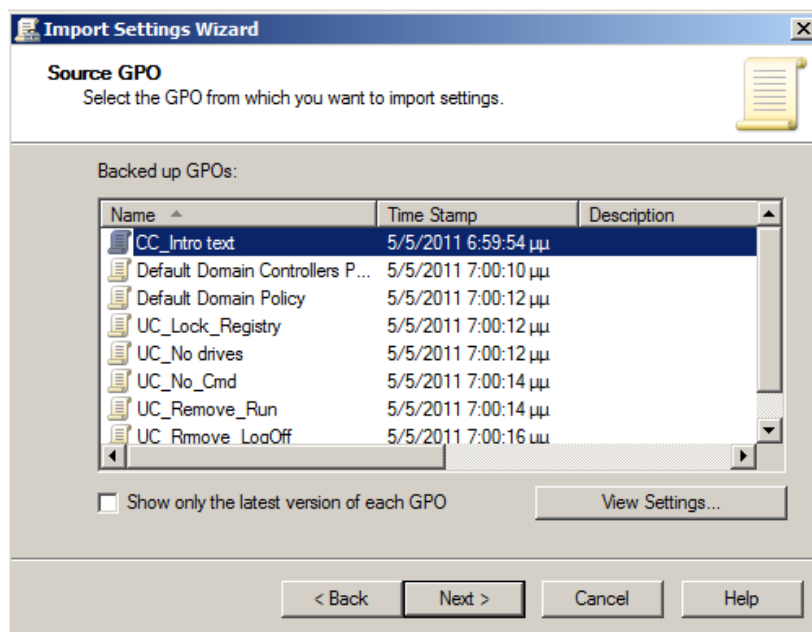
στην οποία θα πρέπει να αντιστοιχίσουμε τα στοιχεία (security principals, UNC paths) του παλιού domain στο νέο domain, να αποθηκεύσουμε το αρχείο (*.migtable) μαζί με το backup και να το χρησιμοποιήσουμε σαν «μεταφραστή» κατά το restore.

Μπορούμε να αποφύγουμε την παραπάνω διαδικασία για επαναφορά GPO σε άλλα domain ακολουθώντας τα παρακάτω βήματα.

Στο Group policy Objects δημιουργούμε μια νέα GPO με το όνομα που γνωρίζουμε

ότι έχουμε δώσει στο Backup. Αν δεν το θυμόμαστε δίνουμε ένα τυχαίο και στο τέλος το μετονομάζουμε.

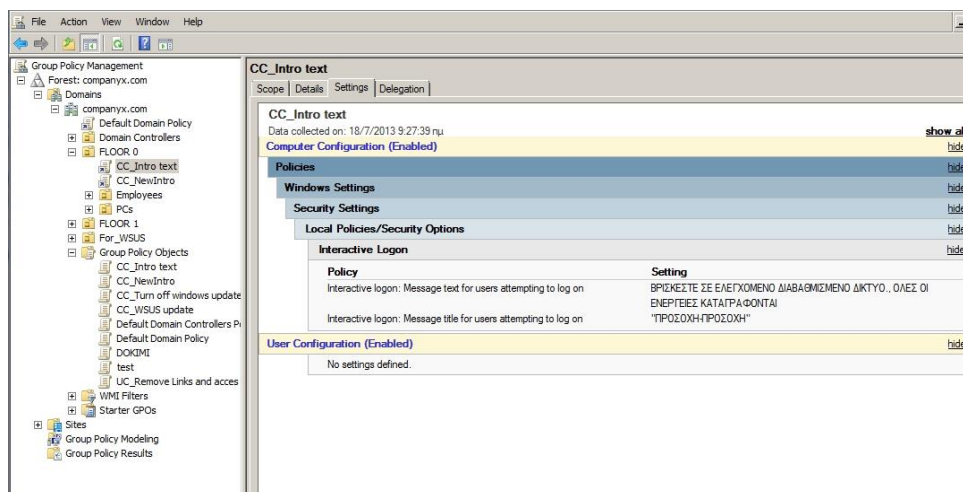
Δεξί κλικ και Import Settings για να ξεκινήσει ο οδηγός εισαγωγής, ο οποίος με



Εικ. 13.32. Εισαγωγή GPO από Backup.

ερωτήσεις, όπως για το αν θέλουμε να πάρουμε backup την υφιστάμενη GPO και πού είναι ο backup φάκελος, οδηγεί στην Εικ. 13.32.

Διαλέγουμε πχ. CC_Intro text και επιλέγοντας view settings, βλέπουμε αναλυτικά τι κάνει η συγκεκριμένη πολιτική Εικ. 13.33.



Εικ. 13.33. CC_Intro text GPO.

Στη συνέχεια στην Εικ. 13.32 επιλέγουμε next και η πολιτική έχει εισαχθεί στο container των πολιτικών, χωρίς να χρειαστεί να τροποποιήσουμε κανένα στοιχείο για να λειτουργήσει στο νέο domain.

13.3.1.9 Group Policy Refresh Rates

Οι πολιτικές ασφαλείας ενώνονται σε OUs και αναμένεται να εφαρμοστούν από τα objects του Domain.

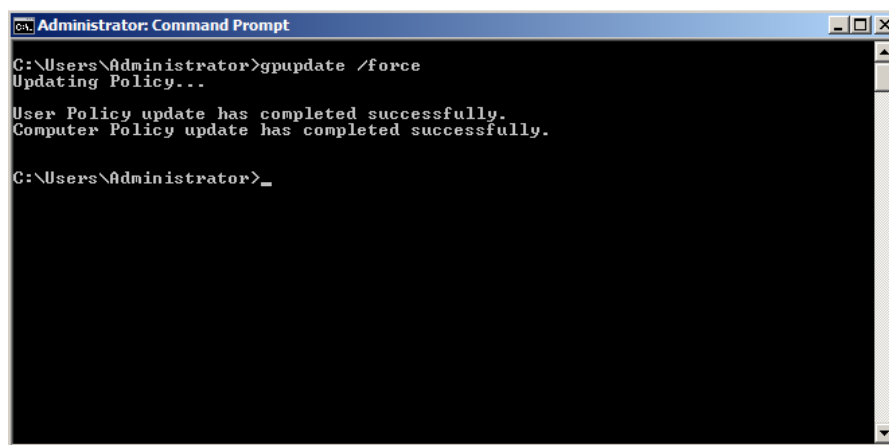
Οι χρόνοι εφαρμογής είναι προκαθορισμένοι, αλλά είναι δυνατόν να αναπροσαρμοσθούν είτε τροποποιώντας τις πολιτικές που τους καθορίζουν ή εφαρμόζοντας νέο GPO.

Τα **Refresh rates** είναι τα παρακάτω:

- Κάθε 5 λεπτά οι domain controllers ενημερώνονται για τις νέες αλλαγές. Ο χρόνος μετρίεται από την προηγούμενη ενημέρωσή και όχι από το πότε ολοκληρώθηκε η δημιουργία μιας νέας πολιτικής.
- Οι clients ενημερώνονται σε κάθε ξεκίνημα και μετά κάθε 90 λεπτά από τον χρόνο που ο Server έκανε την τελευταία ενημέρωση των clients. Στα 90 λεπτά ξεκινά η ενημέρωση και για να μη δημιουργηθεί «συμφόρηση», όλοι οι clients έχουν ενημερωθεί στα επόμενα 30 λεπτά.

Συμπερασματικά, για μία πολιτική που ενώθηκε σε ένα OU τη στιγμή που είχαν περάσει 3 λεπτά από τη στιγμή που ο Server ενημέρωσε τους DCs και στα 76 λεπτά από την ενημέρωση των clients, οι DCs θα ενημερωθούν μετά από 2 λεπτά και οι clients μόλις «εκκινήσουν» ή σε 14 λεπτά.

Για να παρακάμψουμε αυτούς τους χρονικούς περιορισμούς υπάρχει η εντολή **gpupdate /force**, την οποία εκτελούμε σε cmd τόσο στον Server όσο και στους clients, εφόσον υπάρχει ανάλογο δικαίωμα, μόλις ολοκληρώσουμε την ανάθεση μιας πολιτικής. Στην Εικ. 13.34 βλέπουμε την επιτυχημένη εκτέλεση της εντολής.

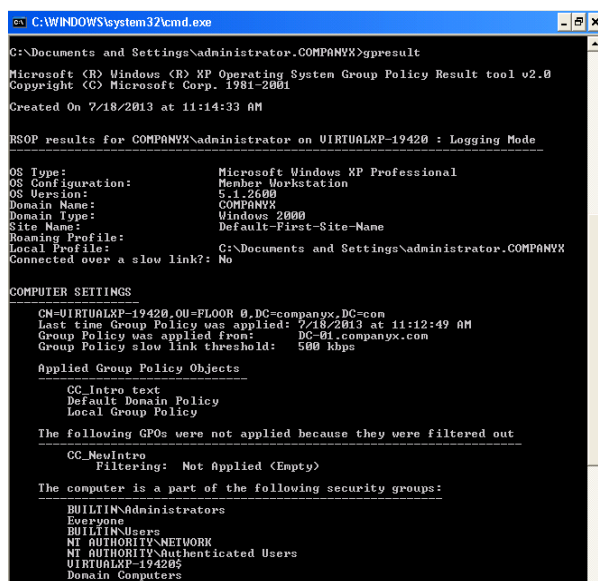


```
Administrator: Command Prompt
C:\Users\Administrator>gpupdate /force
Updating Policy...
User Policy update has completed successfully.
Computer Policy update has completed successfully.
C:\Users\Administrator>
```

Εικ. 13.34. Εντολή gpupdate.

Οι πολιτικές θα εφαρμοστούν στο επόμενο restart, αν αφορούν computer configuration policies και στο log off για user configuration πολιτικές.

Μία επιπλέον χρήσιμη εντολή για troubleshooting client είναι η **gpresult** η οποία αν εκτελεστεί σε cmd στον client με ανάλογα δικαιώματα δείχνει ποιες πολιτικές ήδη εφαρμόζονται (Εικ. 13.35).



Εικ. 13.35. Εντολή gpresult.

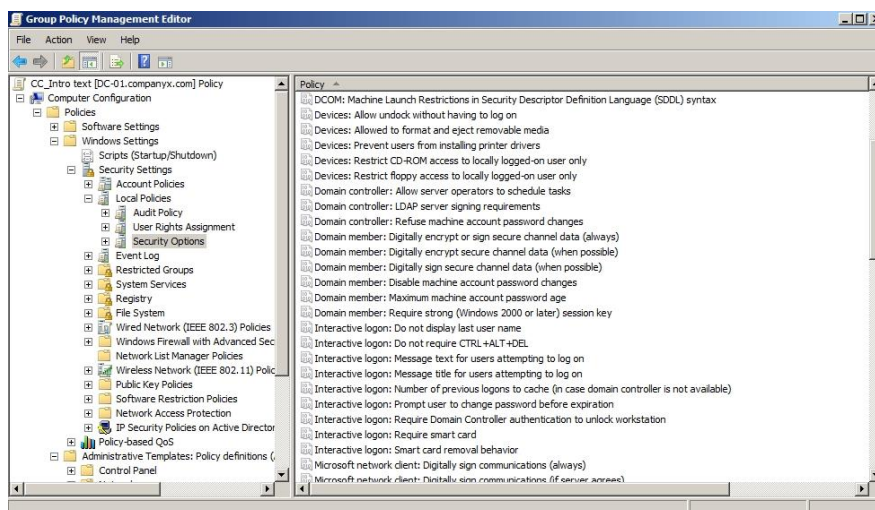
13.3.1.10 Παράδειγμα υλοποίησης GPO

Ακολουθώντας τις διαδικασίες που αναλύθηκαν στις προηγούμενες ενότητες θα δημιουργήσουμε και εφαρμόσουμε την πολιτική CC_Intro text, με την οποία επιθυμούμε οι clients πριν το login να βλέπουν μια pop up φόρμα που να τους ενημερώνει ότι:

ΠΡΟΣΟΧΗ-ΠΡΟΣΟΧΗ (κεφαλίδα φόρμας)

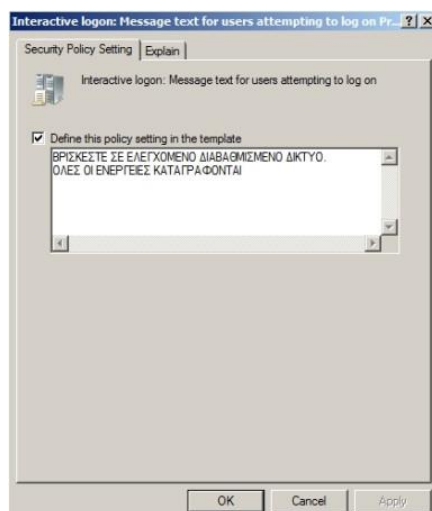
ΒΡΙΣΚΕΣΤΕ ΣΕ ΕΛΕΓΧΟΜΕΝΟ ΔΙΑΒΑΘΜΙΣΜΕΝΟ ΔΙΚΤΥΟ

ΟΛΕΣ ΟΙ ΕΝΕΡΓΕΙΕΣ ΚΑΤΑΓΡΑΦΟΝΤΑΙ



Εικ. 13.36. CC_Intro text GPO.

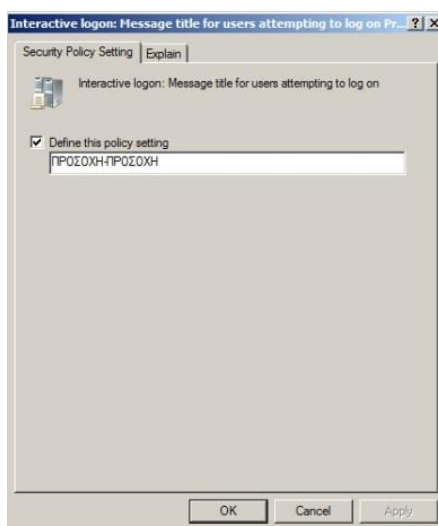
- Ανοίγουμε το group policy management και δεξί κλικ στο OU FLOOR 0 → Create a GPO in this domain and Link it Here.
- Την ονομάζουμε CC_Intro text και Ok.
- Δεξί κλικ στη CC_Intro text, EDIT και παρουσιάζεται η Εικ. 13.36.
- CC\Policies\Windows Settings\Security Options υπάρχουν δύο πολιτικές
 - Interactive logon: Message text for users attempting to logon, στην οποία



Εικ. 13.37. Message text for users attempting to logon.

γραφούμε το κύριο σώμα της πολιτικής (Εικ. 13.37).

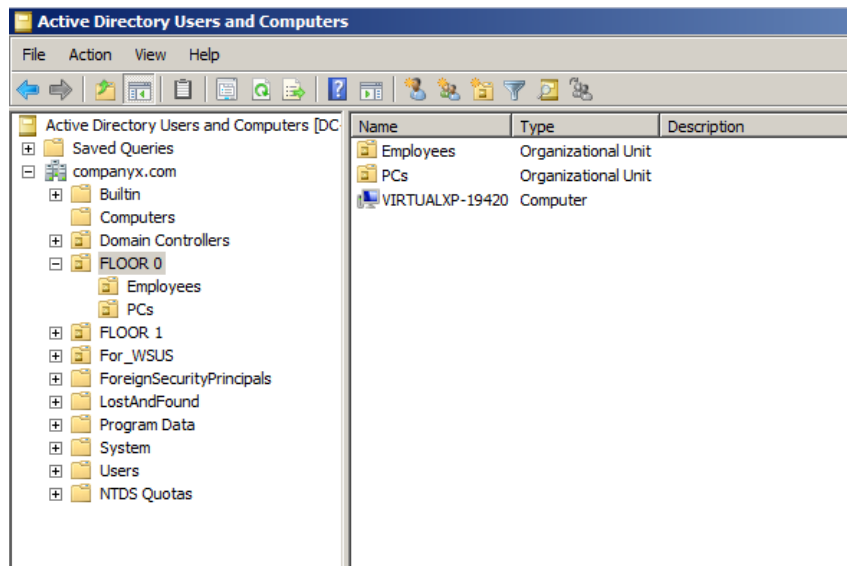
- Interactive logon: Message title for users attempting to logon, στην οποία γραφούμε την κεφαλίδα της πολιτικής (Εικ. 13.38).



Εικ. 13.38. Message title for users attempting to logon.

- Κλείνουμε το GPO και επιστρέφουμε στο group policy management.
- Η πολιτική είναι Computer Configuration και πρέπει να εξασφαλίσουμε ότι στο OU FLOOR 0 βρίσκεται ο υπολογιστής που θα εφαρμόσει την πολιτική.

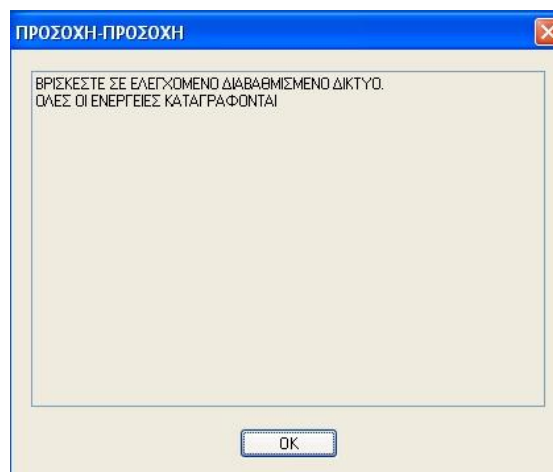
- «Ανοίγουμε» το Active Directory Users and Computers και εξασφαλίζουμε ότι ο υπολογιστής βρίσκεται στο OU FLOOR 0 ή τον μεταφέρουμε εκεί (Εικ. 13.39).



Εικ. 13.39. Έλεγχος υπολογιστή που θα εφαρμόσει το GPO.

Στο παράδειγμα, ο υπολογιστής ονομάζεται VIRTUALXP-19420 και βρίσκεται ήδη στο OU FLOOR 0.

- Start→Run→cmd στο Server και στο παράθυρο εκτελούμε την εντολή **gpupdate /force**, για να ενημερωθούν οι DCs.
- Ξεκινάμε τον client, αν δε λειτουργεί ή αν λειτουργεί, εκτελούμε και εκεί την εντολή (έχοντας ανάλογα δικαιώματα) **gpupdate /force** και κάνουμε restart.
- Πριν από το login ο υπολογιστής θα παρουσιάσει την Εικ. 13.40.



Εικ. 13.40. Πολιτική CC_Intro text.

ΣΕΝΑΡΙΑ GROUP POLICY

14.1 Εισαγωγή

Για την καλύτερη κατανόηση των Group Policies οι παράγραφοι που ακολουθούν περιγράφουν σενάρια βασικών πολιτικών και των αποτελεσμάτων τους στο περιβάλλον εργασίας των Η/Υ και των χρηστών στο Active Directory που διαχειρίζεται ένας administrator.

14.2 Σύνδεση με Remote Desktop στους client Η/Υ

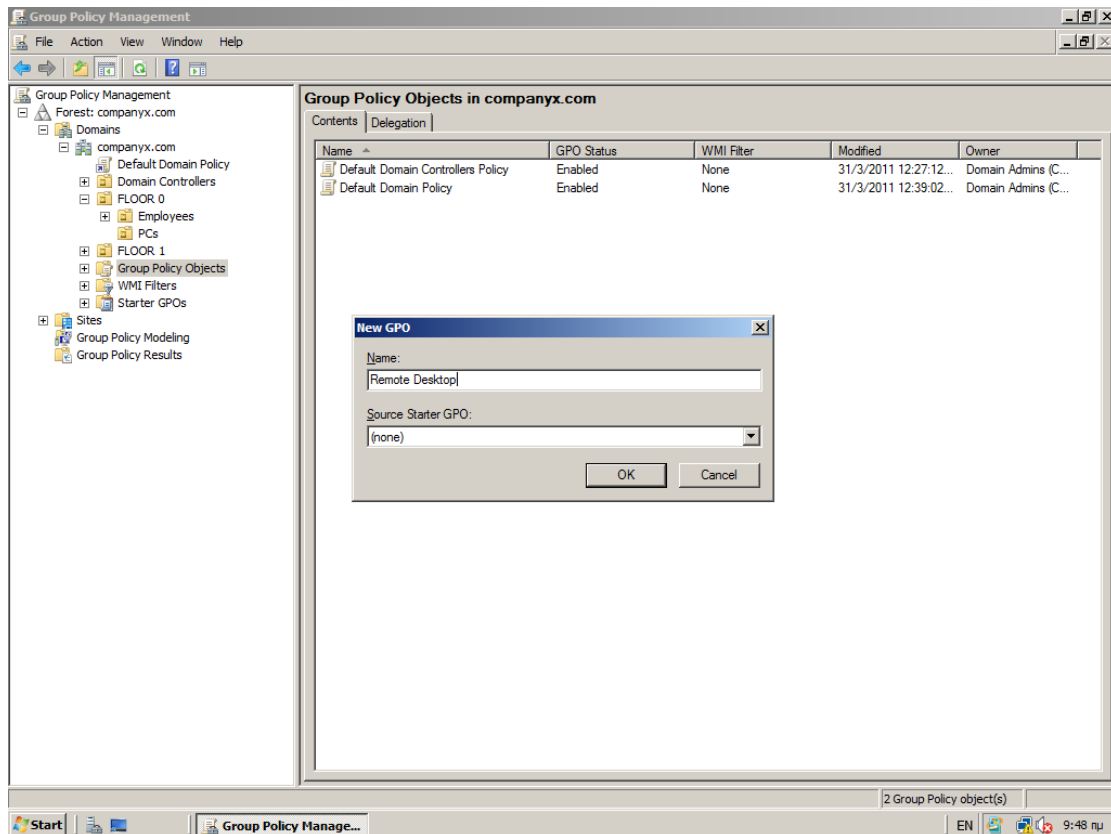
Απαραίτητες προϋποθέσεις για την επιτυχή χρήση του remote desktop ώστε να καταστεί δυνατή η απομακρυσμένη σύνδεση με σκοπό την απομακρυσμένη διαχείριση των Η/Υ του δικτύου ενός διαχειριστή, είναι:

- ☐ Η ενεργοποίηση του χαρακτηριστικού Remote Desktop στον client Η/Υ
- ☐ Η εξαίρεση του Remote Desktop στο Windows Firewall του client Η/Υ ώστε να το παρακάμψει ο διαχειριστής
- ☐ Η ενεργοποίηση σύνδεσης μέσω Terminal Services για τους χρήστες των Η/Υ ώστε να μπορεί ο διαχειριστής να συνδεθεί στο προφίλ του συνδεδεμένου χρήστη και να παράσχει απομακρυσμένη υποστήριξη (remote help desk support).

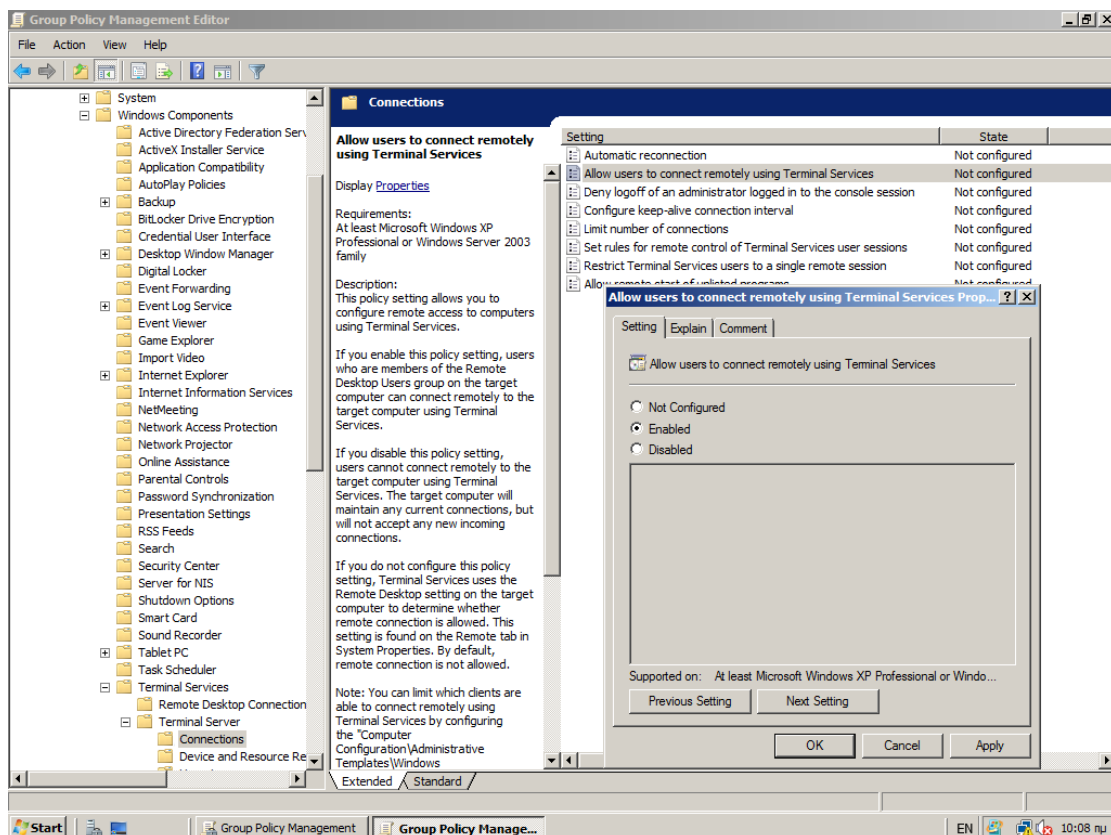
14.2.1 Ενεργοποίηση Remote Desktop στον client Η/Υ

Εκκινούμε την κονσόλα **Group Policy Management** και μεταβαίνουμε στο container **Group Policy Objects**. Μέσα στο container εμφανίζονται όλες οι πολιτικές που ελέγχουν το active directory. Για να δημιουργήσουμε ένα νέο GPO **κάνουμε Δεξί κλικ > New** και στο παράθυρο που εμφανίζεται, **New GPO**, πληκτρολογούμε το όνομα στο πεδίο **Name** και πατάμε **OK** (Εικ. 14.1). Για να επεξεργαστούμε το GPO που μόλις δημιουργήσαμε το επιλέγουμε και στη συνέχεια **κάνουμε Δεξί κλικ > Edit**:

- ☐ Κάτω από το **Computer Configuration** αναπτύσσουμε τα containers **Policies > Administrative Templates > Windows Components > Terminal Services > Terminal Server > Connections** και ανοίγουμε τις ιδιότητες της ρύθμισης **Allow users to connect remotely using Terminal Services** (**Δεξί κλικ > Properties** ή **Διπλό κλικ**) (Εικ. 14.2).
- ☐ Στο παράθυρο ιδιοτήτων που ανοίγει επιλέγουμε **Enabled** και στη συνέχεια **OK**.



Εικ. 14.1. Δημιουργία νέας πολιτικής

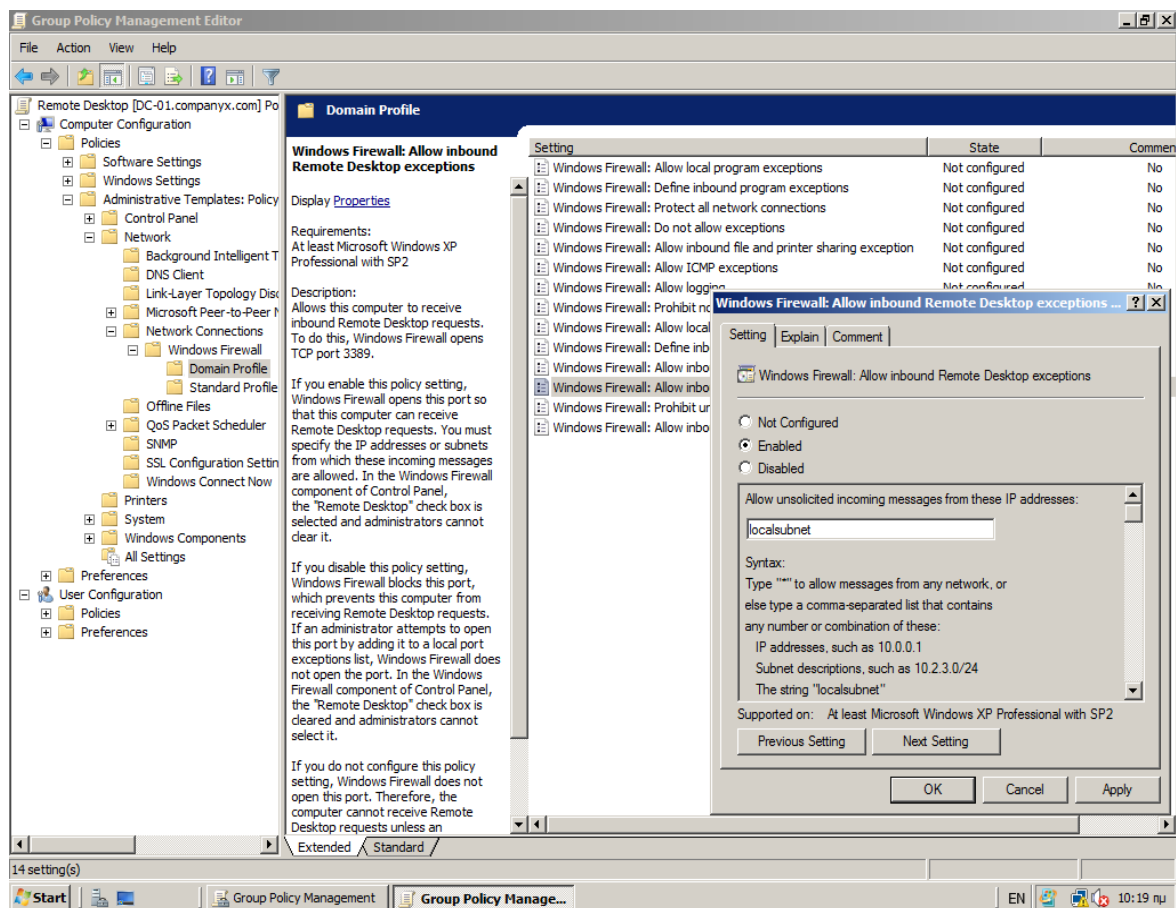


Εικ. 14.2. Επεξεργασία πολιτικής, Ενεργοποίηση Remote Desktop

14.2.2 Εξαιρέση Remote Desktop στο Windows Firewall του client HY

Στην ίδια πολιτική την οποία επεξεργαζόμαστε (παρ. 14.2.1) εκτελούμε τα ακόλουθα βήματα:

- ☐ Κάτω από το **Computer Configuration** αναπτύσσουμε τα containers **Policies** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profile** και ανοίγουμε τις ιδιότητες της ρύθμισης **Windows Firewall: Allow inbound Remote Desktop exeptions** (Δεξί κλικ > **Properties** ή **Διπλό κλικ**) (Εικ. 14.3).
- ☐ Στο παράθυρο ιδιοτήτων που ανοίγει επιλέγουμε **Enabled**
- ☐ Πληκτρολογούμε στο πεδίο **Allow unsolicited incoming messages from these IP addresses:** τον προορισμό από τον οποίο θα επιτρέπουμε τη σύνδεση με Remote Desktop σύμφωνα με τις εμφανιζόμενες οδηγίες σύνταξης.
- ☐ Πατάμε το κουμπί **OK**.

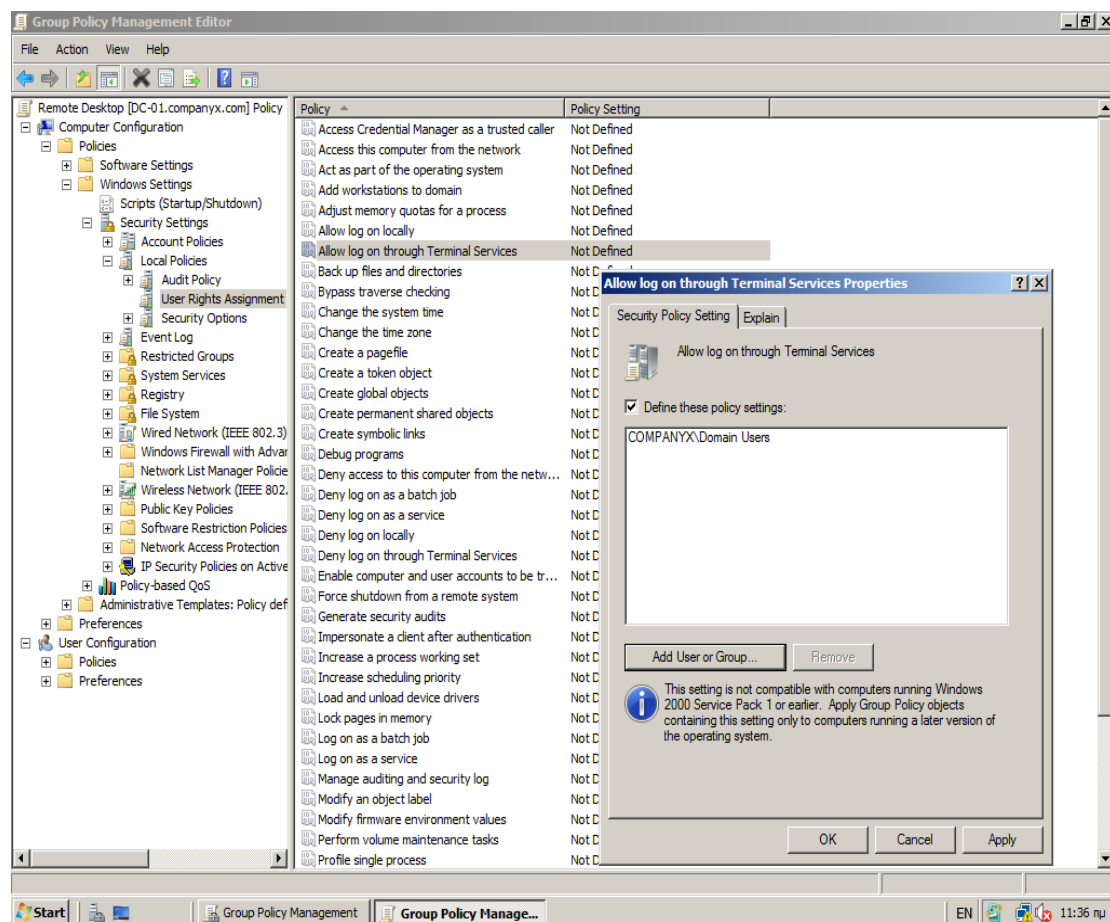


Εικ. 14.3. Ρύθμιση Windows Firewall

14.2.3 Επιλογή απομακρυσμένων χρηστών

Στην ίδια πολιτική την οποία επεξεργαζόμαστε (παρ. 14.2.1 και 14.2.2) εκτελούμε τα ακόλουθα βήματα:

- Κάτω από το **Computer Configuration** αναπτύσσουμε τα containers **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment** και ανοίγουμε τις ιδιότητες της ρύθμισης **Allow log on through Terminal Services** (Δεξί κλικ > **Properties** ή **Διπλό κλικ**) (Εικ. 14.4).
- Στο παράθυρο ιδιοτήτων που ανοίγει επιλέγουμε (check box) **Define these policy settings** και στη συνέχεια πατάμε το κουμπί **Add User or Group...**
- Βρίσκουμε (**Browse**) και επιλέγουμε τους χρήστες ή/και τις ομάδες χρηστών για τους οποίους επιθυμούμε να ενεργοποιήσουμε αυτή τη ρύθμιση και πατάμε **OK** δύο (2) φορές.
- Πατάμε **OK** για να αποθηκεύσουμε και να κλείσουμε το παράθυρο ιδιοτήτων.



Εικ. 14.4. Επιλογή χρηστών για σύνδεση με Terminal Services

Η πολιτική είναι έτοιμη να εφαρμοστεί φτάνει να τη συνδέσουμε στο domain ή σε όποιο(α) ΟΥ επιθυμούμε.

14.3 Ρυθμίσεις Internet Explorer

Η πολιτική που ακολουθεί ρυθμίζει τις βασικές παραμέτρους του Internet Explorer και εμποδίζει τους χρήστες από το να τις αλλάζουν.

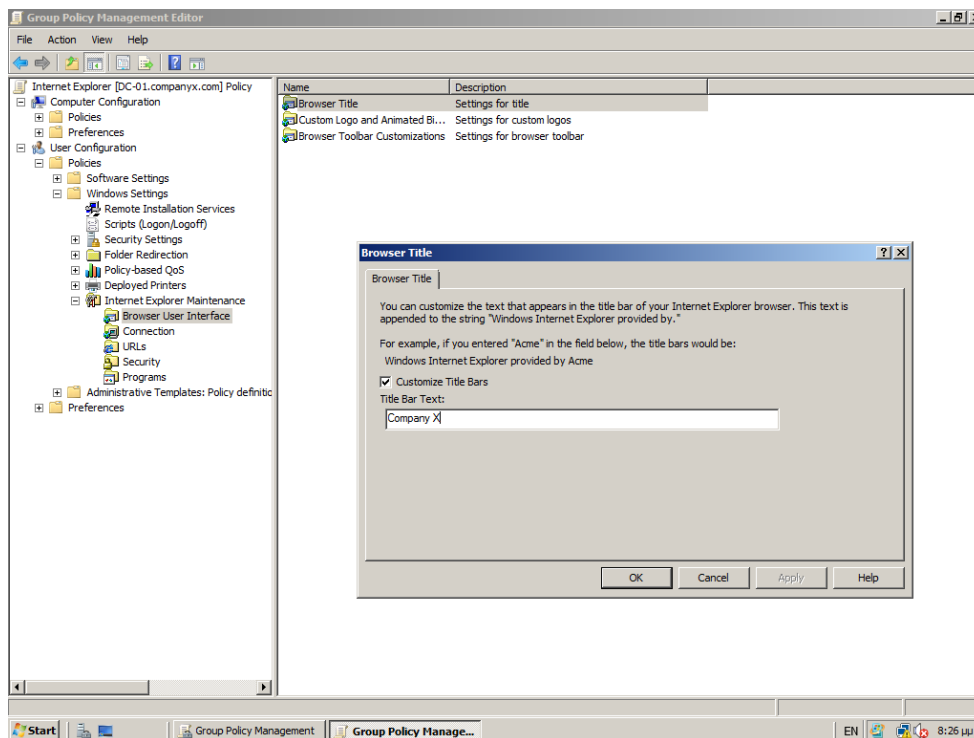
14.3.1 Internet Explorer User Interface

Εκκινούμε την κονσόλα **Group Policy Management** και μεταβαίνουμε στο container **Group Policy Objects**. Μέσα στο container εμφανίζονται όλες οι πολιτικές που ελέγχουν το active directory. Για να δημιουργήσουμε ένα νέο GPO κάνουμε **Δεξί κλικ > New** και στο παράθυρο που εμφανίζεται, **New GPO**, πληκτρολογούμε το όνομα στο πεδίο **Name** και πατάμε **OK**. Για να επεξεργαστούμε το GPO που μόλις δημιουργήσαμε το επιλέγουμε και στη συνέχεια κάνουμε **Δεξί κλικ > Edit**:

□ Κάτω από το **User Configuration** αναπτύσσουμε τα containers **Policies > Windows Settings > Internet Explorer Maintenance > Browser User Interface** και ανοίγουμε τις ιδιότητες της ρύθμισης **Browser Title** (**Δεξί κλικ > Properties** ή **Διπλό κλικ**) (Εικ. 14.5).

□ Στο νέο παράθυρο που ανοίγει τσεκάρουμε την επιλογή **Customize Title Bars** και στο πεδίο **Title Bar Text** πληκτρολογούμε το κείμενο που επιθυμούμε. Για παράδειγμα αν πληκτρολογήσουμε το «Όνομα Εταιρείας / Οργανισμού» η γραμμή τίτλου Internet Explorer, μετά την εφαρμογή της πολιτικής, θα εμφανίζει στους χρήστες «Windows Internet Explorer provided by Όνομα Εταιρείας / Οργανισμού»

□ Πατάμε **OK** για να αποθηκεύσουμε τις αλλαγές και να κλείσουμε το παράθυρο.

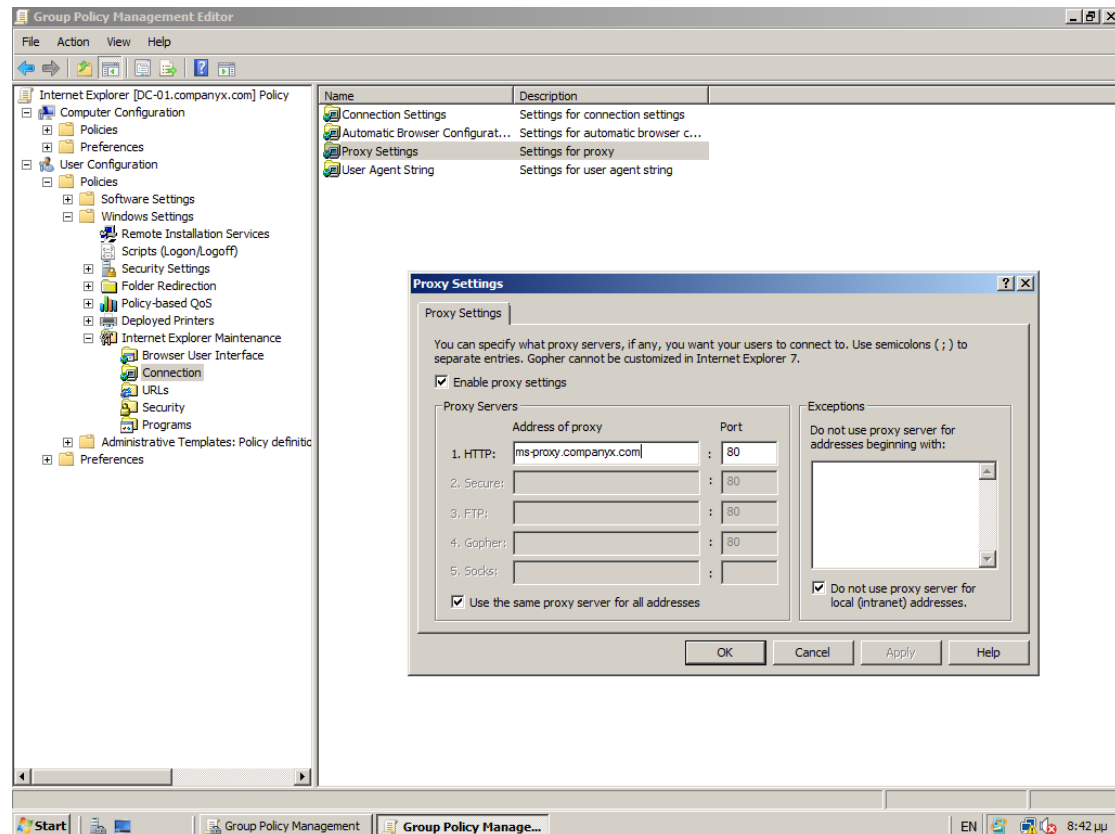


Εικ. 14.5. Browser User Interface

14.3.2 Ρυθμίσεις Proxy

Στην ίδια πολιτική την οποία επεξεργαζόμαστε (παρ. 14.3.1) εκτελούμε τα ακόλουθα βήματα:

- Κάτω από το **User Configuration** αναπτύσσουμε τα containers **Policies > Windows Settings > Internet Explorer Maintenance > Connection** και ανοίγουμε τις ιδιότητες της ρύθμισης **Proxy Settings** (Δεξί κλικ > **Properties** ή Διπλό κλικ) (Εικ. 14.6).
- Στο νέο παράθυρο που ανοίγει τσεκάρουμε την επιλογή **Enable proxy settings**
- Στο αριστερό τμήμα του παραθύρου, **Proxy Servers**, πληκτρολογούμε στο πεδίο **Address of proxy** τη διεύθυνση και στο πεδίο **Port** την πόρτα λειτουργίας για το πρωτόκολλο HTTP και για τα υπόλοιπα (αν υπάρχουν – βγάζοντας την επιλογή **Use the same proxy server for all addresses**)
- Στο δεξιό τμήμα του παραθύρου, **Exceptions**, τσεκάρουμε την επιλογή **Do not use proxy server for local (intranet) addresses**
- Πατάμε **OK** για να αποθηκεύσουμε τις αλλαγές και να κλείσουμε το παράθυρο.

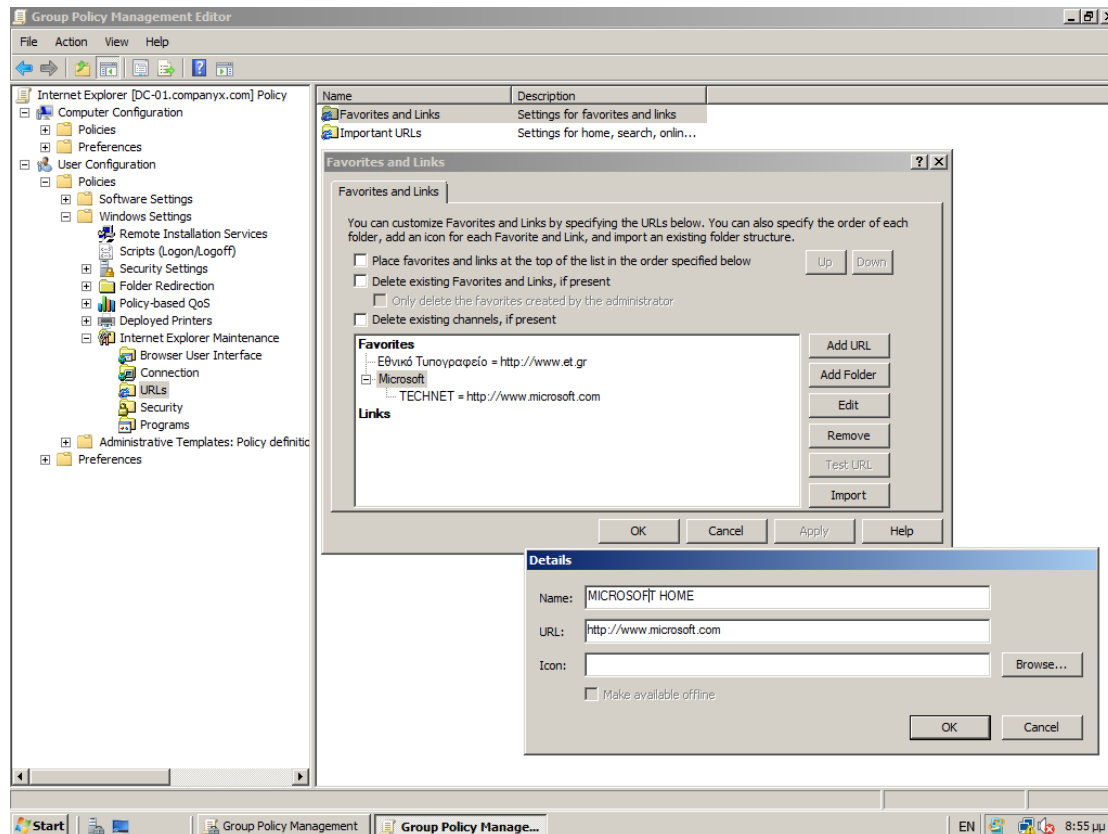


Εικ. 14.6. Proxy Settings

14.3.3 Αρχική Σελίδα, Αγαπημένα και Συνδέσεις

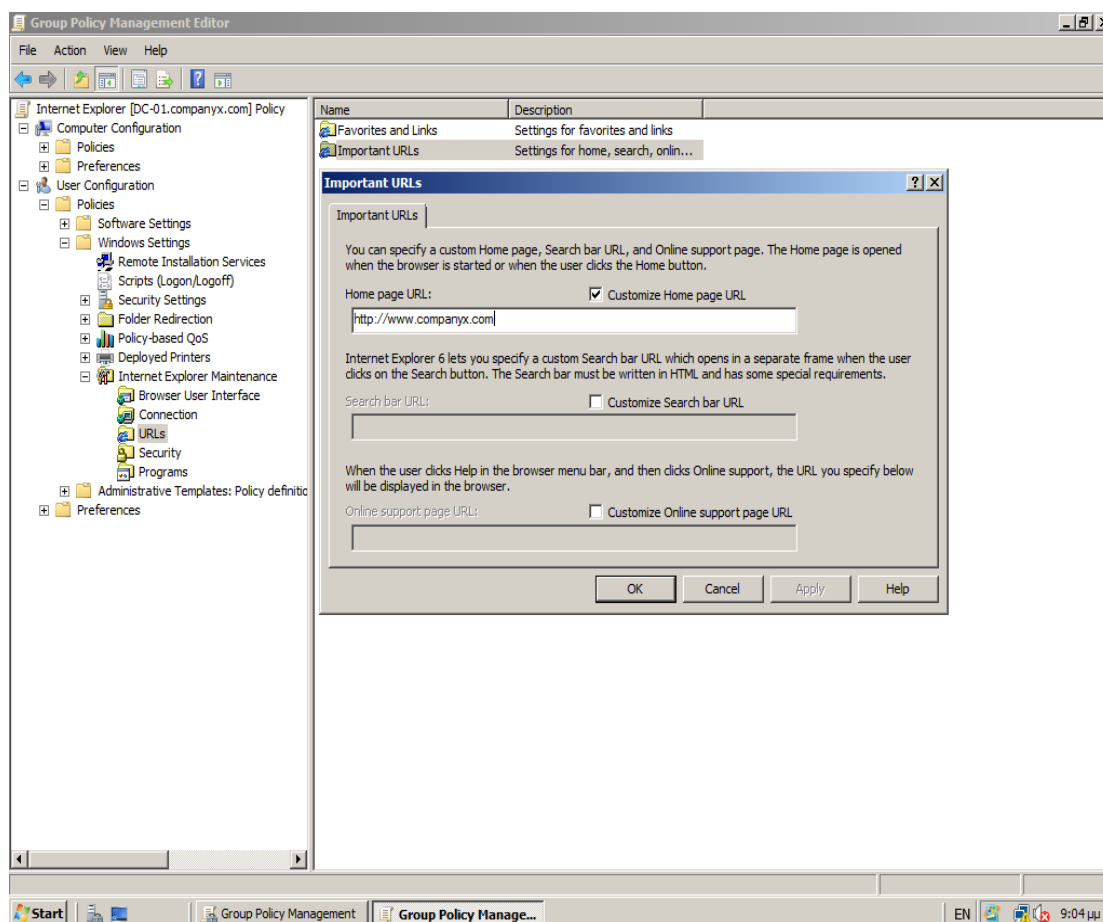
Στην ίδια πολιτική την οποία επεξεργαζόμαστε (παρ. 14.3.1 και 14.3.2) εκτελούμε τα ακόλουθα βήματα:

- Κάτω από το **User Configuration** αναπτύσσουμε τα containers **Policies > Windows Settings > Internet Explorer Maintenance > URLs** και ανοίγουμε τις ιδιότητες της ρύθμισης **Favorites and Links** (Δεξί κλικ > **Properties** ή Διπλό κλικ) (Εικ. 14.7).
- Στο νέο παράθυρο που ανοίγει χρησιμοποιούμε τα κουμπιά **Add URL** και **Add Folder** για να προσθέσουμε διευθύνσεις και φακέλους διευθύνσεων
 - ✓ Στο πεδίο **Name** πληκτρολογούμε το όνομα του αγαπημένου
 - ✓ Στο πεδίο **URL** τη διεύθυνσή του
 - ✓ Στο πεδίο **Icon** επιλέγουμε (**Browse**) εικονίδιο για το αγαπημένο
 - ✓ Πατάμε **OK** για να προσθέσουμε το αγαπημένο
- Με το κουμπί **Edit** μπορούμε να μετονομάσουμε URLs και με το **Remove** να αφαιρέσουμε URLs
- Πατάμε **OK** για να αποθηκεύσουμε τις αλλαγές και να κλείσουμε το παράθυρο.



Εικ. 14.7. Favorites and Links

- Στη συνέχεια ανοίγουμε τις ιδιότητες της ρύθμισης **Important URLs** (Δεξί κλικ > **Properties** ή **Διπλό κλικ**) (Εικ. 14.8)
- Στο νέο παράθυρο που ανοίγει τσεκάρουμε την επιλογή **Customize Home page URL** και στο πεδίο **Home page URL:** πληκτρολογούμε τη διεύθυνση του web site που επιθυμούμε να γίνει αρχική σελίδα στους χρήστες του δικτύου μας.
- (Στο ίδιο παράθυρο μπορούμε να ορίσουμε με τον ίδιο τρόπο τις διευθύνσεις των **Search bar URL** και **Online support page URL**)
- Πατάμε **OK** για να αποθηκεύσουμε τις αλλαγές και να κλείσουμε το παράθυρο.



Εικ. 14.8. Important URLs

14.3.4 Προχωρημένες Ρυθμίσεις Internet Explorer

Στην ίδια πολιτική την οποία επεξεργαζόμαστε (παρ. 14.3.1, 14.3.2 και 14.3.3) εκτελούμε τα ακόλουθα βήματα:

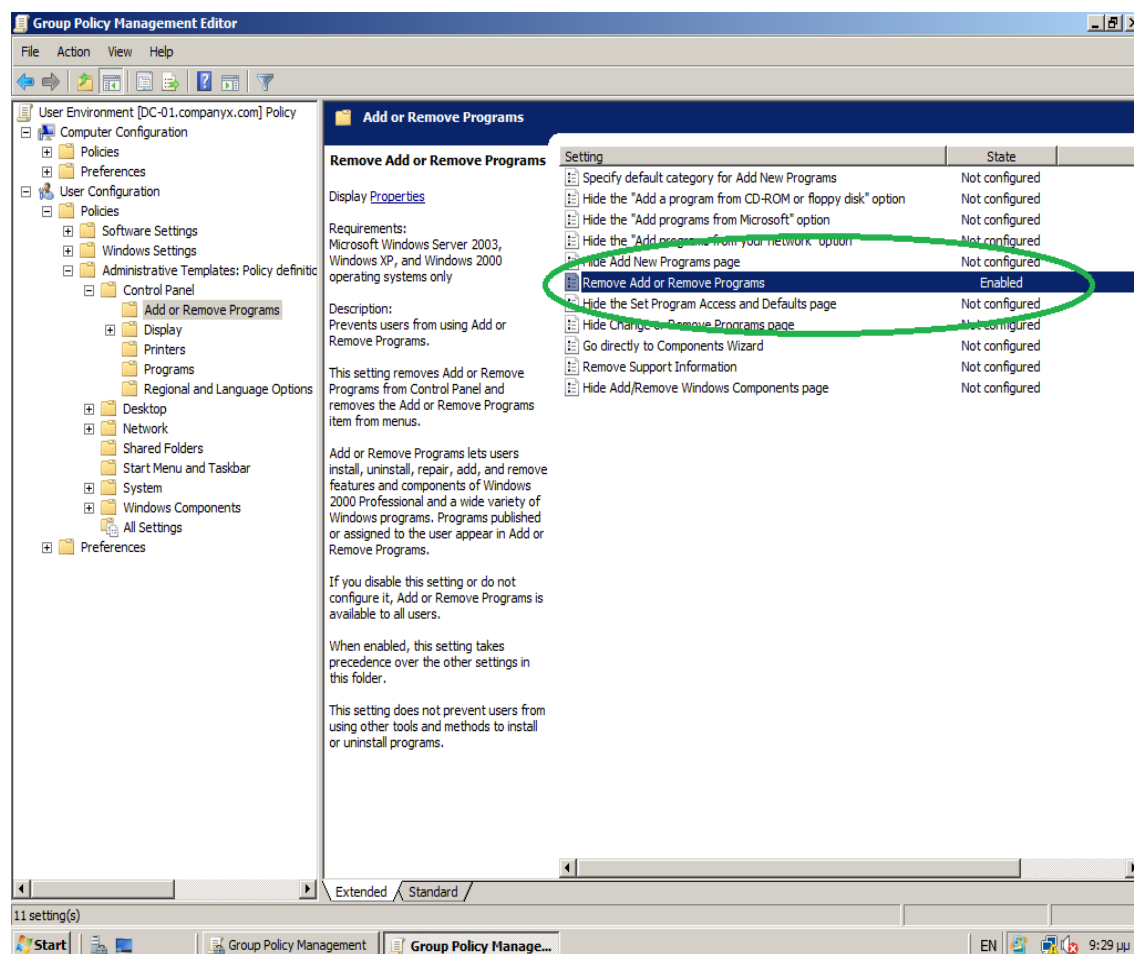
- Κάτω από το **User Configuration** αναπτύσσουμε τα containers **Policies** > **Administrative Templates** > **Windows Components** > **Internet Explorer** όπου μπορούμε να δούμε πληθώρα ρυθμίσεων για τον Internet Explorer

□ Στη συνέχεια κατεβαίνουμε (scroll down) προς τα κάτω και ανοίγουμε τις ιδιότητες της ρύθμισης **Disable changing proxy settings** (Δεξί κλικ > **Properties** ή **Διπλό κλικ**)

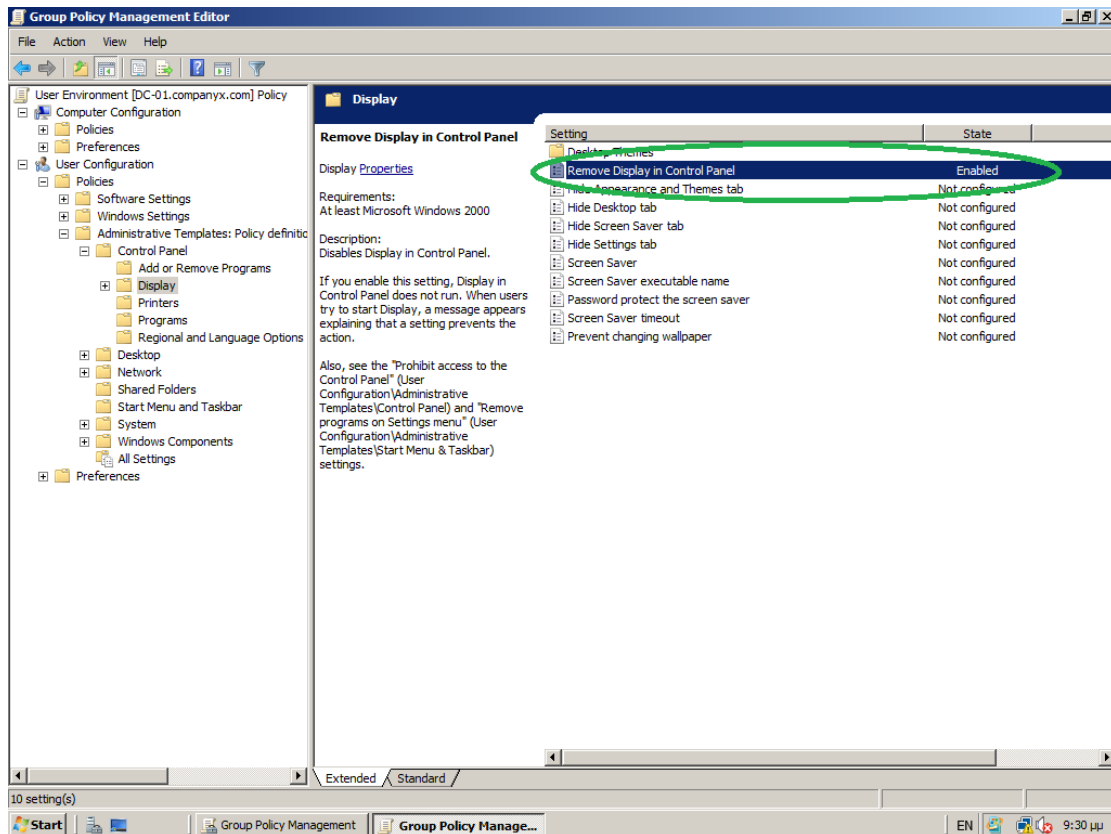
□ Στο παράθυρο ιδιοτήτων που ανοίγει επιλέγουμε **Enabled** και πατάμε **OK**. Μπορούμε να παραμετροποιήσουμε οποιεσδήποτε ρυθμίσεις με σκοπό να δώσουμε συγκεκριμένη λειτουργικότητα και ασφάλεια στους χρήστες του δικτύου μας.

14.4 Περιβάλλον Χρήστη

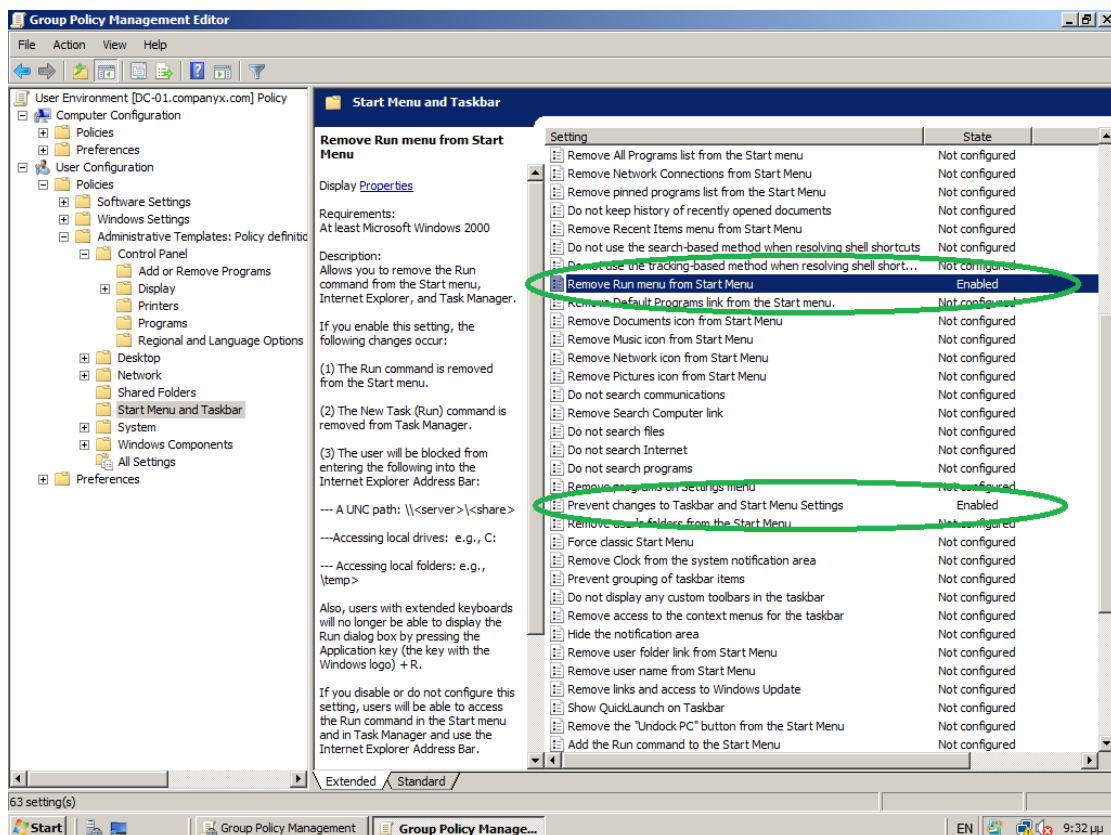
Μπορούμε να περιχαρακώσουμε το περιβάλλον εργασίας των χρηστών επιτρέποντας, απαγορεύοντας και ρυθμίζοντας τα χαρακτηριστικά λειτουργίας των Η/Υ στους οποίους εργάζονται (π.χ. Επιφάνεια Εργασίας, Πίνακας Ελέγχου, Σύστημα, Μενού Εκκίνησης, Γραμμή Εργασιών, Στοιχεία Windows, κ.ο.κ.). Η πολιτική που ακολουθεί (Εικ. 14.9, 14.10, 14.11, 14.12 και 14.13) παρουσιάζει και ρυθμίζει μερικά βασικά χαρακτηριστικά.



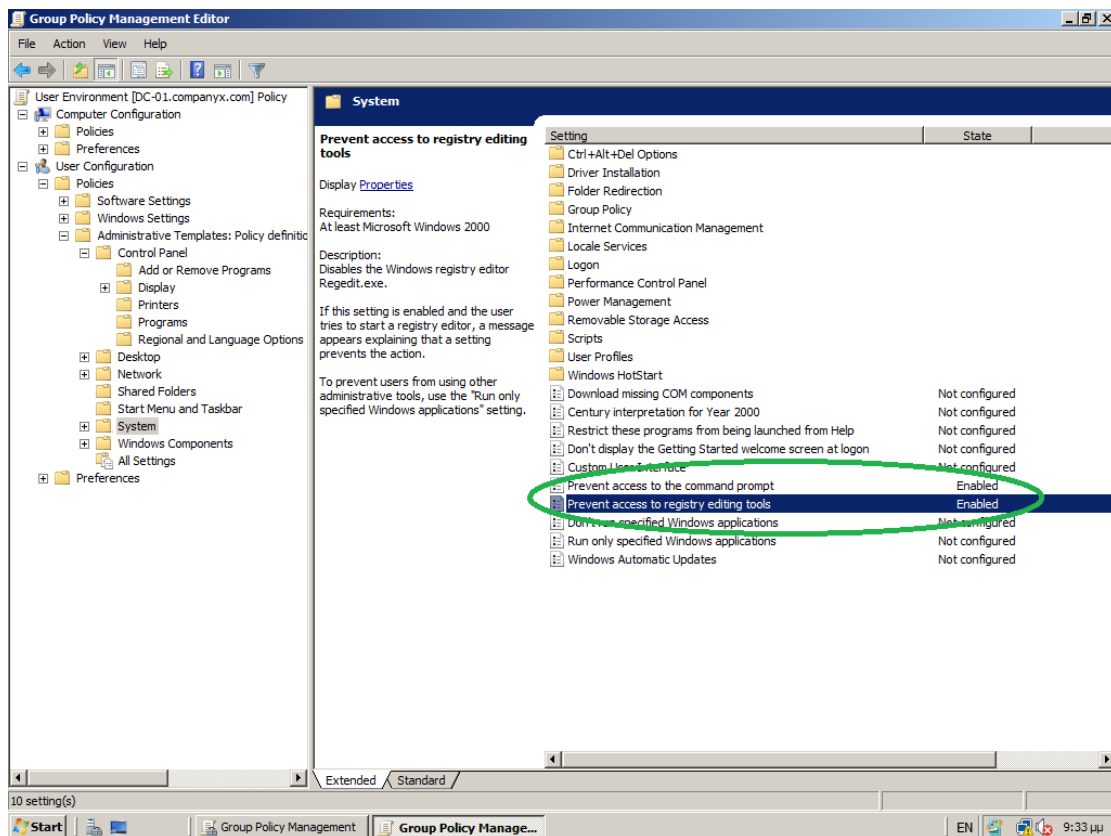
Εικ. 14.9. Add or Remove Programs



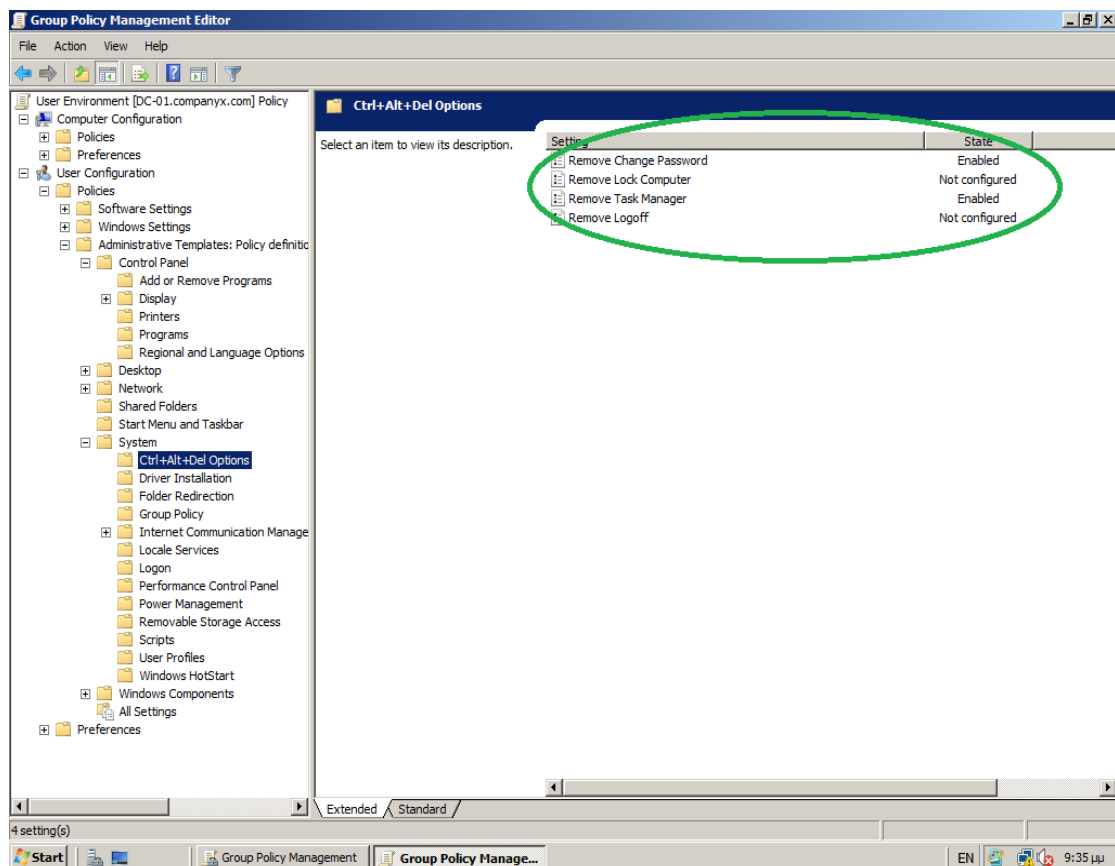
Εικ. 14.10. Display



Εικ. 14.11. Start Menu and Taskbar



Εικ. 14.12. System



Εικ. 14.13. CTRL+ALT+DEL Options

ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΕΓΚΑΤΑΣΤΑΣΗ ΛΟΓΙΣΜΙΚΟΥ

15.1 Εισαγωγή

Μία εργασία με πολύ μεγάλο διαχειριστικό κόστος είναι η εγκατάσταση λογισμικών εφαρμογών στους Η/Υ (client PCs) του εταιρικού δικτύου. Οι προϋποθέσεις και οι ενέργειες που απαιτούνται για την εκτέλεση αυτής της εργασίας αποτελούν πολύπλοκη και χρονοβόρα διαδικασία που πολλαπλασιάζεται με τον αριθμό των Η/Υ στους οποίους εκτελείται, ή πρόκειται να εκτελεστεί, η εγκατάσταση:

- ☐ Απαιτείται η φυσική παρουσία του χρήστη που εκτελεί την εγκατάσταση στον Η/Υ όπου την εκτελεί
- ☐ Ο χρήστης που εκτελεί την εγκατάσταση πρέπει να έχει διαχειριστικά δικαιώματα στον Η/Υ όπου την εκτελεί
- ☐ Πρέπει να έχει μαζί του τα αρχεία εγκατάστασης (media kit)
- ☐ Πρέπει να γνωρίζει και να απαντήσει μια σειρά από ερωτήσεις κατά την εγκατάσταση (οθόνες οδηγού εγκατάστασης), όπως π.χ.:
 - ✓ Ονοματεπώνυμο και όνομα εταιρείας
 - ✓ Εισαγωγή αριθμού (κλειδιού) προϊόντος (product key)
 - ✓ Επιλογή στοιχείων και λεπτομερειών εγκατάστασης, κ.ο.κ.

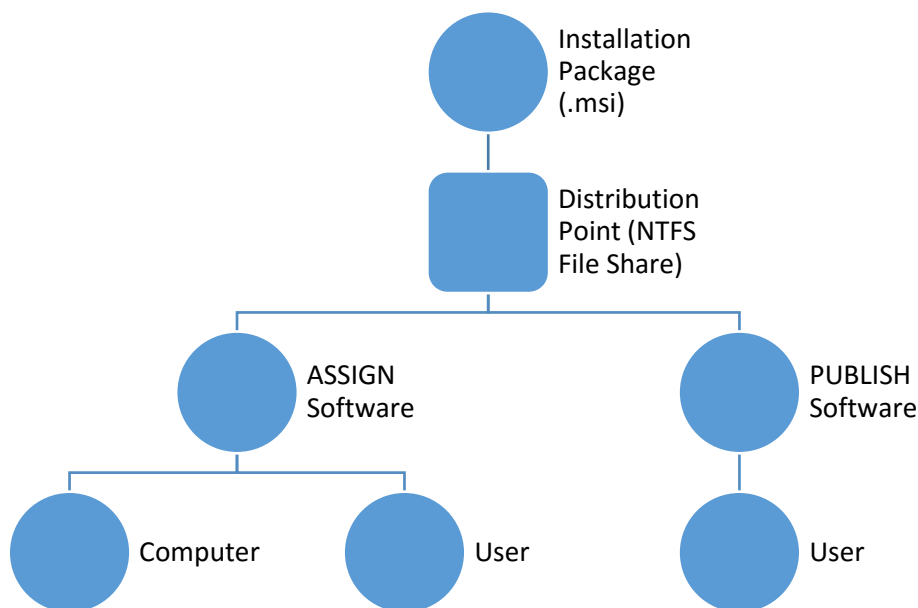
Όταν οι Η/Υ στους οποίους πρέπει να εκτελεστεί η εγκατάσταση λογισμικού βρίσκονται σε απομακρυσμένη τοποθεσία η διαδικασία της εγκατάστασης δυσχεραίνει ακόμα περισσότερο, ιδιαίτερα όταν πρόκειται να εγκατασταθούν περισσότερα του ενός λογισμικά, με διαφορετικές ιδιότητες και ρυθμίσεις.

Ο Windows Server 2008 διαθέτει τις κατάλληλες τεχνολογίες ώστε ο διαχειριστής να είναι σε θέση να αυτοματοποιεί όλες τις παραπάνω διαδικασίες σε πολλαπλούς Η/Υ, χωρίς να απαιτείται η φυσική του παρουσία σε αυτούς (unattended setup), επιλέγοντας ο ίδιος τις ρυθμίσεις που επιθυμεί για τα λογισμικά που εγκαθίστανται στους Η/Υ που συντηρεί. Οι παράγραφοι που ακολουθούν περιγράφουν αναλυτικά το σχεδιασμό και δημιουργία υποδομής, τις ρυθμίσεις και τη χρήση της **Απομακρυσμένης Εγκατάστασης Λογισμικού (Remote Software Installation)**.

15.2 Δημιουργία Υποδομής

Απαραίτητη προϋπόθεση για τη δημιουργία της κατάλληλης υποδομής είναι ύπαρξη υπηρεσιών Active Directory και File Services. Σε ένα File Server δημιουργούμε ένα NTFS File Share (με δικαιώματα Read & Execute, List Folder Contents, Read) – το οποίο ονομάζεται Σημείο Διανομής λογισμικού (**Distribution Point**) - όπου θα

δημιουργήσουμε / αποθέσουμε το Πακέτο Εγκατάστασης λογισμικού (**Installation Package**). Τα πακέτα εγκατάστασης είναι ειδικά διαμορφωμένα αρχεία εγκατάστασης λογισμικού με επέκταση .msi (Windows Installer) τα οποία μπορούμε να προμηθευτούμε από το Software Vendor του λογισμικού που επιθυμούμε να εγκαταστήσουμε απομακρυσμένα (λέξεις κλειδί: software deployment, software distribution, mass installation / distribution, remote installation, multiple clients / computers installation). Περιέχουν τις κατάλληλες πληροφορίες και ρυθμίσεις απομακρυσμένης εγκατάστασης, καθώς και τα αρχεία εγκατάστασης (setup files), είτε εντός του .msi είτε ως συνοδευτικά αρχεία.



Εικ. 15.1. Deployment Methods

Όταν ετοιμαστούν τα επιθυμητά Distribution Points (βλ. παρ. 15.2.1.1 και 15.2.1.2) τότε δημιουργούνται οι κατάλληλες πολιτικές διανομής / εγκατάστασης λογισμικού (Group Policies) ανάλογα με τις απαιτήσεις και τις ανάγκες. Υπάρχουν δύο τρόποι εγκατάστασης λογισμικού (Εικ. 15.1) με Group Policy (**Deployment Method**):

□ Μέθοδος **ASSIGN**

✓ **Σε Η/Υ:** Με τη μέθοδο αυτή ο διαχειριστής εκχωρεί στον υπολογιστή την εγκατάσταση και χρήση λογισμικού, ανεξάρτητα από τον χρήστη που το χρησιμοποιεί και χωρίς παρέμβασή του. Η εγκατάσταση λαμβάνει χώρα κατά το **startup** του Η/Υ (πριν από την προτροπή CTRL+ALT+DEL)

✓ **Σε Χρήστη:** Με τη μέθοδο αυτή ο διαχειριστής εκχωρεί στο χρήστη την εγκατάσταση και χρήση λογισμικού. Ο χρήστης, αμέσως μετά το **logon**, βλέπει τα shortcuts (Start Menu, Επιφάνεια Εργασίας) του εκχωρημένου από το διαχειριστή

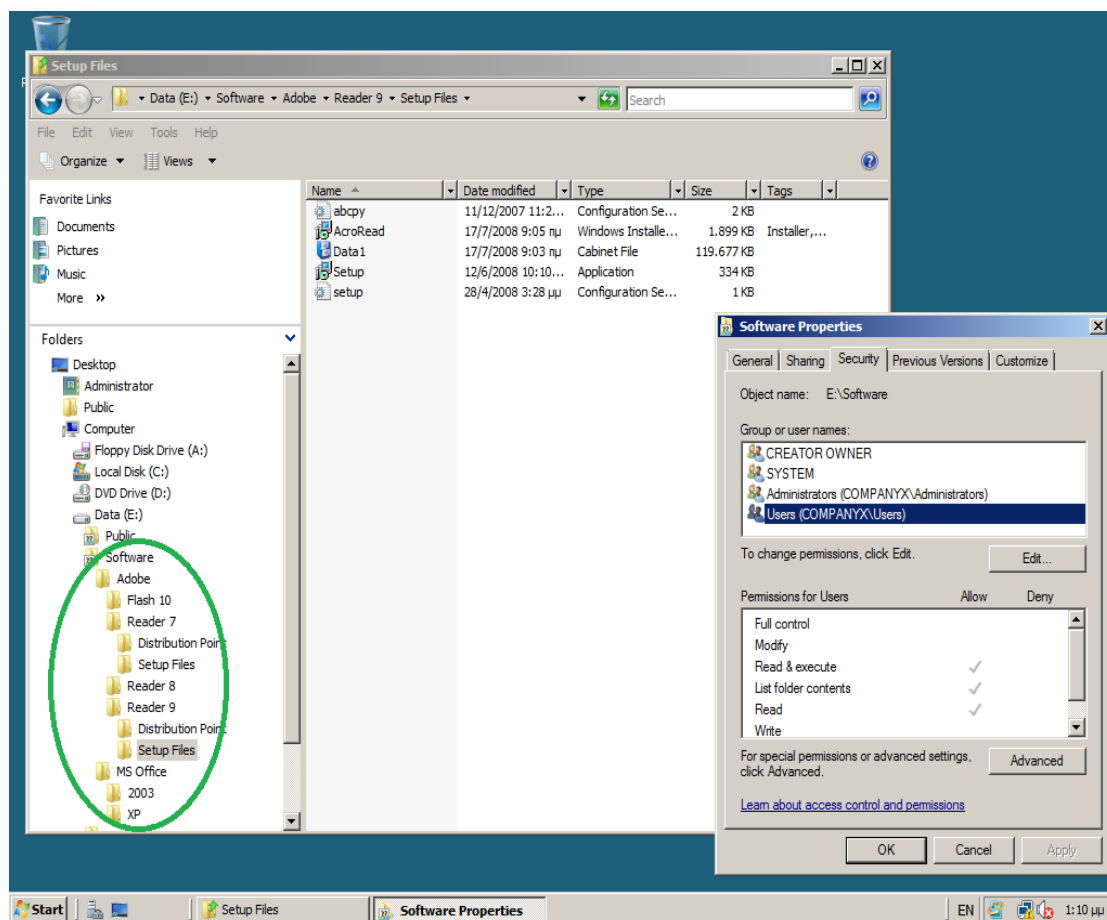
λογισμικού. Την πρώτη φορά που θα εκτελέσει το λογισμικό (είτε από τα shortcuts, π.χ. MS Excel, είτε ανοίγοντας αρχείο συσχετισμένο με το συγκεκριμένο λογισμικό, π.χ. βιβλίο εργασίας του MS Excel) τότε λαμβάνει χώρα η εγκατάστασή του χωρίς δυνατότητα παρέμβασης από το χρήστη.

□ Μέθοδος **PUBLISH**

✓ **Σε χρήστη:** Με τη μέθοδο αυτή ο διαχειριστής δημοσιεύει στο δίκτυό του (Active Directory) τα διαθέσιμα λογισμικά προς εγκατάσταση κατά απαίτηση (on demand), από τους ίδιους τους χρήστες (Πίνακας Ελέγχου > Προσθαφαίρεση Προγραμμάτων) χωρίς να απαιτείται να έχουν οι ίδιοι διαχειριστικό δικαίωμα στον Η/Υ τους.

15.2.1 Πακέτα Εγκατάστασης

Στο Windows Server 2008 δημιουργούμε ένα file share με το όνομα Software και μέσα του δημιουργούμε τόσα distribution points όσα και τα λογισμικά που επιθυμούμε να εγκαταστήσουμε απομακρυσμένα (Εικ. 15.2).



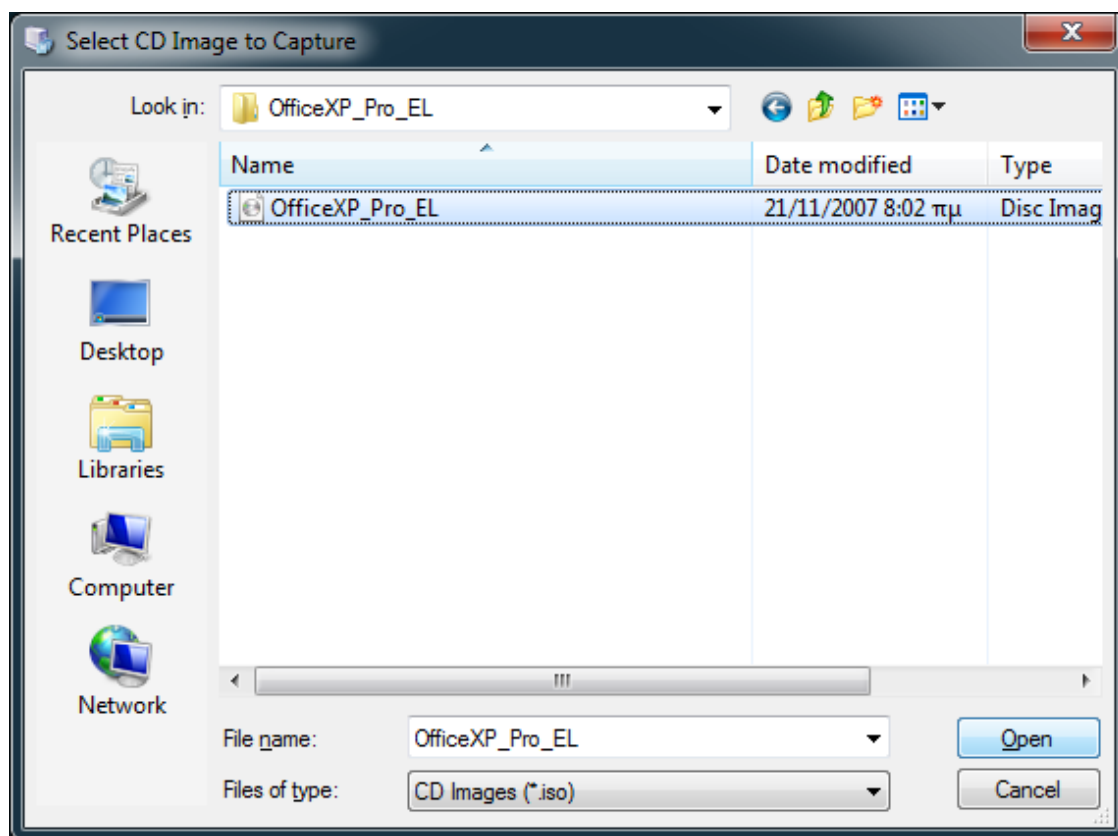
Εικ. 15.2. Distribution Points

Στα σενάρια που ακολουθούν θα δημιουργήσουμε installation packages για τα λογισμικά Adobe Reader, Adobe Flash Player και MS Office. Για τα προϊόντα Adobe

έχουμε ήδη κατεβάσει από το web site της εταιρείας τα αναγκαία για τη διαδικασία αρχεία .msi τα οποία όμως εν είναι ακόμα έτοιμα για διανομή (είναι αποθηκευμένα σε κάθε φάκελο με όνομα **Setup Files** ανά είδος λογισμικού). Απαιτείται μια συγκεκριμένη διαδικασία επεξεργασίας (βλ. παρ. 15.2.1.2) ώστε να δημιουργήσουμε το κατάλληλο installation package και να το αποθέσουμε στο φάκελο Distribution Point ανά είδος λογισμικού. Για το Microsoft Office η διαδικασία είναι απλούστερη και το μόνο που χρειαζόμαστε για να δημιουργήσουμε τα κατάλληλα installation packages είναι το μέσο εγκατάστασης (CD, DVD) του κατασκευαστή.

15.2.1.1 MS Office Installation Packages

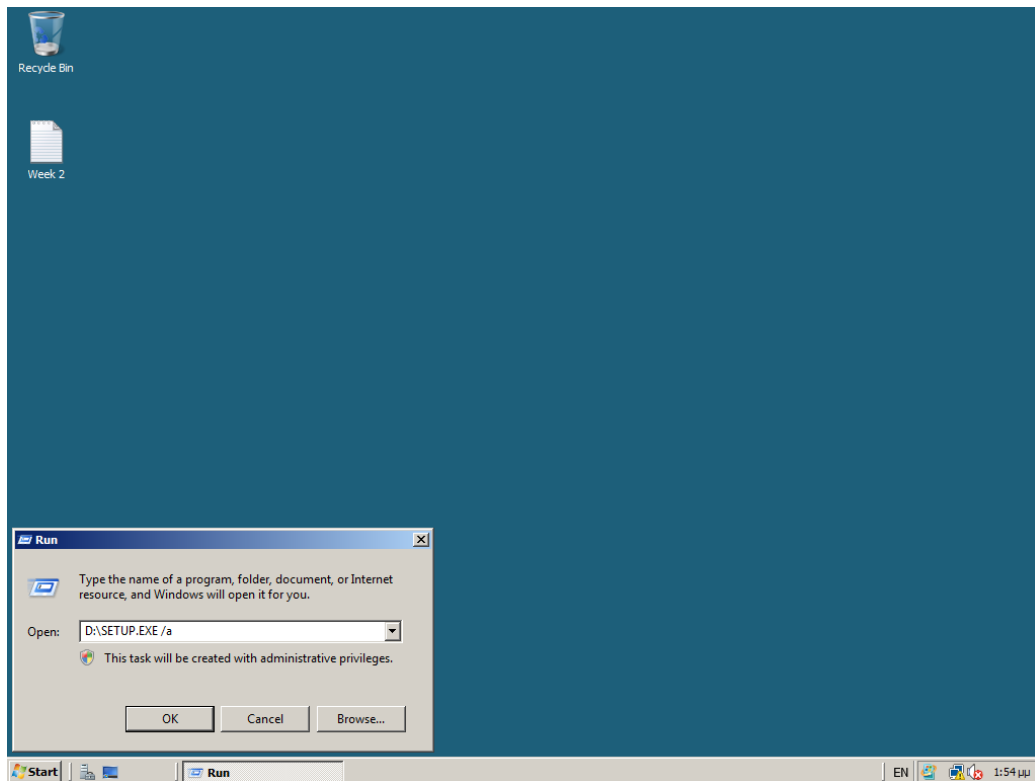
«Φορτώνουμε» στο vm με το Windows Server 2008 το CD του MS Office XP χρησιμοποιώντας το .ISO αρχείο που βρίσκεται στο DVD2 του εργαστηρίου (**OfficeXP_Pro_EL.ISO**, Εικ. 15.3)



Εικ. 15.3 - OfficeXP_Pro_EL.ISO

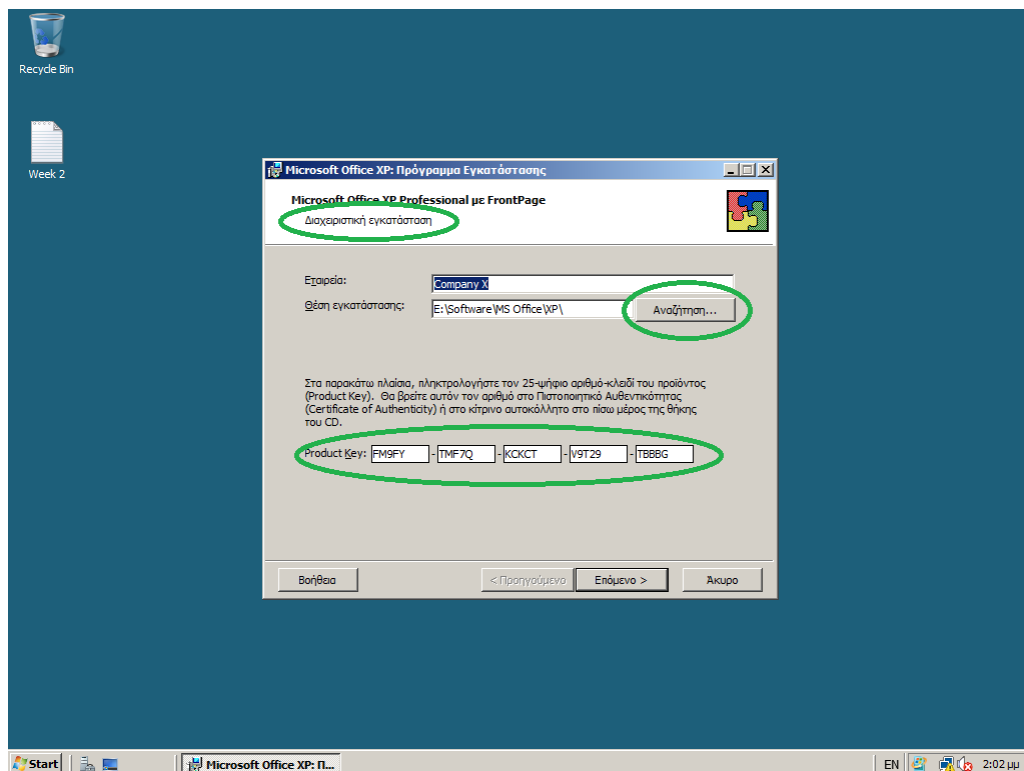
Κλείνουμε το παράθυρο διαλόγου **Autoplay**. Στη συνέχεια εκτελούμε από το παράθυρο εκτέλεσης, **Start > Run**, την εφαρμογή εγκατάστασης από το CD του MS Office XP (**Browse**) χρησιμοποιώντας την ακόλουθη σύνταξη (Εικ. 15.4):

D:\SETUP.EXE /a και **OK**



Εικ. 15.4. Διαχειριστική Εγκατάσταση MS Office

Εμφανίζεται το παράθυρο διαλόγου της διαχειριστικής εγκατάστασης του MS Office XP (Εικ. 15.5) με την οποία θα δημιουργήσουμε το κατάλληλο installation package (.msi) στο distribution point που θα του υποδείξουμε με τον οδηγό εγκατάστασης.



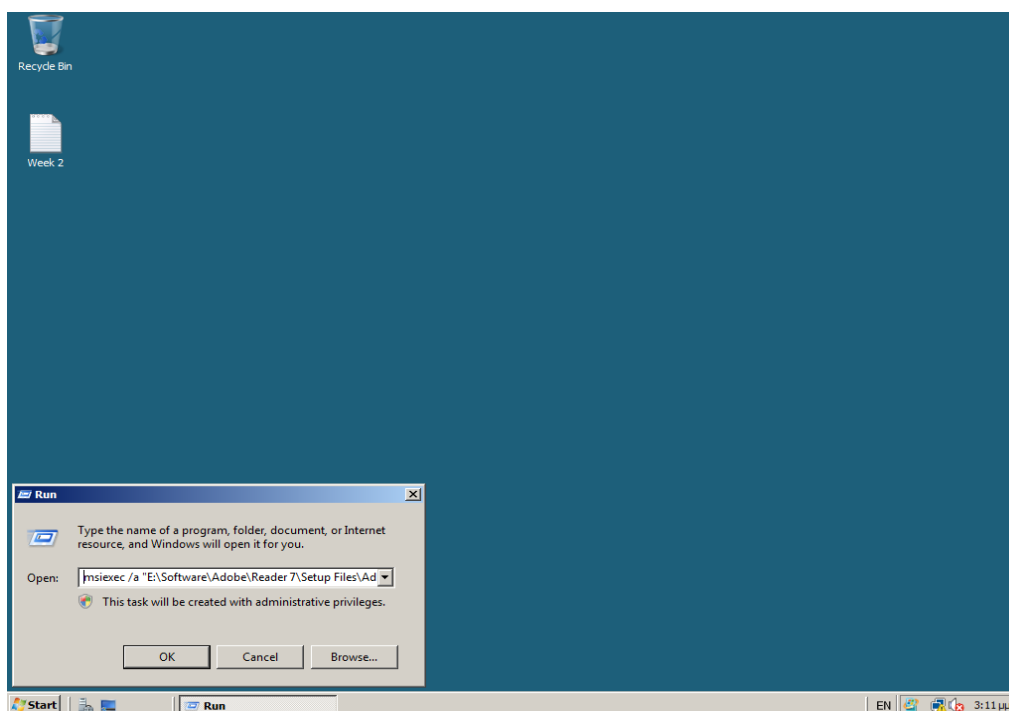
Εικ. 15.5. Παράμετροι Διαχειριστικής Εγκατάστασης MS Office

Πληκτρολογούμε το **Όνομα Εταιρείας**, π.χ. Company X, εισάγουμε τη διαδρομή της θέσης όπου θα δημιουργηθεί το installation package είτε πληκτρολογώντας την στο πεδίο **Θέση Εγκατάστασης**, είτε με το κουμπί **Αναζήτηση**. Στη συνέχεια πληκτρολογούμε το **Product Key** για το προϊόν που εγκαθιστούμε στο αντίστοιχο πεδίο και πατάμε **Επόμενο**. Επιλέγουμε (τσεκάρουμε) την **αποδοχή όρων άδειας χρήσης (EULA)** και πατάμε το κουμπί **Εγκατάσταση**. Όταν τελειώσει η διαδικασία εγκατάστασης (απαιτεί μερικά λεπτά) κάνουμε κλικ στο **OK**.

Αν επισκεφτούμε τώρα το distribution point του MS Office XP θα δούμε το installation package (**PROPLUS.msi**) που δημιουργήθηκε μαζί με τα παρελκόμενα, απαιτούμενα αρχεία εγκατάστασης. Για να δημιουργήσουμε το αντίστοιχο msi για το MS Office 2003, φορτώνουμε το CD του χρησιμοποιώντας το **Office2003_Pro_EL.iso** και ακολουθούμε ξανά τη διαδικασία που περιγράφεται παραπάνω.

15.2.1.2 Adobe Installation Packages

Η διαδικασία δημιουργίας του κατάλληλου για διανομή λογισμικού installation package από το .msi αρχείο διανομής που έχουμε προμηθευτεί από το Software Vendor (π.χ. Adobe) απαιτεί τη χρήση του προγράμματος **msiexec.exe** που βρίσκεται εγκατεστημένο στο λειτουργικό σύστημα Windows Server 2008



Εικ. 15.6. Adobe Reader 7 Installation Package

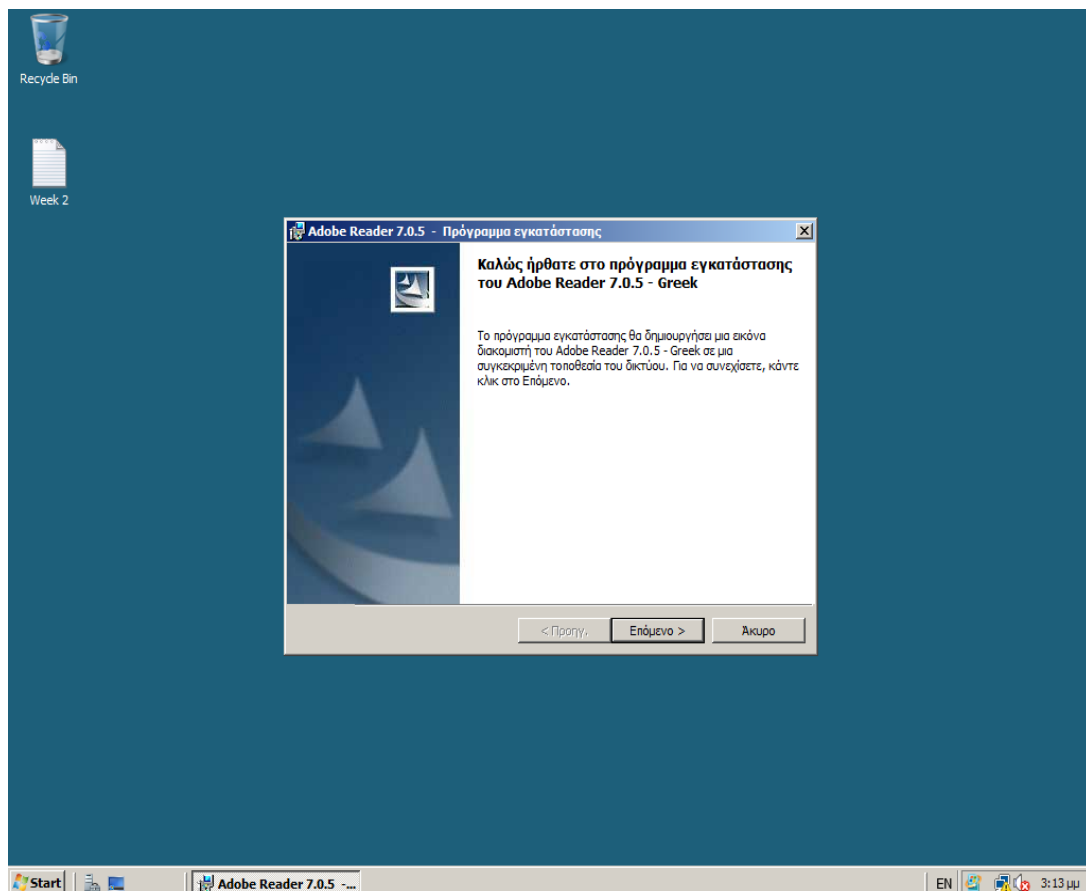
. Ο τρόπος χρήσης / σύνταξης για την εκκίνηση της παραπάνω διαδικασίας είναι:

Start > Run

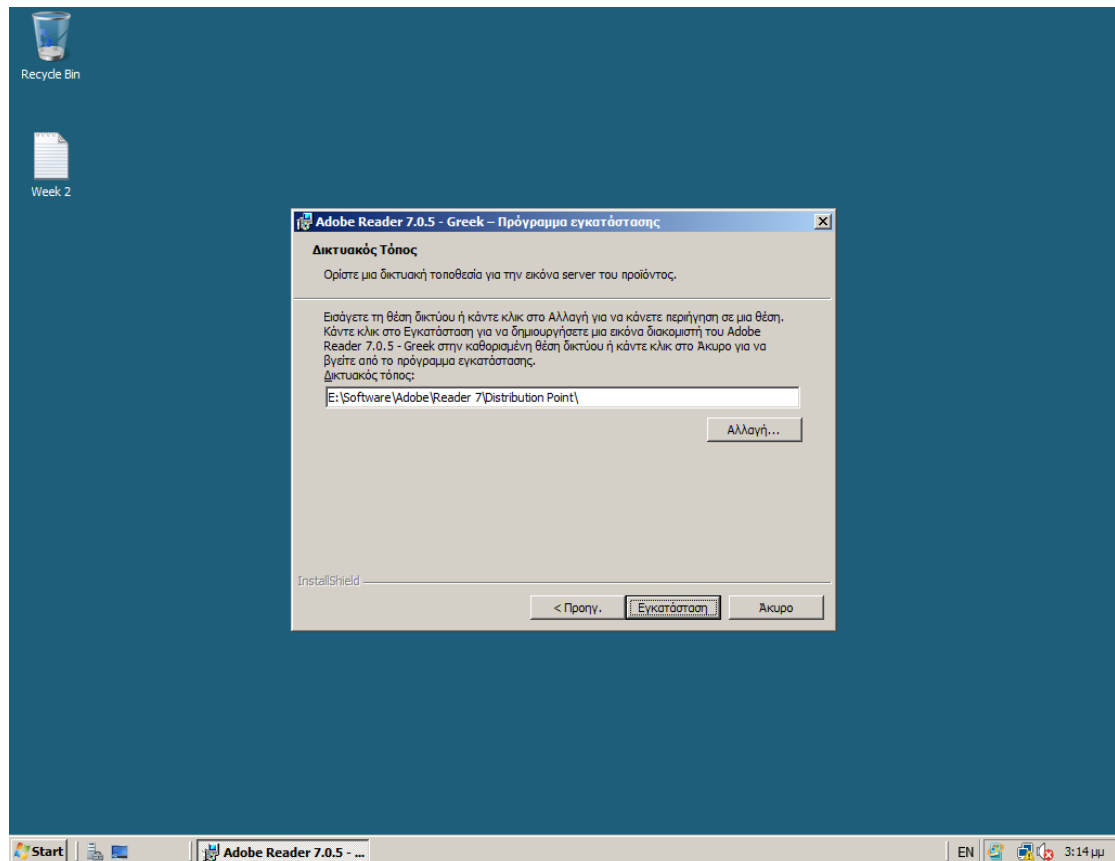
msiexec /a "πλήρης διαδρομή\όνομα αρχείου.msi"

Στην περίπτωση δημιουργίας installation package για το Adobe Reader 7 στο server του εργαστηρίου ακολουθούμε τα παρακάτω βήματα:

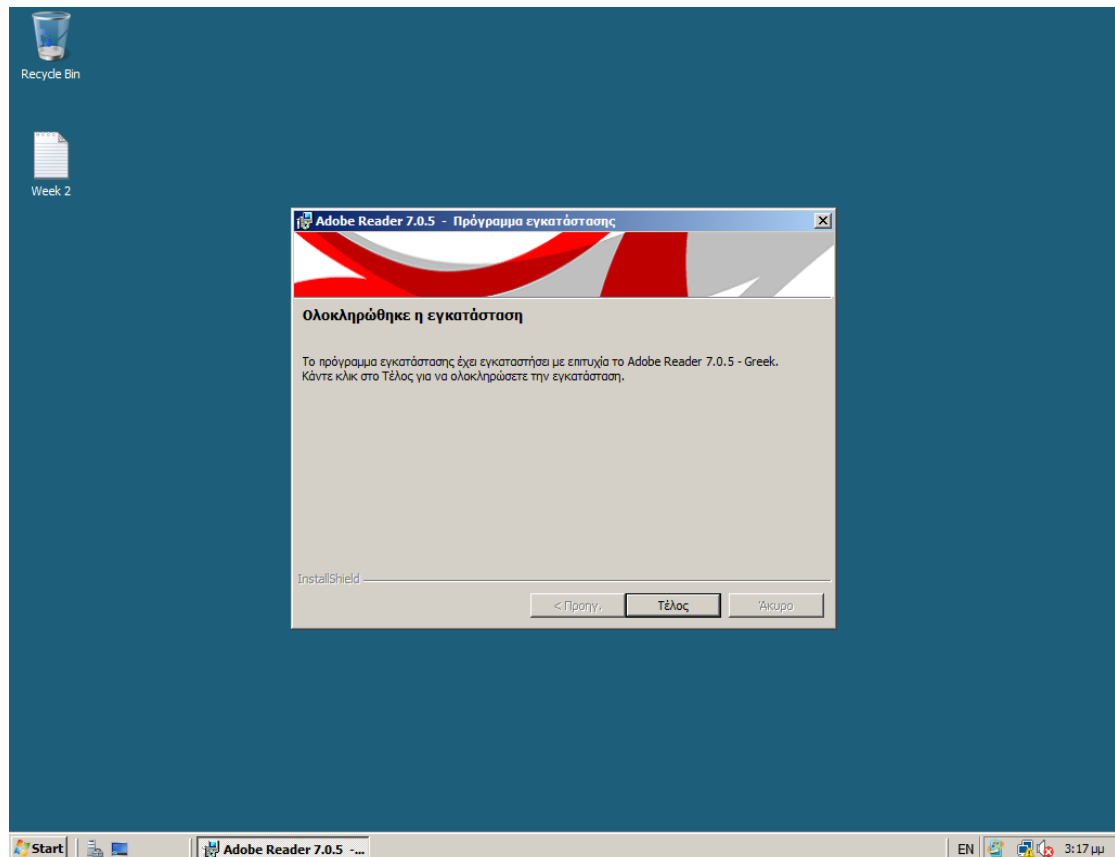
- ✓ **Start > Run**
- ✓ Πληκτρολογούμε στο πεδίο Open **msiexec /a "E:\Software\Adobe\Reader 7\Setup Files\Adobe Reader 7.0.5 - Greek.msi"** και πατάμε **OK** (Εικ. 15.6)
- ✓ Στο παράθυρο καλωσορίσματος του οδηγού εγκατάστασης πληροφορούμαστε πως πρόκειται να δημιουργήσουμε μία **εικόνα διακομιστή** (server image) του λογισμικού (Εικ. 15.7). Για να συνεχίσουμε πατάμε το κουμπί **Επόμενο**.
- ✓ Εισάγουμε στο πεδίο **Δικτυακός τόπος** τη θέση δημιουργίας του installation package είτε πληκτρολογώντας την, είτε επιλέγοντάς την με το κουμπί **Αλλαγή...** Όταν είμαστε έτοιμοι πατάμε το κουμπί **Εγκατάσταση** (Εικ. 15.8)
- ✓ Μετά την ολοκλήρωση της διαδικασίας εγκατάστασης (απαιτεί μερικά λεπτά) πατάμε το κουμπί **Τέλος** (Εικ. 15.9).



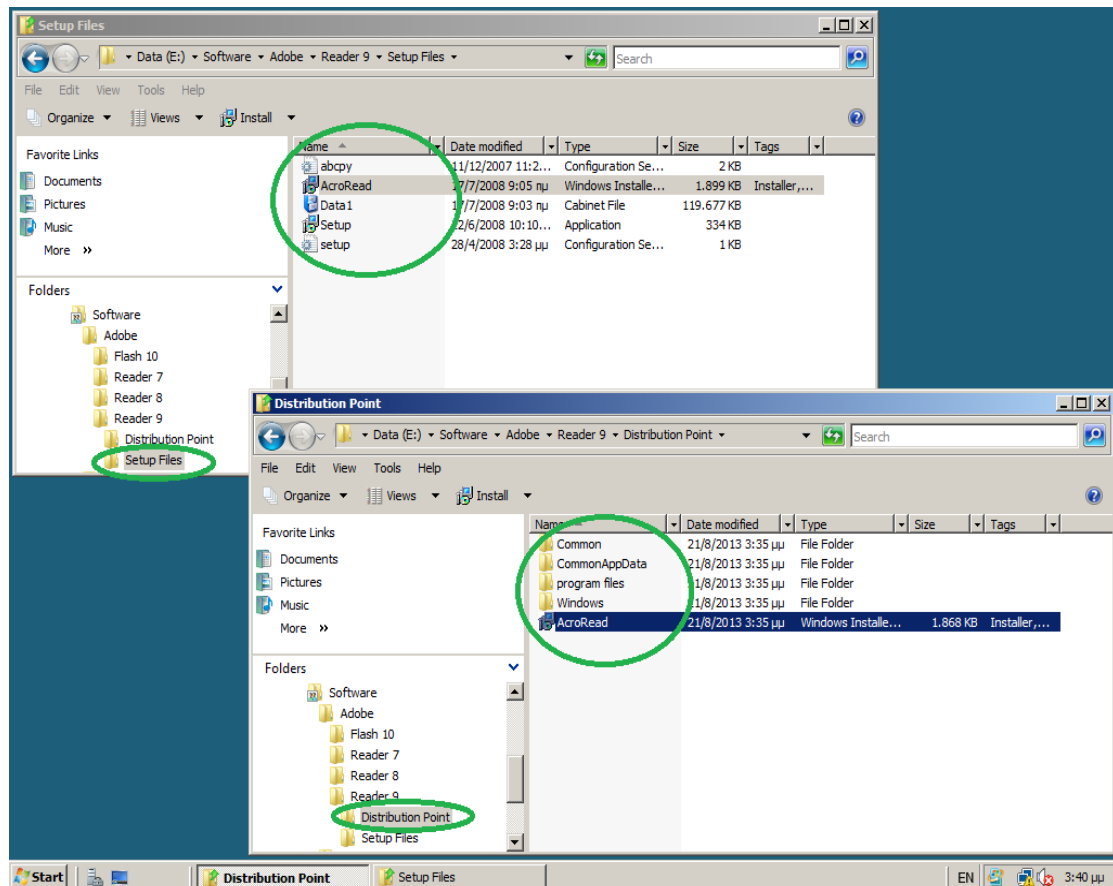
Εικ. 15.7. Adobe Reader 7 Installation Package



Εικ. 15.8. Adobe Reader 7 Installation Package



Εικ. 15.9. Adobe Reader 7 Installation Package



Εικ. 15.10. Adobe Reader 7 Installation Package

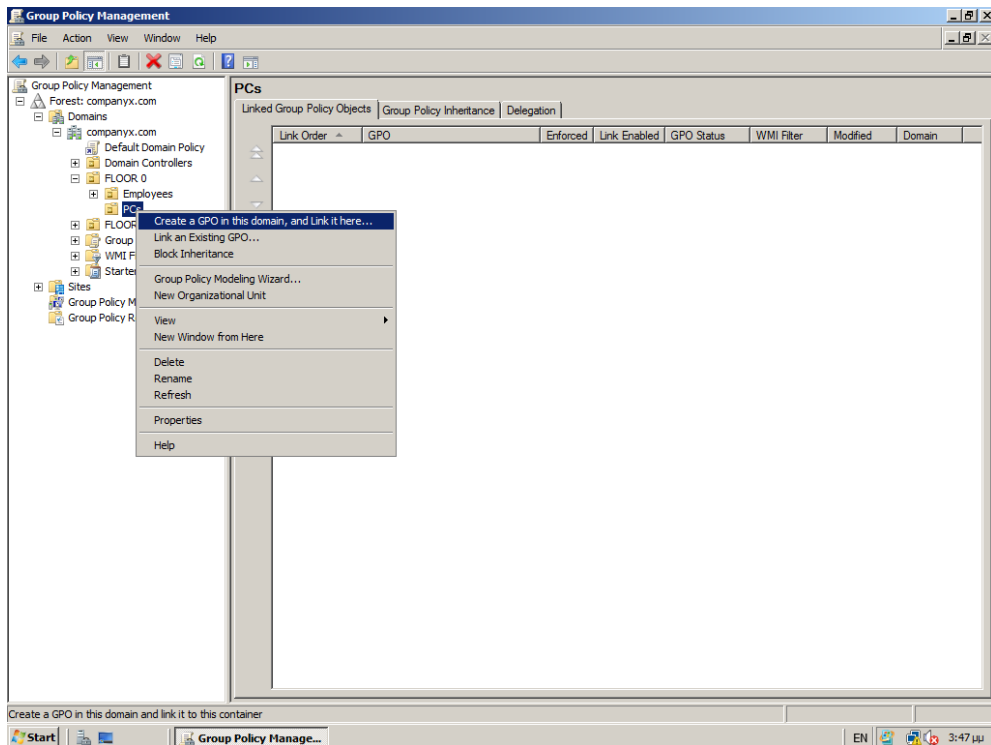
Το αποτέλεσμα της δημιουργίας του installation package (πριν και μετά τη χρήση του εργαλείου msixexec.exe) φαίνεται στην Εικ. 15.10.

Για τη δημιουργία των installation packages των προϊόντων Adobe Reader 8, Adobe Reader 9 και Adobe Flash Player 10 ακολουθούμε την παραπάνω διαδικασία. Οι οθόνες εγκατάστασης ίσως να διαφέρουν από λογισμικό σε λογισμικό αλλά η λογική παραμένει η ίδια.

15.3 Απομακρυσμένη Εγκατάσταση Λογισμικού

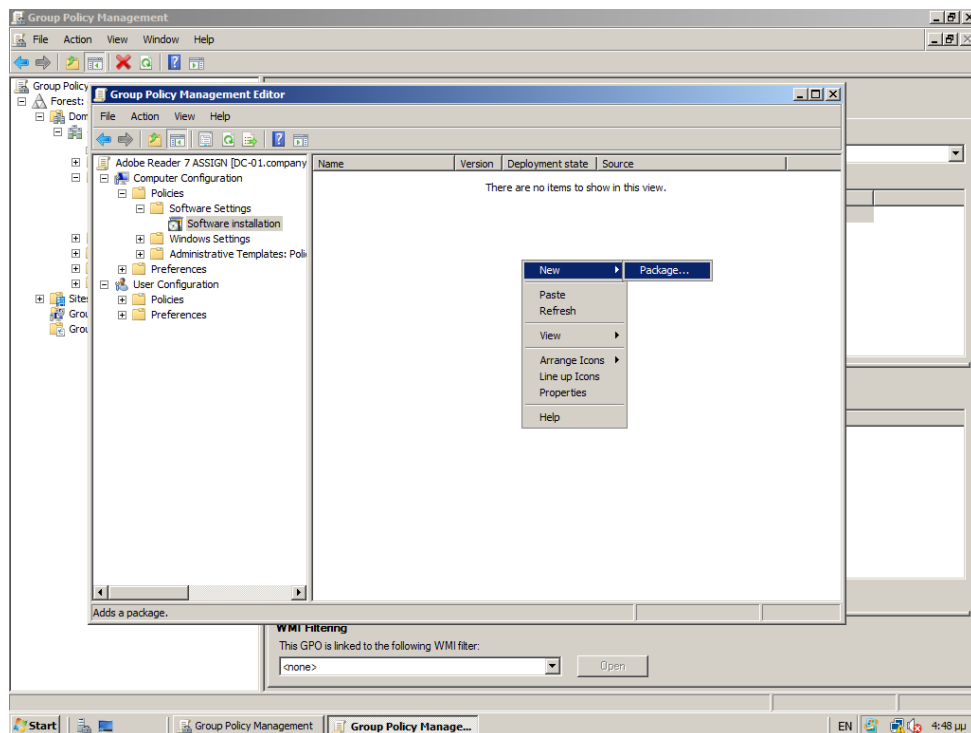
Πρόκειται να εγκαταστήσουμε απομακρυσμένα στους client H/Y του δικτύου μας το λογισμικό Adobe Reader 7. Θα δημιουργήσουμε Group Policy και θα την συνδέσουμε στο OU όπου βρίσκονται οι H/Y για τους οποίους προορίζεται η εγκατάσταση. Όλη η διαδικασία αναλύεται ακολούθως:

- ☐ Εκκινούμε την κονσόλα διαχείρισης Group Policy, **Start > Administrative Tools > Group Policy Management**
- ☐ Αναπτύσσοντας τα κατάλληλα containers βρίσκουμε το OU που μας ενδιαφέρει, κάνουμε **Δεξί κλικ** και επιλέγουμε **Create a GPO in this domain, and Link it here...** (Εικ. 15.11)



Εικ. 15.11. Κονσόλα Group Policy Management

- ☐ Δίνουμε στο νέο GPO το όνομα **Adobe Reader 7 ASSIGN** και πατάμε **OK**
- ☐ Για να επεξεργαστούμε το νέο GPO κάνουμε **Δεξί κλικ** επάνω του και επιλέγουμε **Edit...** ώστε να ανοίξει το πρόγραμμα επεξεργασίας **Group Policy Management Editor**



Εικ. 15.12. Group Policy Management Editor

□ Στο πρόγραμμα Group Policy Management Editor, κάτω από το container **Computer Configuration**, αναπτύσσουμε το container **Policies** και στη συνέχεια αναπτύσσουμε το container **Software Settings**. Επιλέγουμε (κλικ) το **Software Installation** και κάνουμε στο δεξί τμήμα **Δεξί κλικ > New > Package...** (Εικ. 15.12)

□ Στο παράθυρο διαλόγου (Windows Explorer) **Open** για την επιλογή του installation package (Εικ. 15.13), ακολουθούμε τη **δικτυακή διαδρομή** για να βρούμε το πακέτο, η οποία στο σενάριο αυτό είναι:

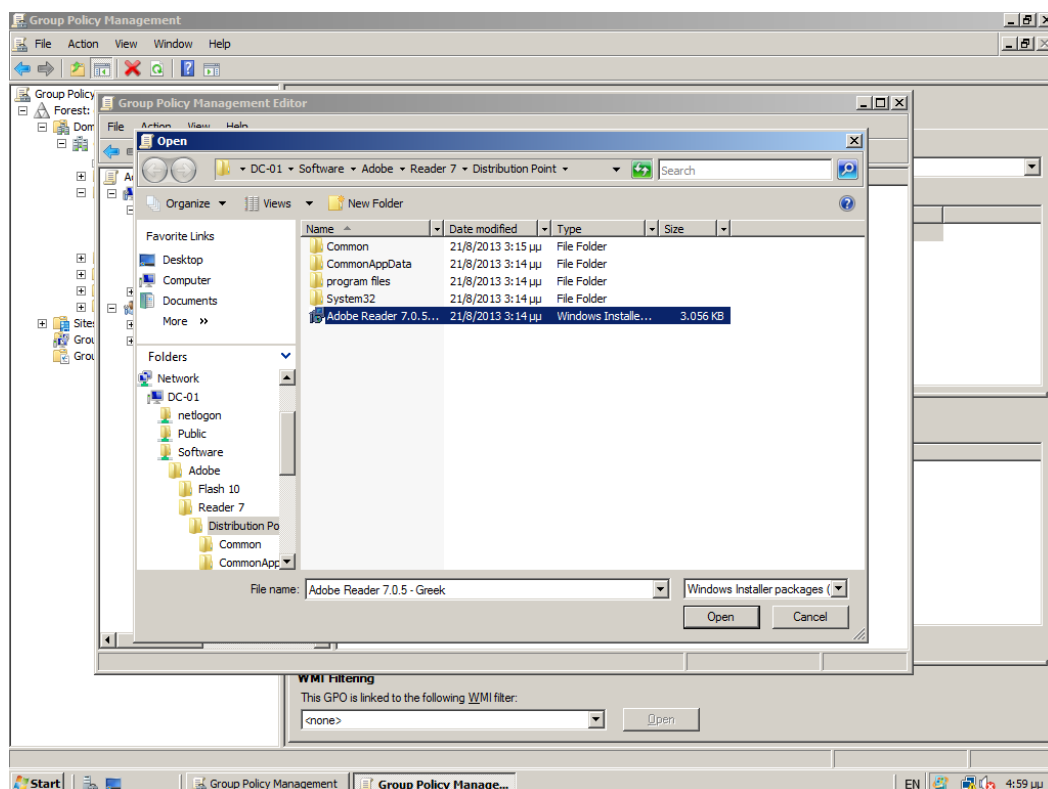
\\DC-01\Software\Adobe\Reader 7\Distribution Point\Adobe Reader 7.0.5 – Greek.msi

□ Το επιλέγουμε και πατάμε στο κουμπί **Open**

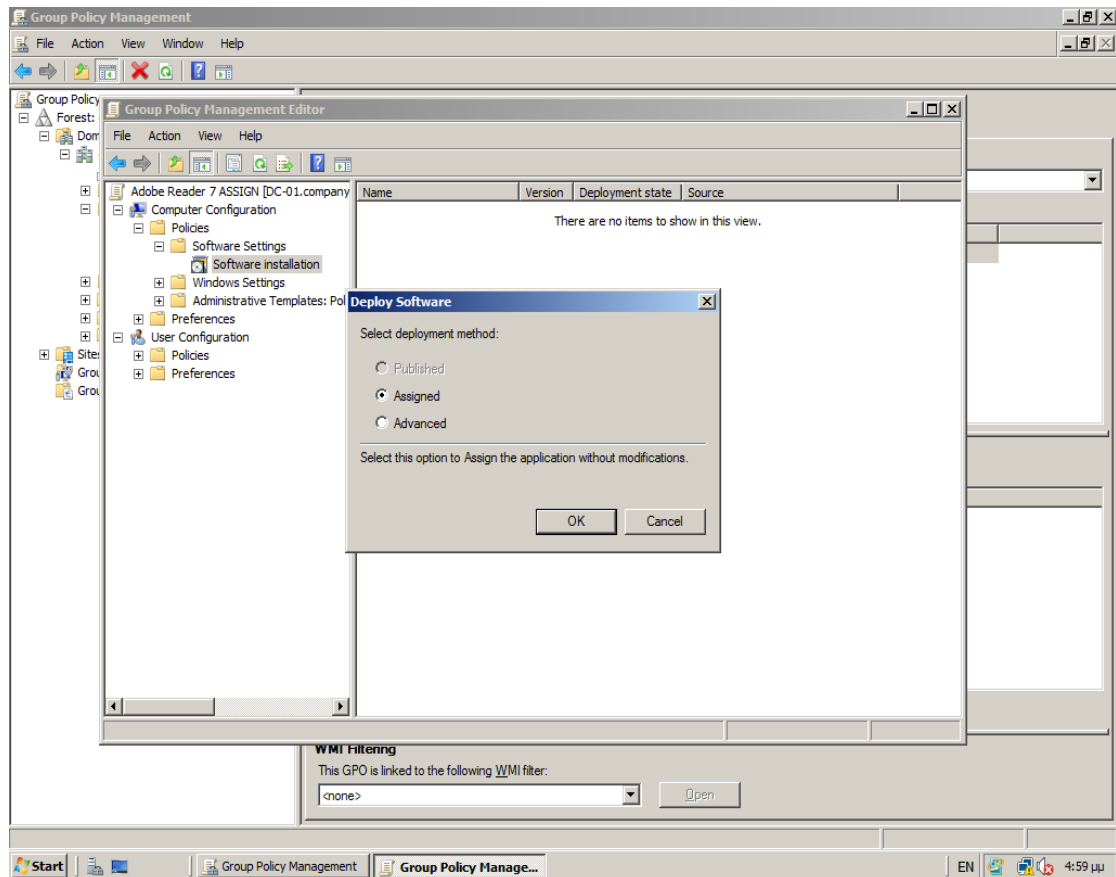
□ Στο επόμενο παράθυρο διαλόγου (Εικ. 15.14), **Deploy Software**, αφήνουμε την προεπιλογή **Assigned** και πατάμε **OK**

□ Η Εικ. 15.15 δείχνει το installation package που θα διανεμηθεί με αυτή την πολιτική στο δίκτυο.

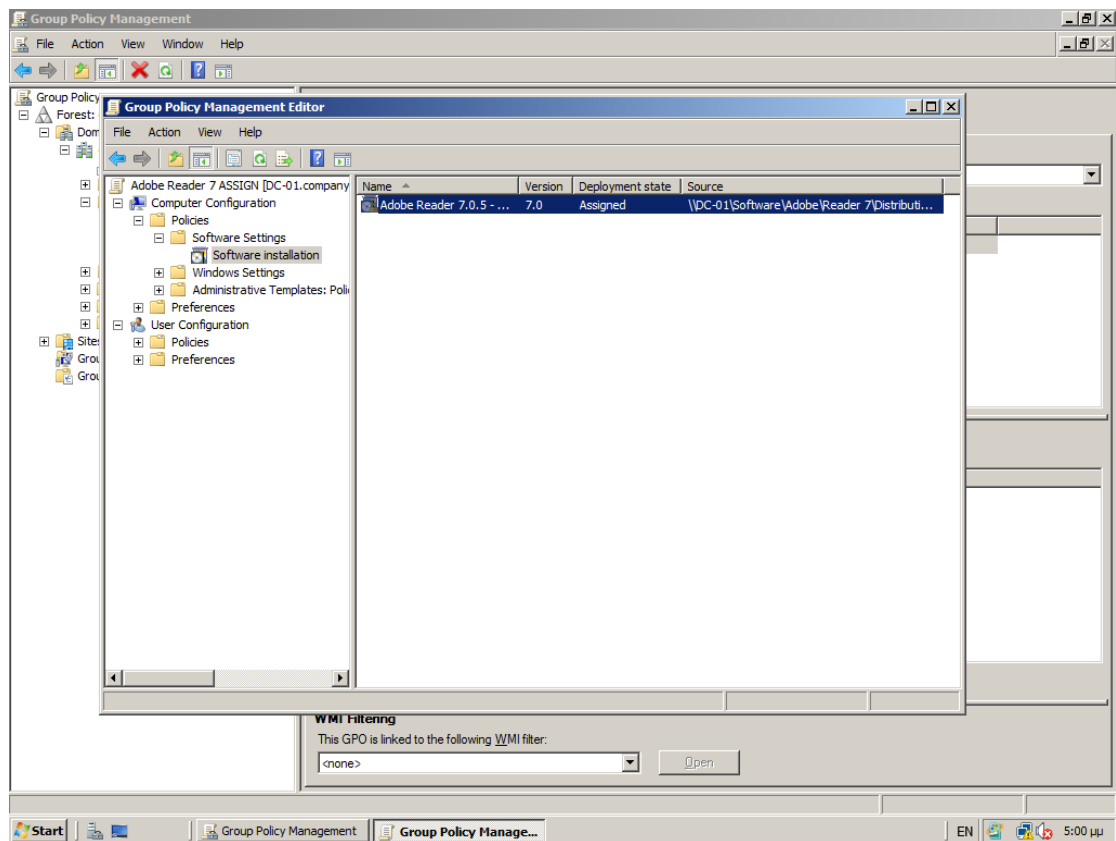
Για να εγκαταστήσουμε το MS Office XP ή/και το Adobe Flash 10 στο δίκτυο με την ίδια μέθοδο (Assigned) δημιουργούμε νέα πολιτική (ή προσθέτουμε το installation package στην ίδια πολιτική) ακολουθώντας την ίδια διαδικασία που αναφέρεται παραπάνω.



Εικ. 15.13. Επιλογή Installation Package



Εικ. 15.14. Επιλογή Deployment Method

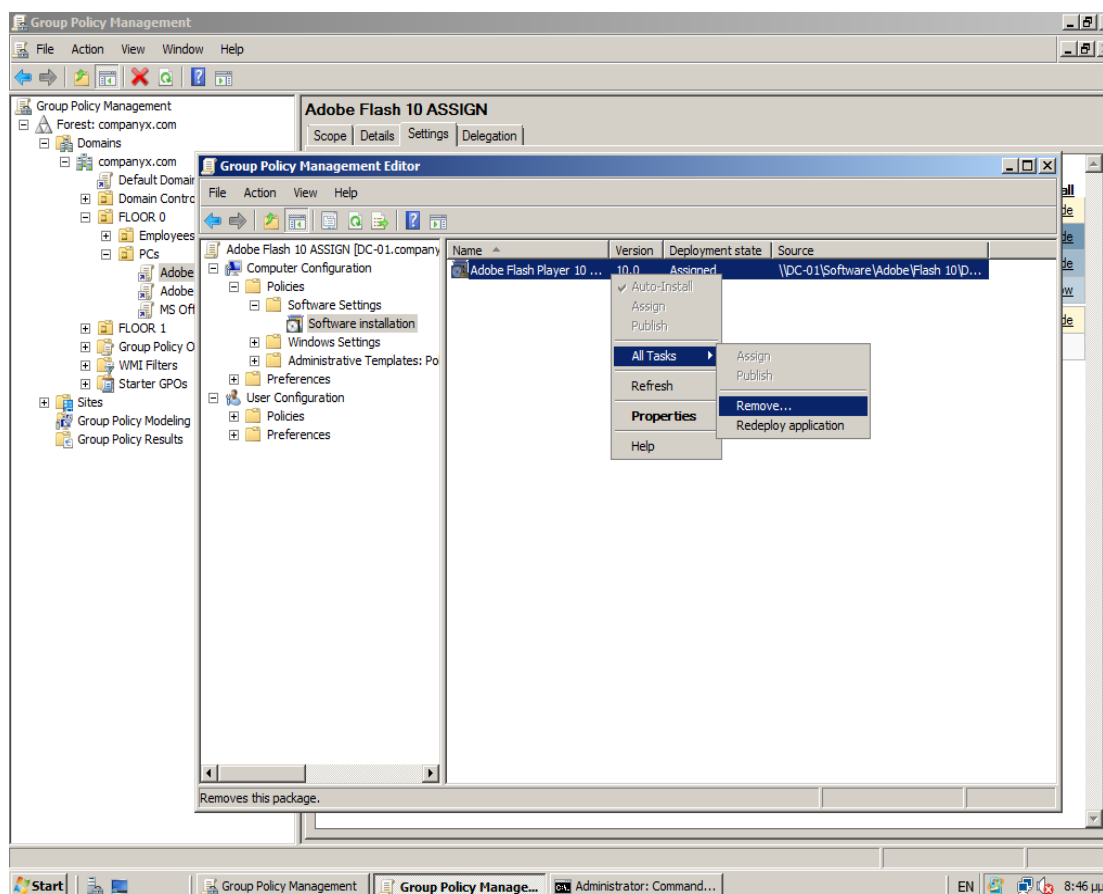


Εικ. 15.15. Installation Package, έτοιμο για εγκατάσταση

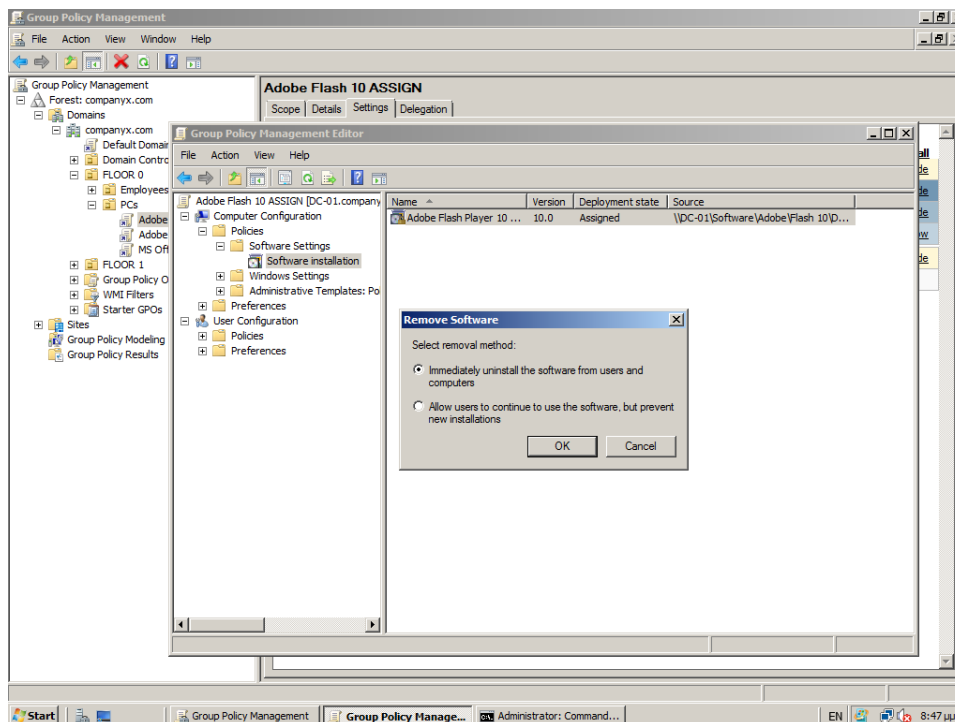
15.4 Απομακρυσμένη Απεγκατάσταση Λογισμικού

Το σενάριο που αναλύεται παρακάτω περιγράφει τη διαδικασία με την οποία *μπορούμε – απομακρυσμένα – να απεγκαταστήσουμε λογισμικό το οποίο έχουμε προηγουμένως εγκαταστήσει με Group Policy*. Το λογισμικό που θα απεγκαταστήσουμε μαζικά από τους client H/Y είναι το Adobe Flash Player 10:

- Εκκινούμε την κονσόλα διαχείρισης Group Policy, **Start > Administrative Tools > Group Policy Management**
- Το GPO με το οποίο έχουμε εγκαταστήσει το λογισμικό είναι το **Adobe Flash 10 ASSIGN**. Για να το επεξεργαστούμε κάνουμε **Δεξί κλικ** επάνω του και επιλέγουμε **Edit...** ώστε να ανοίξει το πρόγραμμα επεξεργασίας **Group Policy Management Editor**
- Στο πρόγραμμα Group Policy Management Editor, κάτω από το container **Computer Configuration**, αναπτύσσουμε το container **Policies** και στη συνέχεια αναπτύσσουμε το container **Software Settings**. Επιλέγουμε (κλικ) το **Software Installation** και στο δεξιό τμήμα, βρίσκουμε το installation package στο οποίο κάνουμε **Δεξί κλικ > All Tasks > Remove...** (Εικ. 15.16)



Εικ. 15.16. Αφαίρεση Πακέτου Εγκατάστασης



Εικ. 15.17. Επιλογές Αφαίρεσης Πακέτου Εγκατάστασης

- Στο παράθυρο διαλόγου Remove Software εμφανίζονται δύο επιλογές αφαίρεσης λογισμικού (Εικ. 15.17):

- ✓ *Immediately uninstall the software from users and computers* – Η επιλογή αυτή απεγκαθιστά το λογισμικό από χρήστες και υπολογιστές στους οποίους έχει προηγουμένως εγκατασταθεί με την πολιτική αυτή
- ✓ *Allow users to continue to use the software, but prevent new installations* – Η επιλογή αυτή δεν απεγκαθιστά το λογισμικό, το εμποδίζει όμως από το να εγκατασταθεί σε νέους χρήστες ή/και υπολογιστές που θα βρεθούν υπό το εύρος διαχείρισης αυτής της Group Policy

- Επιλέγουμε την **πρώτη επιλογή** και πατάμε **OK**

Την επόμενη φορά που θα εκκινήσουν οι Η/Υ που επηρεάζονται από την πολιτική αυτή, θα λάβει χώρα, κατά το start up, η απεγκατάσταση του λογισμικού.

15.5 Απομακρυσμένη Εγκατάσταση νέας έκδοσης – Αναβάθμιση

Λογισμικού

Ένα ιδιαίτερα χρήσιμο στοιχείο στην απομακρυσμένη εγκατάσταση λογισμικού είναι η απομακρυσμένη αναβάθμιση σε νέα έκδοση. Αυτό που πρέπει ο διαχειριστής να προσέξει κατά την εφαρμογή της διαδικασίας είναι η συμπεριφορά του λογισμικού κατά την αναβάθμιση η οποία διαφέρει ανάλογα με τον κατασκευαστή. Πιο

συγκεκριμένα, όταν πρόκειται να αναβαθμίσουμε σε νέα έκδοση πρέπει να επιλέξουμε ανάμεσα από δύο τρόπους:

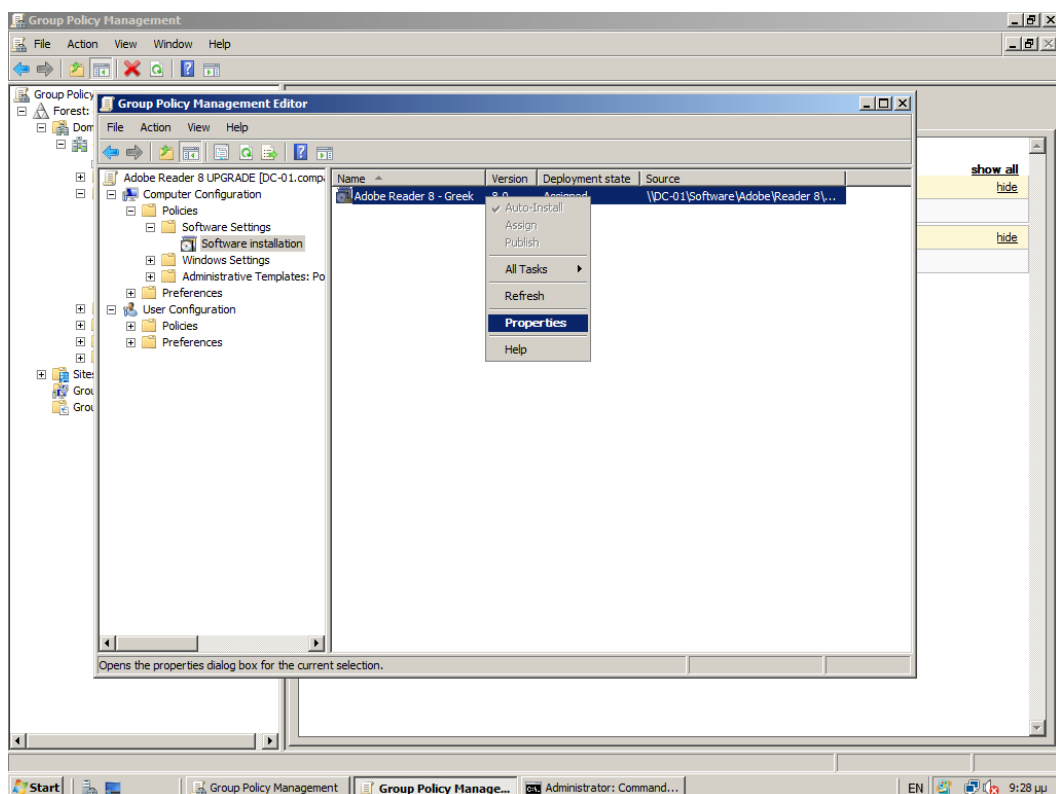
1. Αναβαθμίζουμε το λογισμικό σε νέα έκδοση εγκαθιστώντας την πάνω από την παλιά (**In-place Upgrade**)
2. Αναβαθμίζουμε το λογισμικό σε νέα έκδοση αφαιρώντας πρώτα την παλιά και στη συνέχεια εγκαθιστώντας τη νέα (**Replace**)

Σε κάθε περίπτωση πρέπει να είμαστε **ιδιαίτερα προσεκτικοί** αναφορικά με το τι επιτρέπει ο κατασκευαστής στη **συμπεριφορά αναβάθμισης** του λογισμικού του ώστε να αποφύγουμε λειτουργικά – και σε μερικές περιπτώσεις – μη αναστρέψιμα προβλήματα (ειδικά όταν αυτό γίνεται μαζικά για **πολλαπλούς H/Y**).

15.5.1 Επιτόπια Αναβάθμιση σε νέα έκδοση (In-place Upgrade)

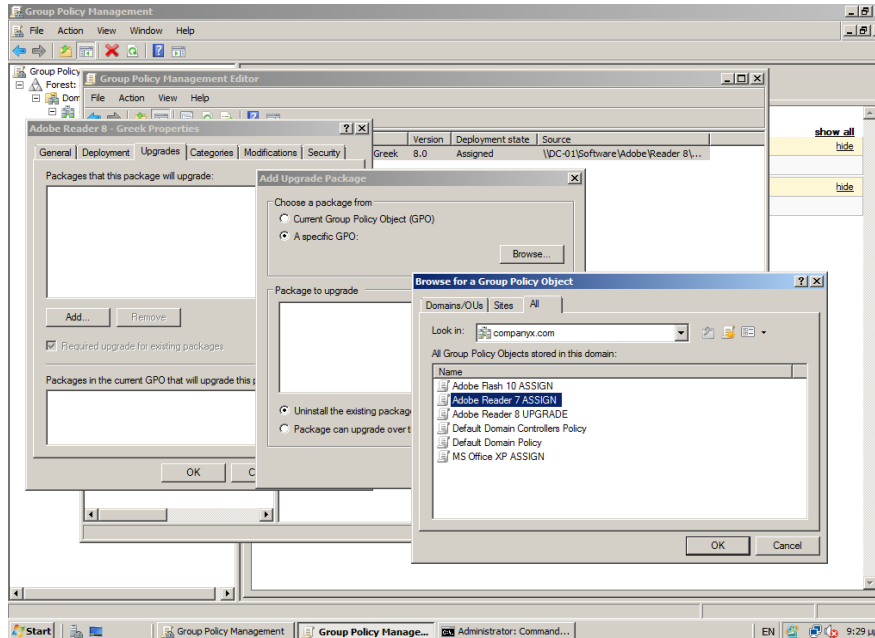
Στο σενάριο αυτό θα εξετάσουμε την αναβάθμιση του Adobe Reader 7 σε Adobe Reader 8. Σύμφωνα με τις τεχνικές προδιαγραφές του κατασκευαστή το λογισμικό επιτρέπει την αναβάθμισή του επάνω από την παλιά. Έχοντας αυτό υπόψη θα δημιουργήσουμε μία πολιτική αναβάθμισης του λογισμικού σύμφωνα με τα ακόλουθα βήματα:

- ☐ Δημιουργούμε μία νέα πολιτική απομακρυσμένης εγκατάστασης της νέας έκδοσης σύμφωνα με τη διαδικασία που αναλύεται στην **παράγραφο 15.3**.



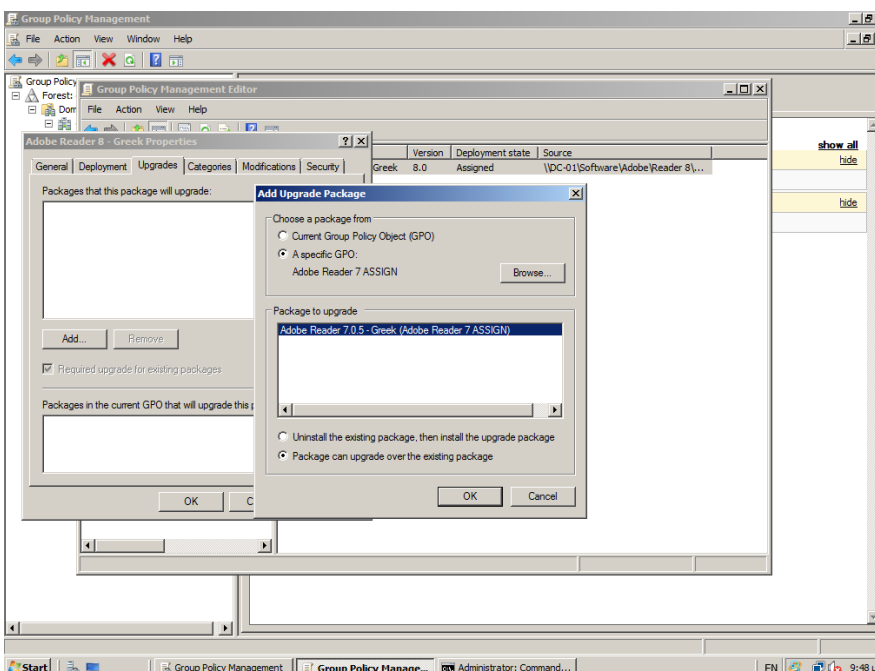
Εικ. 15.18. Ιδιότητες Πακέτου Εγκατάστασης

- Στη συνέχεια, στο installation package κάνουμε **Δεξί κλικ > Properties** (Εικ. 15.18)
- Στο παράθυρο διαλόγου των ιδιοτήτων (Εικ. 15.19) κάνουμε κλικ στην καρτέλα **Upgrades**



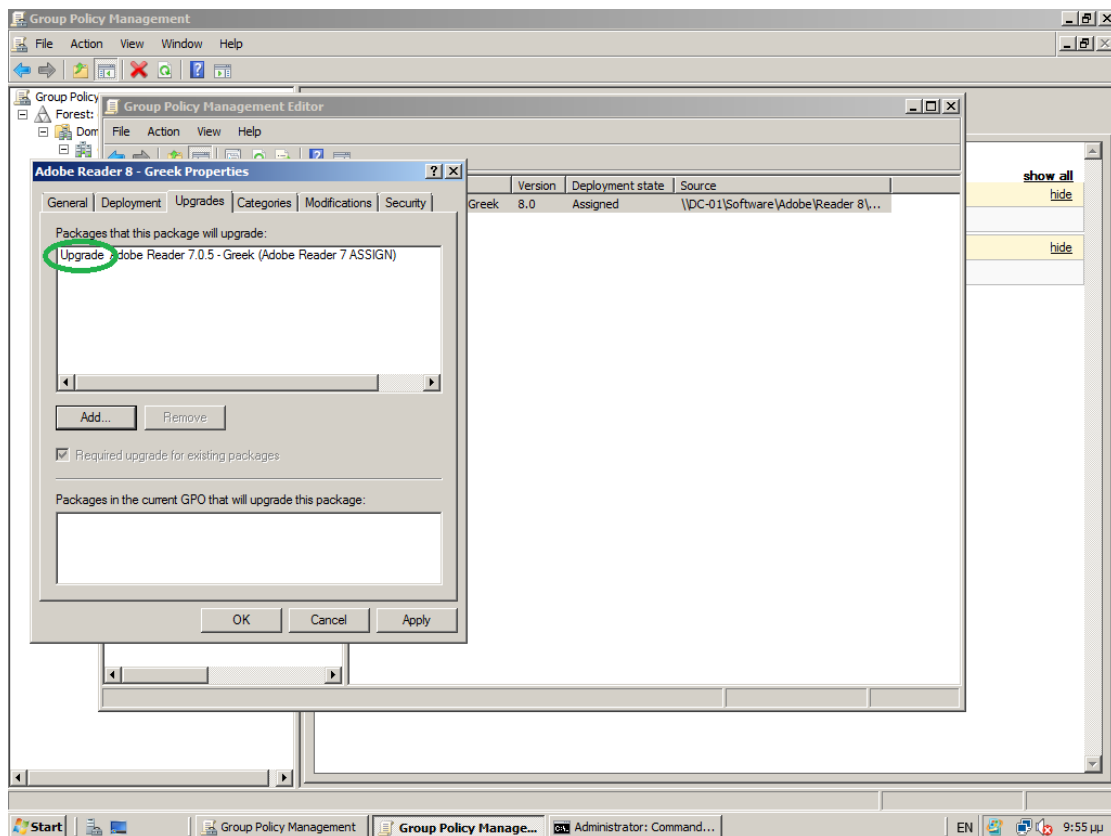
Εικ. 15.19. Συσχέτιση Πακέτου νέας έκδοσης με αυτό της παλιάς έκδοσης προς αναβάθμιση

- Στο νέο παράθυρο διαλόγου Add Upgrade Package (Εικ. 15.19) επιλέγουμε **A specific GPO** και στη συνέχεια πατάμε το κουμπί **Browse**



Εικ. 15.20

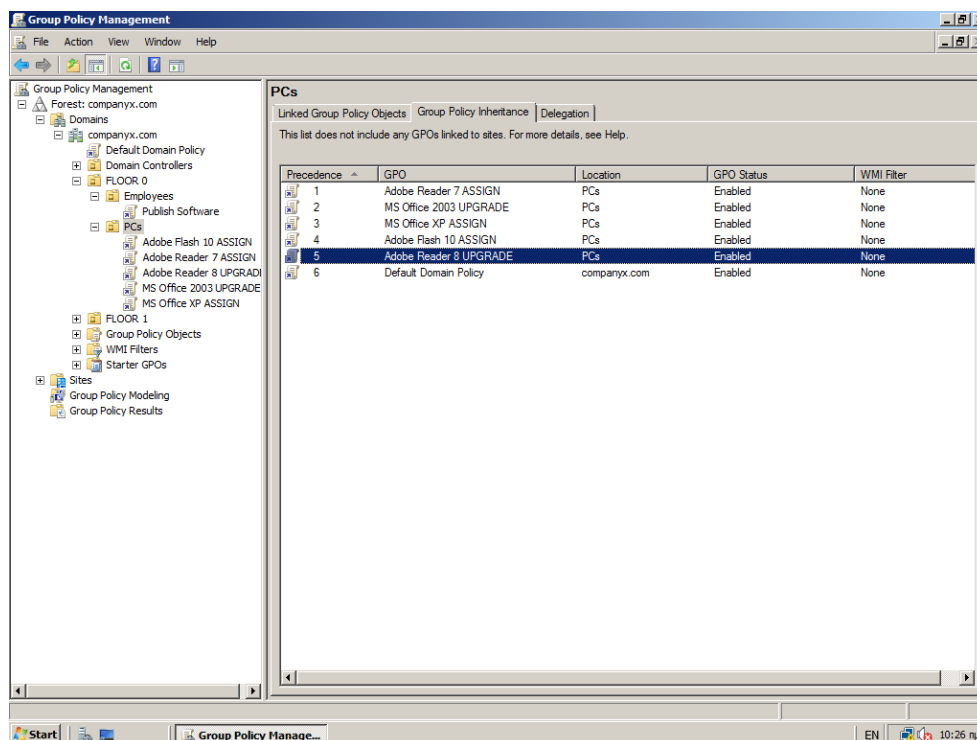
- Στο επόμενο, νέο παράθυρο διαλόγου Browse for a Group Policy Object επιλέγουμε την Group Policy του λογισμικού που επιθυμούμε να αναβαθμίσουμε (Εικ. 15.19) και πατάμε **OK**
- Επιστρέφοντας στο προηγούμενο παράθυρο διαλόγου (Add Upgrade Package, Εικ. 15.20) βλέπουμε τώρα το πακέτο που θα αναβαθμιστεί στην περιοχή **Package to upgrade**. Επιλέγουμε παρακάτω **Package can upgrade over the existing package** και στη συνέχεια πατάμε **OK**
- Επιστρέφοντας στο παράθυρο ιδιοτήτων του πακέτου εγκατάστασης / αναβάθμισης (Εικ. 15.21) θεωρούμε τις πληροφορίες αναβάθμισης του λογισμικού (**Upgrade...**) και πατάμε το κουμπί **OK**
- Κλείνουμε το πρόγραμμα Group Policy Management Editor



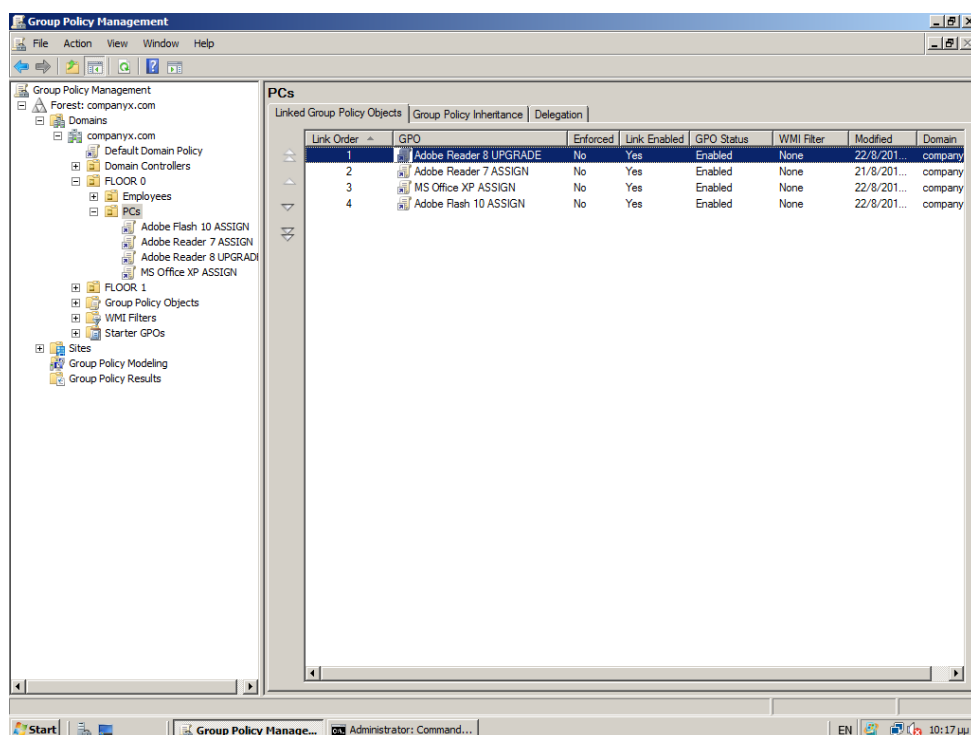
Εικ. 15.21

Η Group Policy εγκατάστασης / αναβάθμισης της παλιάς έκδοσης λογισμικού στην καινούρια είναι έτοιμη, εντούτοις χρειάζονται κάποια επιπρόσθετα βήματα ρυθμίσεων για να λάβει χώρα η αναβάθμιση. Πίσω στην κονσόλα Group Policy Management **επιλέγουμε το ΟΥ** στο οποίο έχουμε συνδέσει την πολιτική (αριστερό τμήμα παραθύρου) και στη συνέχεια κάνουμε κλικ στην καρτέλα **Group Policy Inheritance** (δεξιό τμήμα παραθύρου). Παρατηρούμε πως η πολιτική αναβάθμισης

βρίσκεται σε χαμηλότερη προτεραιότητα από την πολιτική εγκατάστασης της παλιάς έκδοσης (Εικ. 15.22).



Εικ. 15.22. Group Policy Inheritance



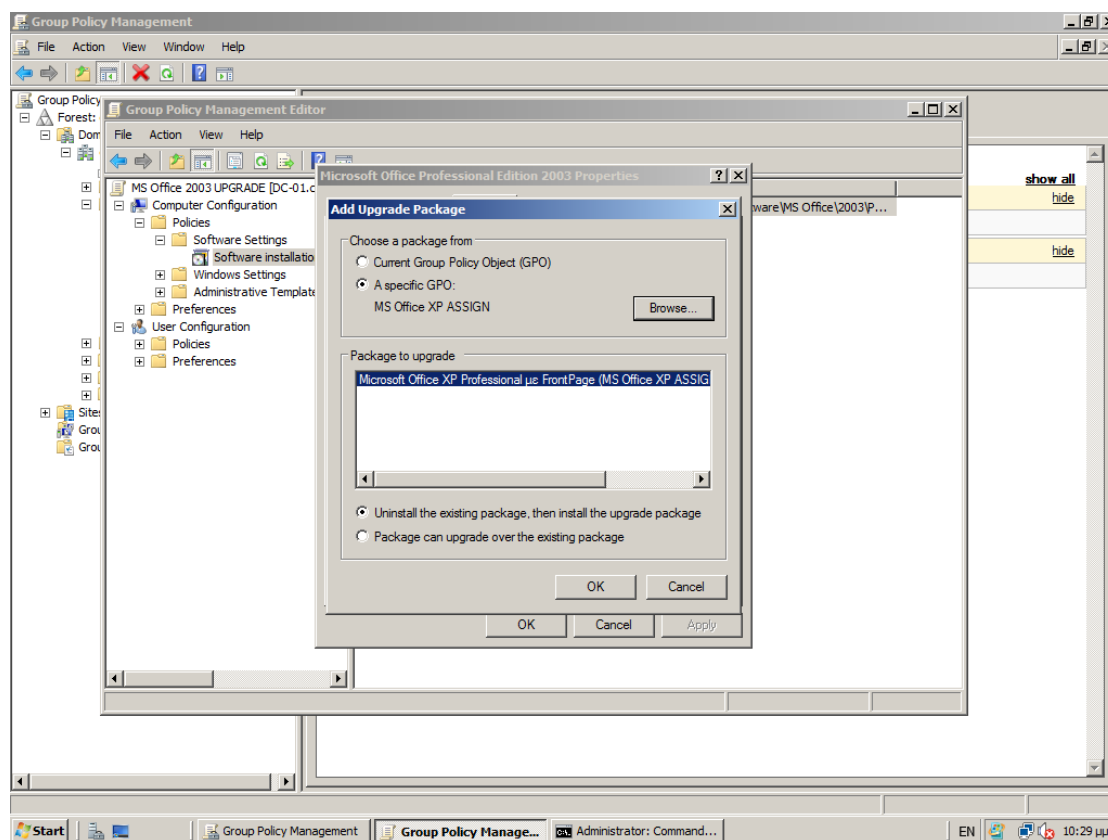
Εικ. 15.23. Αλλαγή σειράς προτεραιότητας πολιτικών

εισέλθουν στο ΟΥ θα εγκαταστήσουν αυτόματα την παλιά έκδοση και όχι τη νέα έκδοση λογισμικού. Για να επιλυθεί αυτό το πρόβλημα θα αλλάξουμε τη σειρά των

πολιτικών ώστε να υπερισχύει η νέα έκδοση λογισμικού. Κάνουμε κλικ στην καρτέλα **Linked Group Policy Objects** (Εικ. 15.23) και στη συνέχεια χρησιμοποιώντας τα βελάκια στην αριστερή στήλη αλλάζουμε τη σειρά προτεραιότητας των πολιτικών που μας ενδιαφέρουν.

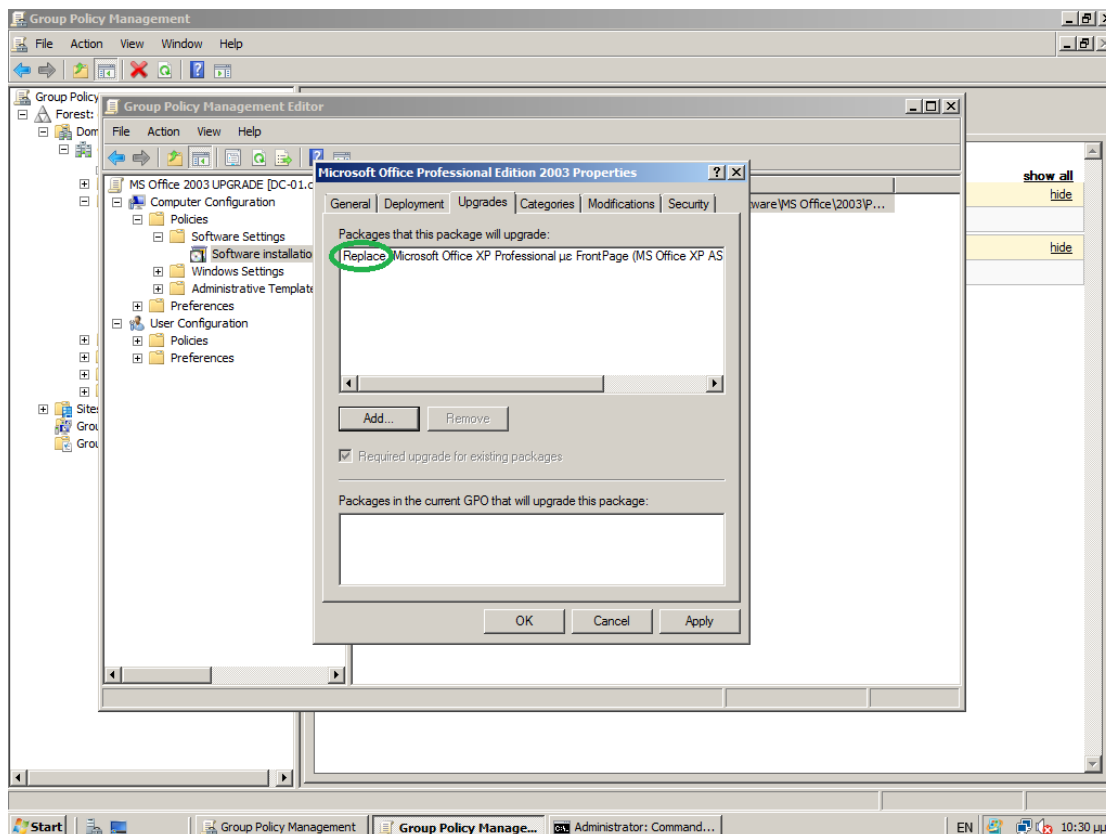
15.5.2 Αντικατάσταση με νέα έκδοση (Replace)

Στο σενάριο αυτό θα εξετάσουμε την αναβάθμιση του MS Office XP σε MS Office 2003. Σύμφωνα με τις τεχνικές προδιαγραφές του κατασκευαστή πρέπει πρώτα να αφαιρεθεί η παλιά έκδοση και μετά να εγκατασταθεί η νέα έκδοση λογισμικού. Έχοντας αυτό υπόψη θα δημιουργήσουμε μία πολιτική αναβάθμισης του λογισμικού σύμφωνα με τα βήματα που ακολουθήσαμε στην **παράγραφο 15.5.1** με μια μικρή διαφορά – θα επιλέξουμε την επιλογή **Uninstall the existing package, then install the upgrade package** (Εικ. 15.24):



Εικ. 15.24

Επιστρέφοντας στο παράθυρο ιδιοτήτων του πακέτου εγκατάστασης / αναβάθμισης (Εικ. 15.25) θεωρούμε τις πληροφορίες αναβάθμισης του λογισμικού (**Replace...**) και πατάμε το κουμπί **OK**. Αλλάζουμε στη συνέχεια τη **σειρά προτεραιότητας** των πολιτικών και η πολιτική αντικατάστασης παλιάς έκδοσης από νέα έκδοση λογισμικού είναι έτοιμη.



Εικ. 15.25

15.6 Δημοσίευση Λογισμικού (Publish Software)

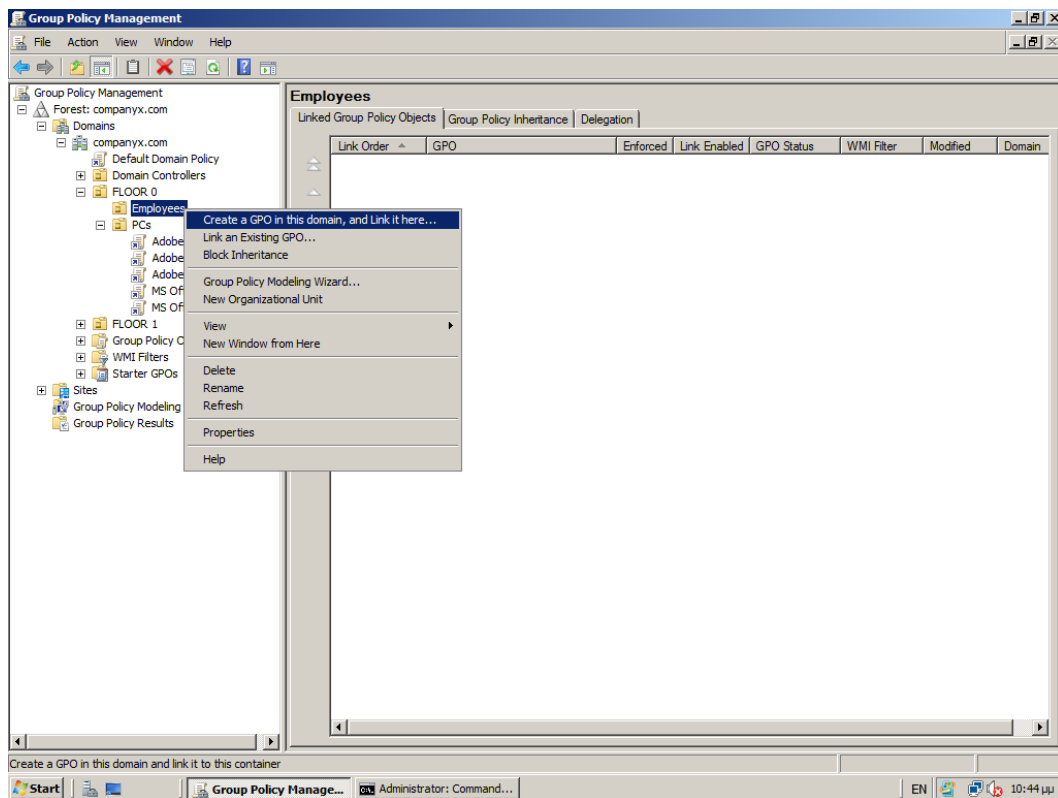
Η τεχνολογία δημοσίευσης λογισμικού δίνει τη δυνατότητα στο διαχειριστή να δημοσιεύει στο Active Directory λογισμικά που εκείνος επιλέγει / εγκρίνει, εκχωρώντας παράλληλα το δικαίωμα εγκατάστασής τους στους ίδιους τους χρήστες από την επιφάνεια εργασίας των Η/Υ τους (Πίνακας Ελέγχου > Προσθαφαίρεση Προγραμμάτων). Την ίδια στιγμή οι χρήστες:

- ☐ δε χρειάζεται να έχουν διαχειριστικό δικαίωμα στον Η/Υ τους
- ☐ δε χρειάζεται να έχουν το μέσο εγκατάστασης (CD, DVD, USB, network share)
- ☐ δε χρειάζεται να έχουν το product key
- ☐ δε χρειάζεται να συμφωνήσουν με τους όρους άδειας χρήσης EULA

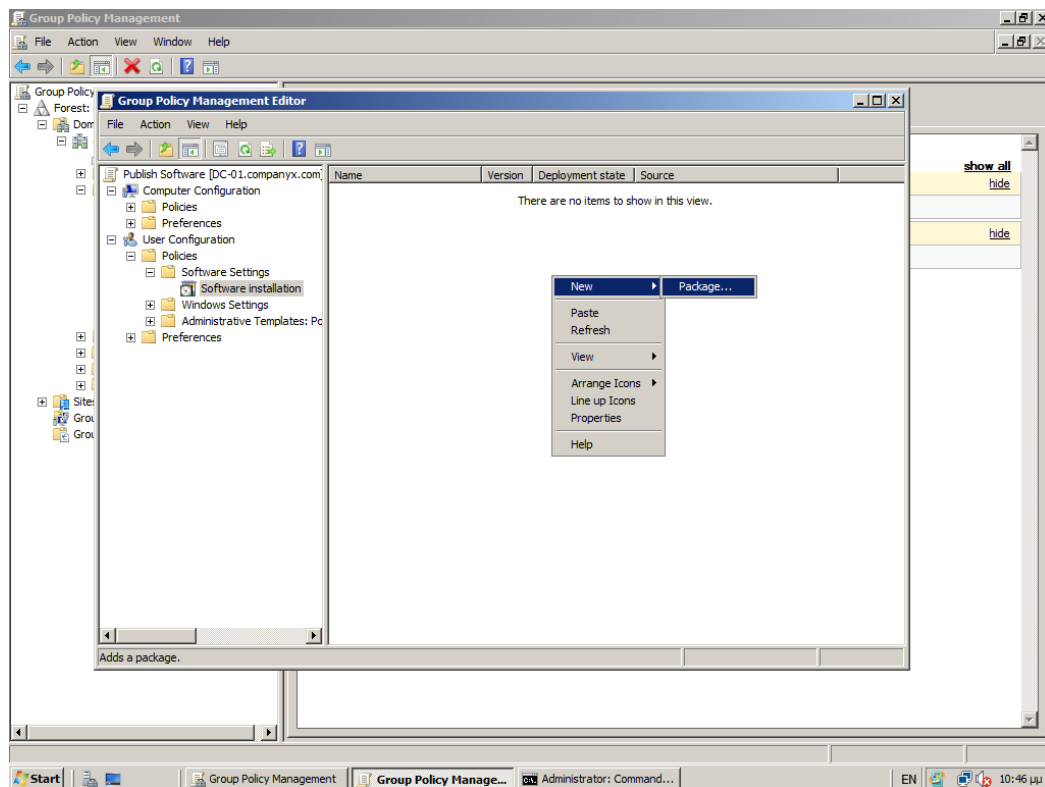
Στο σενάριο που ακολουθεί θα δημιουργήσουμε ένα Group Policy με το οποίο θα δημοσιεύουμε όλα τα λογισμικά για τα οποία έχουμε έτοιμα installation packages.

- ☐ Εκκινούμε την κονσόλα Group Policy Management (Start > Administrative Tools > **Group Policy Management**) και επιλέγουμε το ΟΥ με τους χρήστες στους οποίους θέλουμε να εκχωρήσουμε το δικαίωμα εγκατάστασής τους (Εικ. 15.26).

- Κάνουμε **Δεξί κλικ** και επιλέγουμε **Create a GPO in this domain, and Link it here...**
it here...

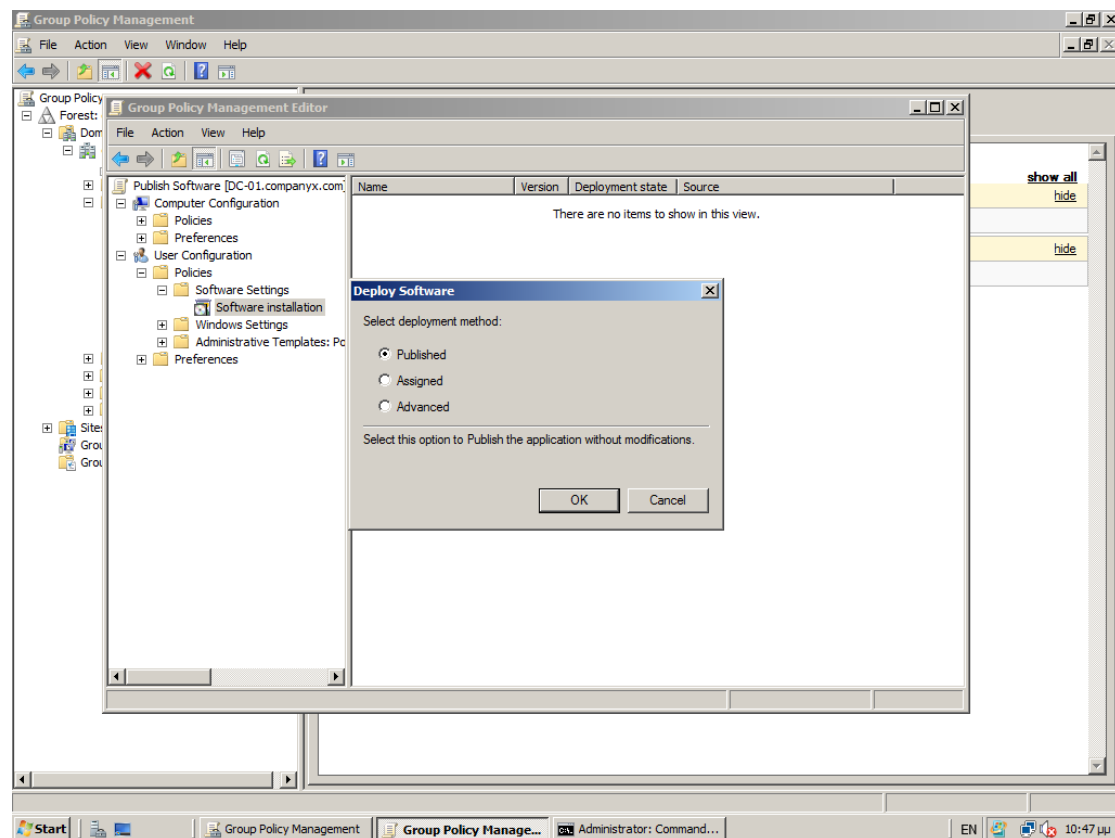


Εικ. 15.26



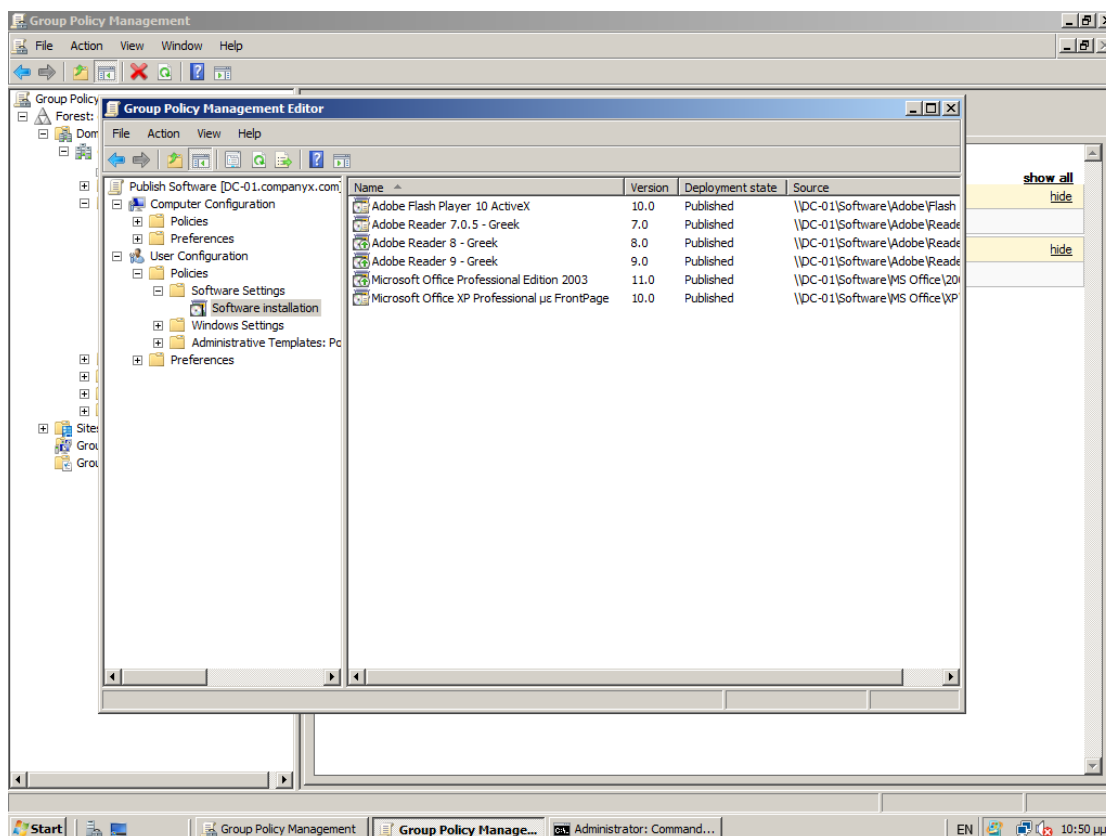
Εικ. 15.27. Group Policy Management Editor

- Δίνουμε στο νέο GPO το όνομα **Publish Software** και πατάμε **OK**
- Για να επεξεργαστούμε το νέο GPO κάνουμε **Δεξί κλικ** επάνω του και επιλέγουμε **Edit...** ώστε να ανοίξει το πρόγραμμα επεξεργασίας **Group Policy Management Editor**
- Στο πρόγραμμα Group Policy Management Editor (Εικ. 15.27), κάτω από το container **User Configuration**, αναπτύσσουμε το container **Policies** και στη συνέχεια αναπτύσσουμε το container **Software Settings**. Επιλέγουμε (κλικ) το **Software Installation** και κάνουμε στο δεξί τμήμα **Δεξί κλικ > New > Package...** (Εικ. 15.12)
- Επιλέγουμε το installation package που μας ενδιαφέρει να δημοσιεύσουμε και πατάμε **Open**
- Στο επόμενο παράθυρο διαλόγου (Εικ. 15.28), **Deploy Software**, επιλέγουμε τη μέθοδο **Published** και πατάμε **OK**



Εικ. 15.28. Επιλογή Deployment Method

- Επαναλαμβάνουμε τα προηγούμενα βήματα για να προσθέσουμε και τα άλλα installation packages στην ίδια πολιτική
- Η Εικ. 15.29 δείχνει το installation packages που θα δημοσιευθούν με αυτή την πολιτική στο δίκτυο.

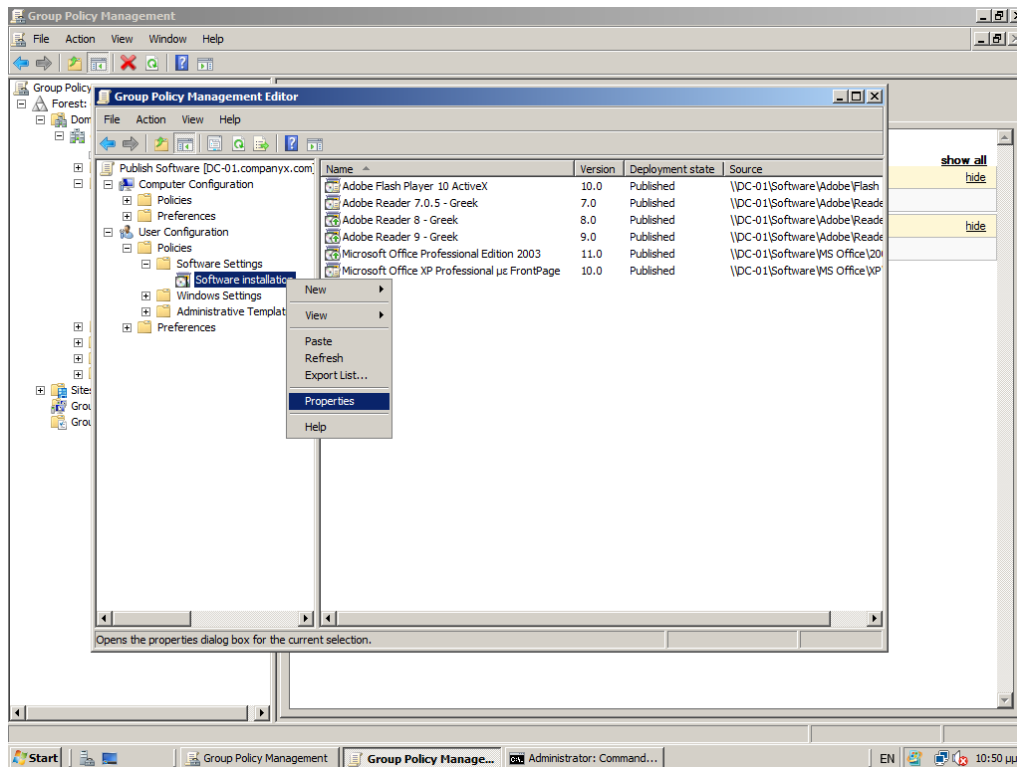


Εικ. 15.29. Πακέτα Δημοσιευμένων Λογισμικών

15.6.1 Προχωρημένες Ρυθμίσεις Δημοσίευσης

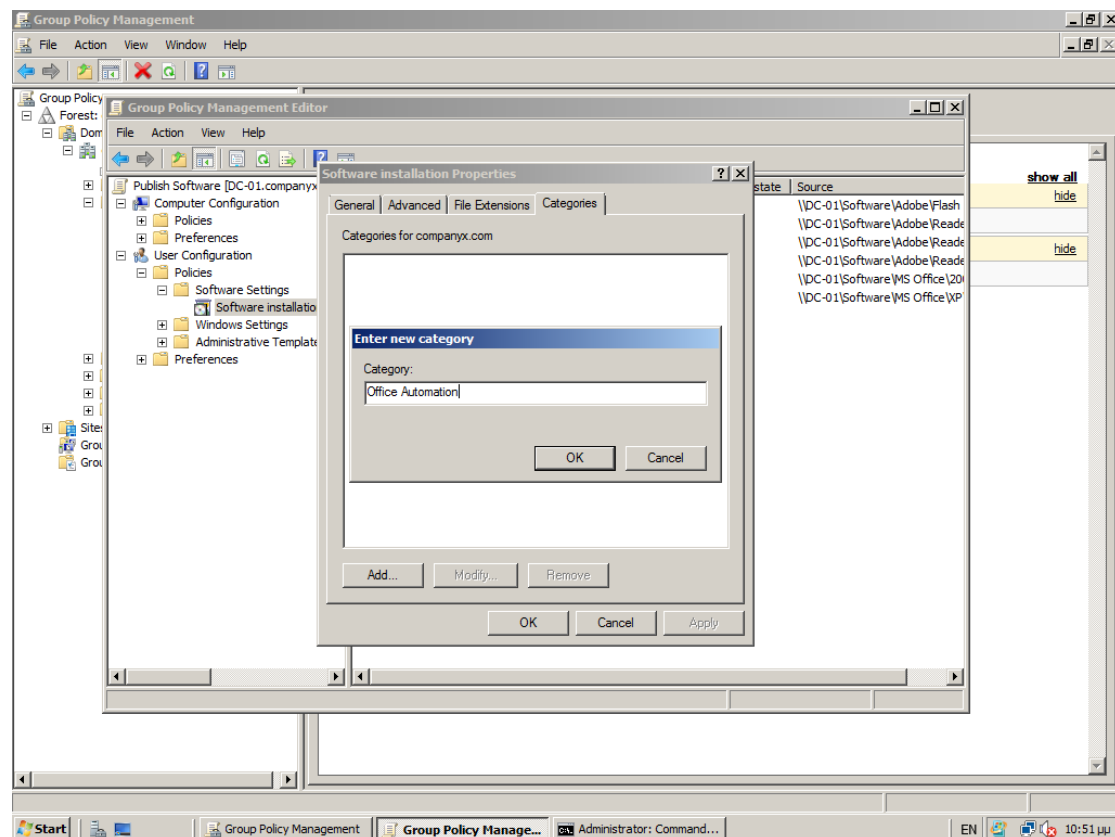
Μπορούμε να βελτιστοποιήσουμε την τελική εμπειρία των χρηστών (User Experience) παραμετροποιώντας κάποια χαρακτηριστικά της πολιτικής δημοσίευσης λογισμικών. Στο συγκεκριμένο σενάριο θα προσθέσουμε και θα χωρίσουμε τα δημοσιευμένα λογισμικά σε Κατηγορίες, διευκολύνοντας τους χρήστες στην επιλογή του λογισμικού που επιθυμούν να εγκαταστήσουν. Το χαρακτηριστικό αυτό είναι ιδιαίτερα χρήσιμο όταν το πλήθος των λογισμικών είναι μεγάλο.

- ☐ Εκκινούμε το πρόγραμμα επεξεργασίας Group Policy Management Editor για να επεξεργαστούμε την πολιτική δημοσίευσης λογισμικού
- ☐ Στο πρόγραμμα Group Policy Management Editor, κάτω από το container **User Configuration**, αναπτύσσουμε το container **Policies** και στη συνέχεια αναπτύσσουμε το container **Software Settings**. Κάνουμε **Δεξί κλικ** στο **Software Installation** και επιλέγουμε (κλικ) **Properties** (Εικ. 15.30)
- ☐ Στο νέο παράθυρο διαλόγου που ανοίγει **Software Installation Properties** επιλέγουμε την καρτέλα **Categories**
- ☐ Για να προσθέσουμε κατηγορία πατάμε το κουμπί **Add**



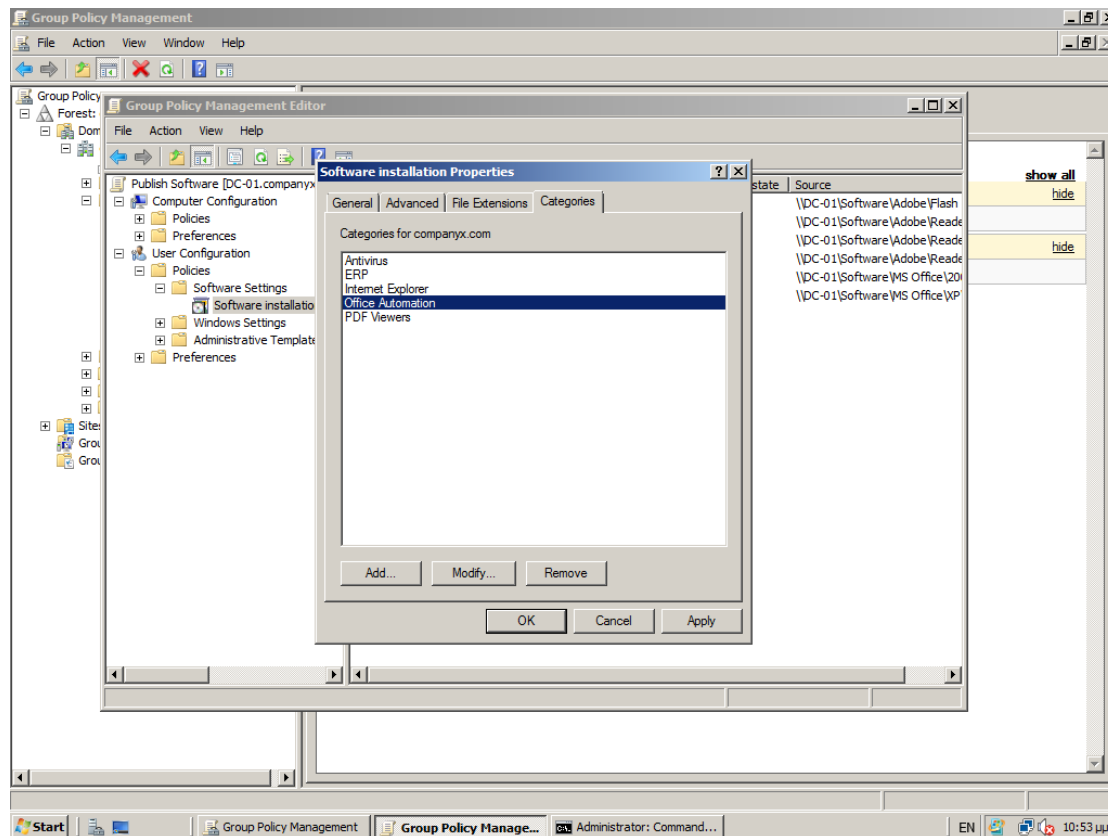
Εικ. 15.30. Software Installation Properties

- Στο επόμενο νέο παράθυρο διαλόγου **Enter new category** (Εικ. 15.31) πληκτρολογούμε το όνομα της νέας κατηγορίας και πατάμε **OK**



Εικ. 15. 31. Προσθέτοντας Κατηγορίες

□ Επαναλαμβάνουμε τα δύο προηγούμενα βήματα για να προσθέσουμε όσες κατηγορίες επιθυμούμε. Μπορούμε επίσης να επιλέξουμε κατηγορία και να αλλάξουμε το όνομά της (**Modify...**) ή να την αφαιρέσουμε (**Remove**). Όταν τελειώσουμε με τις κατηγορίες πατάμε **OK** (Εικ. 15.32)



Εικ. 15. 32. Διαχείριση Κατηγοριών

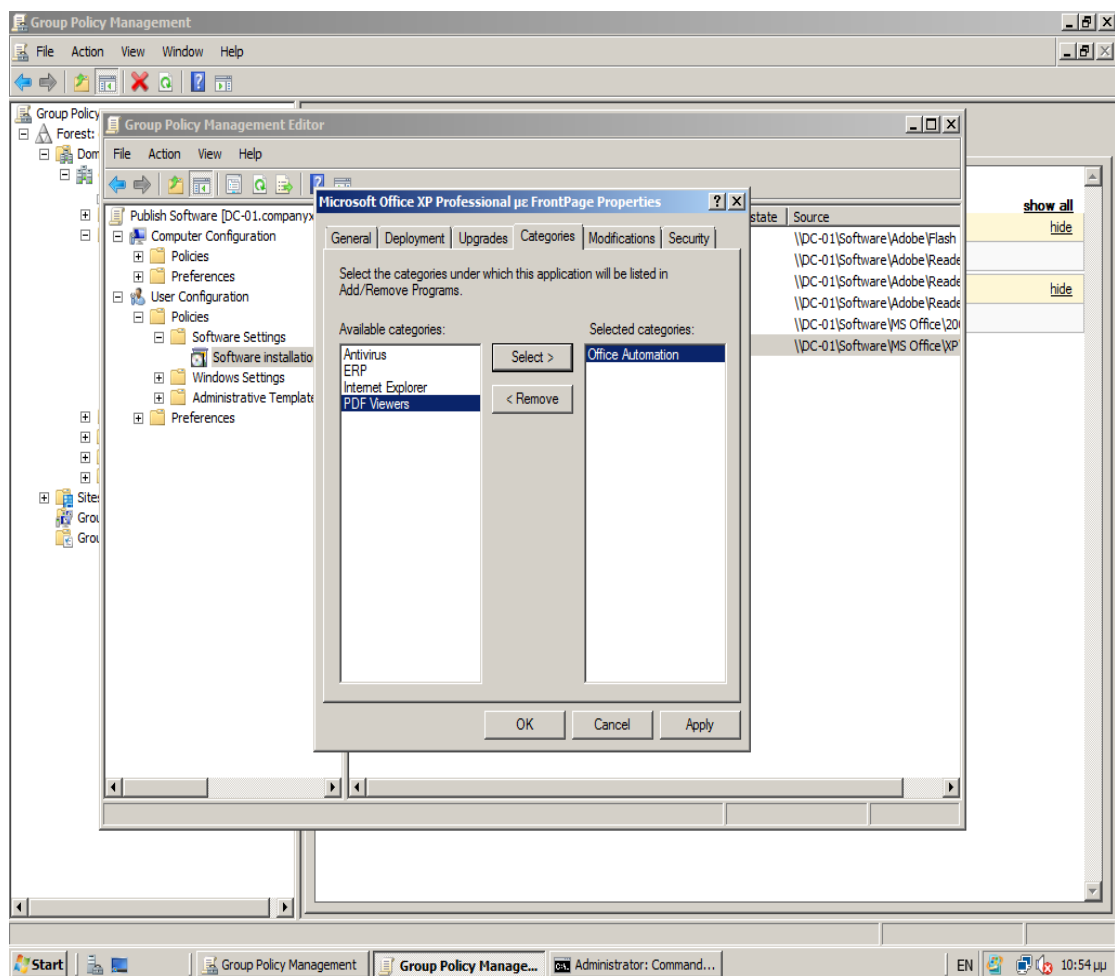
Η κατηγοριοποίηση των installation packages γίνεται αντιστοιχίζοντας ένα – ένα τα πακέτα στην κατηγορία(ες) που επιθυμούμε:

□ Εμφανίζουμε τις ιδιότητες του installation package επιλέγοντάς το και **Δεξί κλικ > Properties**

□ Επιλέγουμε την καρτέλα **Categories** (Εικ. 15.33)

✓ Στην αριστερή στήλη (Available categories) βρίσκονται οι διαθέσιμες κατηγορίες που προσθέσαμε προηγουμένως και στη δεξιά (Selected categories) οι κατηγορίες που θα επιλέγουμε για το συγκεκριμένο installation package

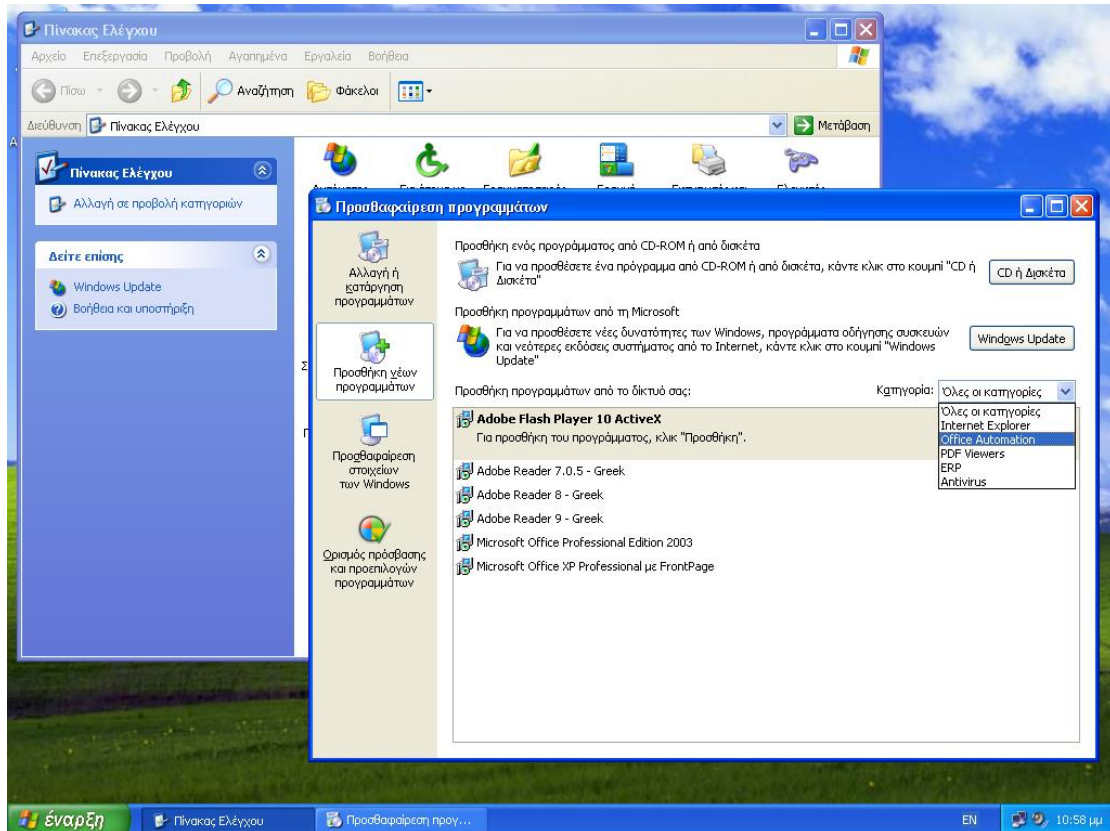
□ Για να επιλέξουμε μια κατηγορία από τα αριστερά κάνουμε **κλικ στο όνομά της** και στη συνέχεια πατάμε το κουμπί **Select**. Για να αφαιρέσουμε κατηγορία από τα δεξιά κάνουμε **κλικ στο όνομά της** και στη συνέχεια πατάμε το κουμπί **Remove**. Επαναλαμβάνουμε τα προηγούμενα τρία (3) βήματα για να κατηγοριοποιήσουμε κάθε installation package στην Group Policy.



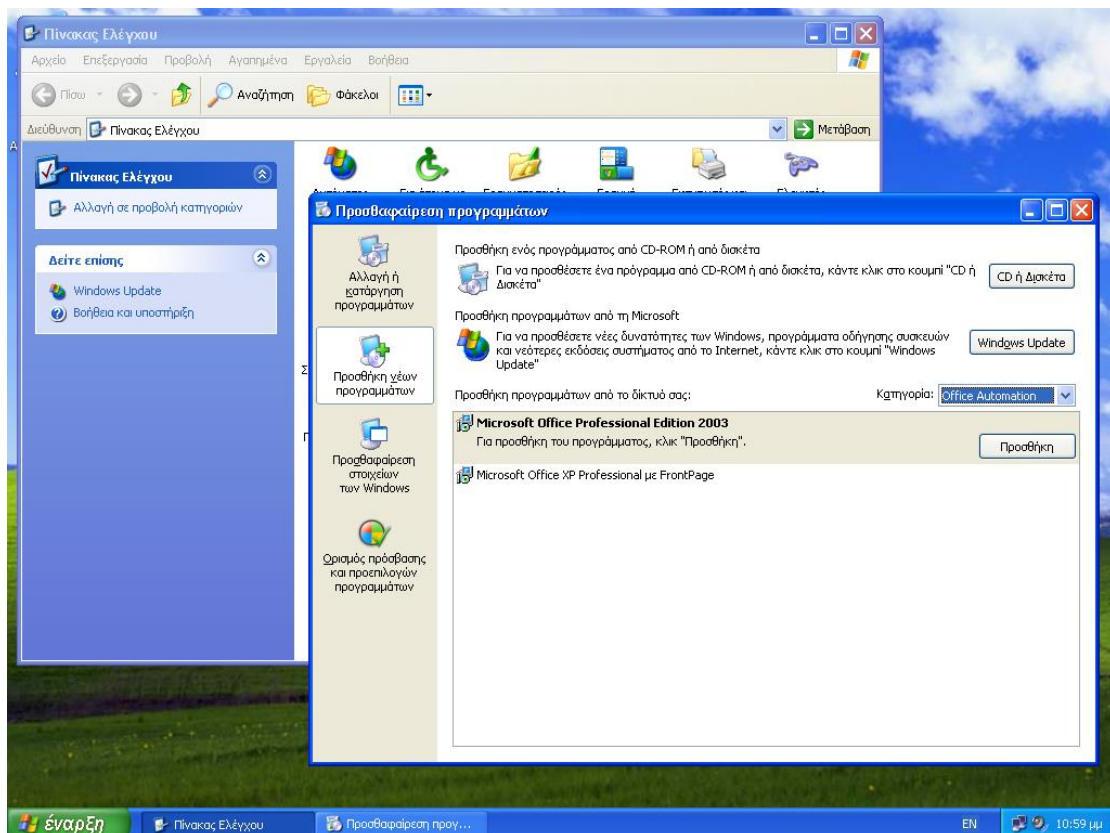
Εικ. 15. 33. Κατηγοριοποίηση Πακέτων Εγκατάστασης

15.6.2 Εγκατάσταση Δημοσιευμένου Λογισμικού (user-side)

Ανοίγουμε τον client H/Y και κάνουμε login με το λογαριασμό χρήστη του υπαλλήλου που τον χρησιμοποιεί. Ανοίγουμε στη συνέχεια τον **Πίνακα Ελέγχου** (Control Panel) και στη συνέχεια «τρέχουμε» την **Προσθαφαίρεση προγραμμάτων** (Add/Remove Programs). Στο παράθυρο που ανοίγει, στην αριστερή στήλη, κάνουμε κλικ στο κουμπί **Προσθήκη νέων προγραμμάτων** (Εικ. 15.34). Αμέσως εμφανίζονται σε λίστα τα λογισμικά τα οποία ο διαχειριστής έχει δημοσιεύσει στο Active Directory και είναι διαθέσιμα για on demand εγκατάσταση (**Προσθήκη προγραμμάτων από το δίκτυό σας**). Αναπτύσσοντας το πτυσσόμενο μενού **Κατηγορίες** μπορούμε να επιλέξουμε από τις κατηγορίες των λογισμικών που προσθέσαμε / αντιστοιχίσαμε στην παράγραφο 15.6.1. Επιλέγοντας κατηγορία η λίστα των δημοσιευμένων λογισμικών φιλτράρεται ως προς αυτή (Εικ. 15.35). Για να εγκαταστήσουμε το λογισμικό που επιθυμούμε κάνουμε κλικ στο κουμπί **Προσθήκη** ώστε να εκκινήσει η διαδικασία εγκατάστασης.



Εικ. 15. 34. Πίνακας Ελέγχου



Εικ. 15. 35. Φιλτράρισμα ως προς κατηγορία

WINDOWS DEPLOYMENT SERVICES

16.1 Εισαγωγή

Ο ρόλος των Windows Deployment Services (WDS) στα Windows Server 2008 είναι η ανανεωμένη και ξανασχεδιασμένη έκδοση των Remote Installation Services (RIS). Με το ρόλο Windows Deployment Services μπορείτε να εγκαταστήσετε λειτουργικά συστήματα Windows, ιδιαίτερα Windows Vista, Windows 7 και Windows 2008. Μπορείτε να τον χρησιμοποιήσετε για να εγκαταστήσετε καινούριους H/Y με τη χρήση δικτυακής εγκατάστασης. Αυτό σημαίνει πως δεν απαιτείται (κατά την εγκατάσταση), ούτε η φυσική σας παρουσία σε κάθε H/Y, ούτε η χρήση μέσου εγκατάστασης (CD ή DVD). Τα στοιχεία που αποτελούν τα Windows Deployment Services ανήκουν στις ακόλουθες τρεις κατηγορίες:

- **Στοιχεία Server.** Αυτά τα στοιχεία περιλαμβάνουν έναν PXE (Pre-Boot Execution Environment) server και έναν TFTP (Trivial File Transfer Protocol) server για να εκκινήσετε ένα client από το δίκτυο (network boot) και να εγκαταστήσετε ένα λειτουργικό σύστημα. Επίσης περιλαμβάνουν ένα κοινόχρηστο φάκελο και αποθήκη εικόνων που περιέχει εικόνες εκκίνησης (boot images), εικόνες εγκατάστασης (install images) και αρχεία που χρειάζεστε ειδικά για την εκκίνηση από το δίκτυο. Υπάρχει επίσης ένα στοιχείο δικτυακού επιπέδου, ένα στοιχείο multicast και ένα διαγνωστικό στοιχείο.
- **Στοιχεία Client.** Αυτά τα στοιχεία περιλαμβάνουν ένα γραφικό περιβάλλον που τρέχει μέσα στο Windows Pre-Installation Environment (Windows PE). Όταν ένας χρήστης επιλέξει μία εικόνα λειτουργικού συστήματος τότε τα στοιχεία client επικοινωνούν με τα στοιχεία server για να γίνει η συγκεκριμένη εγκατάσταση.
- **Στοιχεία Management.** Αυτά τα στοιχεία αποτελούν ένα σετ εργαλείων που θα χρησιμοποιήσετε για να διαχειριστείτε το server, τις εικόνες λειτουργικού συστήματος και τους λογαριασμούς των client H/Y.

16.2 Διαφορές μεταξύ WDS και RIS

Τα Windows Deployment Services για Windows Server 2008 περιλαμβάνουν πολλές μετατροπές σε σχέση με τα χαρακτηριστικά των RIS. Υπάρχουν ακόμα μετατροπές και σε σχέση με τα Windows Deployment Services για Windows Server 2003. Ο πίνακας που ακολουθεί συνοψίζει αυτές τις διαφορές:

Αλλαγές από τα RIS	Αλλαγές από τα WDS σε Windows Server 2003
<ul style="list-style-type: none"> • Δυνατότητα εγκατάστασης Windows Vista, 7 και Server 2008 • Το λειτουργικό σύστημα εκκίνησης είναι πλέον το Windows PE • Εγκατάσταση βάσει εικόνας λειτουργικού συστήματος με τη χρήση αρχείων Windows image (.wim) • Δυνατότητα αποστολής δεδομένων και εικόνων μέσω multicast • Δυνατότητα αποστολής δεδομένων και εικόνων μέσω multicast σε standalone server (όταν εγκαταστήσετε τον Transport Server). • Το στοιχείο server PXE είναι επεκτάσιμο και αποδοτικότερο. • Νέο γραφικό περιβάλλον εγκατάστασης στον client • MMC κονσόλα διαχείρισης των Windows Deployment Services στο server για να διαχειρίζεστε όλα τα χαρακτηριστικά 	<ul style="list-style-type: none"> • Δυνατότητα αποστολής δεδομένων και εικόνων μέσω multicast • Δυνατότητα αποστολής δεδομένων και εικόνων μέσω multicast σε standalone server (όταν εγκαταστήσετε τον Transport Server). • Δεν υποστηρίζονται πλέον οι εικόνες RISEUP και οι οθόνες OSChooser. • Βελτιωμένος TFTP server. • Υποστήριξη δικτυακής εκκίνησης σε 64-bit H/Y με EFI (Extensible Firmware Interface). • Αναφορές εγκαταστάσεων

Πλεονεκτήματα

Τα Windows Deployment Services παρέχουν τα ακόλουθα πλεονεκτήματα:

- Μειώνουν την πολυπλοκότητα των εγκαταστάσεων και τα κόστη που σχετίζονται με τις ανεπαρκείς χειροκίνητες διαδικασίες.
- Επιτρέπουν τη δικτυακή εγκατάσταση λειτουργικών συστημάτων όπως Windows Vista, Windows 7 και Windows Server 2008.
- Εγκαθιστούν εικόνες των Windows σε H/Y χωρίς λειτουργικά συστήματα.
- Υποστηρίζουν μικτά περιβάλλοντα που περιλαμβάνουν Windows Vista, Windows 7, Windows Server 2008, Windows XP και Windows Server 2003.

- Παρέχουν μία όλα-σε-ένα, ολοκληρωμένη λύση ανάπτυξης λειτουργικών συστημάτων σε Η/Υ και servers.
- Χρησιμοποιούν τεχνολογίες εγκατάστασης των Windows Server 2008, συμπεριλαμβάνοντας Windows PE, αρχεία .wim και εγκατάσταση βάσει εικόνας συστήματος.

Αναβάθμιση από server με RIS και Windows Server 2003 SP1 ή SP2

Υπάρχουν δύο μέθοδοι για να μεταφέρετε μία υπάρχουσα υποδομή RIS σε WDS. Αυτή η ενότητα περιγράφει την πρώτη μέθοδο.

Μέθοδος 1: Αναβάθμιση των RIS servers	Μέθοδος 2: Εγκατάσταση των WDS σε νέους servers
<p>Με αυτή τη μέθοδο εγκαθιστάτε τα WDS στους υπάρχοντες RIS servers σας. Οι τρεις τρόποι λειτουργίας του server και η δυνατότητα να μετατρέπετε RIPREP εικόνες σας επιτρέπει την ομαλή μετάβαση από RIS σε WDS. Αυτή είναι και η προτεινόμενη μέθοδος.</p>	<p>Με αυτή τη μέθοδο εγκαθιστάτε WDS σε νέους servers στο περιβάλλον σας συνεχίζοντας ταυτόχρονα να διατηρείτε τους υπάρχοντες RIS servers. Στο τέλος, μετά την ολοκληρωτική μετάβαση σε WDS, οι RIS servers αποσύρονται. Αυτή η μέθοδος δεν προτείνεται διότι απαιτεί επιπρόσθετο hardware και διαχειριστικό κόστος.</p> <ul style="list-style-type: none"> • Hardware. Κάθε νέα εγκατάσταση WDS τρέχει σε ξεχωριστό server από τα RIS • Διαχειριστικό κόστος. Το να διατηρείς δύο PXE servers με διαφορετικές ρυθμίσεις στο ίδιο δίκτυο μπορεί να οδηγήσει σε απρόβλεπτα αποτελέσματα. Γενικά, για να μπορέσει αυτό το σενάριο να είναι προβλέψιμο θα πρέπει να κάνετε prestage κάθε Η/Υ και να ορίσετε αν το κάθε client θα απαντάται ή όχι από τον WDS server ή τον RIS server.

Υπάρχουν τρεις τρόποι λειτουργίας των Windows Deployment Services για Windows Server 2003: **Legacy**, **Mixed** και **Native**. Ο server σας πρέπει να είναι σε Native τρόπο λειτουργίας για να τον αναβαθμίσετε σε Windows Server 2008. Η αναβάθμισή σας θα σταματήσει αν έχετε ρυθμίσει τα RIS ή αν ο server σας είναι σε λειτουργία Legacy ή Mixed. Για να δείτε σε ποια λειτουργία βρίσκεται εκείνη τη στιγμή ο server εκτελέστε την εντολή **WDSUTIL /get-server /show:config**.

Ακολουθούν διάφορα σενάρια ανάλογα με την περίπτωση:

- Αν τρέχετε RIS στο server σας αλλά δεν έχετε εγκαταστήσει WDS, πρέπει να τα εγκαταστήσετε πριν αναβαθμίσετε. Τα Windows Deployment Services περιλαμβάνονται στο Windows AIK και στο Service Pack 2 των Windows Server 2003. Στη συνέχεια χρησιμοποιείτε τις ακόλουθες διαδικασίες για να αλλάξετε από Legacy mode (default ρύθμιση) σε Native mode.
- Αν τα RIS ήταν εγκατεστημένα στο server όταν εγκαταστήσατε τα WDS, τότε θα είναι είτε σε Legacy είτε σε Mixed mode - θα χρειαστεί να το αλλάξετε σε Native mode πριν αναβαθμίσετε.
- Αν τα RIS **δεν** ήταν εγκατεστημένα στο server όταν εγκαταστήσατε τα WDS, τότε θα είναι σε Native mode και επομένως έτοιμος για αναβάθμιση σε Windows Server 2008.

Για να αλλάξετε τον τρόπο λειτουργίας του server σε Native χρησιμοποιείτε μία από τις παρακάτω διαδικασίες:

Από Legacy σε Mixed

- Αρχικοποιείτε (Initialize) το server με έναν από τους ακόλουθους τρόπους:
 - ✓ **Χρήση κονσόλας MMC.** Στο μενού **Start**, κάντε κλικ στο **Administrative Tools** και μετά κλικ στο **Windows Deployment Services**. Δεξί κλικ στο όνομα του server και στη συνέχεια επιλέξτε **Initialize Server**.
 - ✓ **Χρήση εντολής WDSUTIL.** Εκτελέστε την εντολή **WDSUTIL /Initialize-Server /RemInst:C:\RemoteInstall** (με την προϋπόθεση πως το C:\RemoteInstall είναι η τοποθεσία του κοινόχρηστου φακέλου REMINST).
- Όταν η διαδικασία ολοκληρωθεί χρησιμοποιείτε την ακόλουθη διαδικασία για να αλλάξετε τον τρόπο λειτουργίας του server από Mixed σε Native.

Από Mixed σε Native

- Αποσύρατε τις εικόνες σας RISEUP και RIPRPEP, ή μετατρέψτε τις σε .wim format. Για να τις αποσύρετε απλά διαγράψτε τις. Αν θέλετε να τις μετατρέψετε έχετε

δύο επιλογές:

- ✓ Offline μετατροπή (μόνο για εικόνες RIPREP)
- ✓ Αναπτύξτε τις και κάντε τις capture με τον image capture wizard (εικόνες RIPREP και RISEUP). Περισσότερες πληροφορίες στη ενότητα *, σελίδα *
- Εκτελέστε την εντολή **WDSUTIL /Set-Server /ForceNative**
- Όταν η διαδικασία ολοκληρωθεί ο server είναι έτοιμος να αναβαθμιστεί σε Windows Server 2008.

16.3 Εγκατάσταση Windows Deployment Services

16.3.1 Προαπαιτούμενα Στοιχεία

Ο πίνακας που ακολουθεί εμφανίζει τις απαιτήσεις που θα πρέπει να προηγηθούν της εγκατάστασης του ρόλου Windows Deployment Services, ανάλογα με το αν επιλέξετε (κατά την εγκατάσταση) τον Deployment server ή τον Transport server:

Deployment Server	Transport Server
<ul style="list-style-type: none"> • AD DS. Ένας WDS server πρέπει είτε να είναι μέλος ενός AD DS domain είτε να είναι ο ίδιος domain controller ενός AD DS domain. Οι εκδόσεις των domain και forest δεν παίζουν κανένα ρόλο - όλα τα domain και forest υποστηρίζουν WDS • DHCP. Πριν εγκαταστήσετε τα WDS θα πρέπει να έχετε στο δίκτυό σας έναν DHCP server σε λειτουργία διότι το PXE των WDS βασίζεται στο DHCP για τη διευθέτηση IP • DNS. Πριν τρέξετε τα WDS θα πρέπει να έχετε στο δίκτυό σας έναν DNS server σε λειτουργία 	<ul style="list-style-type: none"> • Δικαιώματα. Για την εγκατάσταση του ρόλου θα πρέπει να είστε μέλος της ομάδας των Local Administrators του server

<ul style="list-style-type: none"> • NTFS Volume. Ο server που εκτελεί τα WDS χρειάζεται ο δίσκος όπου θα αποθηκεύει τα images να είναι σε σύστημα αρχείων NTFS • Δικαιώματα. Για την εγκατάσταση του ρόλου θα πρέπει να είστε μέλος της ομάδας των Local Administrators του server 	
---	--

16.3.2 Διαδικασία Εγκατάστασης Windows Deployment Services

Μπορείτε να εγκαταστήσετε τα Windows Deployment Services χρησιμοποιώντας είτε τον Initial Configuration Wizard, είτε τον Server Manager, είτε τη γραμμή εντολών:

- Για να εγκαταστήσετε το ρόλο με το Initial Configuration Wizard, κάντε κλικ στο **Add Roles** στην οθόνη εκκίνησης **Initial Configuration Tasks**. Στη συνέχεια πατήστε **Next** και μετά επιλέξτε **Windows Deployment Services**.

- Για να εγκαταστήσετε το ρόλο με το Server Manager (Εικ. 16.1), κάντε κλικ στο **Add Roles** που βρίσκεται στο παράθυρο εργασιών **Roles Summary** (Εικ. 16.2). Στη συνέχεια κάντε κλικ στο **Next** και επιλέξτε **Windows Deployment Services**. (Εικ. 16.3)

- Για να εγκαταστήσετε το ρόλο από τη γραμμή εντολών, εκτελέστε μία από τις ακόλουθες εντολές:

- ✓ Για τον Deployment Server, **ServerManagerCmd -install WDS**.

- ✓ Για τον Transport Server, **ServerManagerCmd -install WDS-Transport**

Κατά τη διάρκεια της εγκατάστασης έχετε να επιλέξετε μεταξύ των δύο ακόλουθων υπηρεσιών (Εικ. 16.4):

- ✓ **Transport Server.** Για να εγκαταστήσετε αυτή την επιλογή, αποσεκάρτε την επιλογή **Deployment Server** στη δεύτερη οθόνη του οδηγού εγκατάστασης. Αυτή η επιλογή παρέχει ένα υποσύνολο των λειτουργιών των Windows Deployment Services. Περιέχει μόνο τα βασικά δικτυακά μέρη.. Μπορείτε να χρησιμοποιήσετε τον Transport Server για να δημιουργήσετε δίκτυα multicast για την αποστολή δεδομένων (συμπ. εικόνων λειτουργικών συστημάτων) από ένα standalone server. Η χρήση της

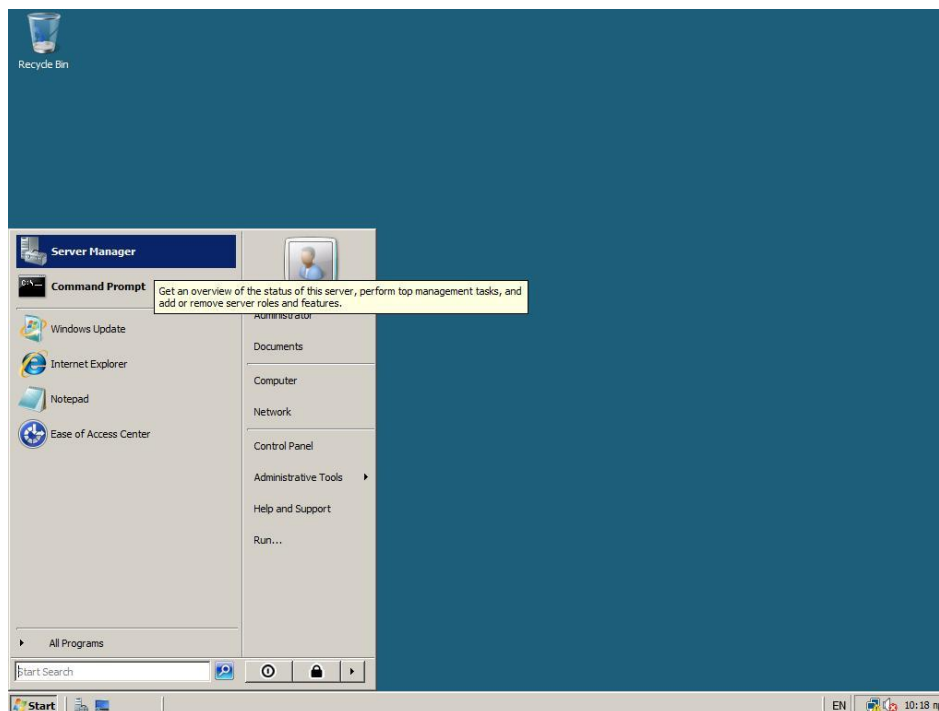
επιλογής ενδείκνυται μόνο για multicasting χωρίς όμως την εμπλοκή όλων των υπηρεσιών WDS.

✓ **Deployment Server.** Για να εγκαταστήσετε αυτή την επιλογή, βεβαιωθείτε πως και ο **Deployment Server** και ο **Transport Server** είναι επιλεγμένοι στη δεύτερη οθόνη του οδηγού εγκατάστασης. Αυτή η επιλογή παρέχει πλήρη λειτουργικότητα των Windows Deployment Services ώστε να τις ρυθμίσετε για εγκαταστήσετε απομακρυσμένα λειτουργικά συστήματα Windows. Σημειώστε ότι ο Deployment Server εξαρτάται από τα βασικά μέρη του Transport Server.

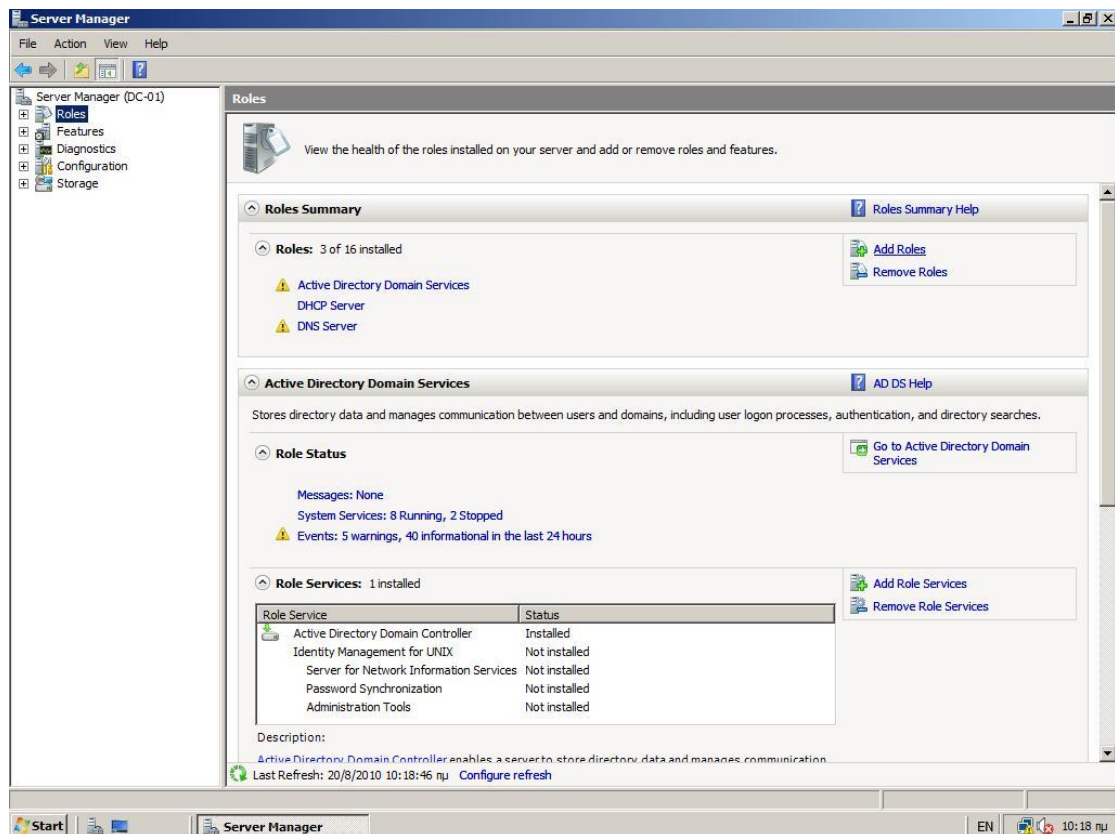
Σημείωση

Αν επιθυμείτε να διαχειριστείτε τα Windows Deployment Services σε ένα απομακρυσμένο server που εκτελεί Windows Server 2008, μπορείτε να εγκαταστήσετε τα Remote Server Administration Tools. Για να το κάνετε αυτό ανοίξτε το Server Manager, κάντε δεξί κλικ στο κόμβο **Features** (αριστερά του παραθύρου) και μετά κλικ στο **Add Features**. Στο παράθυρο που ανοίγει εντοπίστε και επιλέξτε το **Remote Server Administration Tools**. Με τον τρόπο αυτό θα εγκαταστήσετε WDSUTIL και κονσόλα διαχείρισης Windows Deployment Services (MMC) στο server.

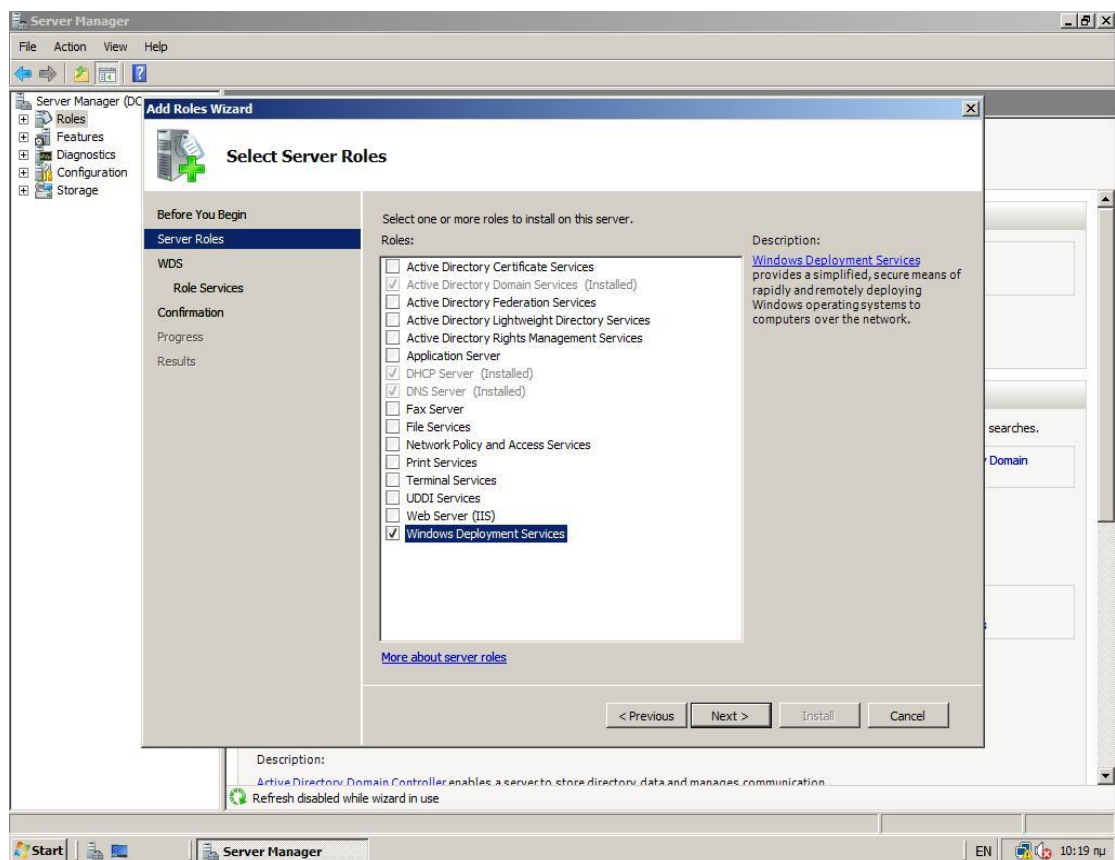
Οι εικόνες που ακολουθούν δείχνουν την εγκατάσταση του ρόλου με χρήση του Server Manager:



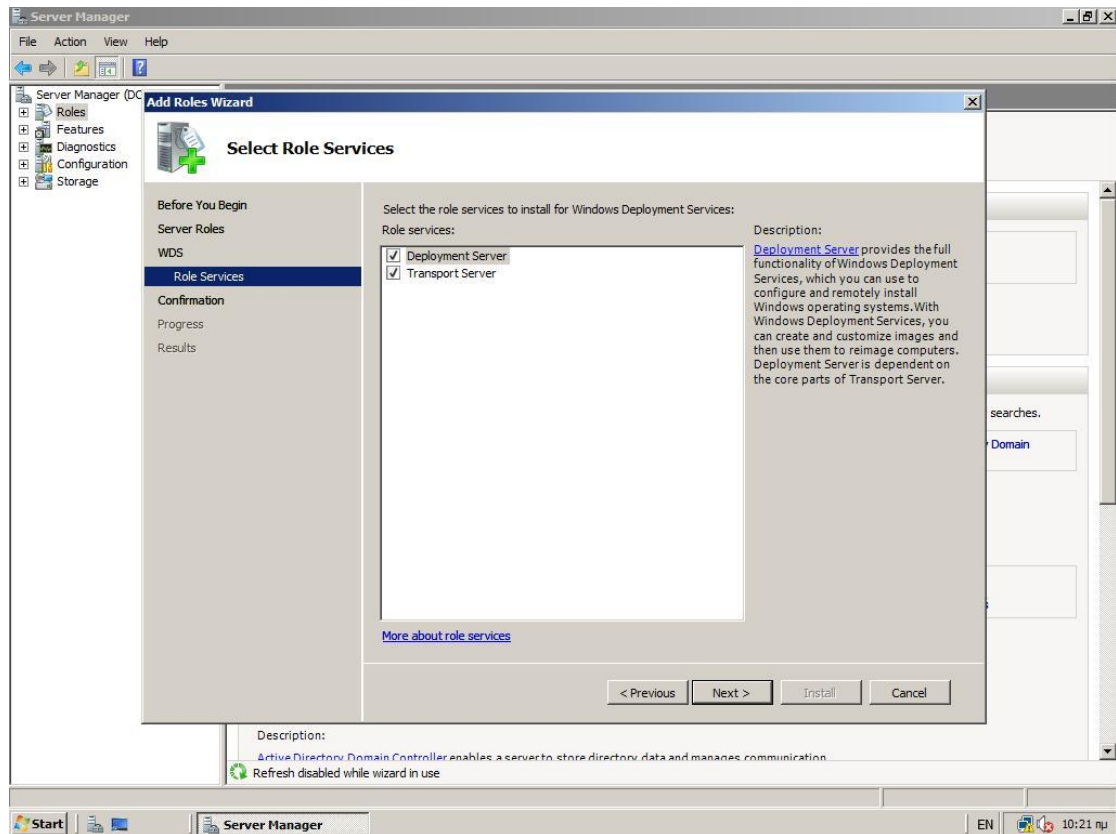
Εικ. 16.1



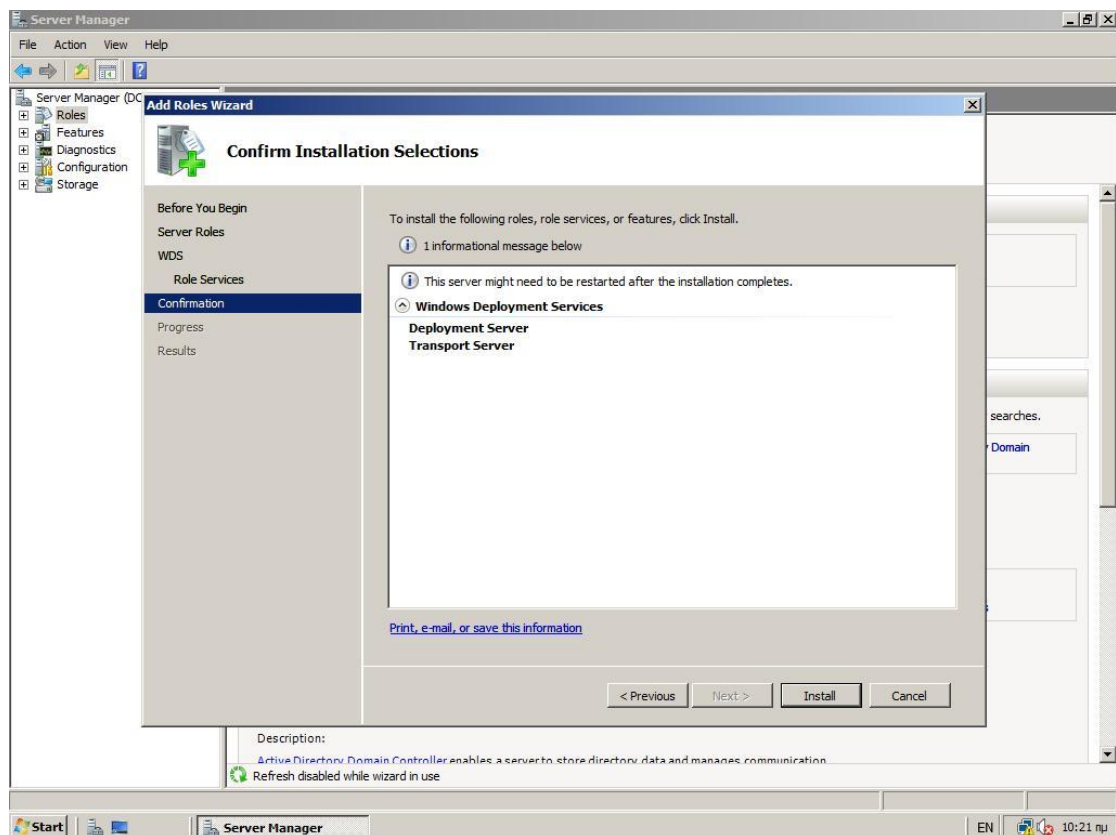
Εικ. 16.2



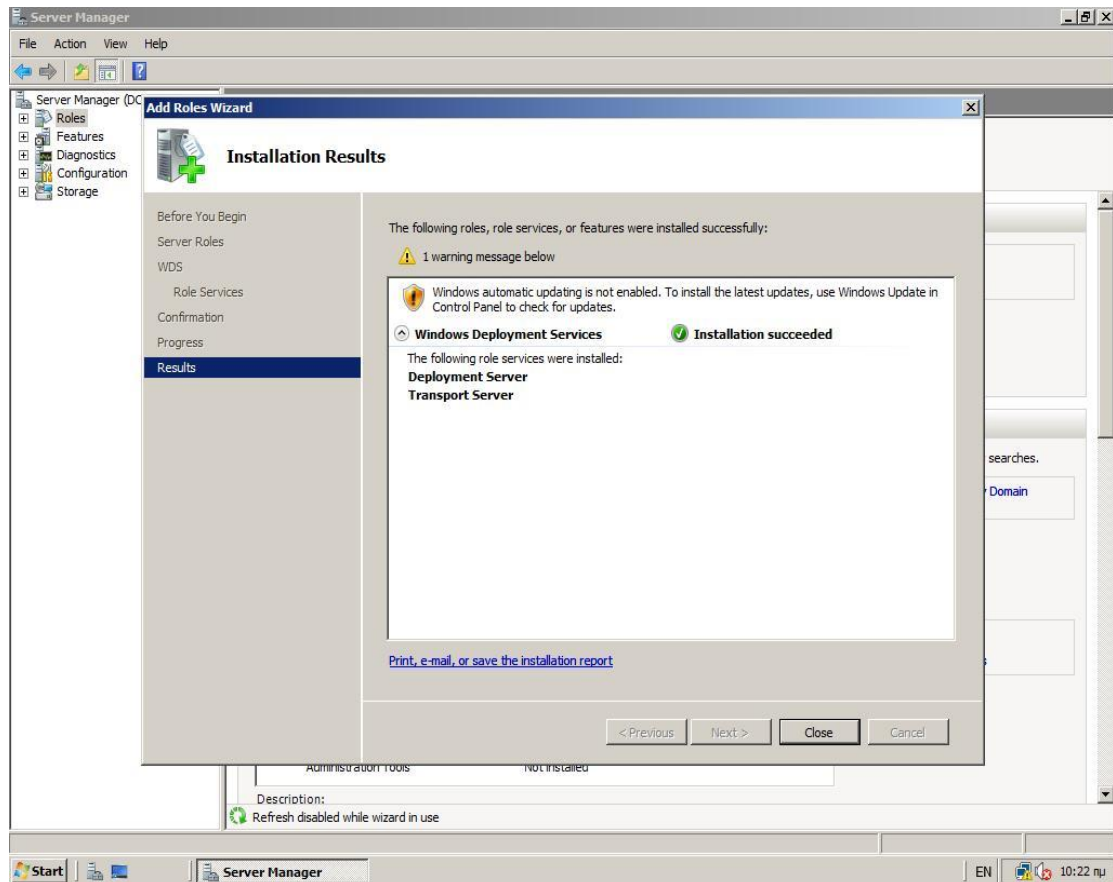
Εικ. 16.3



Εικ. 16.4



Εικ. 16.5



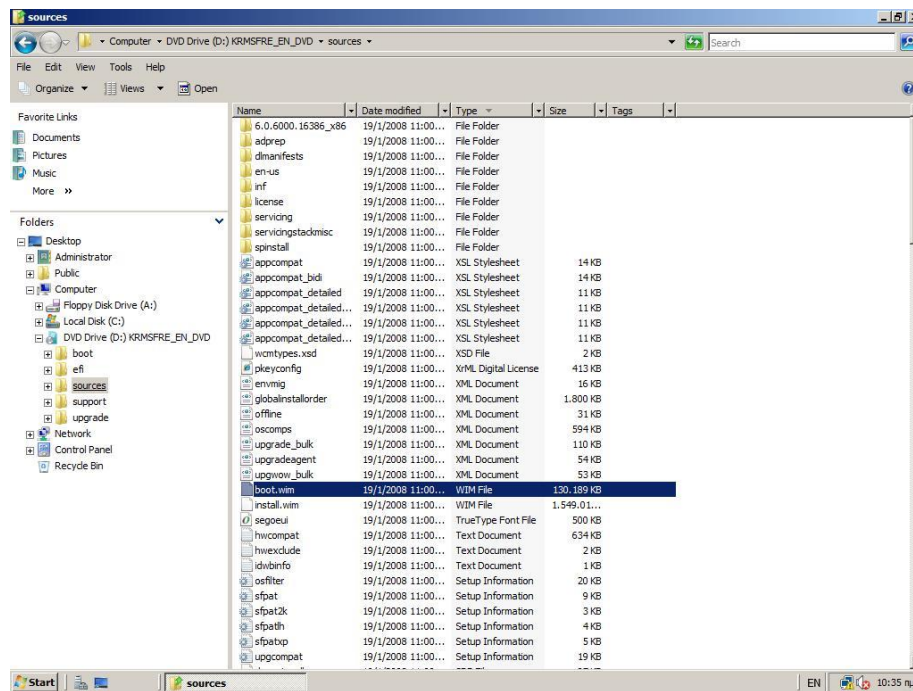
Εικ. 16.6

16.4 Παραμετροποίηση Windows Deployment Services

Μετά τη εγκατάσταση του ρόλου πρέπει να ρυθμίσετε τα Windows Deployment Services χρησιμοποιώντας είτε την κονσόλα MMC είτε την εντολή WDSUTIL (για βοήθεια σχετικά με την εν λόγω εντολή και τον τρόπο σύνταξής της πληκτρολογήστε **WDSUTIL /?** σε γραμμή εντολών (command prompt) ή online στη Microsoft κάτω από την λέξη κλειδί WDSUTIL.

Κατά την παραμετροποίηση του server σας πρέπει να λάβετε υπόψη σας τα παρακάτω θέματα:

- Στις περισσότερες των περιπτώσεων χρησιμοποιήστε τη standard εικόνα εκκίνησης (boot image) που περιέχεται στο DVD των Windows Server 2008 (στο φάκελο \Sources\boot.wim) χωρίς τροποποιήσεις (Εικ. 16.7).
- Αν τρέχετε Windows Deployment Services και έναν όχι-της-Microsoft DHCP Server στον ίδιο υπολογιστή, επιπρόσθετα της ρύθμισης του server να μην κάνει listen στην πόρτα 67, θα χρειαστεί να χρησιμοποιήσετε τα εργαλεία σας DHCP για να προσθέσετε την επιλογή Option 60 στα DHCP scopes που διαθέτετε.



Εικ. 16.7

- Αν το DHCP είναι εγκατεστημένο σε ένα server που βρίσκεται σε διαφορετικό δίκτυο (subnet) θα χρειαστεί να κάνετε μία από τις ακόλουθες ενέργειες:

✓ (Προτεινόμενη) Ρυθμίστε τους πίνακες IP Helper. Όλες οι εκπομπές DHCP που γίνονται από τους client υπολογιστές στην πόρτα UDP 67 θα πρέπει να προωθούνται απευθείας και στον DHCP server και στον Windows Deployment Services PXE server. Επίσης όλη η κίνηση στην πόρτα UDP 4011 από τους client υπολογιστές στον Windows Deployment Services PXE server πρέπει να δρομολογείται κατάλληλα (αυτές οι αιτήσεις δρομολογούν την κίνηση (traffic), και όχι τις εκπομπές (broadcasts), στο server).

- ✓ Προσθέστε τις DHCP επιλογές 66 και 67.

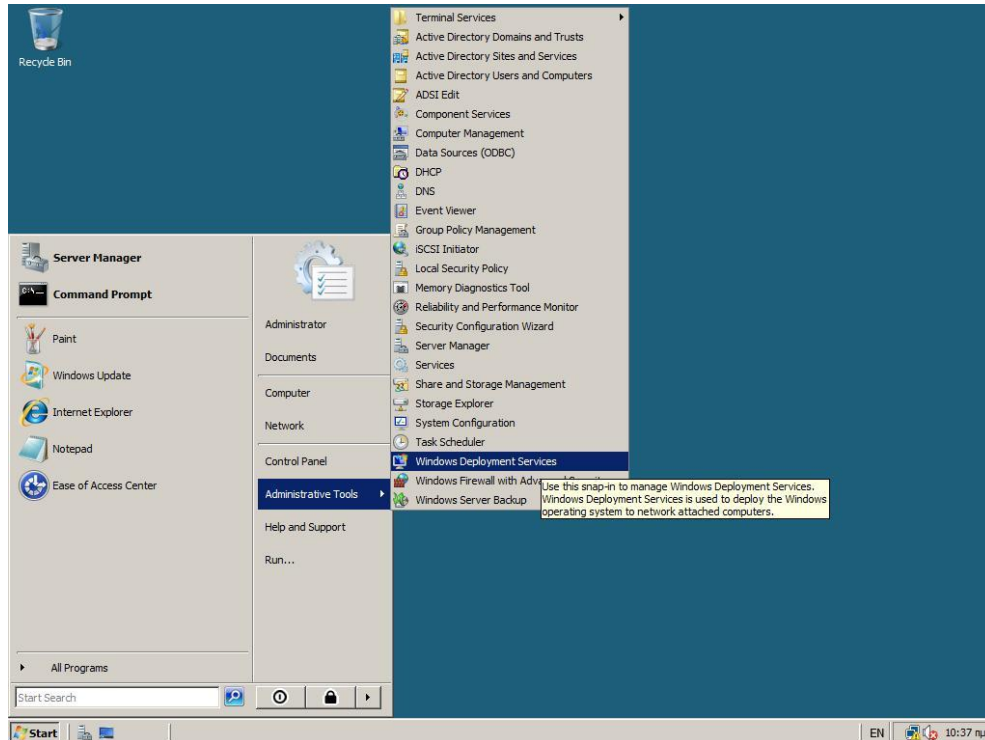
16.4.1 Διαδικασία Ρύθμισης Windows Deployment Services

Για να ρυθμίσετε το ρόλο Windows Deployment Services ακολουθείστε την παρακάτω διαδικασία:

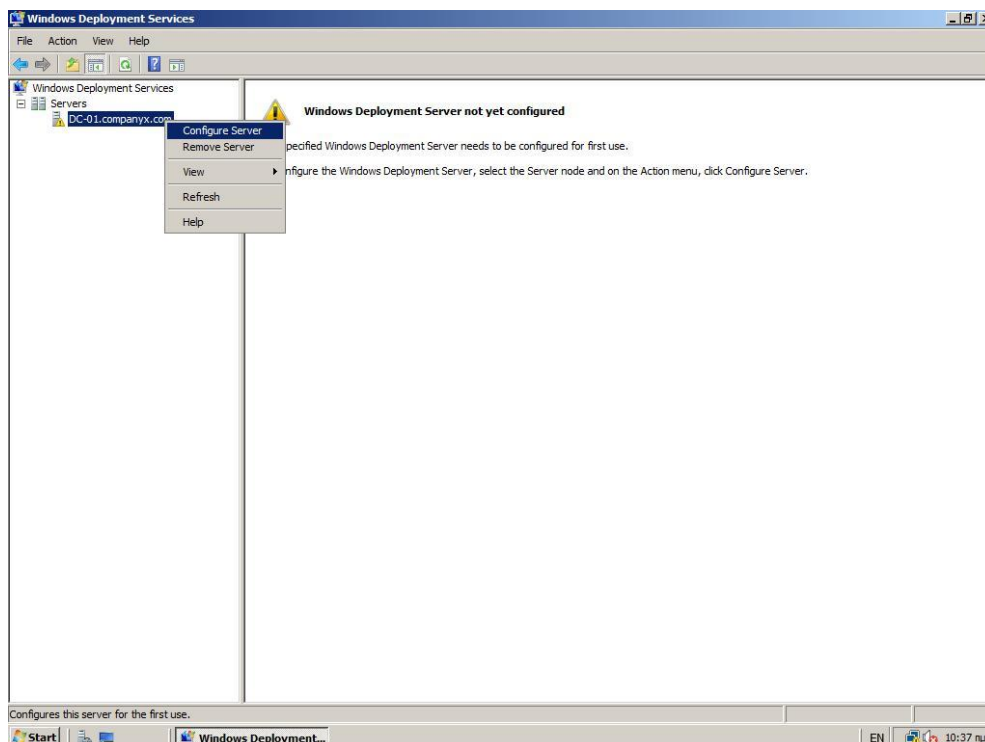
1. Βεβαιωθείτε πως είστε Domain Administrator
2. Κάντε κλικ στο **Start**, μετά **Administrative Tools** και στη συνέχεια κλικ στο **Windows Deployment Services** (Εικ. 16.8)
3. Στο αριστερό τμήμα της κονσόλας Windows Deployment Services αναπτύξτε τη λίστα των servers
4. Κάντε δεξί κλικ στο server και στη συνέχεια κλικ στο **Configure Server** (Εικ. 16.9)

5. Ακολουθείστε τις οδηγίες στον οδηγό διαμόρφωσης (Εικόνες 10 - 13)
6. Όταν η διαμόρφωση ολοκληρωθεί αποτσεκάρετε την επιλογή **Add images to Windows Deployment Services now** και κάντε κλικ στο **Finish** (Εικ. 16.14)

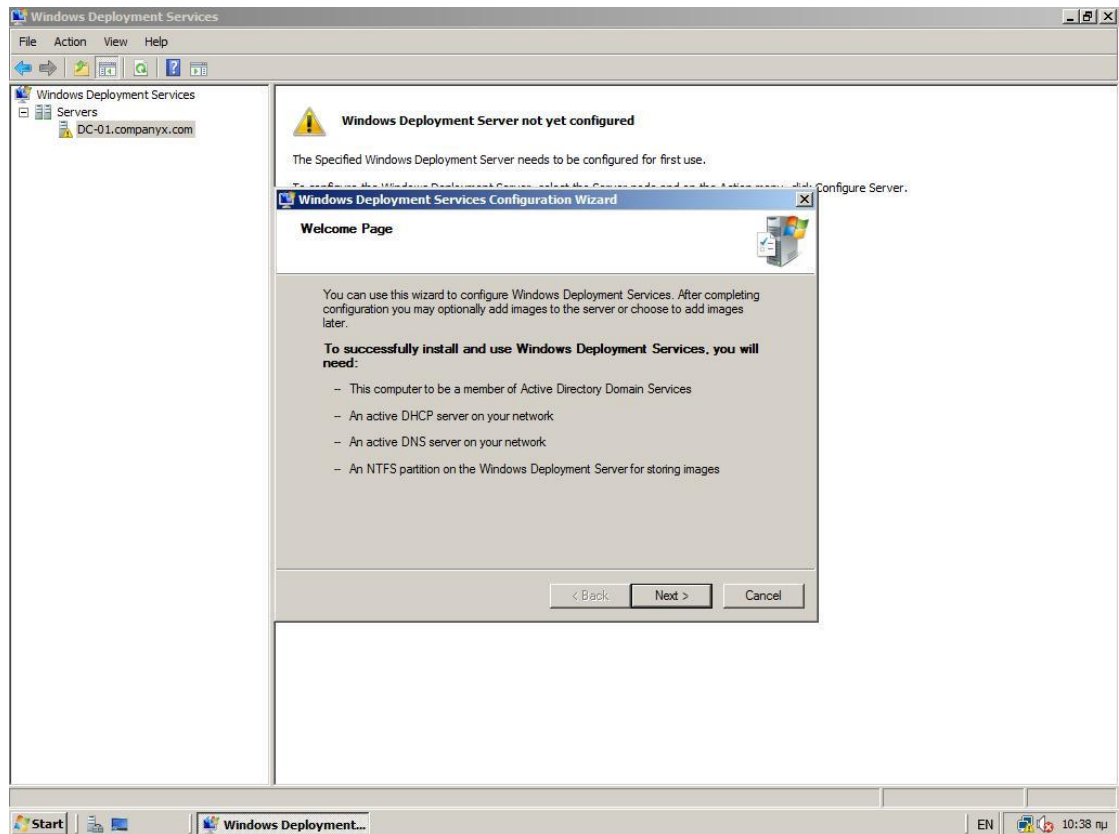
Ακολουθούν οι εικόνες εγκατάστασης:



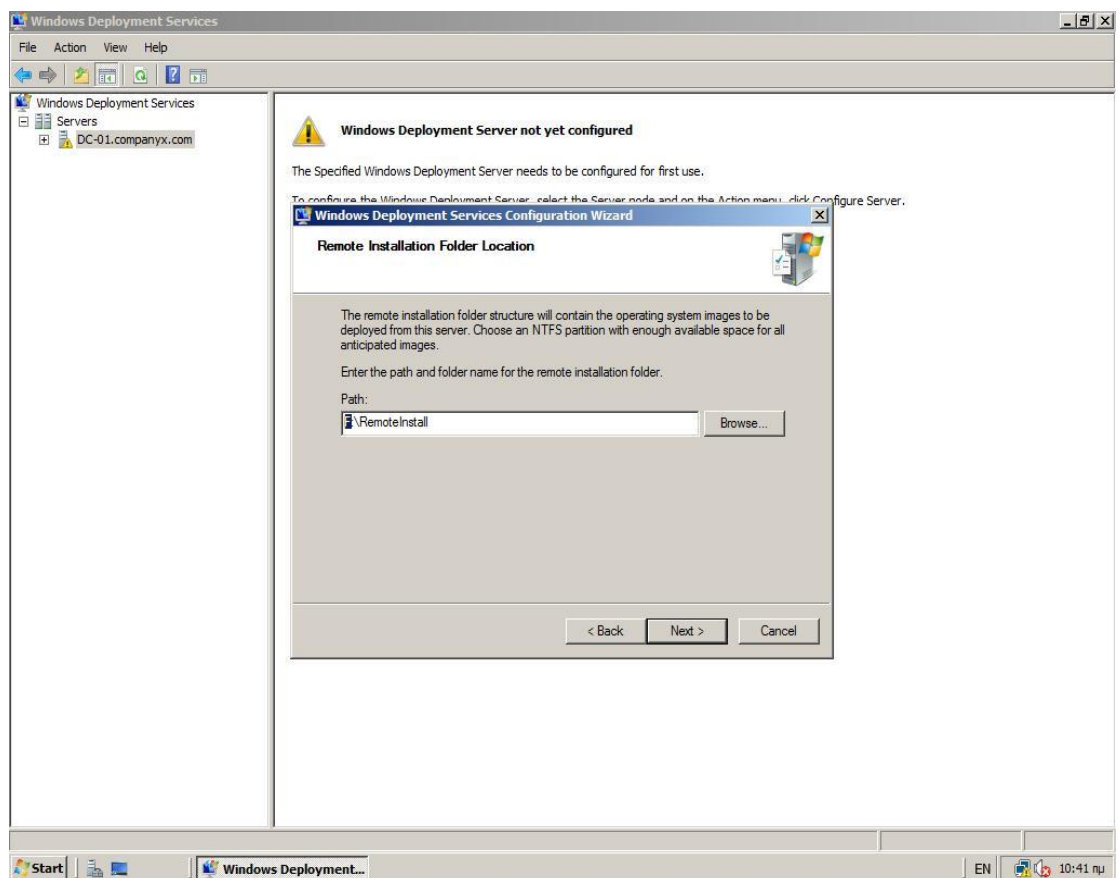
Εικ. 16.8



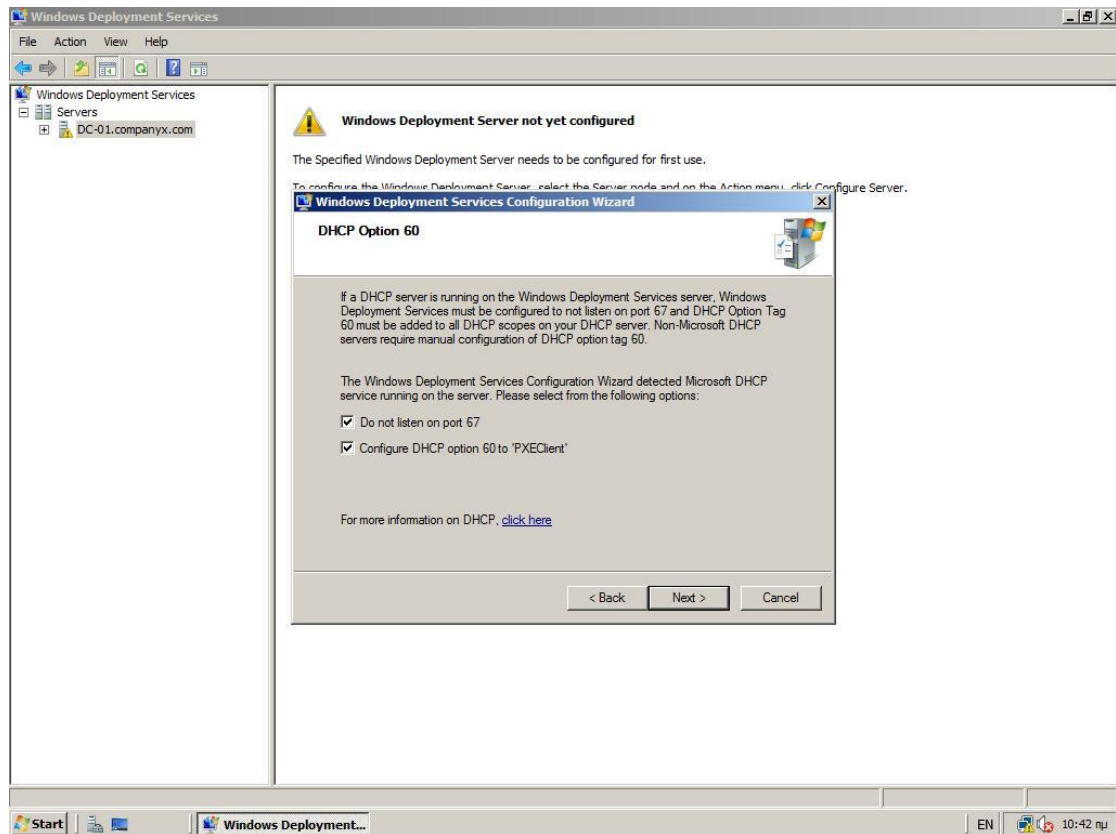
Εικ. 16.9



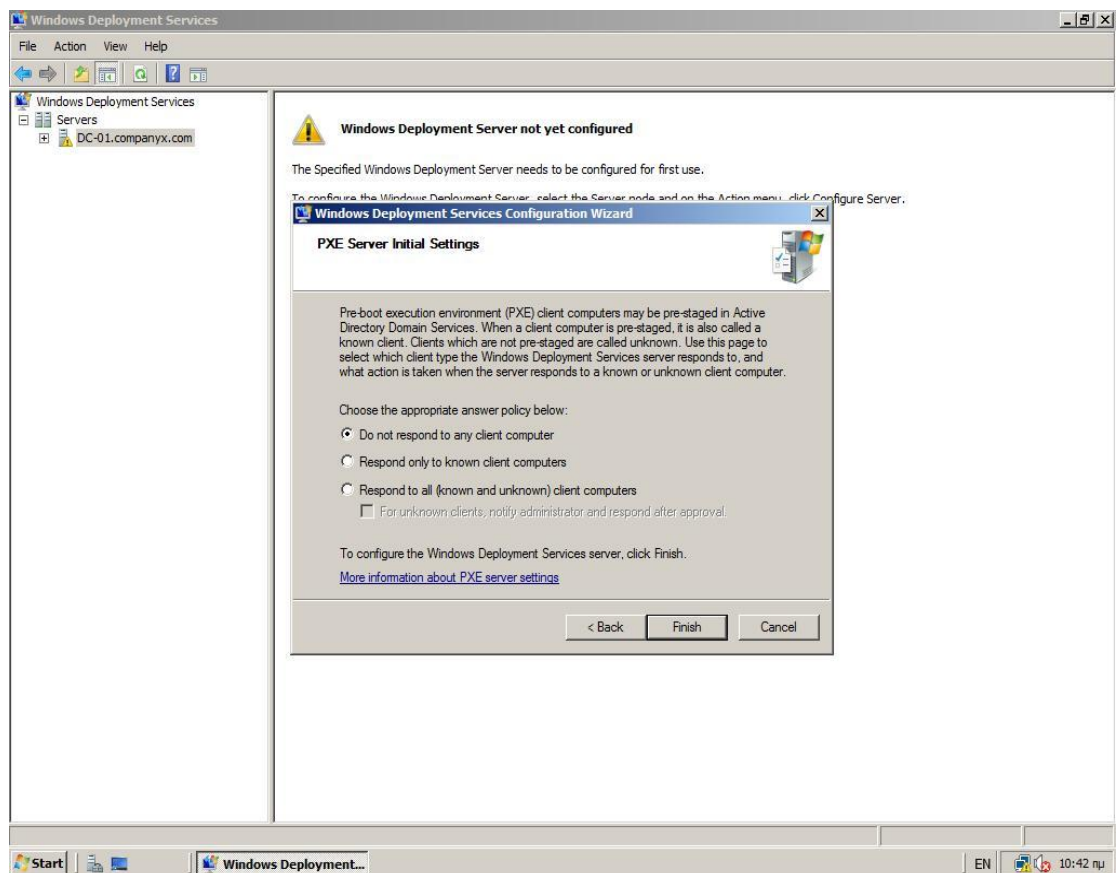
Εικ. 16.10



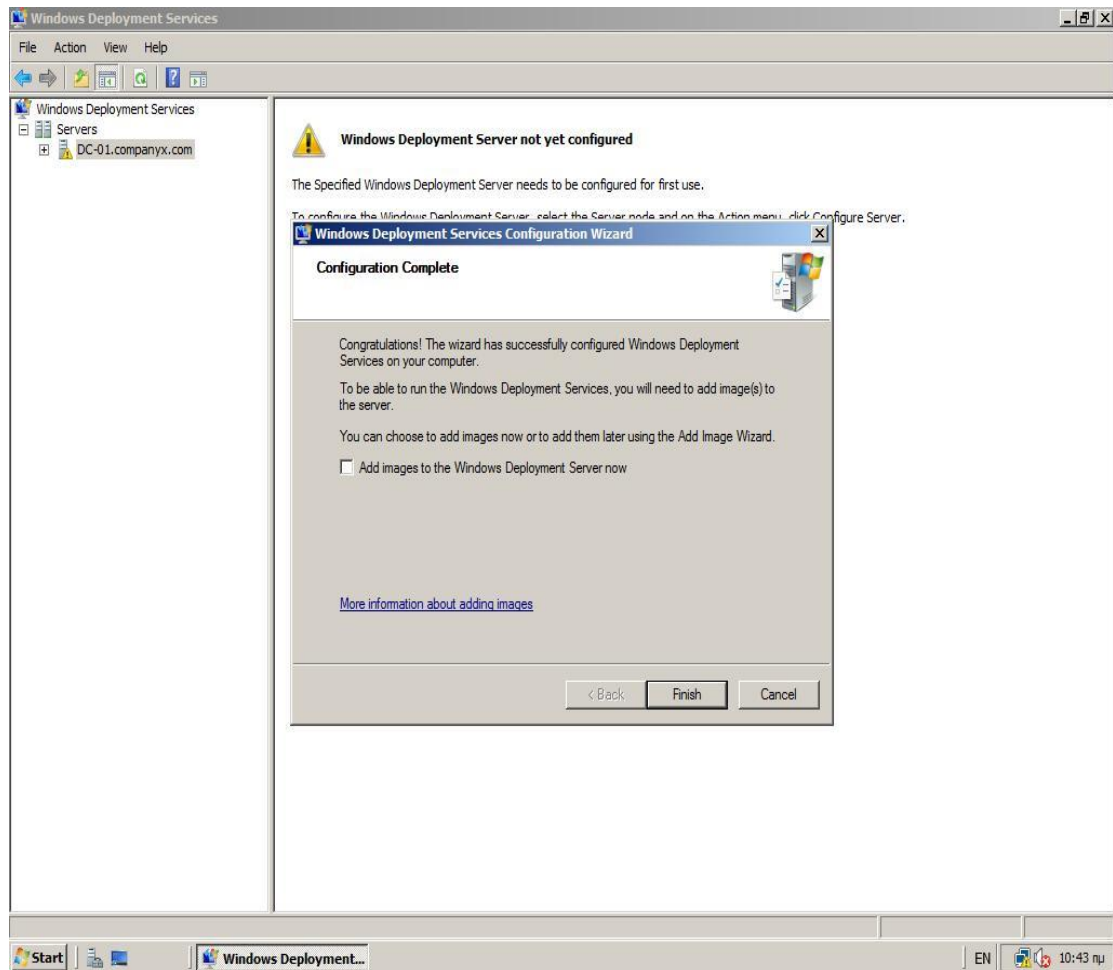
Εικ. 16.11



Εικ. 16.12



Εικ. 16.13

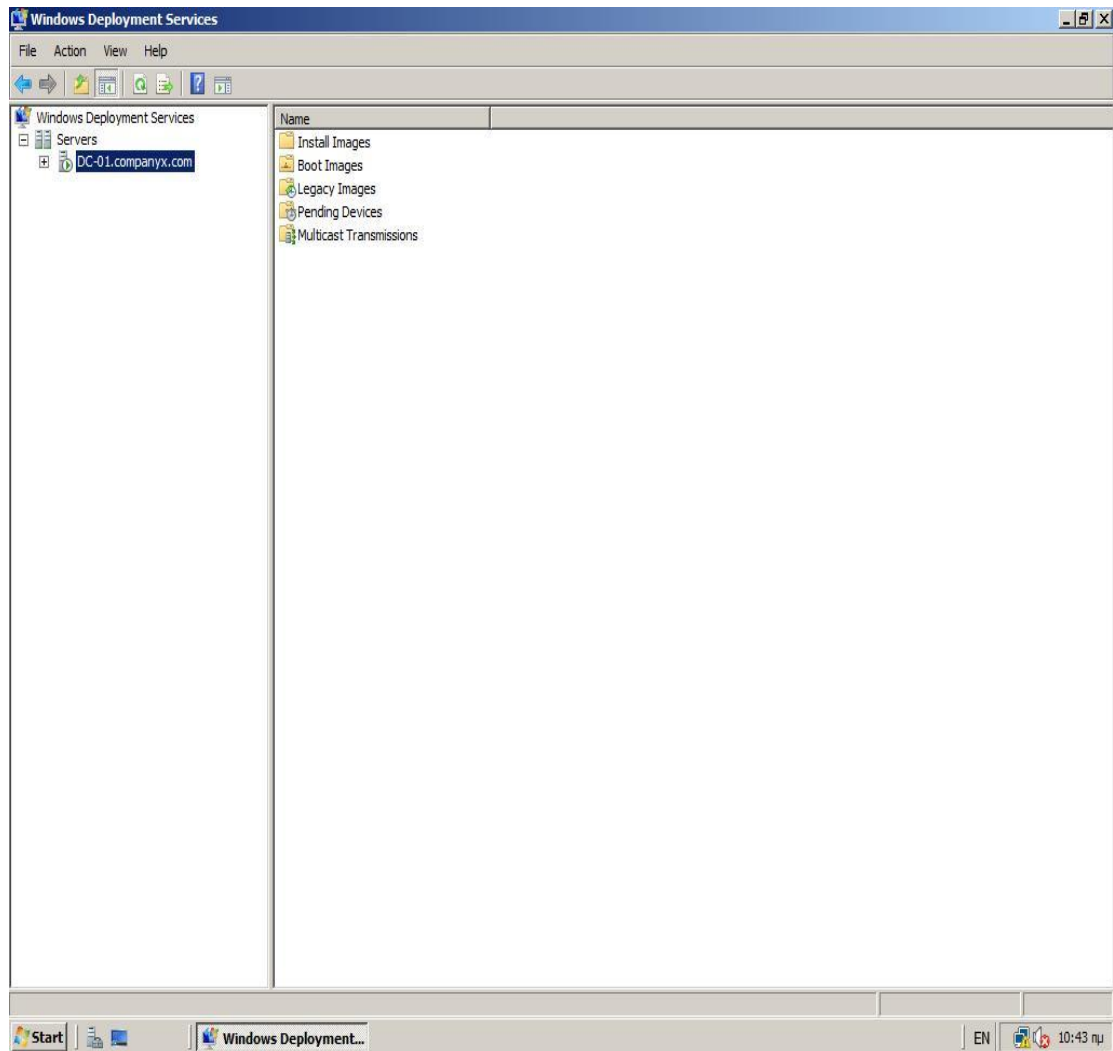


Εικ. 16.14

16.4.2 Προσθήκη Εικόνων (Images)

Αφού διαμορφώσετε τα Windows Deployment Services πρέπει να προσθέσετε τουλάχιστον μία εικόνα εκκίνησης (boot image) και μία εικόνα εγκατάστασης (install image) πριν μπορέσετε να εκκινήσετε από τον Windows Deployment Services server και να εγκαταστήσετε ένα λειτουργικό σύστημα.

- **Boot Images.** Τα boot images είναι εικόνες μέσα από τις οποίες εκκινείτε ένα client υπολογιστή για να εκτελέσετε την εγκατάσταση λειτουργικού συστήματος. Στις περισσότερες περιπτώσεις μπορείτε να χρησιμοποιήσετε το Boot.wim αρχείο που περιέχεται στο DVD των Windows Server 2008 (στο φάκελο \Sources). Το αρχείο Boot.wim περιέχει το Windows PE και το Windows Deployment Services client.
- **Install Images.** Τα install images είναι οι εικόνες που περιέχουν τα λειτουργικά συστήματα που κάνετε εγκατάσταση στον client υπολογιστή. Μπορείτε να χρησιμοποιήσετε το αρχείο Install.wim από το DVD εγκατάστασης ή μπορείτε να δημιουργήσετε τις δικές σας εικόνες εγκατάστασης.

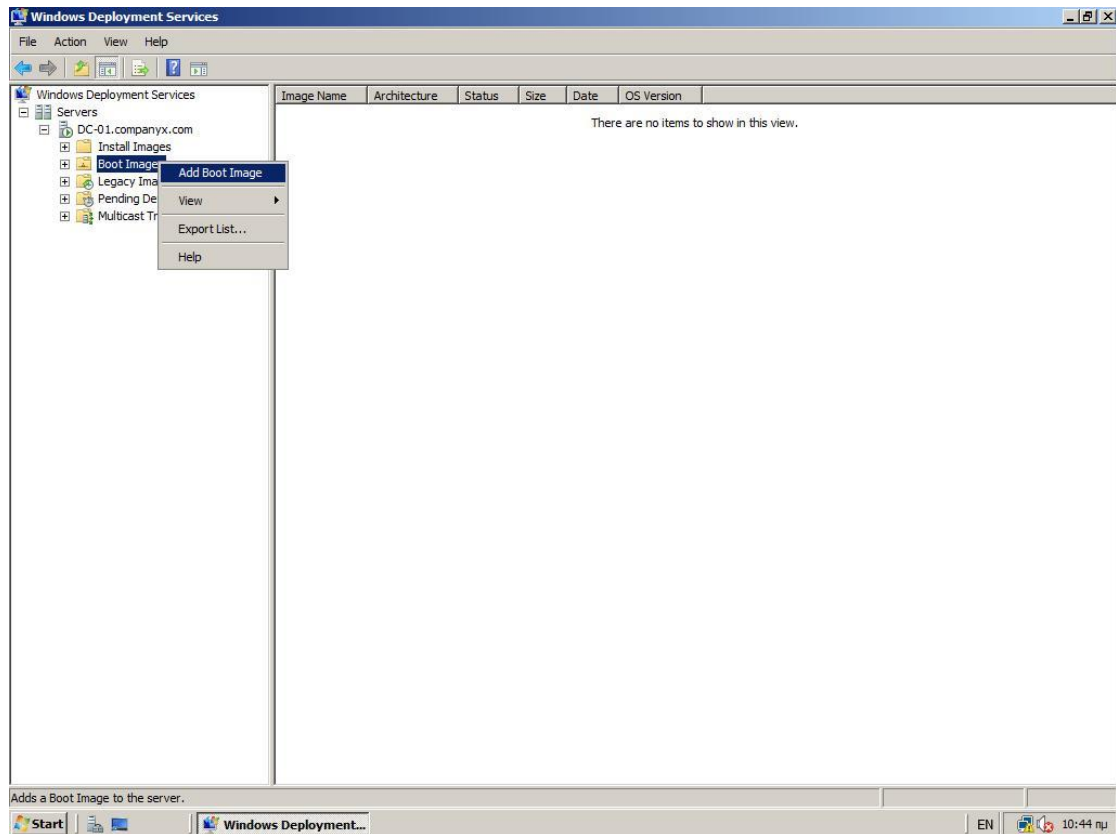


Εικ. 16.15

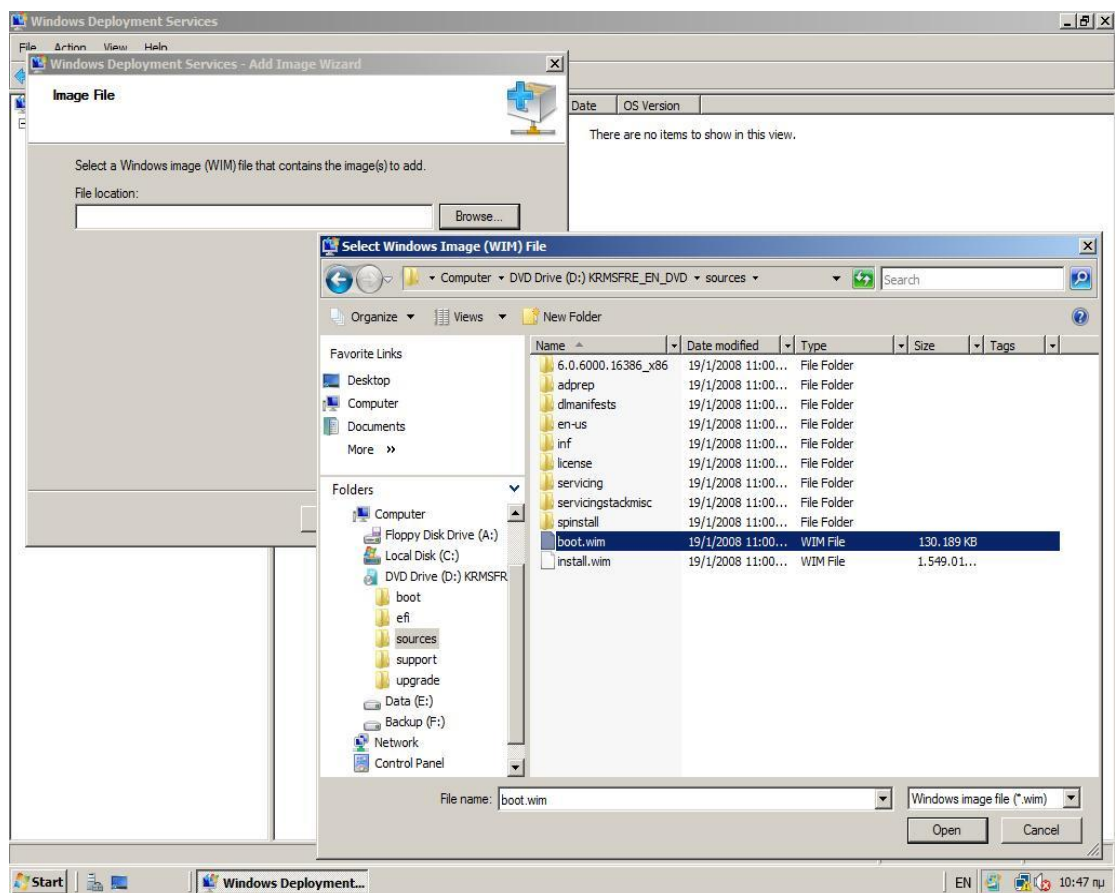
Για να προσθέσετε τις default εικόνες ακολουθείστε τις παρακάτω διαδικασίες. Αφού προσθέσετε boot image και install image στο server είστε έτοιμοι να εκκινήσετε με PXE boot ένα client υπολογιστή για να εγκαταστήσετε λειτουργικό σύστημα.

Για να προσθέσετε την default boot image που περιλαμβάνεται στο DVD εγκατάστασης του προϊόντος:

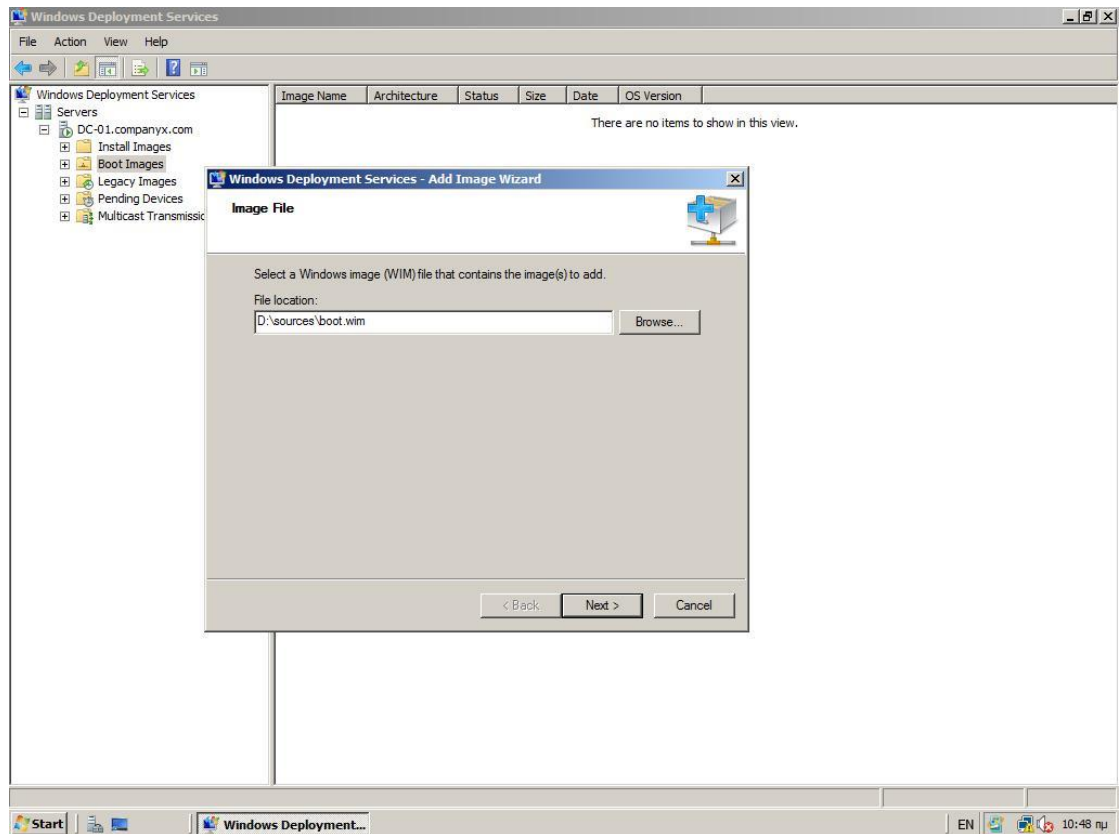
1. Στο αριστερό παράθυρο της κονσόλας MMC κάντε δεξί κλικ στο container **Boot Images** και στη συνέχεια κλικ στο **Add Boot Image** (Εικ. 16.16)
2. Βρείτε το αρχείο Boot.wim στο DVD εγκατάστασης των Windows Server 2008, στο φάκελο \Sources και επιλέξτε το (Εικ. 16.17)
3. Κάντε κλικ στο **Open** και στη συνέχεια κλικ στο **Next** (Εικ. 16.18)
4. Ακολουθείστε τις οδηγίες στο wizard για να ολοκληρώσετε την προσθήκη της εικόνας (Εικόνες 19 - 23)



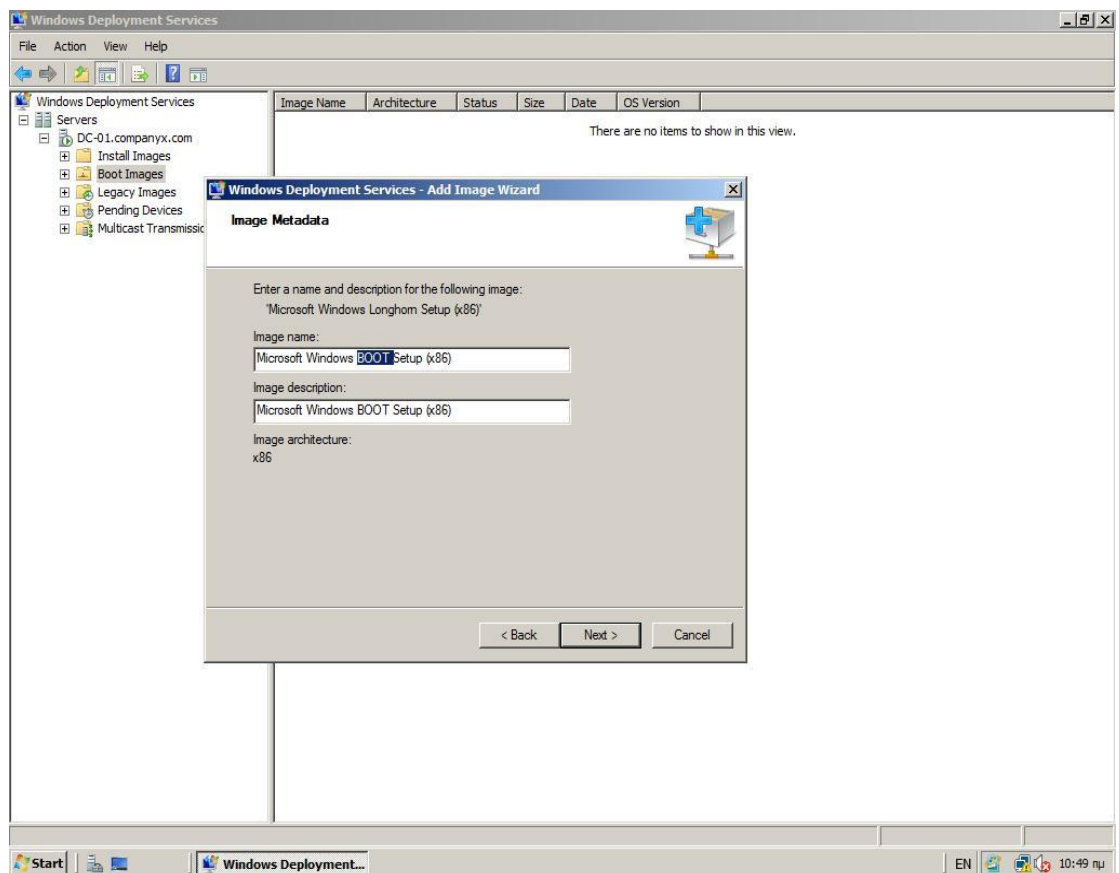
Εικ. 16.16



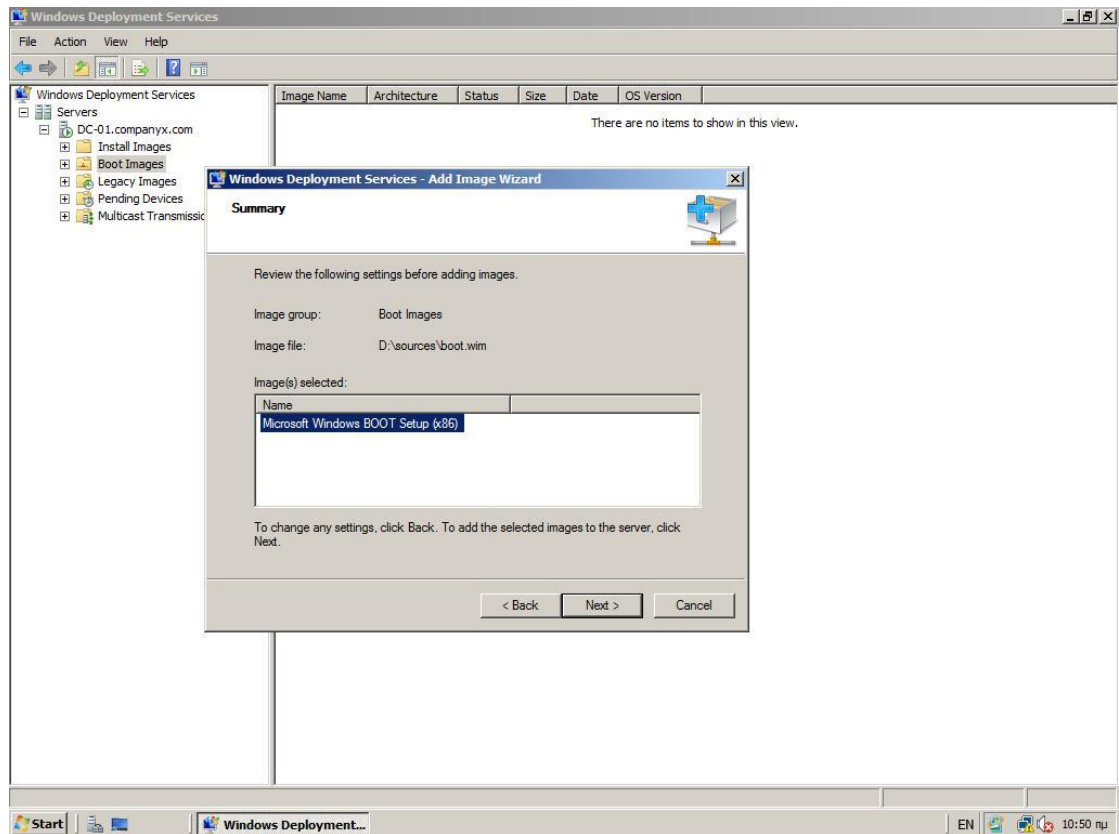
Εικ. 16.17



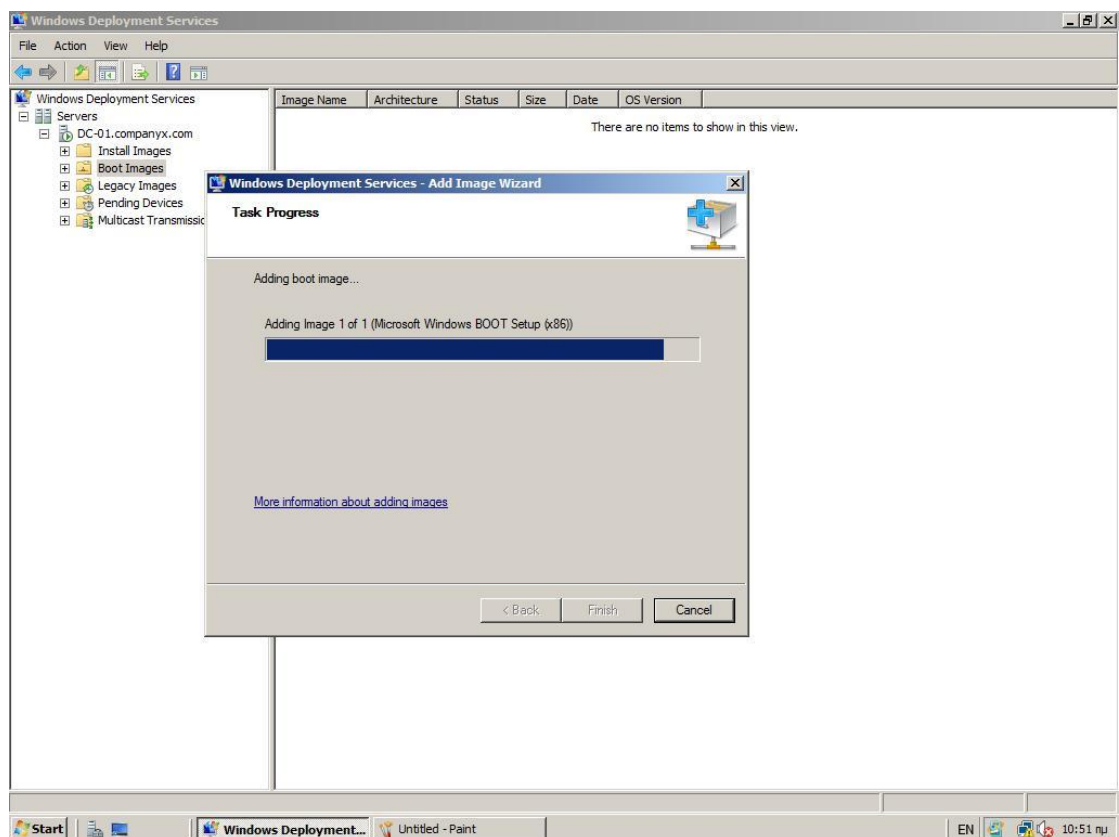
Εικ. 16.18



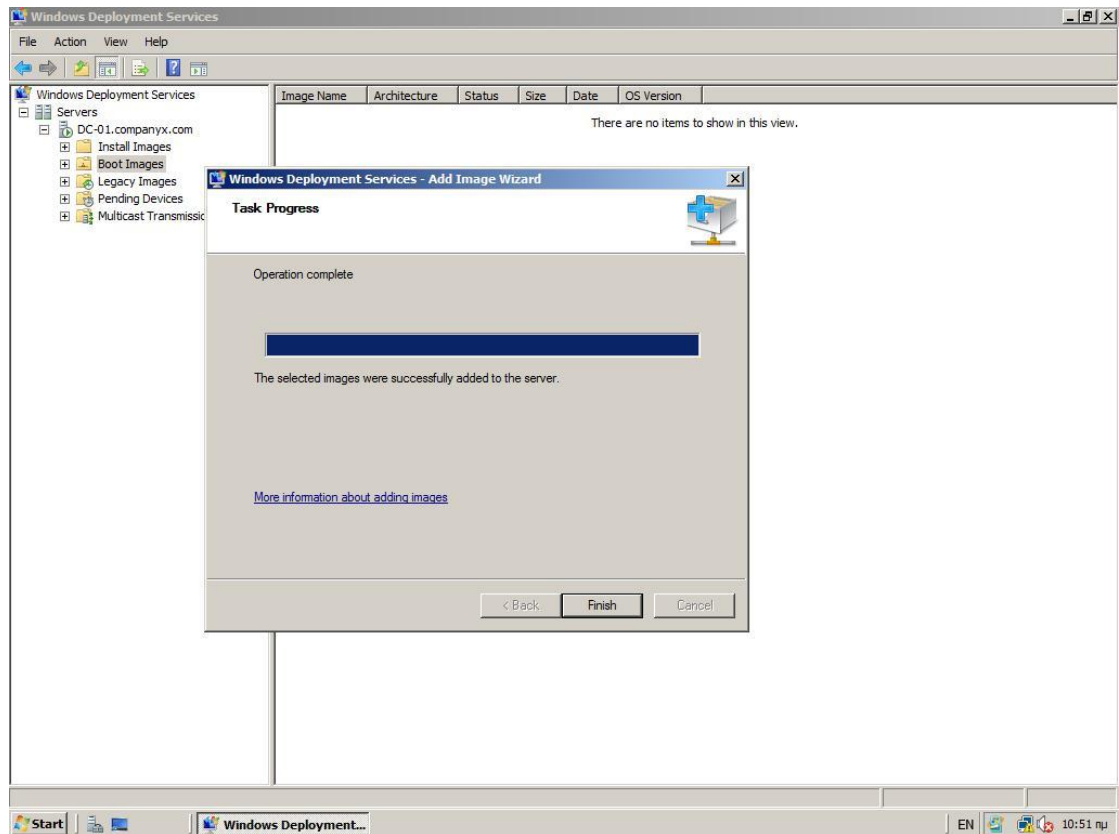
Εικ. 16.19



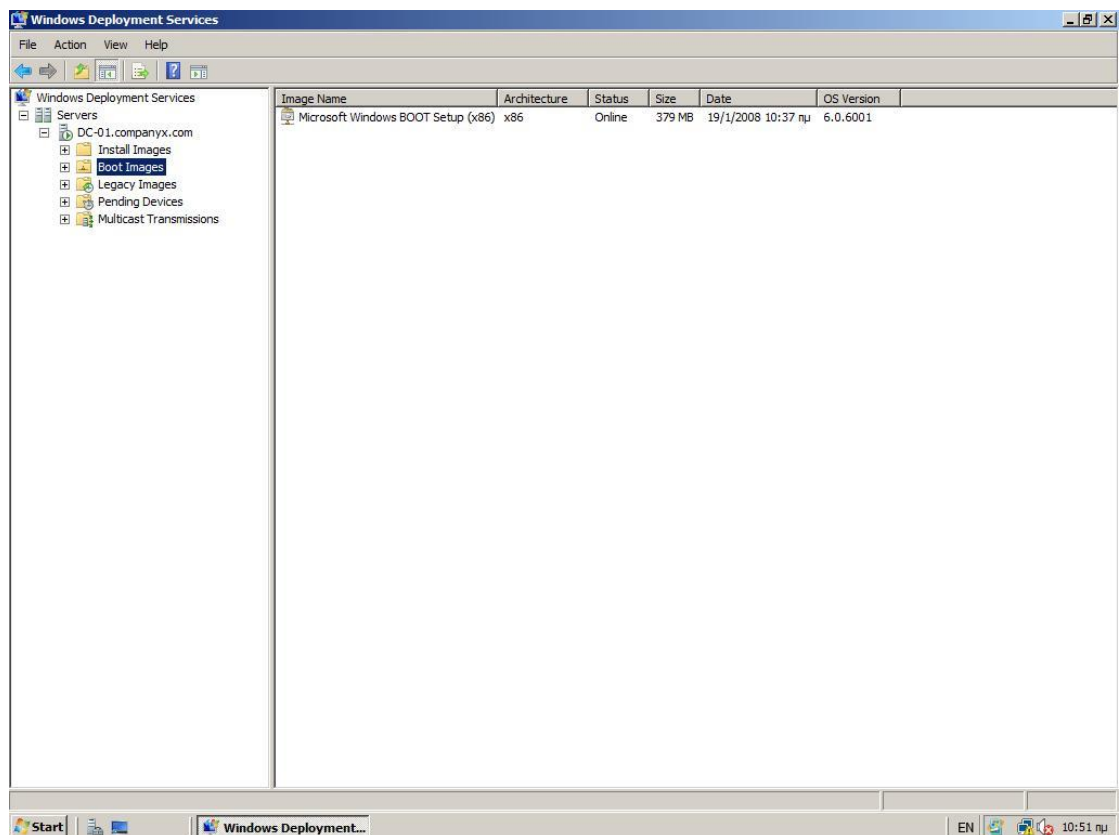
Εικ. 16.20



Εικ. 16.21



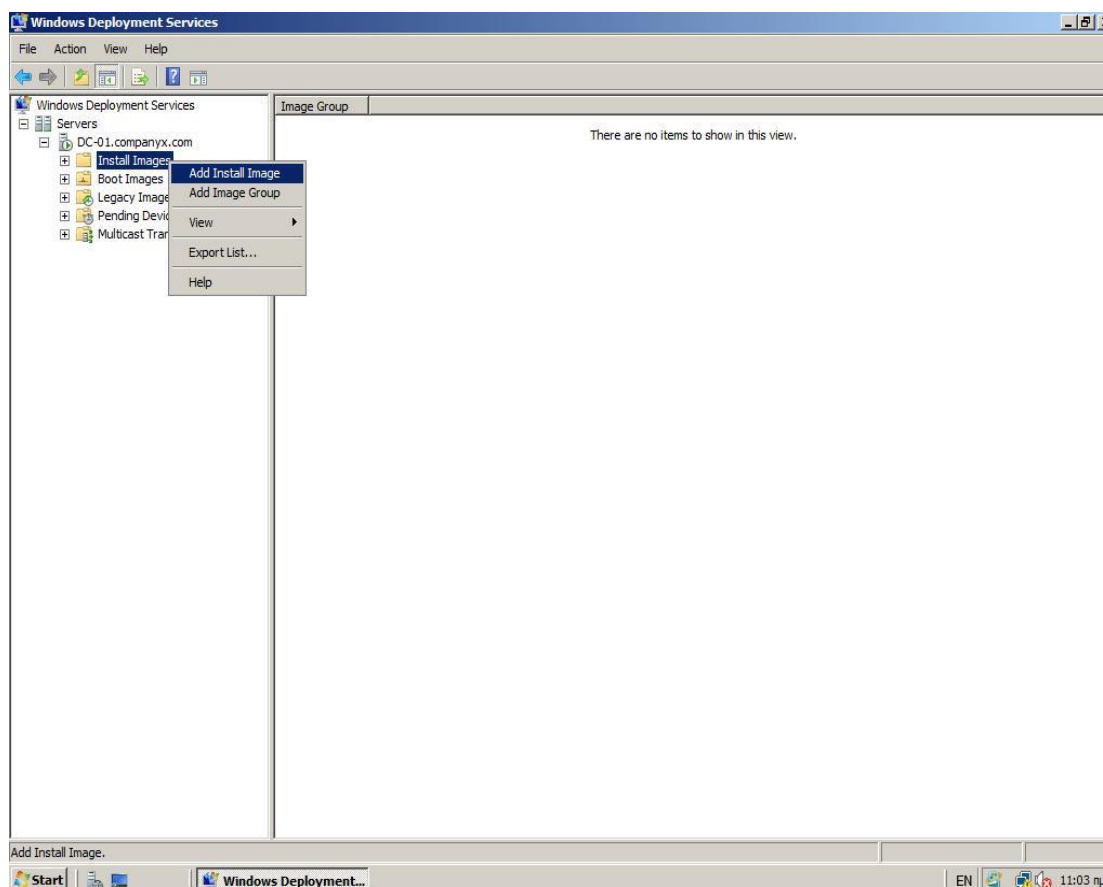
Εικ. 16.22



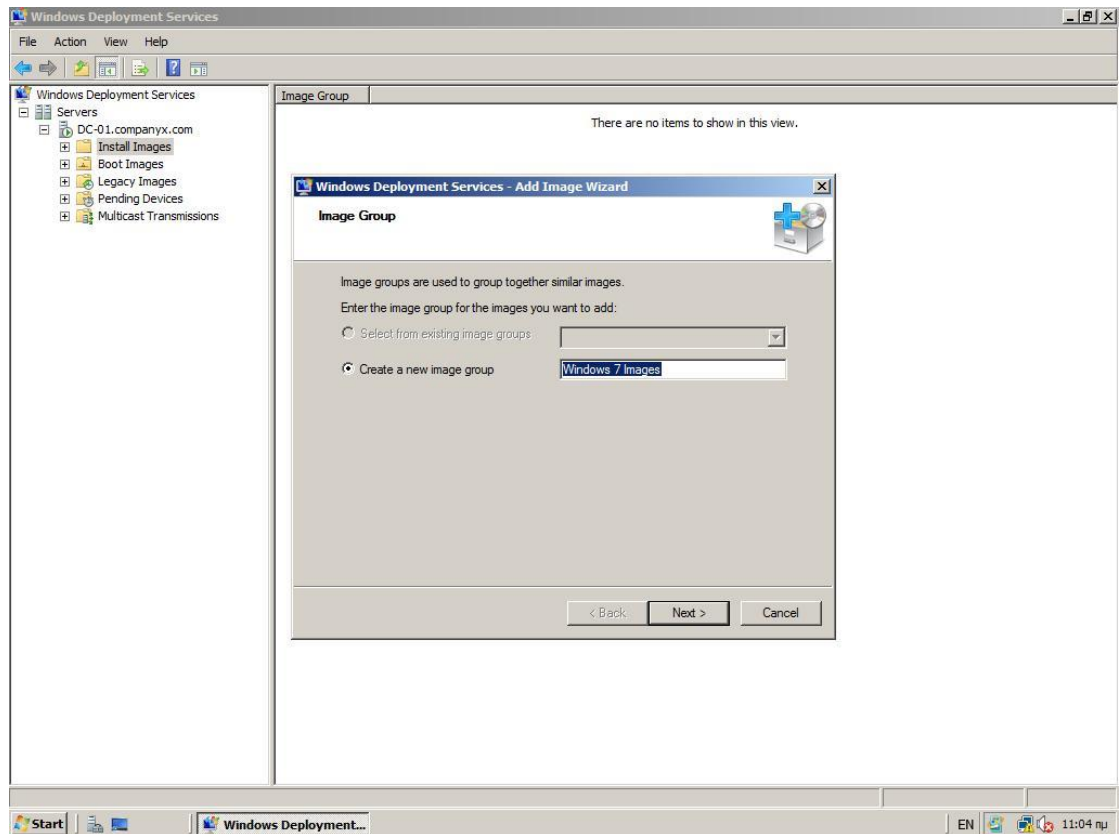
Εικ. 16.23

Για να προσθέσετε την **default install image** που περιλαμβάνεται στο **DVD** εγκατάστασης του προϊόντος:

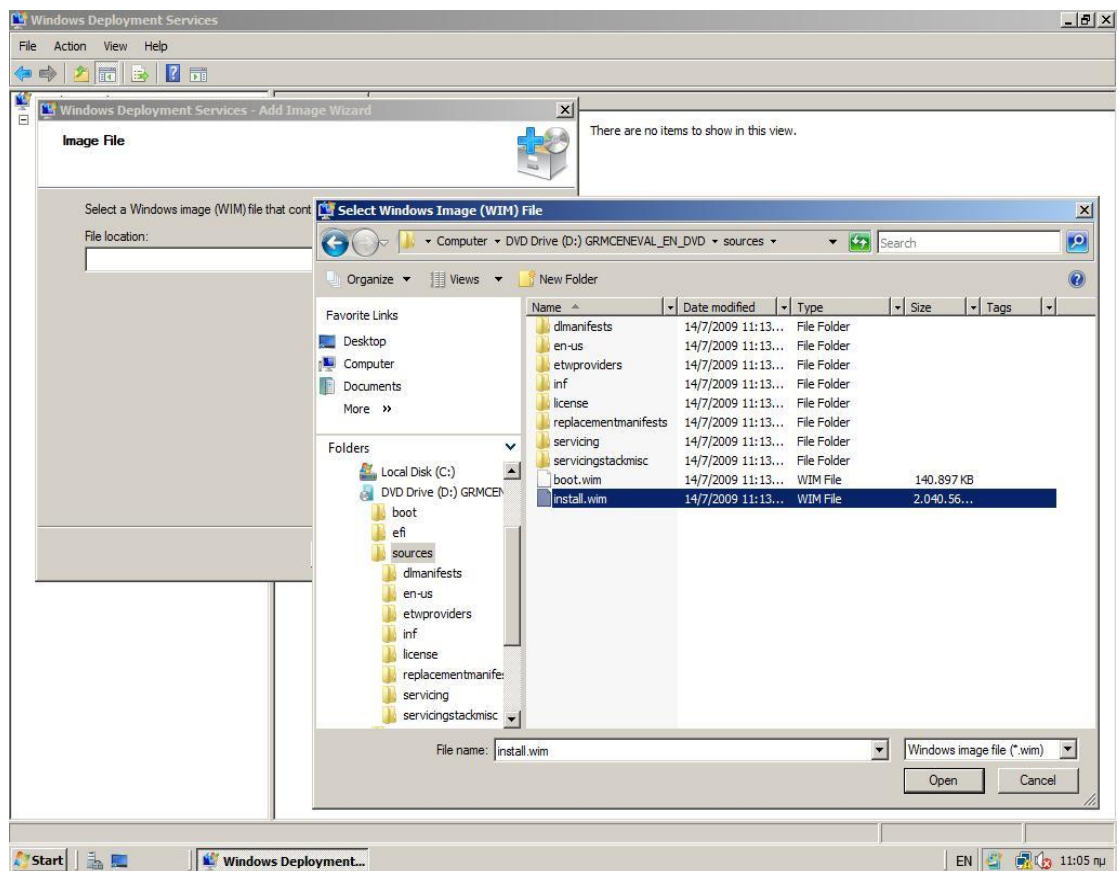
1. Στο αριστερό παράθυρο της κονσόλας MMC κάντε δεξί κλικ στο container **Install Images** και στη συνέχεια κλικ στο **Add Install Image** (Εικ. 16.24)
2. Ορίστε ένα όνομα για το image group και κάντε κλικ στο **Next** (Εικ. 16.25)
3. Βρείτε το αρχείο **Install.wim** στο DVD εγκατάστασης των Windows 7 ή Windows Vista, ή Windows Server 2008, στο φάκελο **\Sources**, επιλέξτε το και κάντε κλικ στο **Open** και μετά στο **Next** (Εικόνες 26 - 27)
4. Για να προσθέσετε ένα υποσύνολο των λειτουργικών συστημάτων που περιλαμβάνονται στο αρχείο **Install.wim**, αποτσεκάρτε τα **check boxes** των συστημάτων που δε θέλετε να προσθέσετε στο server. (Εικ. 16.28)
5. Ακολουθείστε τις οδηγίες στο wizard για να ολοκληρώσετε την προσθήκη των εικόνων (Εικόνες 29 - 32)
6. Τώρα που έχετε boot image και install image στο server είστε έτοιμοι να εκκινήσετε με PXE boot ένα client υπολογιστή για να εγκαταστήσετε λειτουργικό σύστημα.



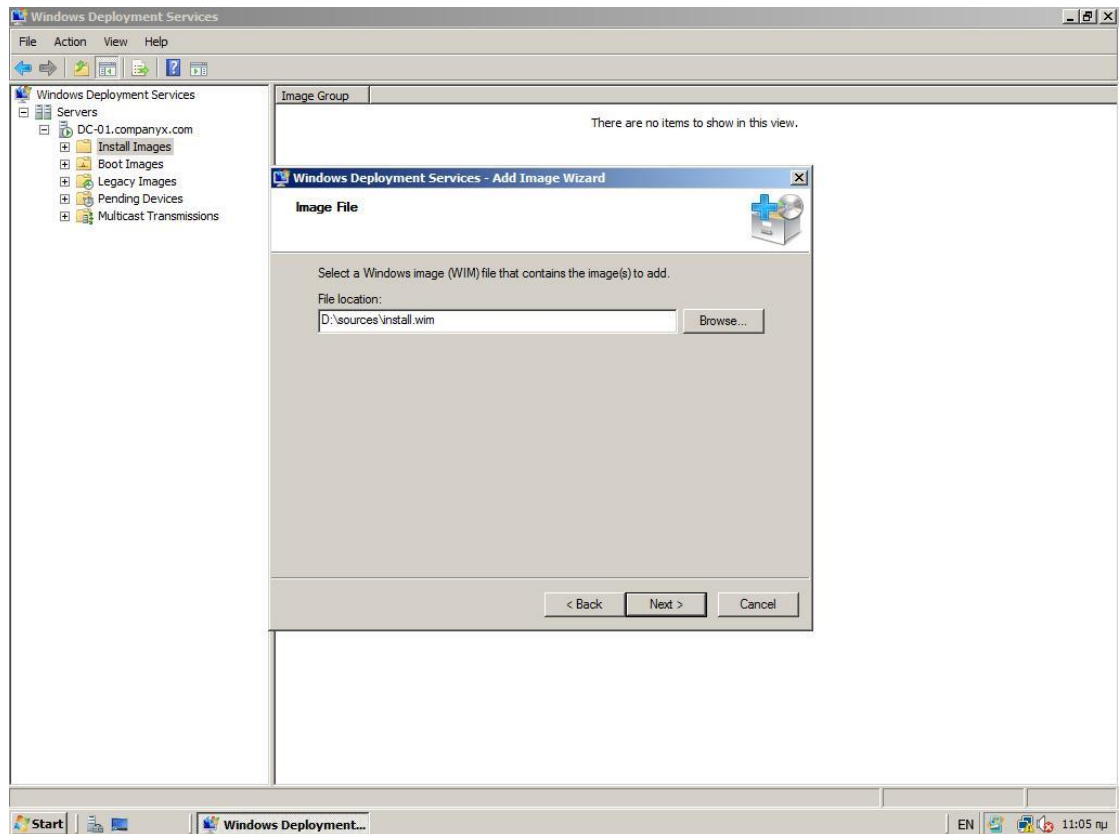
Εικ. 16.24



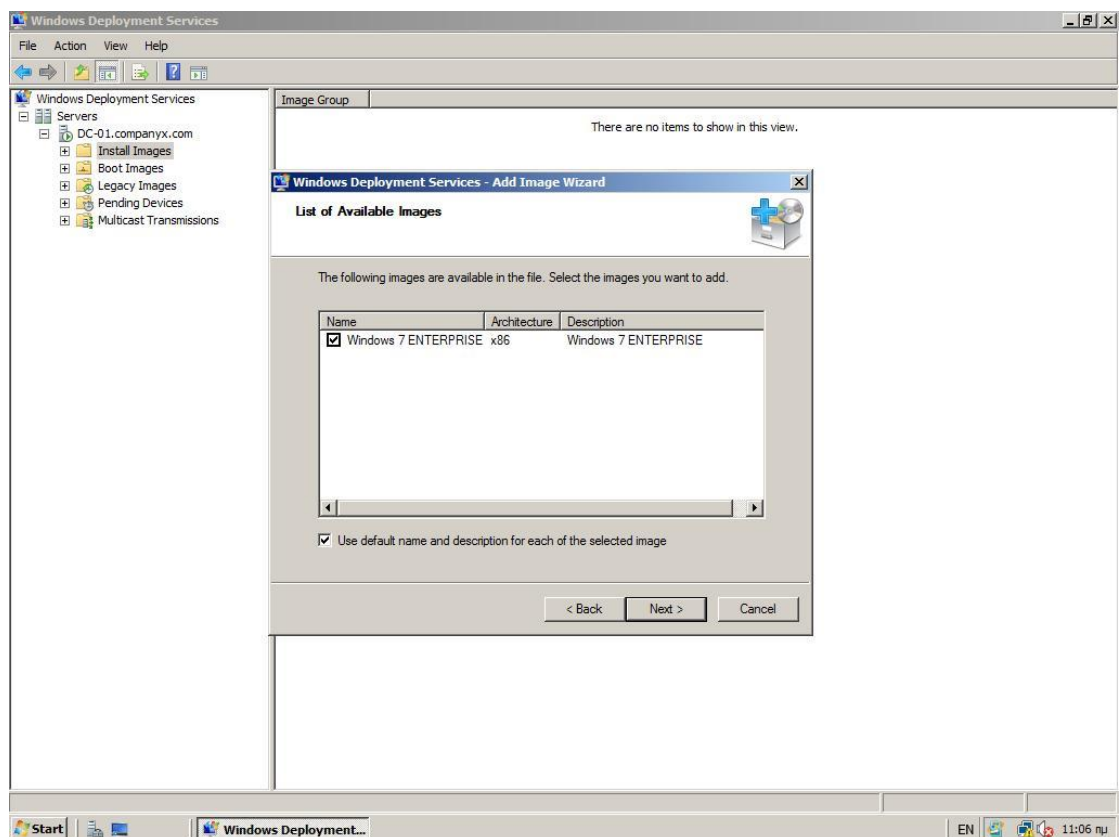
Εικ. 16.25



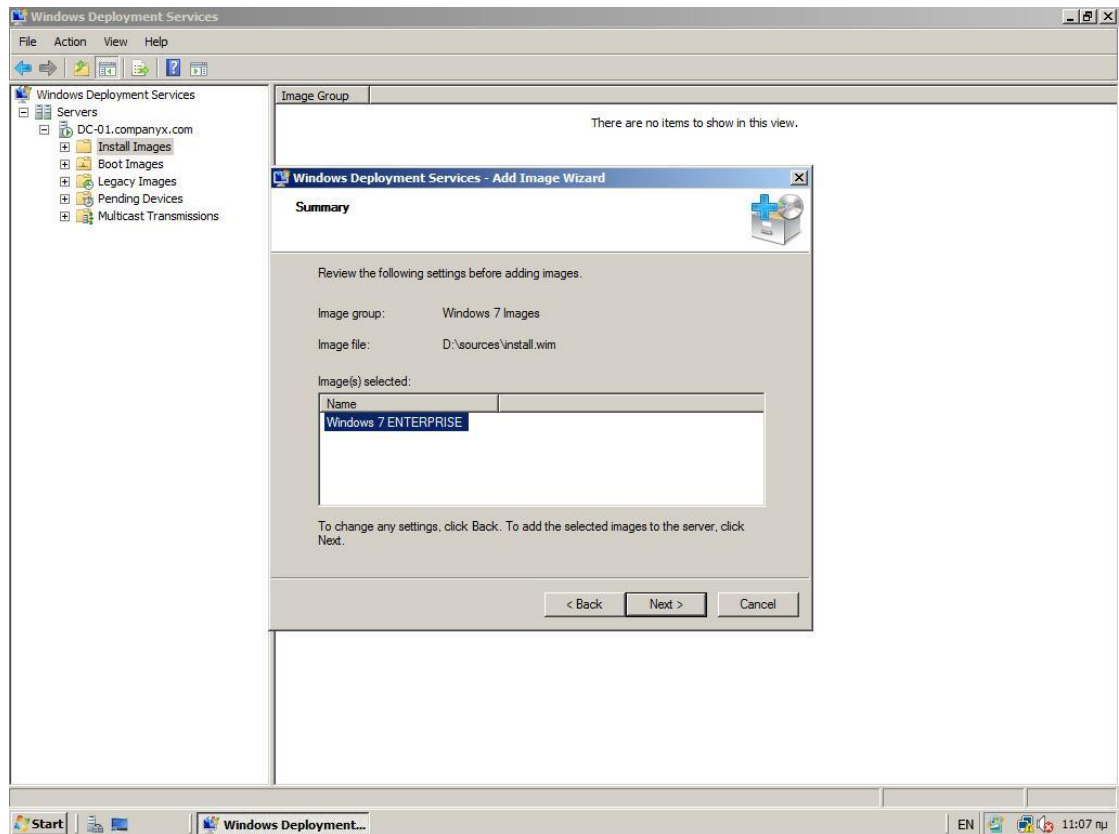
Εικ. 16.26



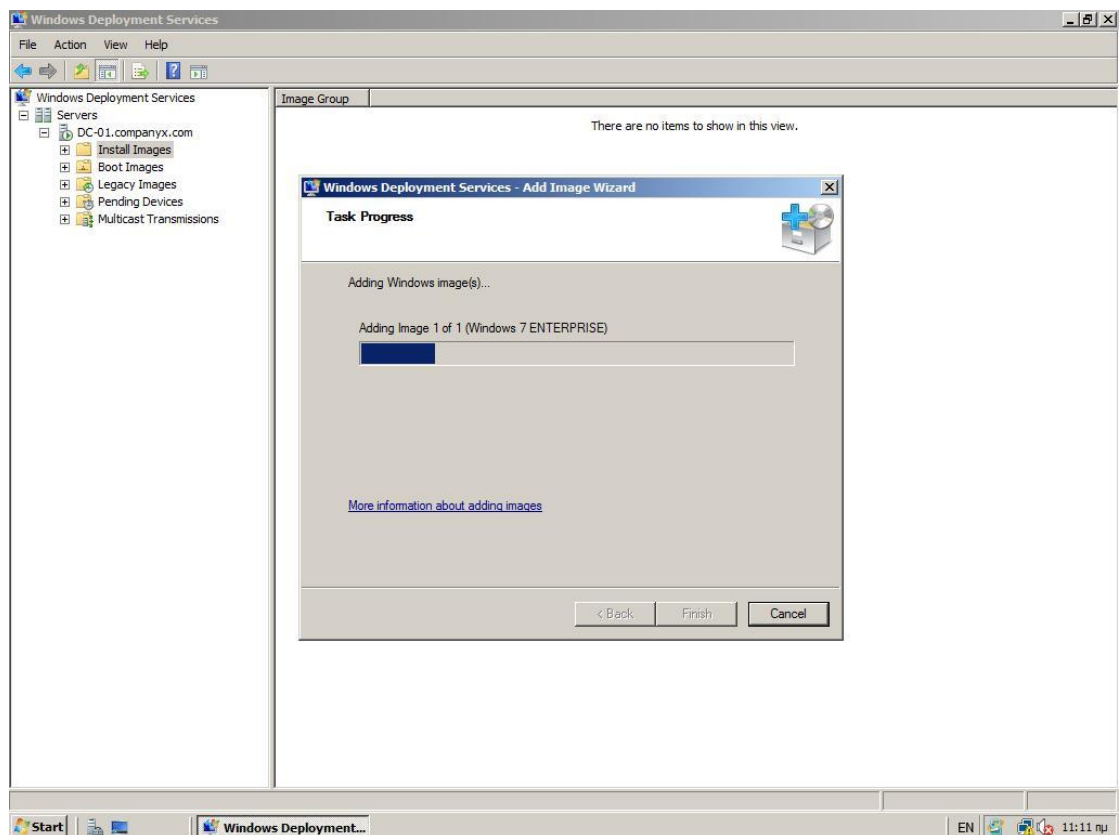
Εικ. 16.27



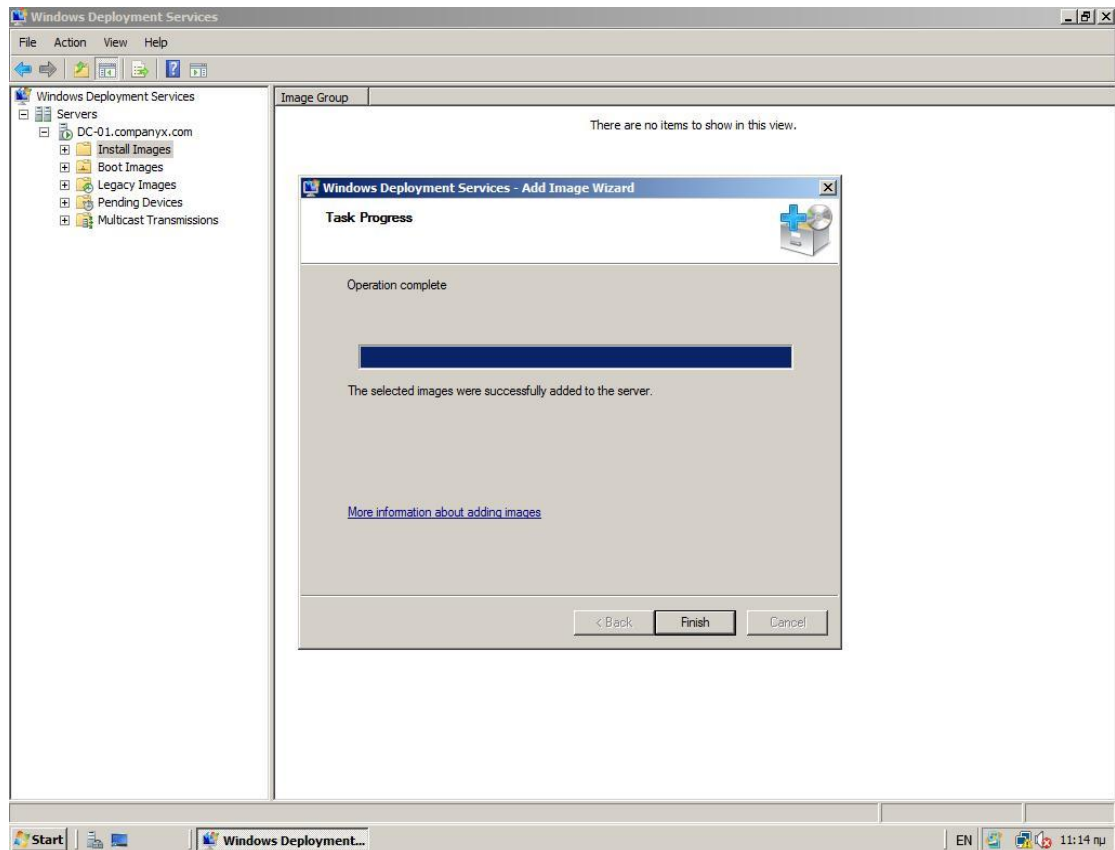
Εικ. 16.28



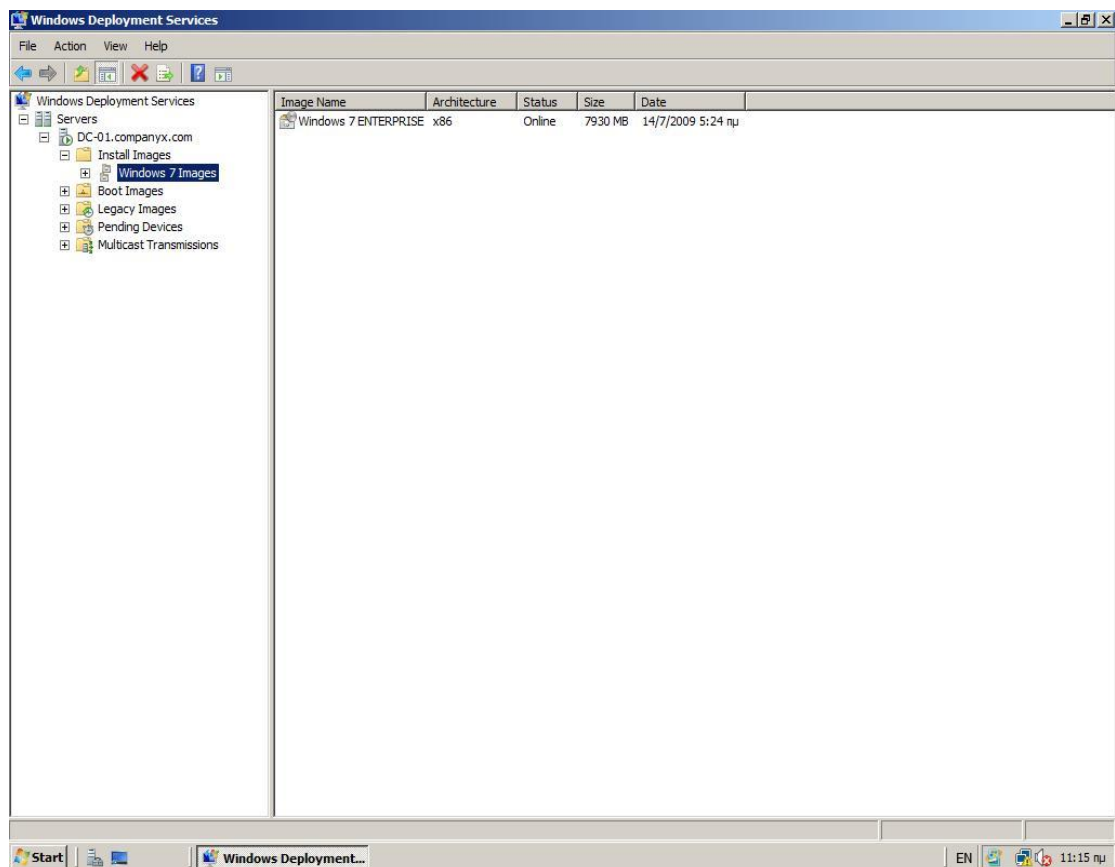
Εικ. 16.29



Εικ. 16.30



Εικ. 16.31



Εικ. 16.32

16.5 Ρύθμιση του boot menu

Boot images είναι οι εικόνες που περιέχουν το Windows PE στο οποίο εκκινούν οι client υπολογιστές για να επιλέξουν την εικόνα λειτουργικού συστήματος που θέλουν να εγκαταστήσουν. Όταν έχετε πολλαπλές boot images διαθέσιμες στους client υπολογιστές τότε σε αυτούς θα εμφανιστεί ένα boot menu που θα εμφανίζει τα boot images. Οι χρήστες θα πρέπει πρώτα να επιλέξουν μια boot image και έπειτα θα εμφανιστούν οι install images. Το boot menu σας δίνει τη δυνατότητα να έχετε πολλαπλές boot images για διαφορετικές εργασίες και αρχιτεκτονικές. Θα μπορούσατε δηλαδή να έχετε boot images για τις παρακάτω εργασίες:

- Να ξεκινήσετε την εγκατάσταση για τα Windows
- Να ξαναδιαμορφώσετε τους σκληρούς δίσκους για να υποστηρίζουν BitLocker Drive Encryption (με τη χρήση unattend) και στη συνέχεια να εγκαταστήσετε τα Windows
- Να περιέχουν το Windows Recovery Environment (Windows RE) για να το χρησιμοποιήσετε όταν ένας υπολογιστής δεν εκκινεί επιτυχώς
- Να περιέχει τον Windows Deployment Services capture wizard ο οποίος δημιουργεί install images από λειτουργικά συστήματα υπολογιστών αναφοράς
- Να περιέχει μία Windows PE image για διαχειριστές που θέλουν να εκτελούν ειδικές εργασίες μέσα στο Windows PE.

Επιπρόσθετα, οι 64μπιτοι υπολογιστές μπορούν να τρέξουν και 32-bit και 64-bit boot images. Επομένως για κάθε μία από αυτές τις εργασίες θα μπορούσατε να έχετε από δύο boot images - μία για τις 32-bit και μία για τις 64-bit. Το boot menu στους 32-bit (x86) υπολογιστές θα εμφανίζει μόνο τις 32-bit boot images (διότι οι 32μπιτοι υπολογιστές δεν μπορούν να τρέξουν 64μπιτες boot images). Σημειώστε επίσης ότι η εξ' ορισμού συμπεριφορά των 64μπιτων υπολογιστών είναι να εμφανίζουν και τις x86 και τις x64 boot images (όταν βεβαίως είναι διαθέσιμες και οι δύο). Για να αλλάξετε αυτή τη ρύθμιση εκτελέστε την εντολή:

WDSUTIL /Set-Server /Defaultx86x64ImageType:{x86|x64|both}.

Υπάρχουν κάποια γνωστά ζητήματα και περιορισμοί που αφορούν στο boot menu:

- Το boot menu δεν μπορεί να περιέχει περισσότερες από 13 boot images.
- Το όνομα του αρχείου .wim δεν μπορεί να περιέχει κενά. Μπορεί να περιέχει μόνο γράμματα και αριθμούς.

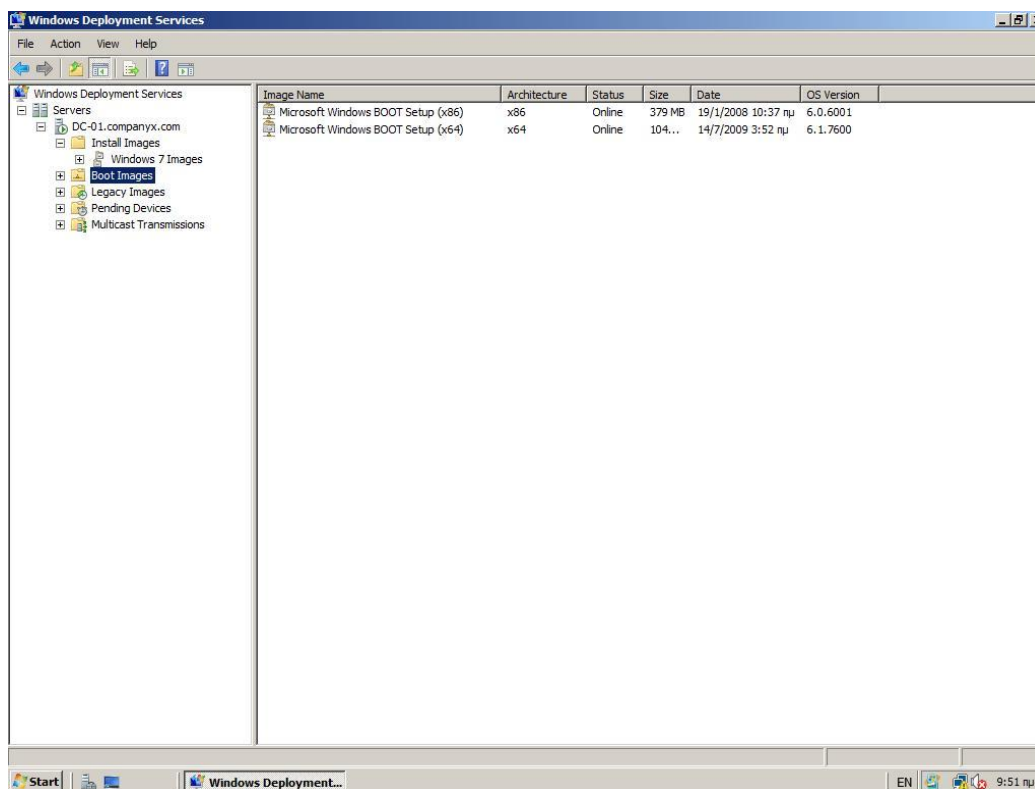
- Χρησιμοποιείτε το **Boot.wim** από το **DVD εγκατάστασης των Windows Server 2008**. Μην χρησιμοποιείτε το Boot.wim των Windows Vista εκτός κι αν έχει ενσωματωμένο το SP1 (η έκδοση των Windows Vista χωρίς SP1 δεν υποστηρίζει multicasting). Μπορείτε επίσης να χρησιμοποιήσετε το Boot.wim των Windows 7.
- Η χρήση χαρακτήρων **double-byte** στα ονόματα των **images** μπορεί να έχει ως αποτέλεσμα να μην εμφανίζονται σωστά στο **boot menu**. Αυτό έχει να κάνει συνήθως με συγκεκριμένες γλώσσες (π.χ. ρώσικα) και το πρόβλημα εμφάνισής τους στο BIOS.

16.5.1 Διαδικασίες Ρύθμισης του Boot Menu

Οι διαδικασίες που ακολουθούν δείχνουν τον τρόπο με τον οποίο μπορείτε να προσθέσετε περισσότερες boot images στο boot menu:

Χρήση κονσόλας MMC

1. Ανοίξτε την κονσόλα Windows Deployment Services
2. Κάντε δεξί κλικ στο container **Boot Images** και στη συνέχεια επιλέξτε **Add Boot Image**
3. Κάντε κλικ στο **Browse** για να εντοπίσετε και να επιλέξετε το αρχείο .wim που θέλετε να προσθέσετε. Το boot image πρέπει να βρίσκεται στο server και μπορεί να είναι ίδιας ή διαφορετικής αρχιτεκτονικής. Πατήστε **Open** και στη συνέχεια **Next**



Εικ. 16.33

4. Ακολουθείστε τις οδηγίες επί της οθόνης
5. Όταν ολοκληρώσετε τη διαδικασία μπορείτε να εκτελέσετε PXE boot σε έναν client υπολογιστή για να δείτε ένα boot menu και με τις δύο images (αν βεβαίως υποστηρίζονται και οι δύο από τον υπολογιστή) (Εικ. 16.33)

Χρήση command prompt

1. Ανοίξτε ένα command prompt
2. Εκτελέστε την ακόλουθη εντολή για να προσθέσετε μία boot image, όπου <bootimage> είναι η πλήρης διαδρομή του αντίστοιχου αρχείου στο server το οποίο μπορεί να είναι ίδιας ή διαφορετικής αρχιτεκτονικής

WDSUTIL /Add-Image /ImageFile:<bootimage> /ImageType:boot

3. Όταν ολοκληρώσετε τη διαδικασία μπορείτε να εκτελέσετε PXE boot σε έναν client υπολογιστή για να δείτε ένα boot menu και με τις δύο images (αν βεβαίως υποστηρίζονται και οι δύο από τον υπολογιστή)

Μπορείτε επίσης να κάνετε επιπρόσθετες αλλαγές στο boot menu χρησιμοποιώντας το εργαλείο Bcdedit.exe για να επεξεργαστείτε το αρχείο Default.bcd που βρίσκεται στο φάκελο %REMINST%\boot\<αρχιτεκτονική>.

16.6 Δημιουργία Custom Install Images

Με τη χρήση Windows Deployment Services μπορείτε να δημιουργήσετε custom install images. Αυτό σημαίνει πως πέρα από τις standard install images που μπορείτε να προσθέσετε στο server χρησιμοποιώντας το DVD εγκατάστασης του λειτουργικού συστήματος, μπορείτε να δημιουργήσετε εικόνες οι οποίες, εκτός από το λειτουργικό σύστημα, μπορούν να περιέχουν επιπρόσθετα και εφαρμογές, ρυθμίσεις περιβάλλοντος εργασίας, drivers κ.λπ. ώστε να τις κάνετε deploy σε πολλαπλούς client υπολογιστές.

Η διαδικασία περιλαμβάνει τα εξής στάδια: **α)** Πρώτα δημιουργείτε μία ειδική boot image η οποία ονομάζεται **capture image**. **β)** Στη συνέχεια φτιάχνετε ένα υπολογιστή αναφοράς. Ο υπολογιστής αυτός περιέχει το λειτουργικό σύστημα, τους drivers, τις εφαρμογές και τις ρυθμίσεις περιβάλλοντος (δίκτυο, εκτυπωτές, desktop, shortcuts, domain κ.α.) που θέλετε να έχει η custom install image που θέλετε να δημιουργήσετε για να την εγκαταστήσετε στη συνέχεια στους υπόλοιπους client υπολογιστές χρησιμοποιώντας Windows Deployment Services. **γ)** Αφού ολοκληρώσετε τον υπολογιστή αναφοράς, τον "προετοιμάζετε" με το εργαλείο συστήματος **Sysprep** για να γίνει image, αφαιρώντας πρώτα όλες τις μοναδικές πληροφορίες συστήματος

(συμπεριλαμβανομένου και του security ID (SID) υπολογιστή), και στη συνέχεια εκκινείτε από την capture image (βήμα α) ώστε ο Windows Deployment Services server να συλλάβει το αρχείο .wim και να το καταστήσει έτοιμο για μαζική εγκατάσταση σε πολλαπλούς υπολογιστές.

Για να δημιουργήσετε custom install images βεβαιωθείτε πως υπάρχει **αρκετός χώρος** στο δίσκο για τη δημιουργία και αποθήκευση των νέων εικόνων. Επίσης πρέπει να είστε μέλος των **Local Administrators** στο Windows Deployment Services server.

Υπάρχουν κάποια ζητήματα τα οποία θα πρέπει να θυμάστε και να λάβετε υπόψη ώστε να μη συναντήσετε προβλήματα κατά την δημιουργία custom install images. Όταν εκκινείτε μέσα από την capture image ξεκινά ο capture wizard:

- Θα δείτε μόνο τα drives που περιέχουν λειτουργικό σύστημα που έχει προετοιμαστεί με το εργαλείο Sysprep. Αν δεν έχετε εκτελέσει το Sysprep στον υπολογιστή πριν την εκκίνηση του μέσα από την capture image, δε θα βρείτε drives για σύλληψη (capture).
- Όταν σας ζητηθεί να αποθηκεύσετε την νέα εικόνα θα πρέπει να δώσετε μία τοπική θέση (στον υπολογιστή) αλλιώς δε θα μπορείτε να κάνετε capture την εικόνα. Αυτός ο περιορισμός επιβάλλεται για να αποφύγετε τυχόν καταστροφές ή λάθη στο αρχείο εικόνας σε περίπτωση βλάβης δικτύου.
- Όταν ορίζετε τη θέση αποθήκευσης της εικόνας **θα πρέπει στο όνομα αρχείου να γράψετε και την επέκταση (.wim)**, αλλιώς η λειτουργία θα αποτύχει.
- Αν προσθέσετε μία 64μπιτη boot image και δημιουργήσετε από αυτή μία capture image, τότε μπορείτε να εκκινήσετε από αυτή (capture image) μόνο 64μπιτους υπολογιστές.

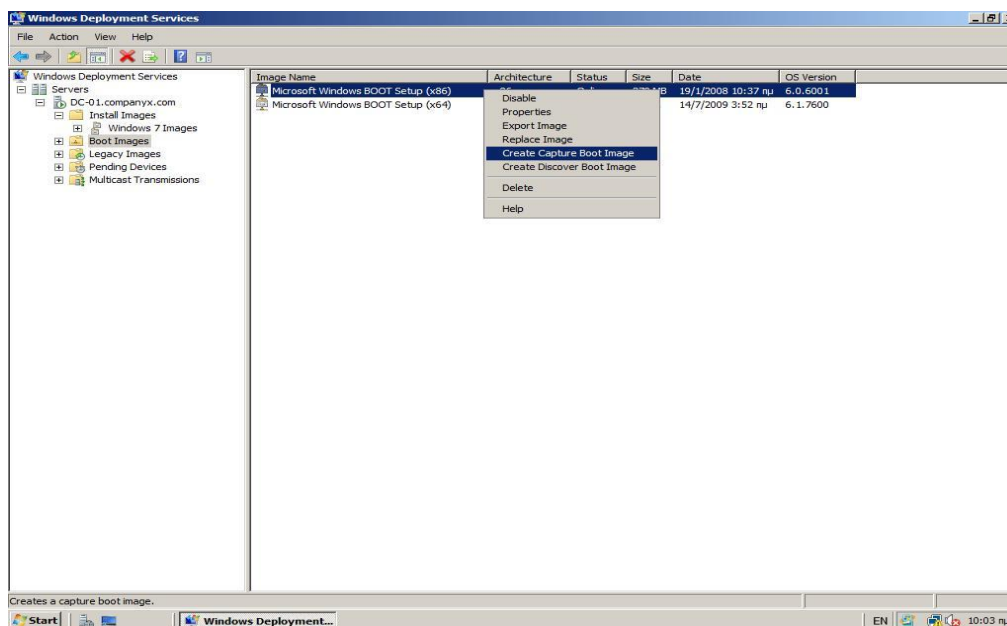
16.6.1 Διαδικασίες Δημιουργίας Capture Image

Όπως αναφέρεται παραπάνω, για να δημιουργήσετε μία custom install image πρέπει πρώτα να δημιουργήσετε μία capture image. Μπορείτε να την δημιουργήσετε χρησιμοποιώντας το αρχείο Boot.wim από το DVD των Windows Server 2008 (που βρίσκεται στο φάκελο \Sources). Για τη δημιουργία της χρησιμοποιείτε μία από τις ακόλουθες διαδικασίες:

Χρήση κονσόλας MMC

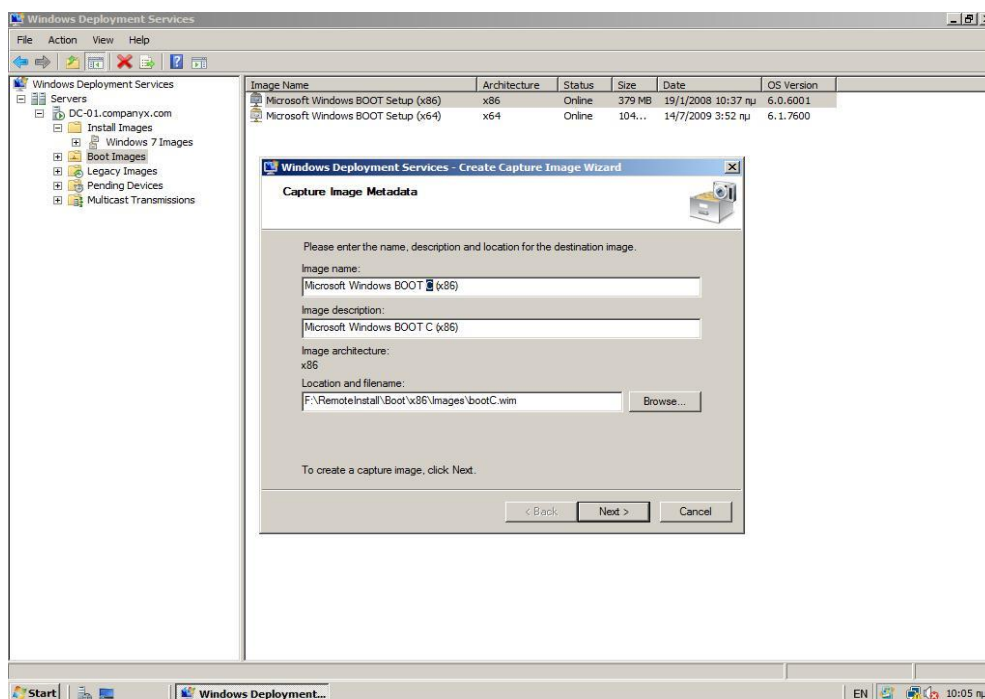
- Στην κονσόλα Windows Deployment Services αναπτύξτε το container **Boot Images**

- Κάντε δεξί κλικ στην εικόνα που θα χρησιμοποιήσετε σαν capture image. Στις περισσότερες περιπτώσεις μπορείτε απλά να χρησιμοποιήσετε το αρχείο Boot.wim από το DVD που προσθέσατε στα προηγούμενα κεφάλαια (Εικ. 16.34)



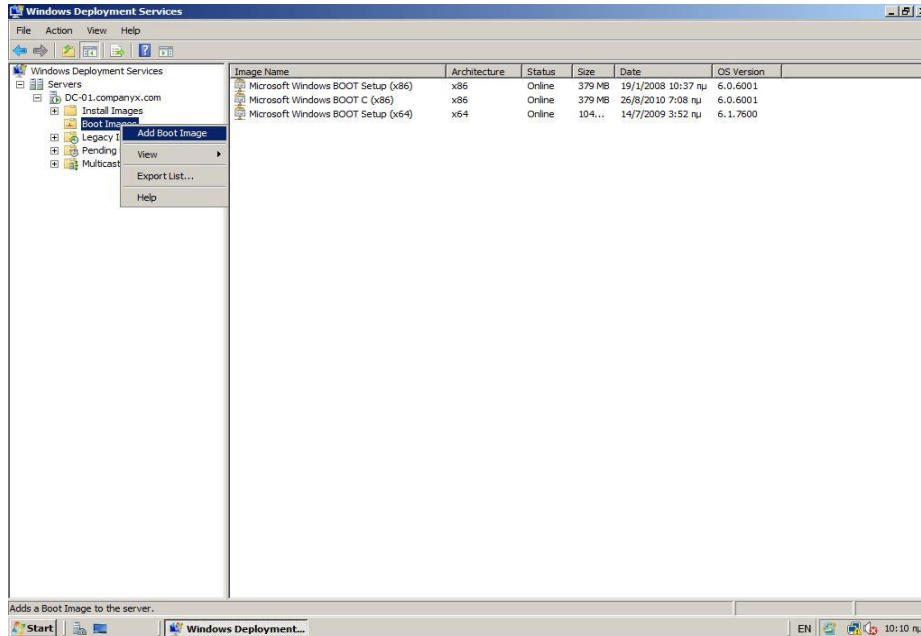
Εικ. 16.34

- Κάντε κλικ στο **Create Capture Boot Image**
- Πληκτρολογήστε ένα όνομα, μία περιγραφή και τη θέση αποθήκευσης του τοπικού αντιγράφου του αρχείου .wim. Πρέπει να ορίσετε μία τοπική τοποθεσία ώστε να είστε καλυμμένοι σε περίπτωση δικτυακού προβλήματος (Εικ. 16.35)



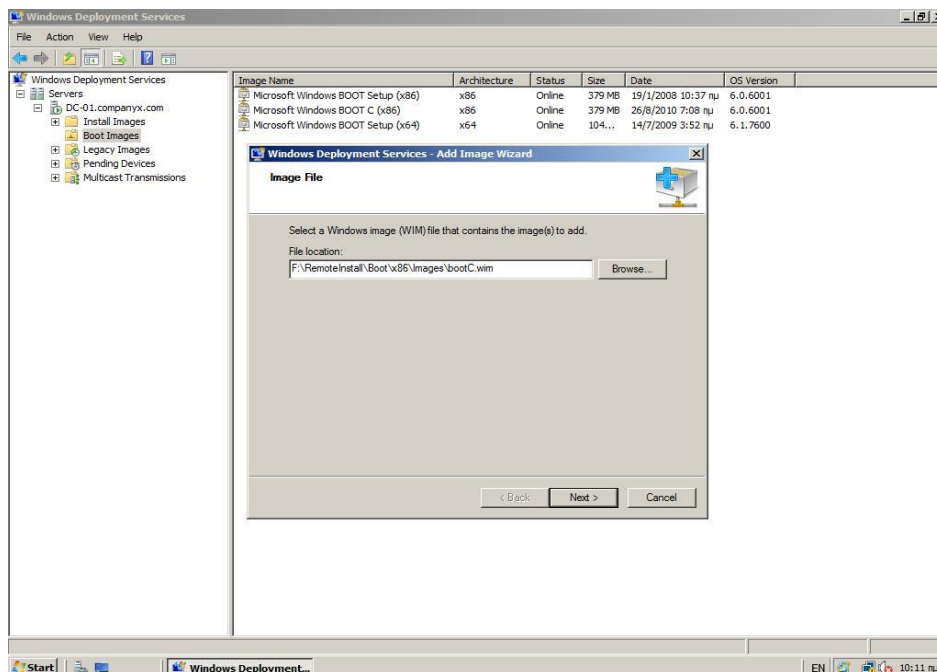
Εικ. 16.35

- Ακολουθήστε τις οδηγίες του wizard και όταν ολοκληρωθεί η διαδικασία πατήστε **Finish**
- Κάντε δεξί κλικ στο φάκελο **Boot Images** και μετά κλικ στο **Add Boot Image** (Εικ. 16.36)



Εικ. 16.36

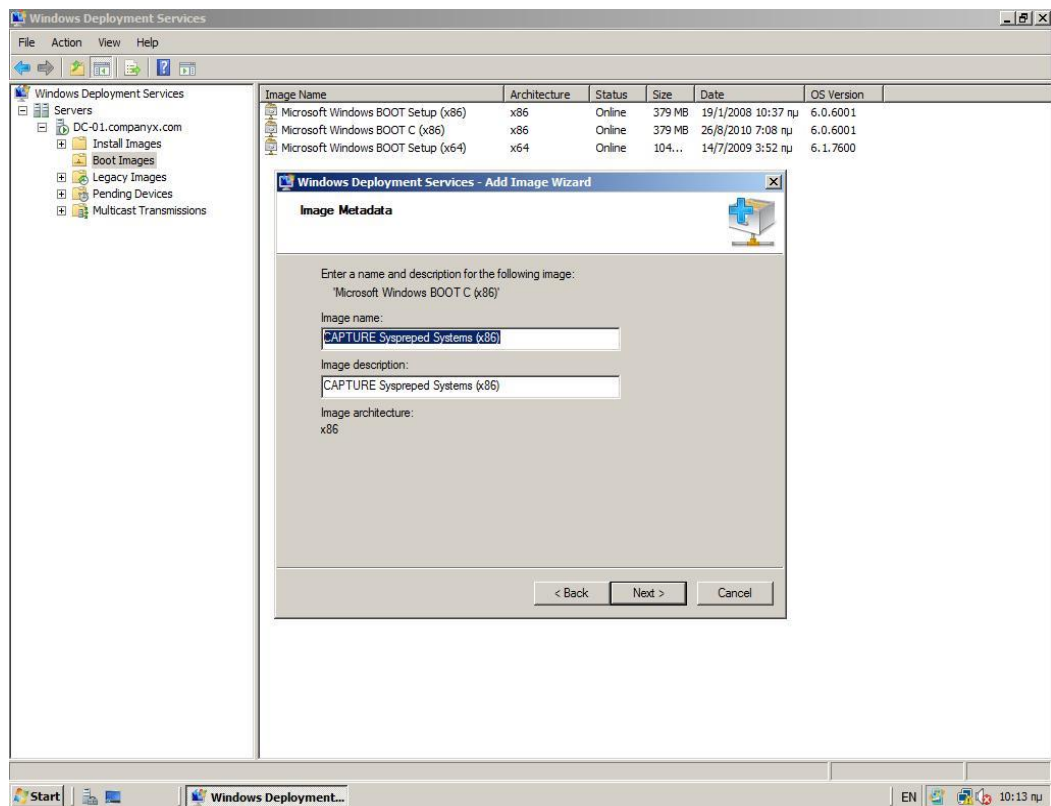
- Εντοπίστε και επιλέξτε τη νέα capture image και στη συνέχεια κάντε κλικ στο **Next** (Εικ. 16.37)



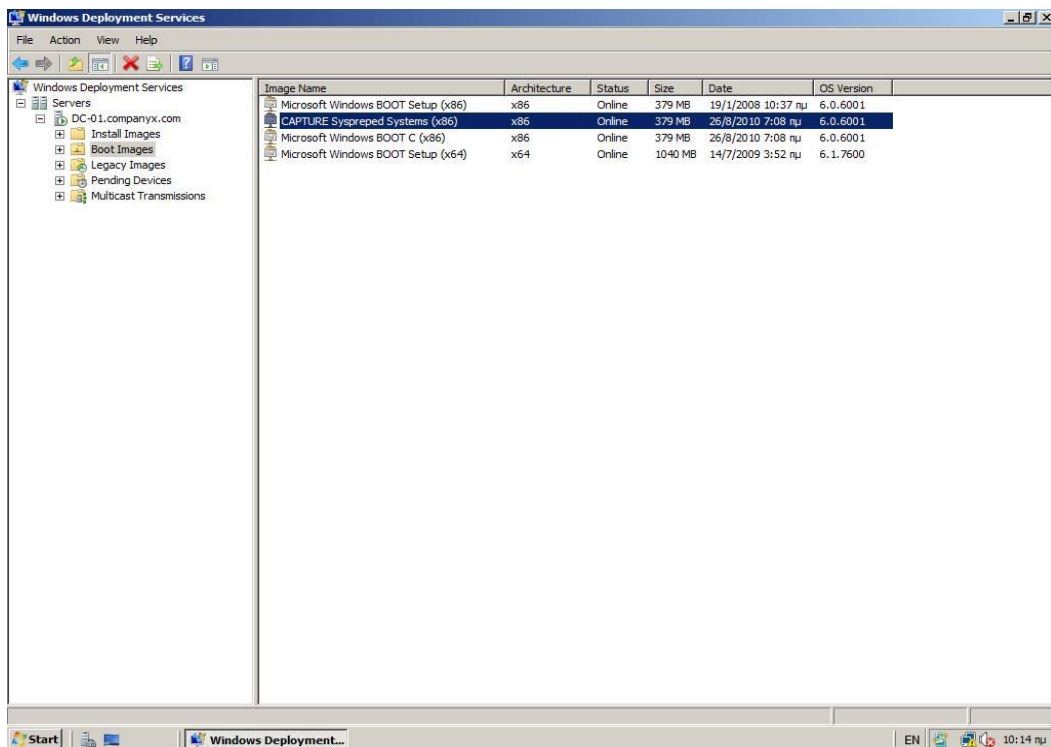
Εικ. 16.37

- Ακολουθήστε τις οδηγίες επί της οθόνης (Εικ. 16.38)

- Αφού δημιουργήσετε την capture image είστε έτοιμοι να εκκινήσετε από αυτή έναν client υπολογιστή για να κάνετε capture το λειτουργικό του σύστημα (Εικ. 16.39)



Εικ. 16.38



Εικ. 16.39

Χρήση command prompt

- Ανοίξτε ένα command prompt παράθυρο με διαχειριστικά δικαιώματα
- Πληκτρολογήστε την ακόλουθη εντολή, όπου <bootimage> το όνομα της boot image που θέλετε να χρησιμοποιήσετε για να δημιουργήσετε την capture image και <captureimage> η πλήρης διαδρομή και το πλήρες όνομα του αρχείου .wim της νέας capture image που θέλετε να δημιουργηθεί

**WDSUTIL /New-CaptureImage /Image:<bootimage> /Architecture:x86
/Filepath:<captureimage>**

- Πληκτρολογήστε την ακόλουθη εντολή, όπου <captureimage> η πλήρης διαδρομή και το πλήρες όνομα του αρχείου .wim της capture image που θέλετε να προσθέσετε στην αποθήκη εικόνων του Windows Deployment Services server

WDSUTIL /Add-Image /Imagefile:<captureimage> /ImageType:boot

- Αφού δημιουργήσετε την capture image είστε έτοιμοι να εκκινήσετε από αυτή έναν client υπολογιστή για να κάνετε capture το λειτουργικό του σύστημα

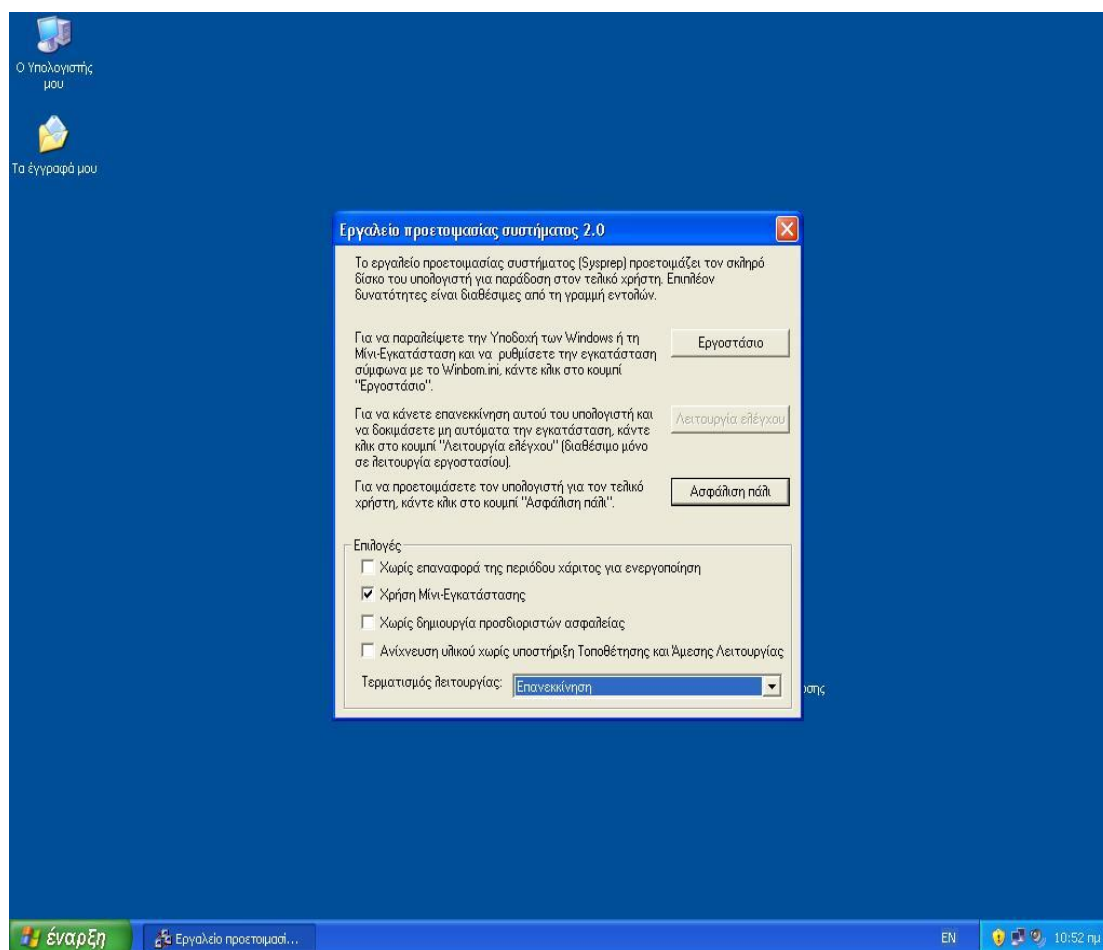
16.6.2 Διαδικασίες Δημιουργίας Install Image

Τώρα που έχετε μία capture image θα χρειαστεί να προετοιμάσετε τον υπολογιστή αναφοράς και στη συνέχεια να δημιουργήσετε την install image. Ο υπολογιστής αναφοράς μπορεί να έχει μία κανονική εγκατάσταση των Windows ή μία εγκατάσταση Windows παραμετροποιημένη για λειτουργία σε συγκεκριμένο περιβάλλον (συνηθέστερο). Εφόσον λοιπόν καταλήξετε στη παραμετροποίηση που θέλετε να έχει ο υπολογιστής (εφαρμογές, ρυθμίσεις περιβάλλοντος εργασίας, drivers κ.λπ.), τον προετοιμάζετε με Sysprep και τον εκκινείτε μέσα από την capture image. Ο οδηγός συλλαμβάνει (capture) την εγκατάσταση από τον υπολογιστή, δημιουργεί την install image και την αποθηκεύει στον υπολογιστή σε αρχείο .wim, δίνοντας παράλληλα τη δυνατότητα να την κάνει upload στον Windows Deployment Services server. Μετά και την ολοκλήρωση του upload η install image είναι έτοιμη για να εγκατασταθεί μαζικά σε πολλαπλούς υπολογιστές.

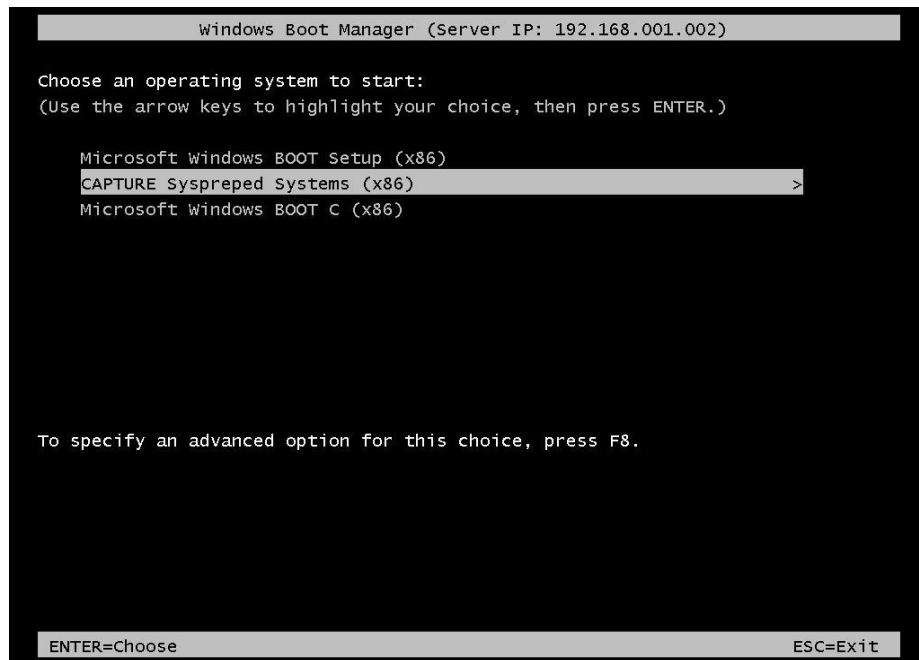
Ακολουθούν τα βήματα δημιουργίας της custom install image:

1. Δημιουργείτε έναν υπολογιστή αναφοράς (εγκαταστήστε λειτουργικό σύστημα, εφαρμογές, drivers και κάντε όσες αλλαγές και ρυθμίσεις επιθυμείτε)
2. Βεβαιωθείτε πως έχετε την σωστή έκδοση του Sysprep.exe στον υπολογιστή σας:

- Για Windows 7 (ή Windows Vista) η αντίστοιχη έκδοση του Sysprep.exe υπάρχει ήδη στο φάκελο **\Windows\System32\Sysprep** μαζί με το Setupcl.exe (χρειάζεται και αυτό)
 - Για Windows XP θα χρειαστεί να ανατρέξετε στο CD των Windows, στο φάκελο **\SUPPORT\TOOLS** όπου θα ανοίξετε το αρχείο **DEPLOY.CAB**. Από εκεί θα αντιγράψετε τα αρχεία sysprep.exe, setupcl.exe, setupmgr.exe σε ένα φάκελο (π.χ. SYSPREP) στον υπολογιστή αναφοράς
3. Ανάλογα λοιπόν με την έκδοση πληκτρολογήστε τα εξής:
- Σε υπολογιστή με Windows 7 (ή Windows Vista) εκτελέστε την εντολή **sysprep /oobe /generalize /reboot** (μπορείτε επίσης να χρησιμοποιήσετε το γραφικό περιβάλλον του Sysprep κάνοντας απλά διπλό κλικ στο **Sysprep.exe**)
 - Σε υπολογιστή με Windows XP εκτελέστε την εντολή **sysprep -mini -reseat -reboot** (μπορείτε επίσης και εδώ να χρησιμοποιήσετε το γραφικό περιβάλλον του Sysprep κάνοντας απλά διπλό κλικ στο **sysprep.exe**) (Εικ. 16.40)



Εικ. 16.40



Εικ. 16.41

4. Ο υπολογιστής θα τρέξει μία εργασία προετοιμασίας του συστήματος και θα κάνει επανεκκίνηση. Στην επανεκκίνηση κάντε boot από τον Windows Deployment Services server πατώντας **F12**
5. Στο boot menu επιλέξτε την capture image που δημιουργήσατε προηγουμένως και πατήστε **Enter** (Εικ. 16.41)
6. Ξεκινάει ο Windows Deployment Services Image Capture Wizard. Πατήστε **Next** (Εικ. 16.42)



Εικ. 16.42

7. Επιλέξτε το drive που θέλετε να γίνει capture και δώστε όνομα και περιγραφή για την εικόνα στα αντίστοιχα πεδία. Πατήστε **Next** για να συνεχίσετε (Εικ. 16.43)

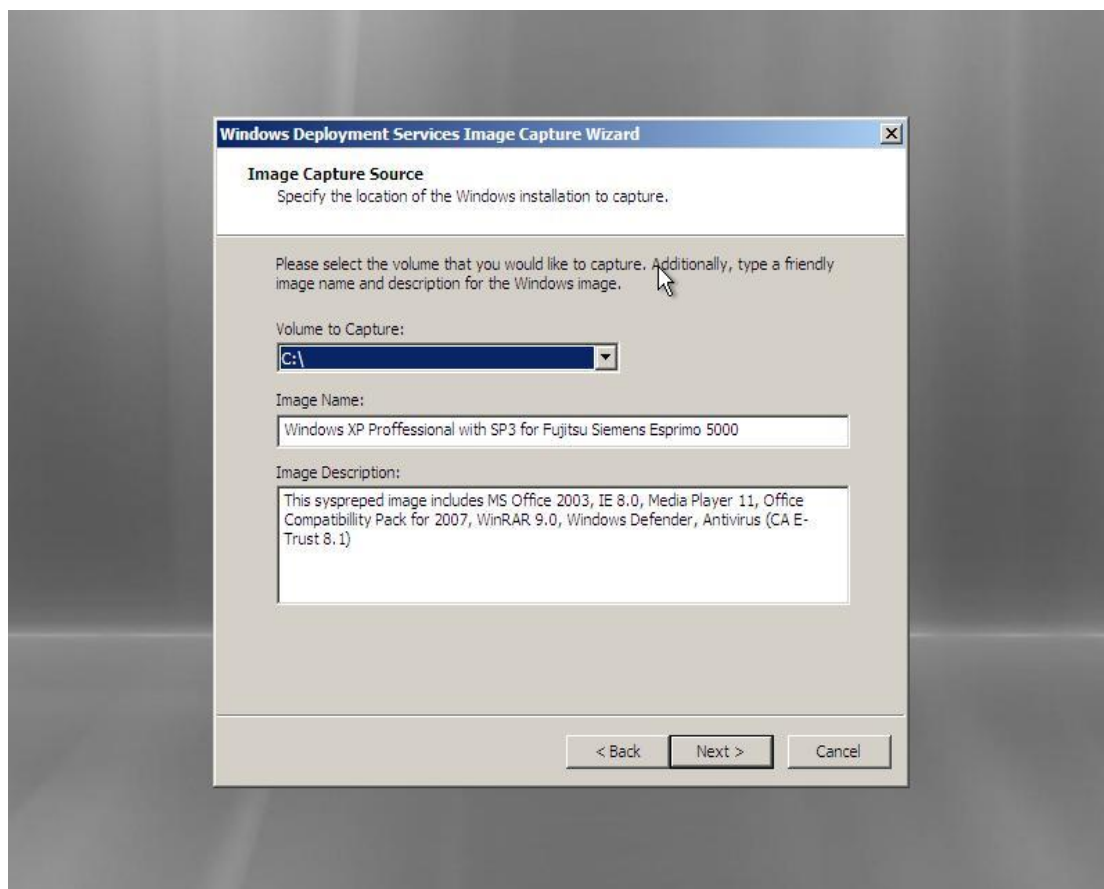
- **Προσοχή (!)** Θα δείτε εκείνα μόνο τα drives τα οποία περιέχουν λειτουργικό σύστημα προετοιμασμένο με Sysprep. Αν δεν εκτελέσετε την εντολή στο βήμα 3 δε θα δείτε drives για capture

8. Κάντε κλικ στο **Browse** για να επιλέξετε τον τοπικό φάκελο όπου θα αποθηκεύσετε την εικόνα

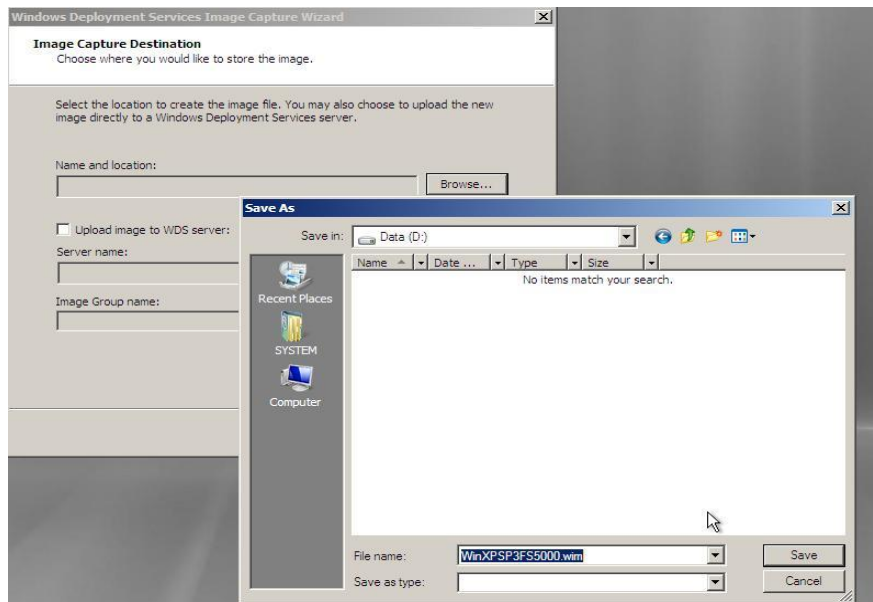
- **Προσοχή (!)** Πρέπει να δώσετε ένα τοπικό φάκελο για να αποθηκεύσετε τη νέα εικόνα αλλιώς η διαδικασία δεν μπορεί να συνεχίσει. Αυτή η απαίτηση επιβάλλεται για να αποφευχθεί αλλοίωση της εικόνας σε περίπτωση δικτυακής βλάβης κατά τη σύλληψη

9. Πληκτρολογήστε ένα όνομα για την εικόνα χρησιμοποιώντας την επέκταση αρχείου .wim και μετά πατήστε **Save** (Εικ. 16.44)

- **Προσοχή (!)** Πρέπει να πληκτρολογήσετε την επέκταση .wim στο όνομα του αρχείου προς αποθήκευση αλλιώς όλη η διαδικασία θα αποτύχει εμφανίζοντας μήνυμα λάθους

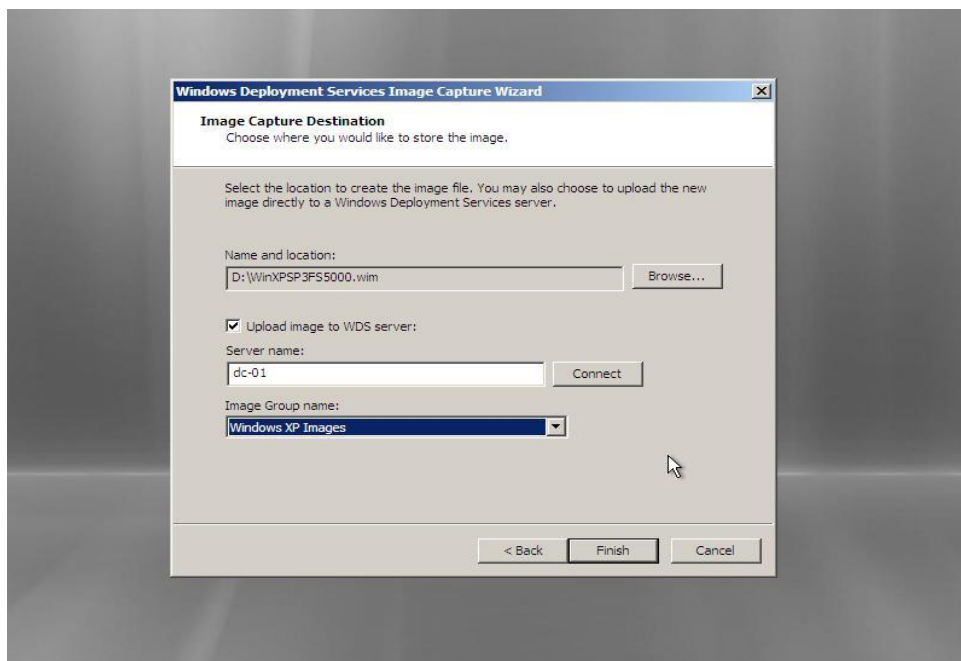


Εικ. 16.43



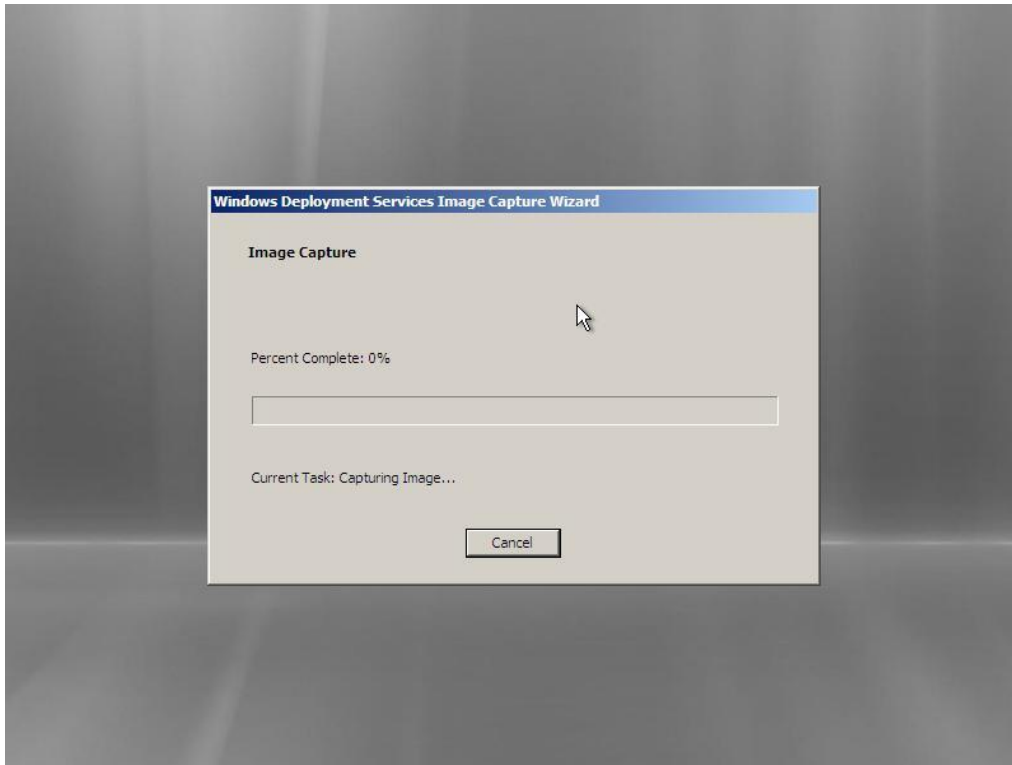
Εικ. 16.44

10. Επιλέξτε **Upload image to WDS server**
11. Πληκτρολογήστε το όνομα του Windows Deployment Services server και στη συνέχεια κάντε κλικ στο **Connect**
12. Στο παράθυρο σύνδεσης που θα εμφανιστεί δώστε όνομα χρήστη και κωδικό πρόσβασης ενός λογαριασμού με επαρκή δικαιώματα για να συνδεθεί στο Windows Deployment Services server
13. Επιλέξτε από τη λίστα **Image Group** την ομάδα εικόνων όπου θέλετε να αποθηκεύσετε την εικόνα και στη συνέχεια κάντε κλικ στο **Finish** (Εικ. 16.45)

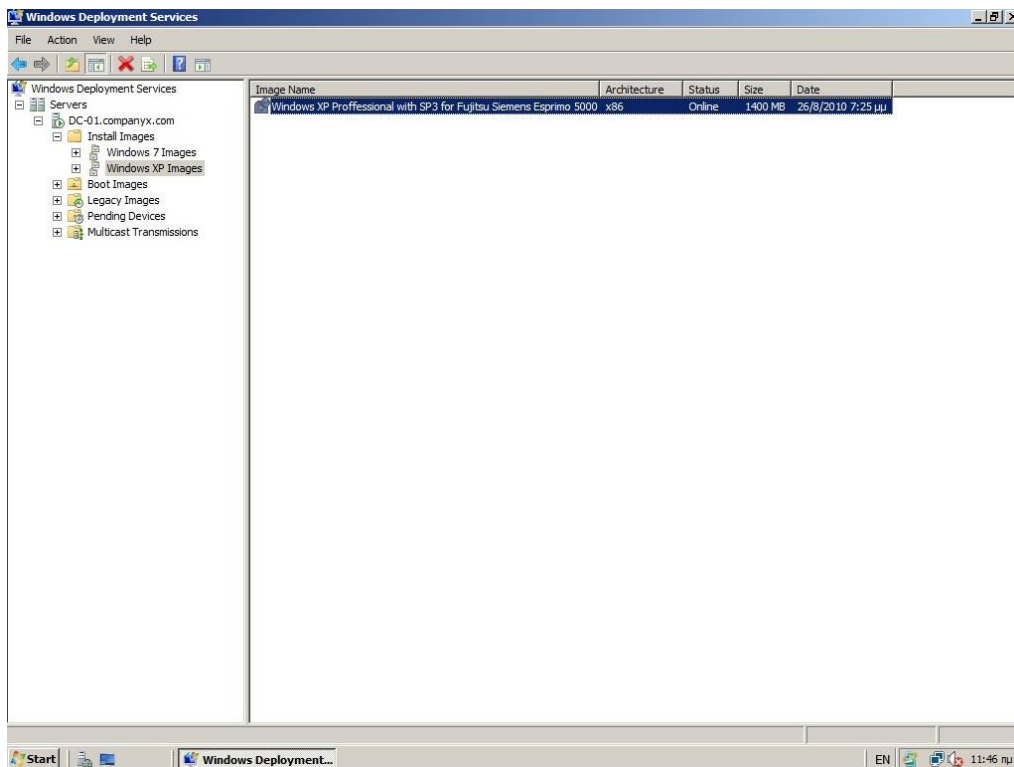


Εικ. 16.45

Όταν ολοκληρωθεί η διαδικασία (Εικ. 16.46) ο Windows Deployment Services server είναι έτοιμος να εγκαταστήσει την custom install image που μόλις δημιουργήσατε σε πολλαπλούς client υπολογιστές (Εικ. 16.47).



Εικ. 16.46



Εικ. 16.47

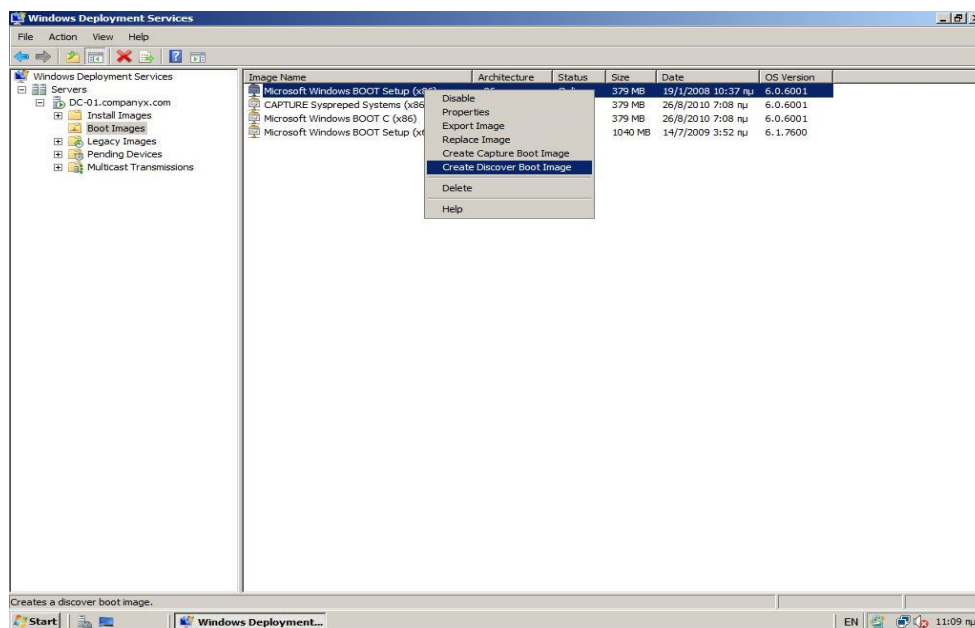
16.7 Discover Images

Οι discover images είναι boot images τις οποίες μπορείτε να χρησιμοποιήσετε για να εγκαταστήσετε λειτουργικό σύστημα σε υπολογιστή που δεν υποστηρίζει PXE. Όταν δημιουργείτε μία discover image την αποθηκεύετε σε ένα μέσο (CD, DVD, USB drive κ.λπ.) και στη συνέχεια εκκινείτε τον υπολογιστή από αυτό το μέσο. Η αποθηκευμένη discover image εντοπίζει τον Windows Deployment Services server και ο server εγκαθιστά την install image του λειτουργικού συστήματος στον client υπολογιστή. Μπορείτε επίσης να ρυθμίσετε discover images να εντοπίζουν συγκεκριμένους servers αν στο δίκτυό σας υπάρχουν πολλαπλοί Windows Deployment Services Servers.

Μπορείτε να δημιουργήσετε discover images είτε με τη χρήση της κονσόλας Windows Deployment Services είτε με την εντολή WDSUTIL.exe. Αφού δημιουργήσετε την discover image δημιουργήστε και το μέσο που θα την περιέχει. Για τη δημιουργία της discover image πρέπει να χρησιμοποιήσετε το Boot.wim αρχείο από το DVD των Windows Server 2008.

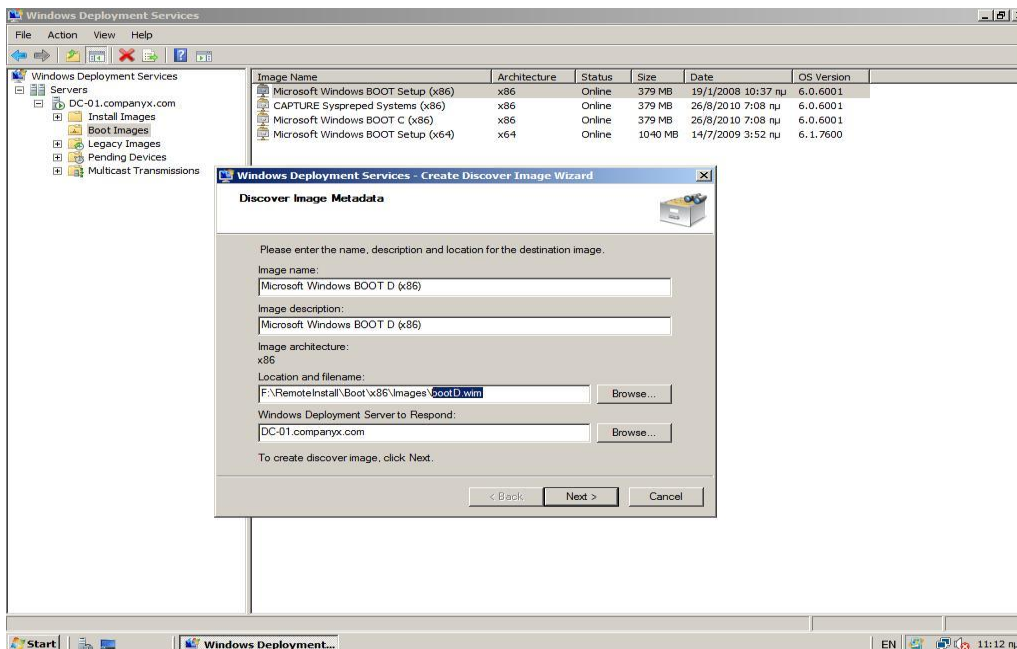
Χρήση κονσόλας MMC

1. Στο αριστερό τμήμα της κονσόλας Windows Deployment Services αναπτύξτε το φάκελο **Boot Images**
2. Κάντε δεξί κλικ στην εικόνα που θέλετε να χρησιμοποιήσετε σαν discover image (boot.wim) και στη συνέχεια κλικ στο **Create Discover Boot Image** (Εικ. 16.48)



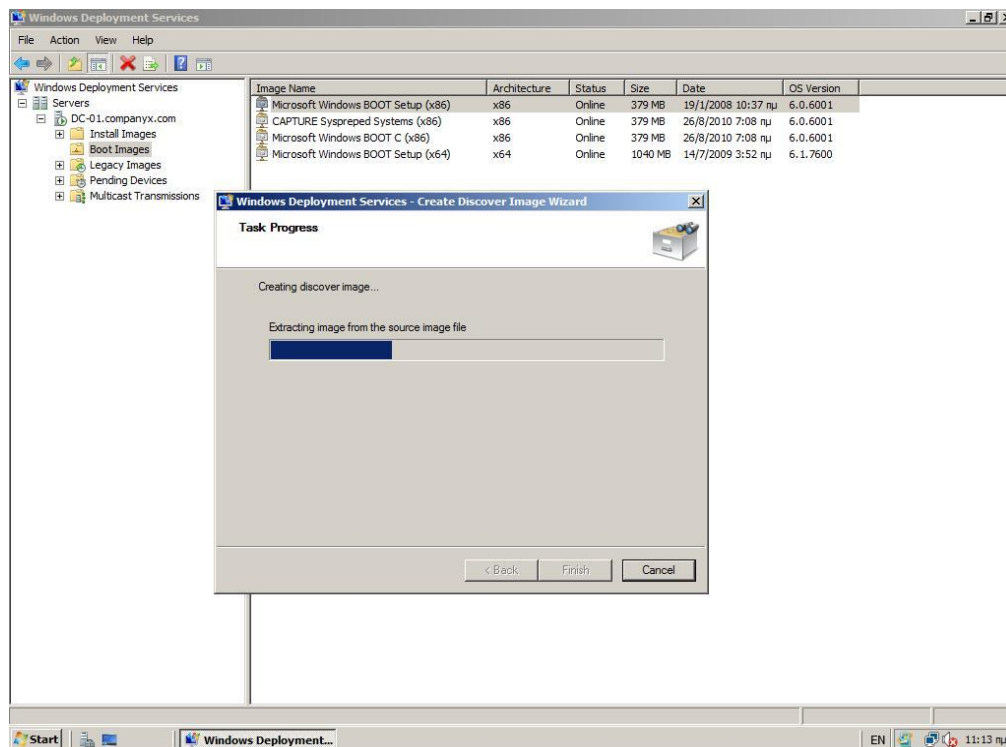
Εικ. 16.48

3. Πληκτρολογήστε όνομα, περιγραφή, πλήρη διαδρομή και όνομα αρχείου .wim (π.χ. **bootD.wim**) για τη discover image που θέλετε να δημιουργήσετε και στη συνέχεια κάντε κλικ στο **Next**. Μπορείτε επίσης να ορίσετε συγκεκριμένο WDS server (Εικ. 16.49)

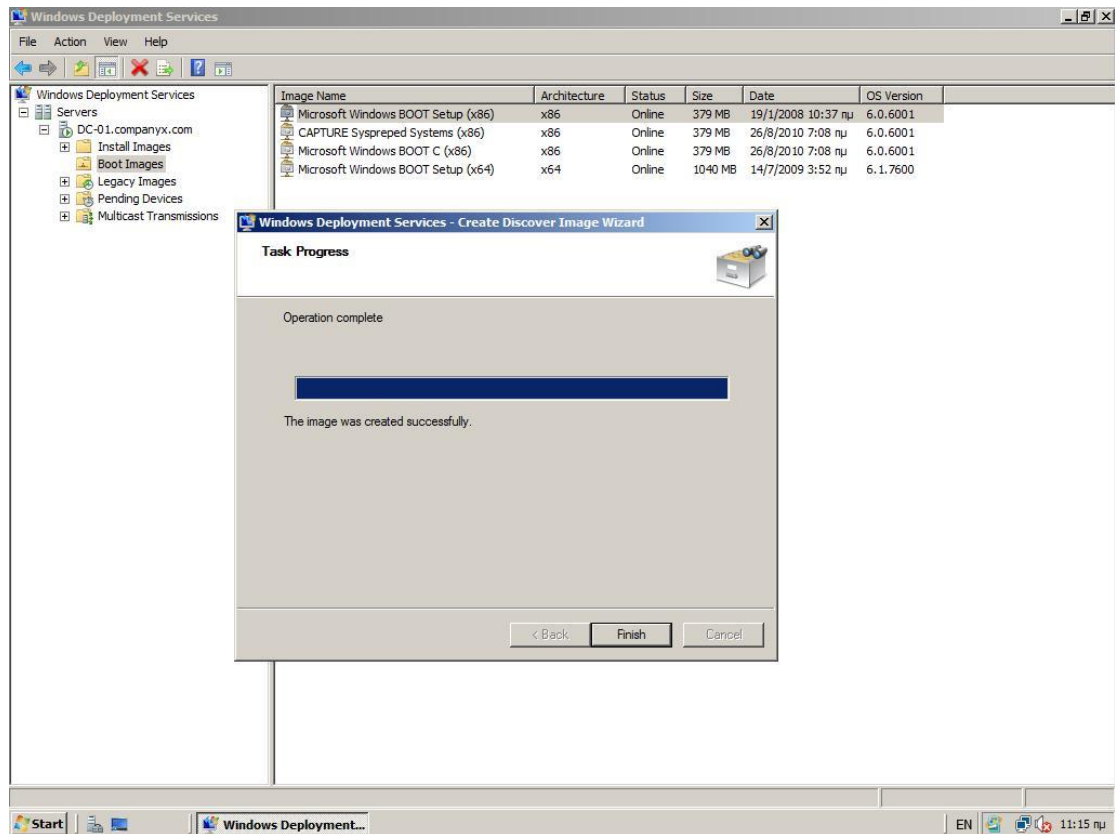


Εικ. 16.49

4. Ξεκινάει η διαδικασία δημιουργίας της εικόνας (Εικ. 16.50) και αφού ολοκληρωθεί πατήστε **Finish** (Εικ. 16.51)

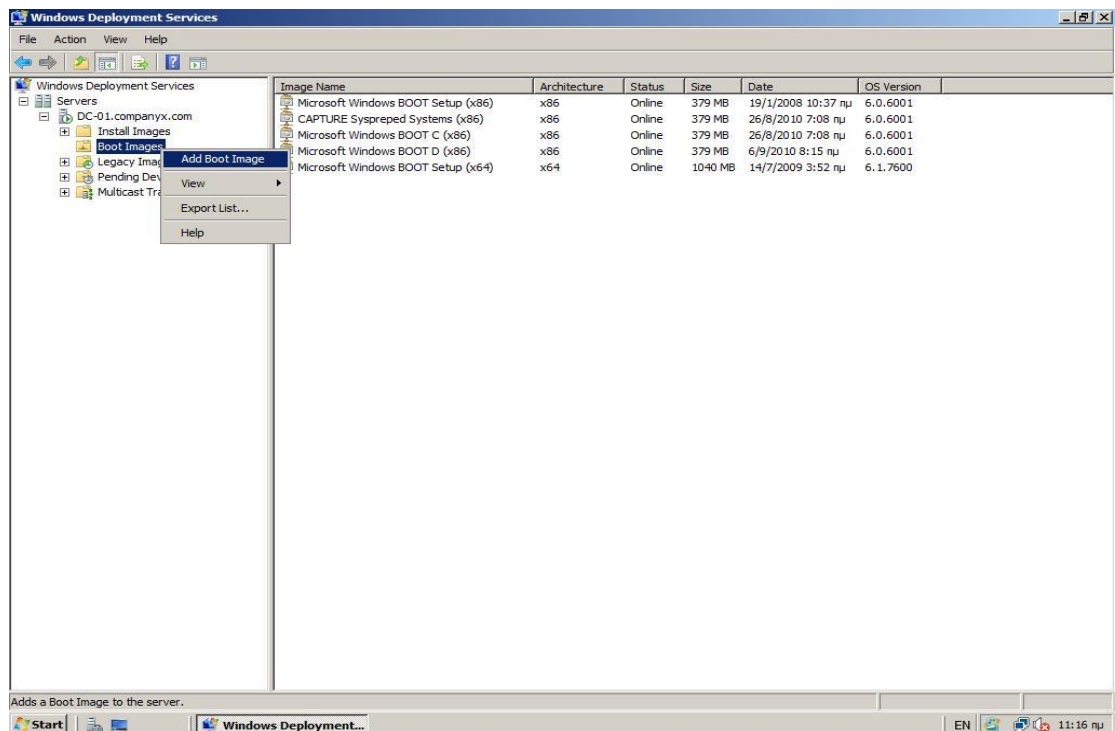


Εικ. 16.50



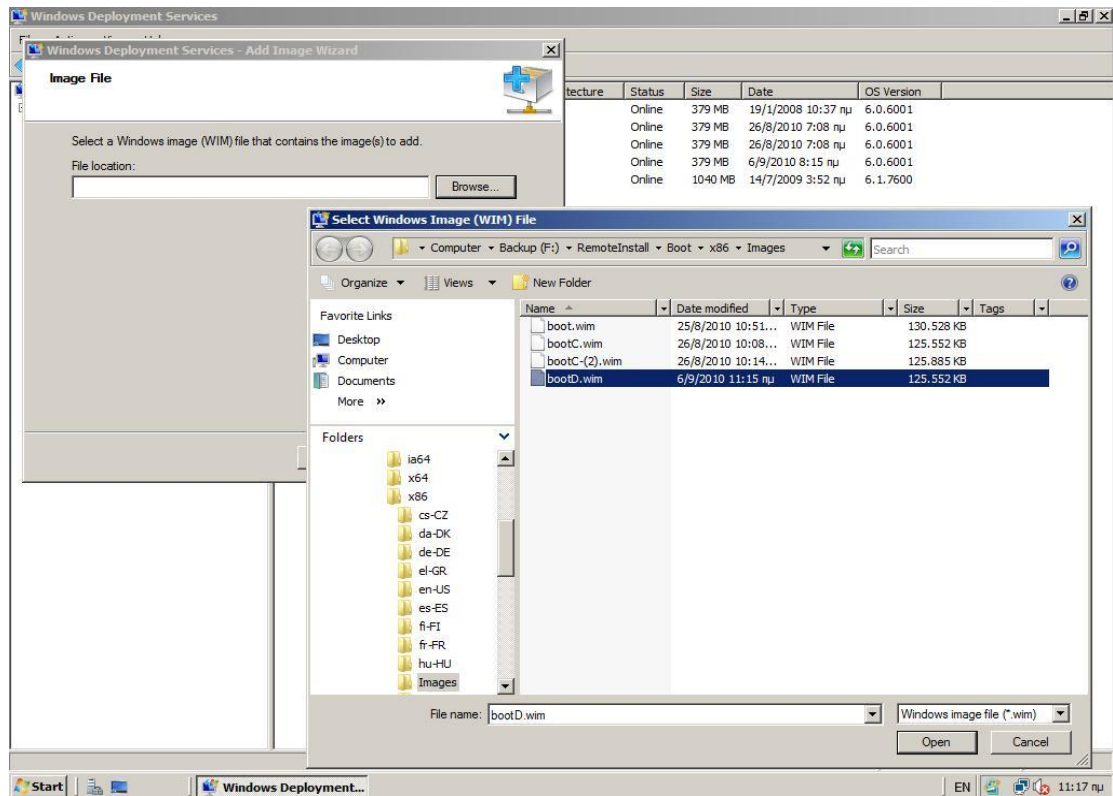
Εικ. 16.51

5. Κάντε δεξί κλικ στο φάκελο **Boot Images** και στη συνέχεια κλικ στο **Add Boot Image** (Εικ. 16.52)

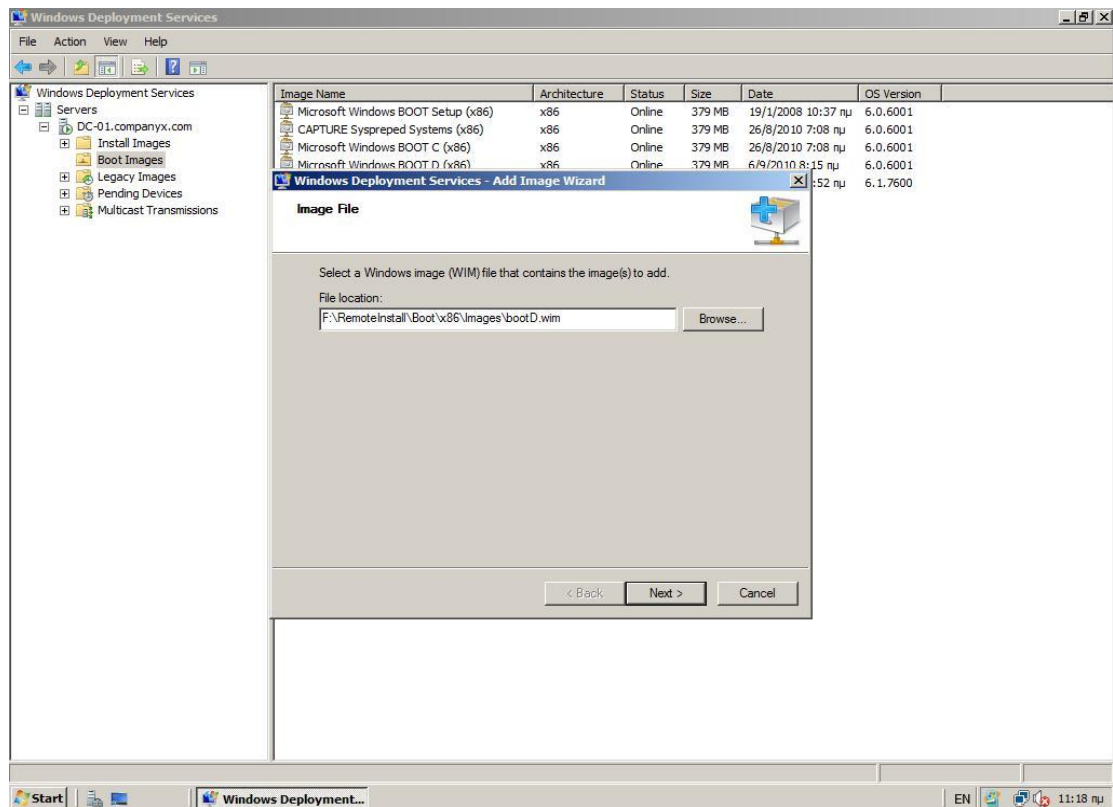


Εικ. 16.52

6. Εντοπίστε (**Browse**) και επιλέξτε τη νέα discover image (Εικ. 16.53) και στη συνέχεια πατήστε **Next** (Εικ. 16.54)

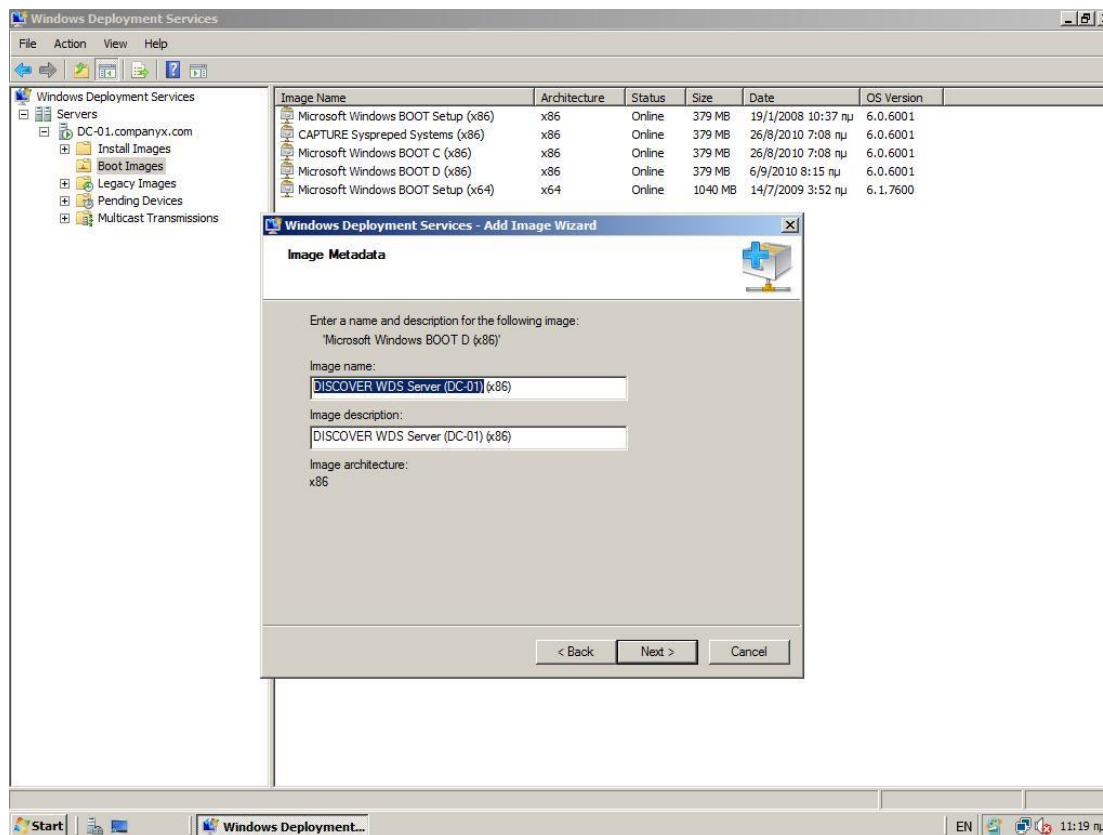


Εικ. 16.53



Εικ. 16.54

7. Πληκτρολογήστε **όνομα** και **περιγραφή** της νέας discover image που θέλετε να προσθέσετε στο boot menu (Εικ. 16.55) και πατήστε **Next**



Εικ. 16.55

8. Όταν ολοκληρωθεί η διαδικασία προσθήκης (Εικ. 16.56) κάντε κλικ στο **Finish** (Εικ. 16.57)

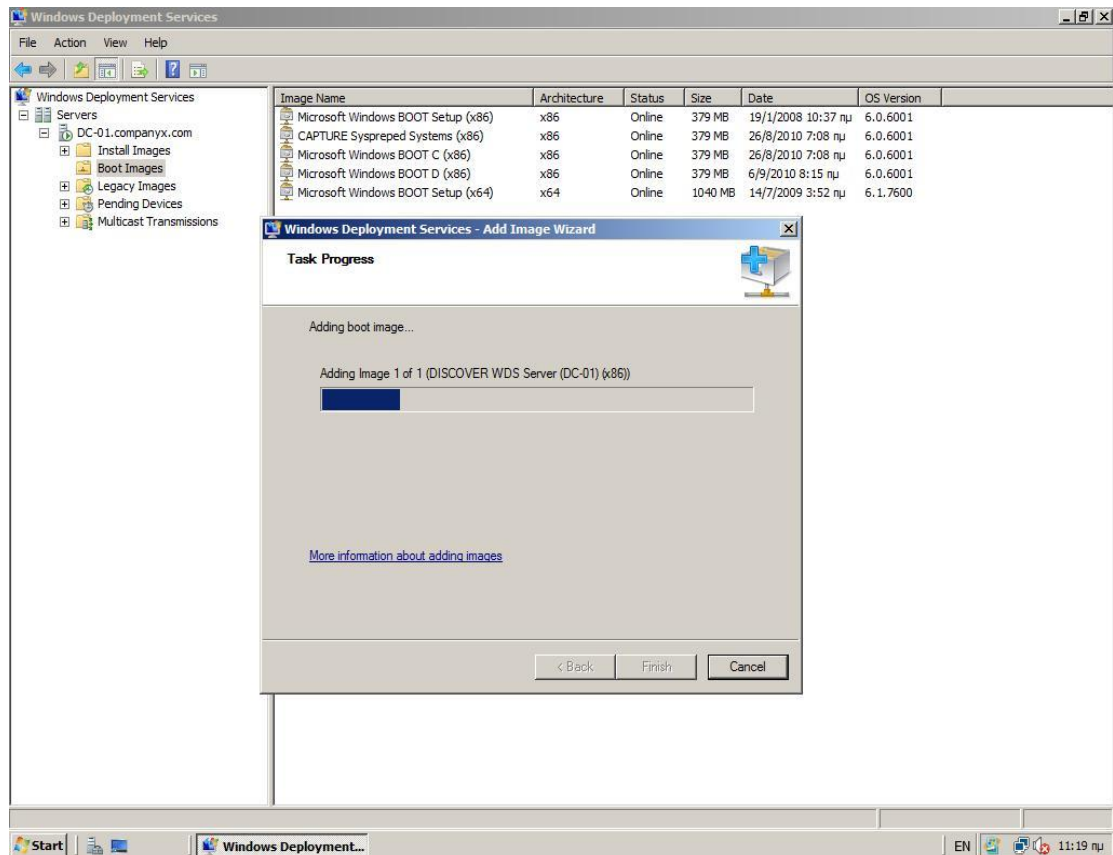
Χρήση command prompt

1. Ανοίξτε ένα παράθυρο command prompt με διαχειριστικά δικαιώματα
2. Πληκτρολογήστε την ακόλουθη εντολή όπου <bootimage> το όνομα της boot image που θα χρησιμοποιήσετε για να δημιουργήσετε την discover image και <discoverimage> η διαδρομή και το όνομα αρχείου της discover image που θα αποθηκευτεί:

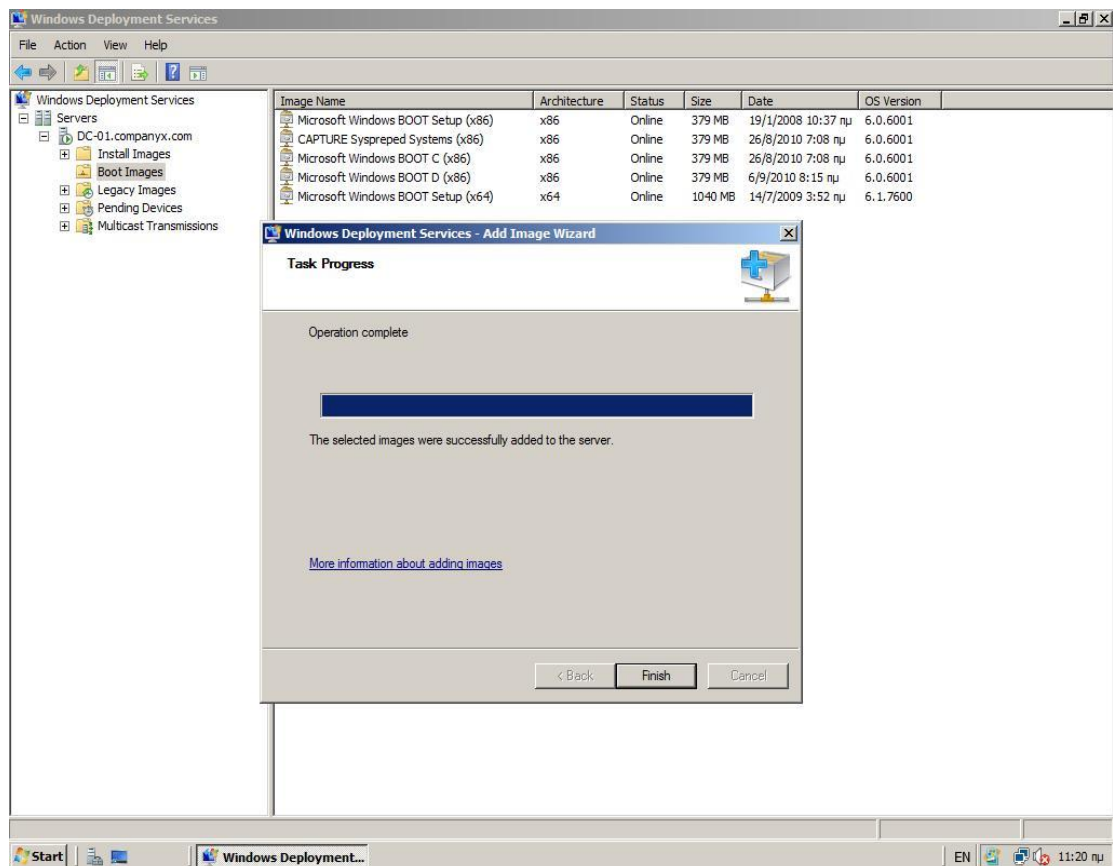
**WDSUTIL /New-DiscoverImage /Image:<bootimage> /Architecture:x86
/Filepath:<discoverimage>**

3. Για να προσθέσετε την discover image στην αποθήκη εικόνων πληκτρολογήστε την ακόλουθη εντολή όπου <discoverimage> η διαδρομή και το όνομα αρχείου της discover image που θα προστεθεί:

WDSUTIL /Add-Image /ImageFile:<discoverimage> /ImageType:boot



Εκ. 16.56



Εκ. 16.57

Δημιουργία μέσου που θα περιέχει την discover image

1. Κατεβάστε και εγκαταστήσατε το Windows AIK
(<http://go.microsoft.com/fwlink/?LinkId=136976>)
2. Ανοίξτε ένα command prompt και πληκτρολογήστε την ακόλουθη εντολή για να μεταβείτε στο φάκελο PETools:

Cd C:\Program Files\Windows AIK\Tools\PETools

3. Για να δημιουργήσετε ένα περιβάλλον Windows PE πληκτρολογήστε:

CopyPE <architecture> C:\Winpe

4. Για να αντιγράψετε την discover image που δημιουργήσατε στην προηγούμενη διαδικασία πληκτρολογήστε:

Copy /y c:\boot.wim c:\Winpe\ISO\Sources

5. Μεταβείτε ξανά στο φάκελο PETools
6. Για να δημιουργήσετε την boot image σε μορφή .iso πληκτρολογήστε:

Oscdimg -n -bc:\winpe\ISO\boot\etfsboot.com c:\winpe\ISO c:\winpe.iso

7. Χρησιμοποιήστε ένα τρίτο πρόγραμμα για να κάψετε ένα boot CD (ή DVD) με το αρχείο .iso
8. Εκκινήστε τον client υπολογιστή από το CD. Ίσως χρειαστεί να αλλάξετε τη σειρά εκκίνησης από το BIOS. Όταν ο client υπολογιστής εκκινήσει η οθόνη σας (και η εμπειρία) θα είναι ακριβώς σαν να είχατε εκκινήσει από το δίκτυο.

Windows Server Update Services (WSUS)

17.1 Γενικά για το WSUS

Ο ρόλος Windows Server Update Services (για συντομία, στο εξής WSUS) 3.0 Service Pack 2 (WSUS 3.0 SP2) προσφέρει μία περιεκτική λύση για τη διαχείριση των ενημερώσεων (updates) στο δίκτυό σας. Σε αυτό το κεφάλαιο θα βρείτε οδηγίες για την εγκατάσταση και τη χρήση των βασικών λειτουργιών του WSUS. Συγκεκριμένα θα βρείτε οδηγίες και διαδικασίες για τα ακόλουθα:

1. Απαιτήσεις εγκατάστασης του WSUS
2. Εγκατάσταση WSUS Server ή Administration Console
3. Ρυθμίσεις δικτύου για το WSUS
4. Παραμετροποίηση ενημερώσεων και συγχρονισμού
5. Παραμετροποίηση WSUS clients με χρήση πολιτικών (GPO)
6. Παραμετροποίηση ομάδων υπολογιστών
7. Έγκριση και διάθεση ενημερώσεων μέσω WSUS
8. Αυτόματη έγκριση ενημερώσεων
9. WSUS για απομονωμένα δίκτυα
10. Διαχείριση αναφορών

17.1.1 Περισσότερες πληροφορίες

Για περισσότερες πληροφορίες σχετικά με την εγκατάσταση και τη χρήση του WSUS, επισκεφθείτε τα ακόλουθα links.

The WSUS Deployment Guide, <http://go.microsoft.com/fwlink/?LinkId=139832>.

The WSUS Operations Guide, <http://go.microsoft.com/fwlink/?LinkId=139838>.

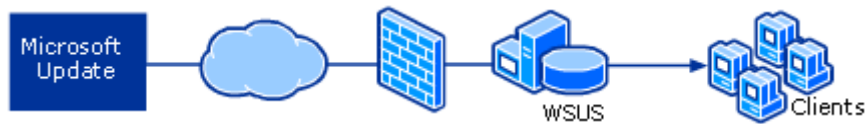
The WSUS Release Notes, <http://go.microsoft.com/fwlink/?LinkId=139840>.

17.1.2 WSUS Clients

Σε αυτό το κεφάλαιο, η χρήση της λέξης clients αναφέρεται και στους clients του δικτύου σας (δηλαδή στους σταθμούς εργασίας) αλλά και στους clients του WSUS. Clients του WSUS όμως, είναι και οι υπόλοιποι servers του δικτύου σας. Η διάκριση είναι προφανής κάθε φορά, εφεξής λοιπόν δεν θα κάνουμε διάκριση μεταξύ workstation και WSUS client.

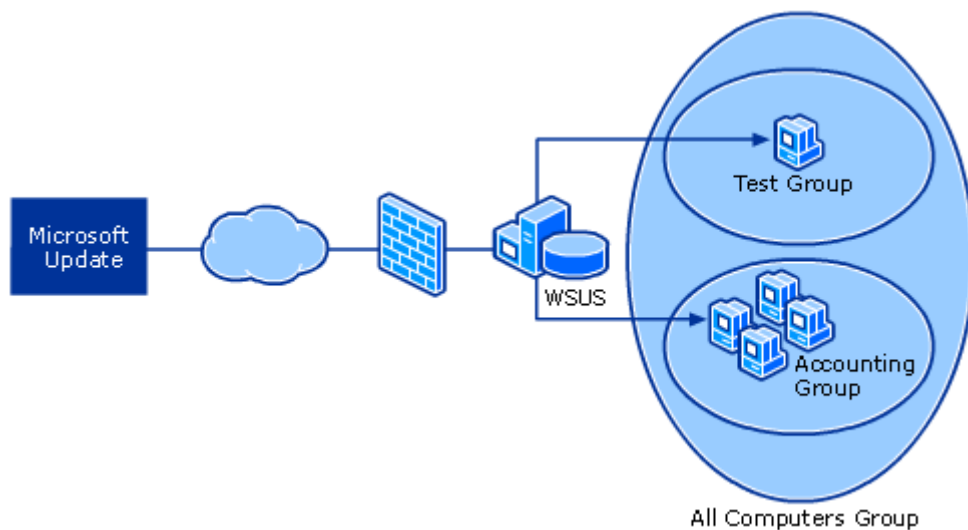
17.1.3 Τοπολογία WSUS

Η απλούστερη δυνατή τοπολογία WSUS είναι να έχετε έναν μόνο WSUS server στο δίκτυο σας και όλοι οι clients να ανήκουν σε μία ομάδα υπολογιστών.



Εικ. 17.1. Απλή τοπολογία WSUS με έναν μόνο server

Λίγο πιο σύνθετη τοπολογία είναι η «παραλλαγή» που ακολουθεί. Σε αυτή την τοπολογία έχουμε πάλι έναν μόνο WSUS server, αλλά τώρα οι clients ανήκουν σε περισσότερες από μία ομάδες υπολογιστών. Έτσι, διαθέτουμε μόνο έναν WSUS να διαχειριστούμε αλλά περισσότερες επιλογές σε ότι αφορά τους clients.



Εικ. 17.2. Ένας WSUS server με ομάδες υπολογιστών

Σε μεγαλύτερες εγκαταστάσεις, μπορεί να χρειαστείτε περισσότερους από έναν WSUS servers. Σε αυτή την περίπτωση μπορείτε να δημιουργήσετε σύνθετες τοπολογίες WSUS servers και να μην αρκεστείτε στην απλοϊκή εκδοχή των πολλαπλών ανεξάρτητων WSUS servers. Αφού έχετε τη δυνατότητα να συγχρονίζετε έναν WSUS server με έναν άλλο αντί του Microsoft Update, χρειάζεται να έχετε έναν μόνο WSUS server που συνδέεται με το Microsoft Update. Όταν συνδέετε μεταξύ τους WSUS servers, υπάρχει ένας *upstream* WSUS server και ένας *downstream* WSUS server, όπως φαίνεται και στην παρακάτω εικόνα.



Εικ. 17.3. Ιεραρχία WSUS Servers

Υπάρχουν δύο τρόποι για να συνδέσετε WSUS servers:

Autonomous mode: Ο upstream WSUS server μοιράζεται τις ενημερώσεις με τον ή τους downstream servers κατά τη διάρκεια του συγχρονισμού, αλλά δεν μοιράζεται

πληροφορίες σχετικά με τις εγκρίσεις των ενημερώσεων ή τις ομάδες υπολογιστών. Έτσι οι downstream WSUS servers χρειάζονται ξεχωριστή διαχείριση. Οι αυτόνομοι servers μπορούν ακόμα να συγχρονίζουν για ένα σύνολο γλωσσών που είναι υποσύνολο των γλωσσών του upstream server με τον οποίο συνδέονται.

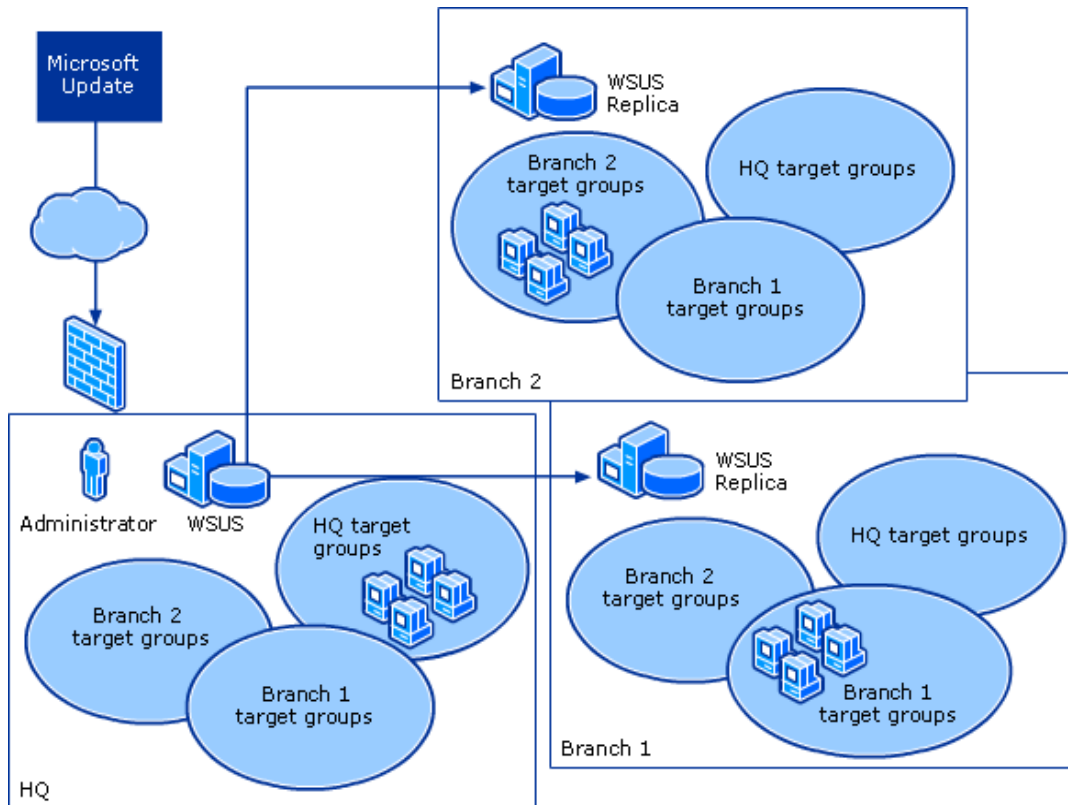
Replica mode: Ο upstream WSUS server μοιράζεται ενημερώσεις, κατάσταση έγκρισεων και ομάδες υπολογιστών με τον ή τους downstream servers. Οι downstream replica servers κληρονομούν τις εγκρίσεις και δε μπορούν να διαχειριστούν ξεχωριστά από τον upstream WSUS server με τον οποίο συνδέονται.

Όταν χρησιμοποιείτε περισσότερους από έναν WSUS servers πρέπει να συνδέονται όλοι οι downstream servers με έναν μόνο WSUS server (αυτόν που επικοινωνεί απευθείας με το Windows Update). Αυτό εξασφαλίζει ταχύτητα διάδοσης των ενημερώσεων και λιγότερα προβλήματα στην επικοινωνία μεταξύ των WSUS servers. Επίσης, πρέπει να εξασφαλίσετε ότι όλοι οι WSUS servers του δικτύου σας έχουν την ίδια ώρα συστήματος. Αν οι WSUS servers σας δεν έχουν την ίδια ώρα, οι downstream servers θα κατεβάζουν τις ενημερώσεις και θα τις διαθέτουν στους clients αλλά δεν θα μπορούν να ενημερώνουν τον upstream server για την πρόοδο των εργασιών τους, με αποτέλεσμα να έχετε συνολικά λανθασμένη εικόνα για την κατάσταση των ενημερώσεων στο δίκτυό σας. Τέλος, καλό θα είναι να χρησιμοποιείτε για κάθε downstream server διαφορετικό πρόγραμμα συγχρονισμού ώστε να μην έχετε προβλήματα με το bandwidth του δικτύου σας.

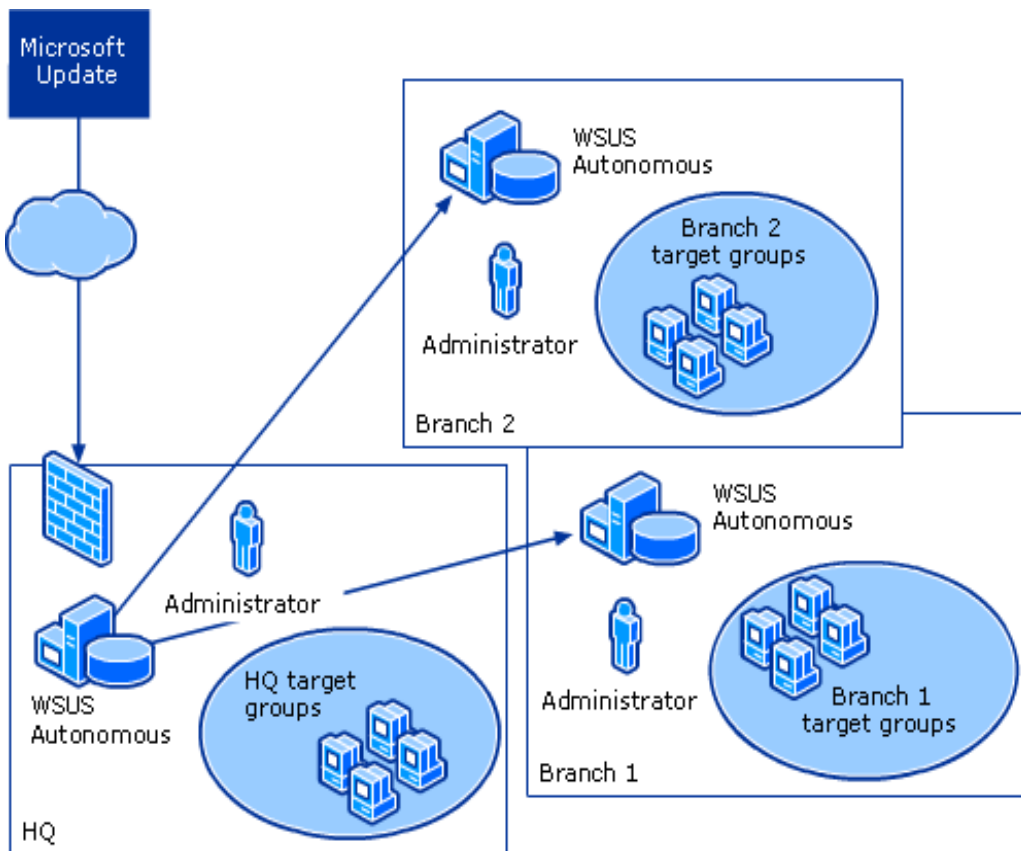
Ακόμα υπάρχει η δυνατότητα υποστήριξης απομονωμένων δικτύων (δικτύων δηλαδή που δεν συνδέονται στο Internet). Περισσότερα για αυτή την περίπτωση καθώς και διαδικασίες που μπορείτε να ακολουθήσετε προκειμένου να υποστηρίξετε απομονωμένα δίκτυα, θα βρείτε στη σχετική παράγραφο.

Για περισσότερο σύνθετες περιπτώσεις, π.χ. χρήση WSUS με SQL cluster ή roaming clients, μπορείτε να συμβουλευτείτε το WSUS Deployment Guide, στη διεύθυνση <http://go.microsoft.com/fwlink/?LinkId=139832>.

Ανάλογα με τη δομή του δικτύου σας και το προσωπικό της υπηρεσίας σας, μπορείτε να χρησιμοποιήσετε δύο τρόπους διαχείρισης του WSUS, όπως φαίνεται στις παρακάτω εικόνες. Ανάλογα με το μοντέλο διαχείρισης που θα επιλέξετε, θα χρησιμοποιήσετε και την επιλογή autonomous ή replica mode για τους downstream servers σας. Φυσικά, ανάλογα με τη δομή και το διαθέσιμο προσωπικό μπορεί να χρειάζεστε συνδυασμό και των δύο τρόπων (autonomous και replica) που αναφέραμε.

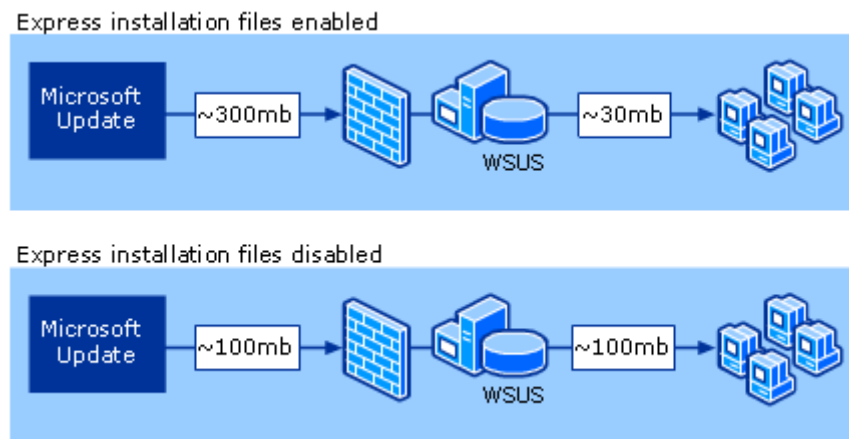


Εικ. 17.4. Κεντρική διαχείριση WSUS (Replica Servers)



Εικ. 17.5. Κατανεμημένη διαχείριση WSUS (Autonomous servers)

Αρχεία express εγκατάστασης (express installation files)



Εικ. 17.6. Αρχεία express εγκατάστασης

Η χρήση των αρχείων express εγκατάστασης προσφέρει έναν εναλλακτικό τρόπο διάθεσης ενημερώσεων. Μπορείτε να χρησιμοποιείτε τα αρχεία express εγκατάστασης για να ελαχιστοποιείται το bandwidth στο εσωτερικό σας δίκτυο, όμως αυτό θα έχει ως επακόλουθο να χρησιμοποιείτε περισσότερο bandwidth στη σύνδεσή σας προς το Internet. Η προκαθορισμένη ρύθμιση του WSUS είναι να μην χρησιμοποιεί αρχεία express εγκατάστασης.

17.2 Εγκατάσταση WSUS

17.2.1 Πριν από την εγκατάσταση

Προτού ξεκινήσετε την εγκατάσταση, επιβεβαιώστε ότι ο server και οι clients σας πληρούν τις απαιτήσεις εγκατάστασης (system requirements) και ότι έχετε τα απαραίτητα δικαιώματα για την ολοκλήρωση της εγκατάστασης.

17.2.2 Υλικό και λογισμικό για την εγκατάσταση του WSUS

- Επιβεβαιώστε ότι ο server πληροί τις απαιτήσεις συστήματος για το υλικό, το λειτουργικό σύστημα και άλλο λογισμικό. Οι απαιτήσεις εγκατάστασης του WSUS 3.0 SP2 είναι διαθέσιμες εδώ: <http://go.microsoft.com/fwlink/?LinkId=139840>. Εάν χρησιμοποιείτε το Server Manager για να εγκαταστήσετε το WSUS, μπορείτε να επιβεβαιώσετε τις απαιτήσεις εγκατάστασης (εν προκειμένω μόνο για άλλο λογισμικό, αφού βρίσκεστε σε server οι απαιτήσεις υλικού και λειτουργικού συστήματος πληρούνται ήδη) ακολουθώντας τις οδηγίες στη παράγραφο «Προετοιμασία εγκατάστασης του WSUS 3.0 SP2», εδώ παρακάτω.
- Εάν έχετε κάνει εγκαταστάσεις ρόλων ή ενημερώσεων λογισμικού που απαιτούν επανεκκίνηση του server σας, επανεκκινήστε το server σας πριν ξεκινήσετε την εγκατάσταση του WSUS.

17.2.3 Απαιτήσεις εγκατάστασης (software requirements) για clients

Ο client για το WSUS είναι η εφαρμογή Automatic Updates, η οποία δεν έχει απαιτήσεις υλικού από τον υπολογιστή στον οποίο εγκαθίσταται παρά μόνο να είναι συνδεδεμένος σε δίκτυο.

- Επιβεβαιώστε ότι ο υπολογιστής στον οποίο εγκαθιστάτε το Automatic Updates πληροί τις προδιαγραφές εγκατάστασης του WSUS για clients. Οι απαιτήσεις εγκατάστασης του WSUS 3.0 SP2 είναι διαθέσιμες στη σελίδα <http://go.microsoft.com/fwlink/?LinkId=139840>.
- Εάν κάνατε εγκαταστάσεις ρόλων ή ενημερώσεων λογισμικού που απαιτούν επανεκκίνηση του client σας, επανεκκινήστε τον πριν ξεκινήσετε την εγκατάσταση του WSUS.

17.2.4 Δικαιώματα

Τα ακόλουθα δικαιώματα απαιτούνται για τους χρήστες και τους φακέλους:

- Ο λογαριασμός NT Authority\Network Service πρέπει να έχει δικαιώματα πλήρους πρόσβασης (Full Control) στους ακόλουθους φακέλους έτσι ώστε η κονσόλα διαχείρισης του WSUS (WSUS Administration MMC snap-in) να εμφανίζεται και να

λειτουργεί κανονικά:

✓ %windir%\Microsoft .NET\Framework\v2.0.50727\Temporary
ASP.NET Files

✓ %windir%\Temp

- Επιβεβαιώστε ότι ο λογαριασμός που σκοπεύετε να χρησιμοποιήσετε για την εγκατάσταση του WSUS είναι μέλος της ομάδας χρηστών Local Administrators.

17.2.5 Προετοιμασία εγκατάστασης του WSUS 3.0 SP2

Στα Windows Server 2008 SP2, μπορείτε να εγκαταστήσετε το WSUS 3.0 SP2 μέσα από το Server Manager. Εάν χρησιμοποιείτε άλλο λειτουργικό σύστημα ή θέλετε να εγκαταστήσετε μόνο την κονσόλα διαχείρισης (WSUS Administration Console), θα χρειαστεί να συμβουλευτείτε επόμενη παράγραφο σχετικά με την εγκατάσταση του WSUS – Με χρήση του αρχείου WSUSSetup.exe.

Διαδικασία: Προετοιμασία εγκατάστασης του WSUS Server με χρήση του Server Manager

1. Κάντε login στο server που θέλετε να εγκαταστήσετε το WSUS 3.0 SP2 με έναν λογαριασμό που ανήκει στην ομάδα χρηστών Local Administrators.
2. Επιλέξτε **Start, Administrative Tools**, και μετά **Server Manager**.
3. Στα δεξιά του Server Manager, στο τμήμα Roles Summary, επιλέξτε **Add Roles**.
4. Αν εμφανιστεί η σελίδα «Before You Begin», επιλέξτε **Next**.
5. Στη σελίδα «Select Server Roles», επιβεβαιώστε ότι έχουν επιλεγεί οι ρόλοι **Application Server** και **Web Server (IIS)**. Εάν είναι επιλεγμένοι, ελέγξτε πως ισχύουν τα παρακάτω, αλλιώς ακολουθήστε τα παρακάτω βήματα προκειμένου να εγκαταστήσετε τους ρόλους αυτούς.
 - Στη σελίδα «Select Server Roles», επιλέξτε **Application Server** και **Web Server (IIS)**. Επιλέξτε **Next**.
 - Εάν εγκαθιστάτε το ρόλο Application Role Services, στη σελίδα «Application Server», επιλέξτε **Next**. Στη σελίδα «Application Server Role Services», κάνετε δεκτές τις προκαθορισμένες ρυθμίσεις και επιλέξτε **Next**.
 - Εάν εγκαθιστάτε το ρόλο Web Server IIS, στη σελίδα «Web Server (IIS)», επιλέξτε **Next**. Στη σελίδα «Web Server (IIS) Role Services», εκτός από τις προκαθορισμένες επιλογές, επιλέξτε επιπλέον **ASP.NET**, **Windows Authentication**, **Dynamic Content Compression** και **IIS 6 Management Compatibility**. Αν

εμφανιστεί ο Add Roles Wizard, επιλέξτε **Add Required Role Services** και **Next**.

- Στη σελίδα «Confirm Installation Selections», επιλέξτε **Install**.
- Στη σελίδα «Installation Results», ελέγξτε ότι εμφανίστηκε το μήνυμα “Installation succeeded” και μετά επιλέξτε **Close**.

17.2.6 Εγκατάσταση WSUS Server ή Administration Console

Αφού σιγουρευτείτε ότι ο server σας πληροί τις απαιτήσεις εγκατάστασης και ότι έχετε αποδώσει τα κατάλληλα δικαιώματα, είσαστε έτοιμοι για την εγκατάσταση του WSUS 3.0 SP2. Ξεκινήστε την εγκατάσταση του χρησιμοποιώντας το Server Manager ή το αρχείο WSUSSetup.exe.

Διαδικασία έναρξης εγκατάστασης του WSUS 3.0 SP2 Server με χρήση του Server Manager

1. Κάντε login στο server που θέλετε να εγκαταστήσετε το WSUS 3.0 SP2 με έναν λογαριασμό που ανήκει στην ομάδα χρηστών Local Administrators.
2. Επιλέξτε **Start, Administrative Tools** και μετά **Server Manager**.
3. Στα δεξιά του Server Manager, στο τμήμα Roles Summary, επιλέξτε **Add Roles**.
4. Αν εμφανιστεί η σελίδα «Before You Begin», επιλέξτε **Next**.
5. Στη σελίδα «Select Server Roles», επιλέξτε **Windows Server Update Services**.
6. Στη σελίδα «Windows Server Update Services», επιλέξτε **Next**.
7. Στη σελίδα «Confirm Installation Selections», επιλέξτε **Install**.
8. Όταν ξεκινήσει ο οδηγός εγκατάστασης του WSUS 3.0 SP2, συνεχίστε στην παράγραφο «Συνέχεια εγκατάστασης του WSUS».

Διαδικασία έναρξης εγκατάστασης του WSUS 3.0 SP2 Server ή του Administration Console με χρήση του αρχείου WSUSSetup.exe

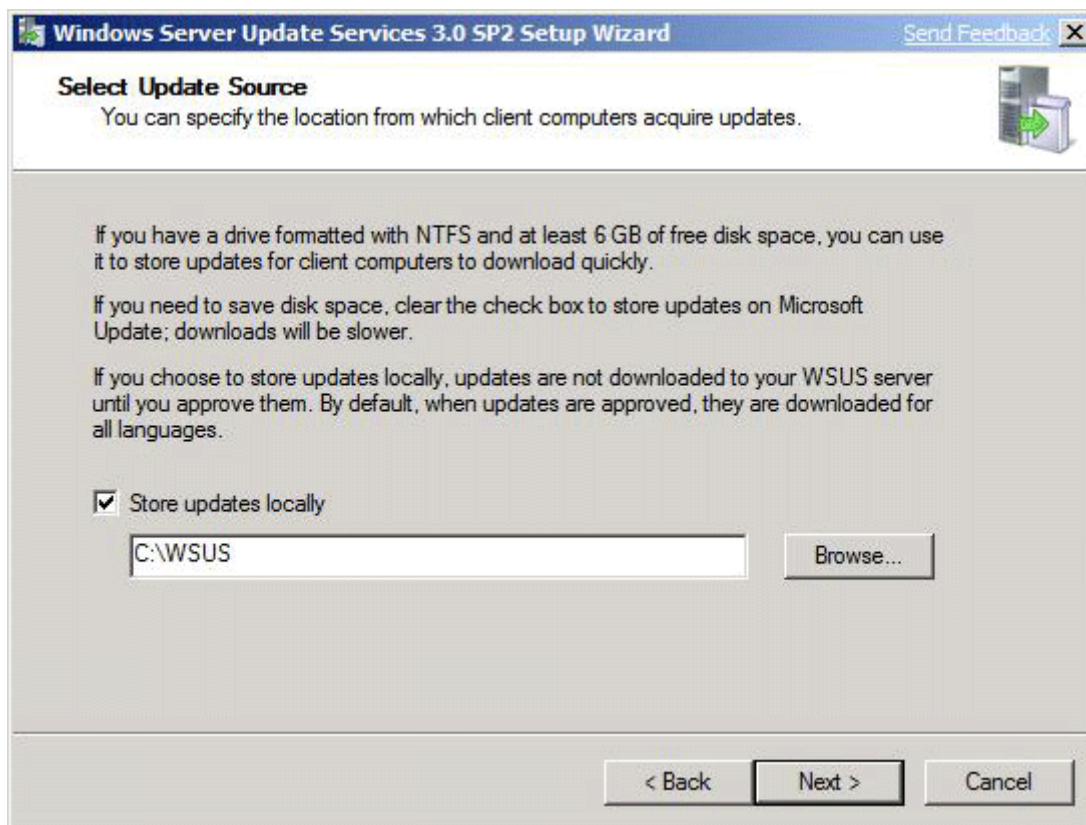
1. Κάντε login στον server που θέλετε να εγκαταστήσετε το WSUS 3.0 SP2 με έναν λογαριασμό που ανήκει στην ομάδα χρηστών Local Administrators.
2. Εκτελέστε το αρχείο **WSUSSetup.exe**.
3. Όταν ξεκινήσει ο οδηγός εγκατάστασης του WSUS 3.0 SP2, συνεχίστε στην παράγραφο «Συνέχεια εγκατάστασης του WSUS».

17.2.7 Χρήση του οδηγού εγκατάστασης WSUS 3.0 SP2

Ο οδηγός εγκατάστασης του WSUS εκκινεί είτε από τον Server Manager είτε από το αρχείο WSUSSetup.exe.

Διαδικασία συνέχειας εγκατάστασης του WSUS 3.0 SP2

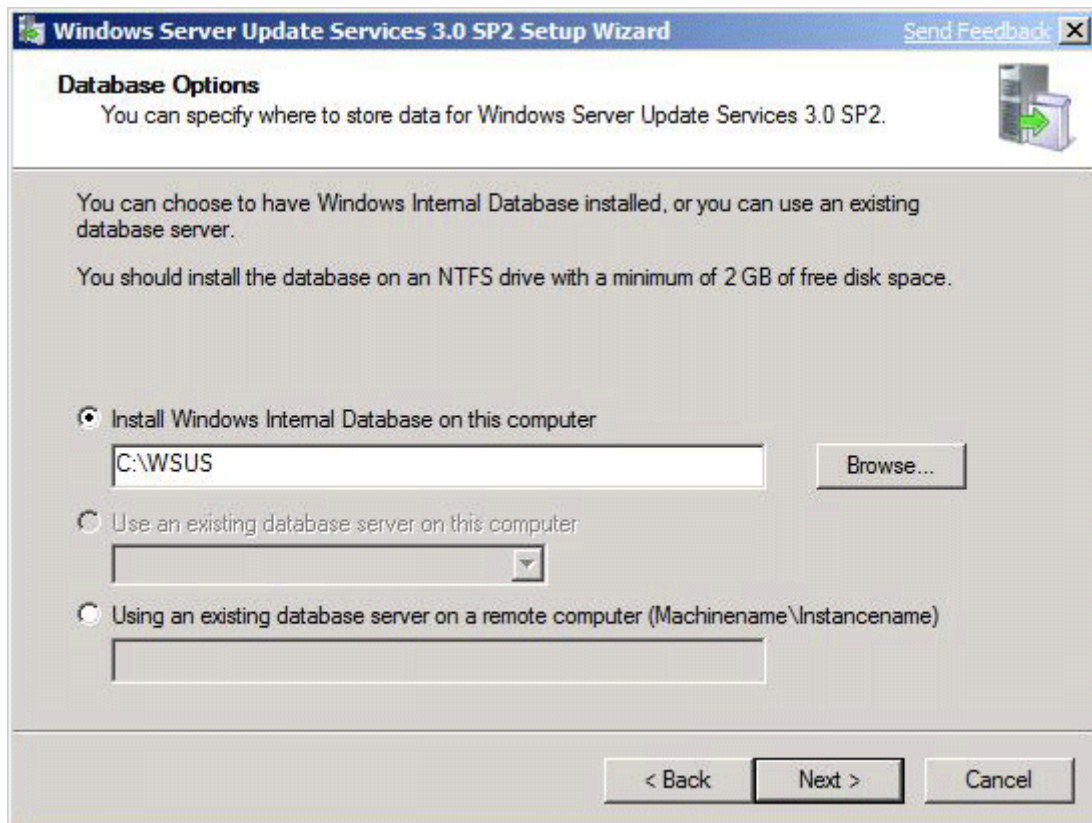
1. Στη σελίδα «Welcome» του οδηγού εγκατάστασης του WSUS, επιλέξτε **Next**.
2. Στη σελίδα «Installation Mode Selection», επιλέξτε **Full server installation including Administration Console** εάν θέλετε να εγκαταστήσετε το WSUS σε αυτόν τον υπολογιστή ή **Administration Console only** εάν θέλετε να εγκαταστήσετε την κονσόλα διαχείρισης μόνο.
3. Στη σελίδα «License Agreement», διαβάστε τους όρους χρήσης, επιλέξτε **I accept the terms of the License agreement** και μετά **Next**.
4. Στη σελίδα «Select Update Source» μπορείτε να καθορίσετε τη θέση από την οποία οι clients θα αντλούν τα updates. Η προκαθορισμένη επιλογή **Store updates locally** σημαίνει ότι οι ενημερώσεις (updates) θα αποθηκεύονται στο WSUS server στο φάκελο που θα καθορίσετε. Εάν αποεπιλέξετε την επιλογή **Store updates locally**, οι clients θα συνδέονται με το Microsoft Update προκειμένου να αποκτήσουν τις εγκεκριμένες ενημερώσεις. Αφού κάνετε την επιλογή σας, επιλέξτε **Next**.



Εικ. 17.7. Επιλογή τοπικής αποθήκευσης ενημερώσεων

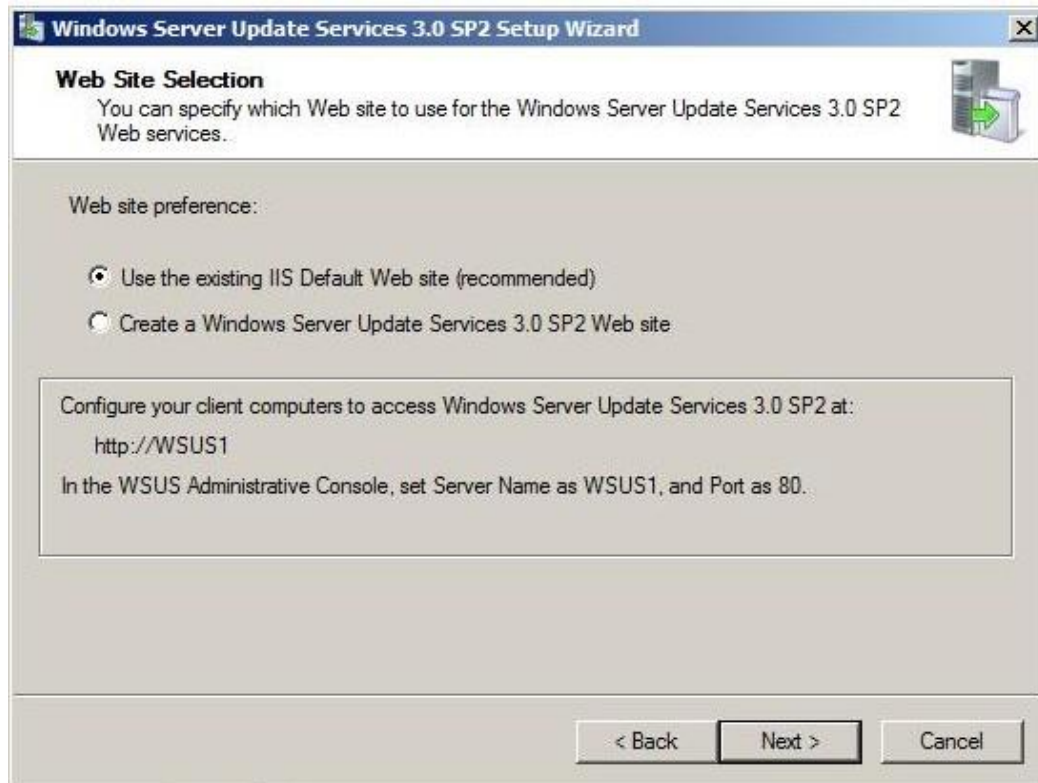
5. Στη σελίδα «Database Options», επιλέξτε το λογισμικό που θα χρησιμοποιείται για τη διαχείριση της βάσης του WSUS. Η προκαθορισμένη επιλογή είναι η εγκατάσταση του Windows Internal Database. Αν δεν θέλετε να

χρησιμοποιήσετε το Windows Internal Database, επιλέξτε **Use an existing database on this server** ή **Use an existing database server on a remote computer**. Στο κατάλληλο πλαίσιο επιλέξτε το instance του SQL Server ή πληκτρολογήστε `<serverName>\<instanceName>`, όπου *serverName* είναι το όνομα του server και *instanceName* είναι το όνομα του SQL instance. Αφού κάνετε την επιλογή σας, επιλέξτε **Next**.



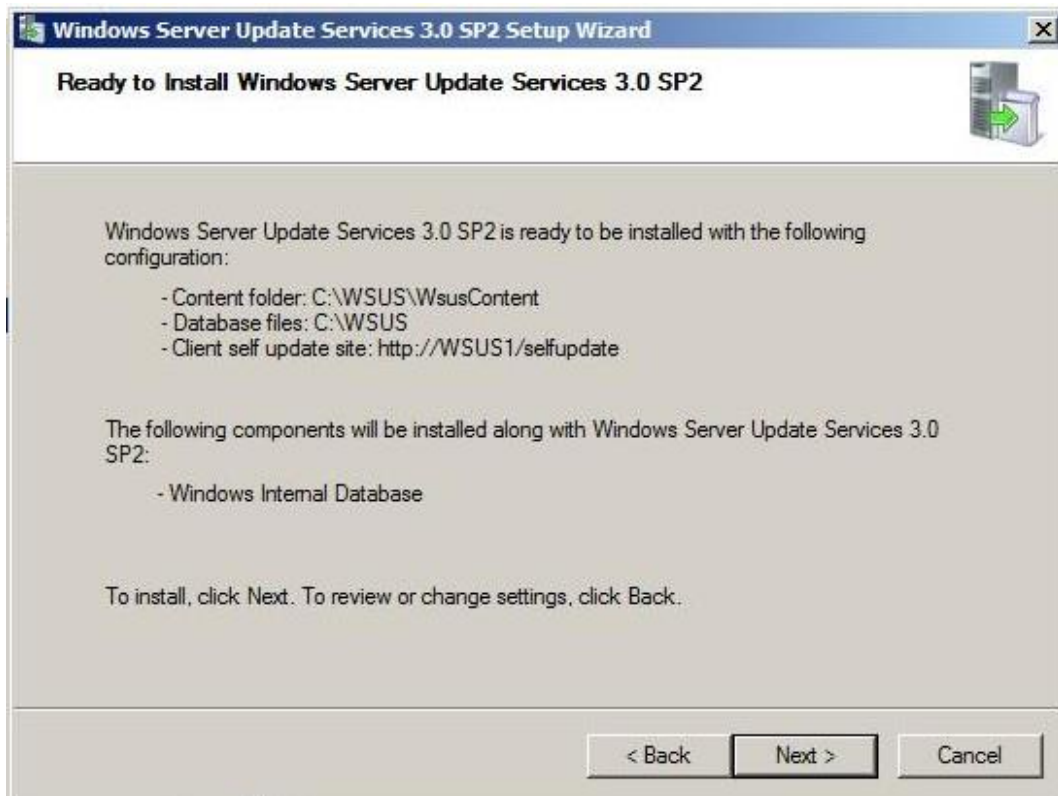
Εικ. 17.8. Επιλογή βάσης δεδομένων για το WSUS

6. Εάν επιλέξατε να συνδεθείτε σε έναν SQL Server, στη σελίδα «**Connecting to SQL Server Instance**», το WSUS θα προσπαθήσει να συνδεθεί στο συγκεκριμένο instance. Αφού συνδεθεί επιτυχώς, επιλέξτε **Next**.
7. Στη σελίδα «**Web Site Selection**», επιλέξτε το Web site που θα χρησιμοποιεί το WSUS. Αν θέλετε να χρησιμοποιήσετε το προκαθορισμένο Web site [πόρτα 80], επιλέξτε **Use the existing IIS Default Web site**. Εναλλακτικά, εάν π.χ. έχετε ήδη ένα Web site στην πόρτα 80, μπορείτε να δημιουργήσετε ένα site στις πόρτες 8530 ή 8531, επιλέγοντας **Create a Windows Server Update Services 3.0 SP2 Web site**. Επιλέξτε **Next**.



Εικ. 17.9. Επιλογή WSUS web site

8. Στη σελίδα «**Ready to Install Windows Server Update Services 3.0 SP2**», ελέγξτε τις επιλογές σας και επιλέξτε **Next**.



Εικ. 17.10. Έλεγχος επιλογών πριν από την εγκατάσταση

9. Στην τελευταία σελίδα του οδηγού θα πληροφορηθείτε σχετικά με την επιτυχία της εγκατάστασης. Αφού επιλέξετε **Finish** θα ξεκινήσει ο οδηγός παραμετροποίησης του WSUS.

17.3 Παραμετροποίηση WSUS

17.3.1 Παραμετροποίηση δικτυακών ρυθμίσεων WSUS

Μετά την εγκατάσταση του WSUS, θα ξεκινήσει αυτόματα ο οδηγός παραμετροποίησης του WSUS. Όλες οι ρυθμίσεις που γίνονται με χρήση του οδηγού μπορούν να γίνουν και αργότερα, εάν επιλέξετε από την κονσόλα διαχείρισης του WSUS την εντολή **Options**.

Πριν ξεκινήσετε τη διαδικασία παραμετροποίησης, σιγουρευτείτε ότι γνωρίζετε τις απαντήσεις στις ακόλουθες ερωτήσεις:

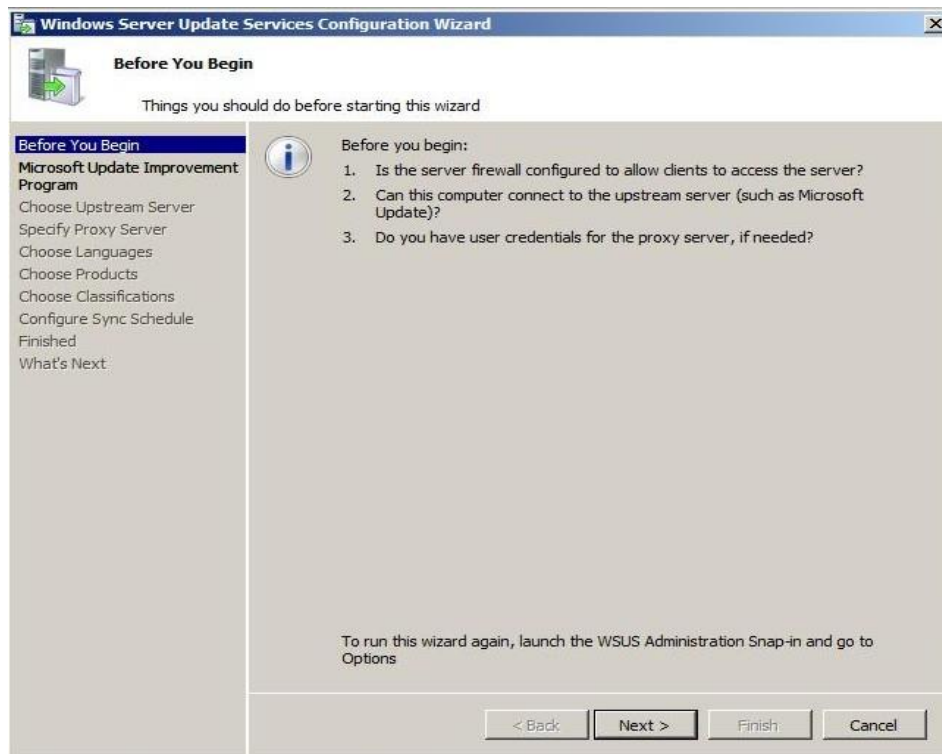
1. Είναι το firewall του server παραμετροποιημένο έτσι ώστε να επιτρέπεται η πρόσβαση των clients στον server;
2. Μπορεί αυτός ο server να συνδεθεί στον upstream server (όπως πχ. ο Microsoft Update);
3. Διαθέτετε το όνομα του proxy server και τα στοιχεία χρήστη (username & password) για πρόσβαση στον proxy server, σε περίπτωση που τα χρειαστείτε;

Η προκαθορισμένη επιλογή για το WSUS είναι να χρησιμοποιεί το Microsoft Update ως τη θέση από την οποία θα προμηθεύεται τις ενημερώσεις λογισμικού. Αν έχετε proxy server στο δίκτυό σας, μπορείτε να ρυθμίσετε τον WSUS έτσι ώστε να τον χρησιμοποιεί. Αν υπάρχει κεντρικό (corporate, εταιρικό) firewall μεταξύ WSUS και Internet, θα πρέπει πιθανώς να ρυθμίσετε το firewall σας έτσι ώστε ο WSUS να μπορεί να κατεβάσει τις ενημερώσεις λογισμικού.

Σημείωση: Αν και απαιτείται σύνδεση στο Internet προκειμένου να κατεβάσετε ενημερώσεις από το Microsoft Update, ο WSUS σας προσφέρει τη δυνατότητα να μεταφέρετε ενημερώσεις σε δίκτυα τα οποία δεν είναι συνδεδεμένα στο Internet.

Ακολουθώς θα δείτε πως:

- Να ρυθμίσετε το firewall σας.
- Να ρυθμίσετε με ποιο τρόπο ο server σας θα λαμβάνει ενημερώσεις (είτε από το Microsoft Update είτε από άλλον WSUS server).
- Να ρυθμίσετε τον WSUS ώστε να συνδέεται στο Internet μέσω του proxy server για να κατεβάζει τις ενημερώσεις.



Εικ. 17.11. Αρχική σελίδα του οδηγού παραμετροποίησης του WSUS

Διαδικασία παραμετροποίησης firewall

Εάν υπάρχει κεντρικό firewall μεταξύ WSUS server και Internet, ίσως χρειαστεί να παραμετροποιήσετε το firewall σας έτσι ώστε να μπορεί ο WSUS να κατεβάζει ενημερώσεις. Για να επικοινωνεί ο WSUS με το Microsoft Update και να λαμβάνει ενημερώσεις, ο WSUS server χρησιμοποιεί τις πόρτες 80 για το πρωτόκολλο HTTP και 443 για το πρωτόκολλο HTTPS. Αυτή η ρύθμιση δεν μπορεί να αλλάξει.

Εάν η πολιτική ασφαλείας του οργανισμού σας δεν επιτρέπει την απεριόριστη πρόσβαση στις πόρτες 80 ή 443 προς όλες τις διευθύνσεις, μπορείτε να περιορίσετε την πρόσβαση στα ακόλουθα domains μόνο, έτσι ώστε ο WSUS και τα Automatic Updates να μπορούν να επικοινωνούν με το Microsoft Update:

- <http://windowsupdate.microsoft.com>
- http://*.windowsupdate.microsoft.com
- https://*.windowsupdate.microsoft.com
- http://*.update.microsoft.com
- https://*.update.microsoft.com
- http://*.windowsupdate.com
- <http://download.windowsupdate.com>
- <http://download.microsoft.com>

- http://*.download.windowsupdate.com
- <http://wustat.windows.com>
- <http://ntservicepack.microsoft.com>

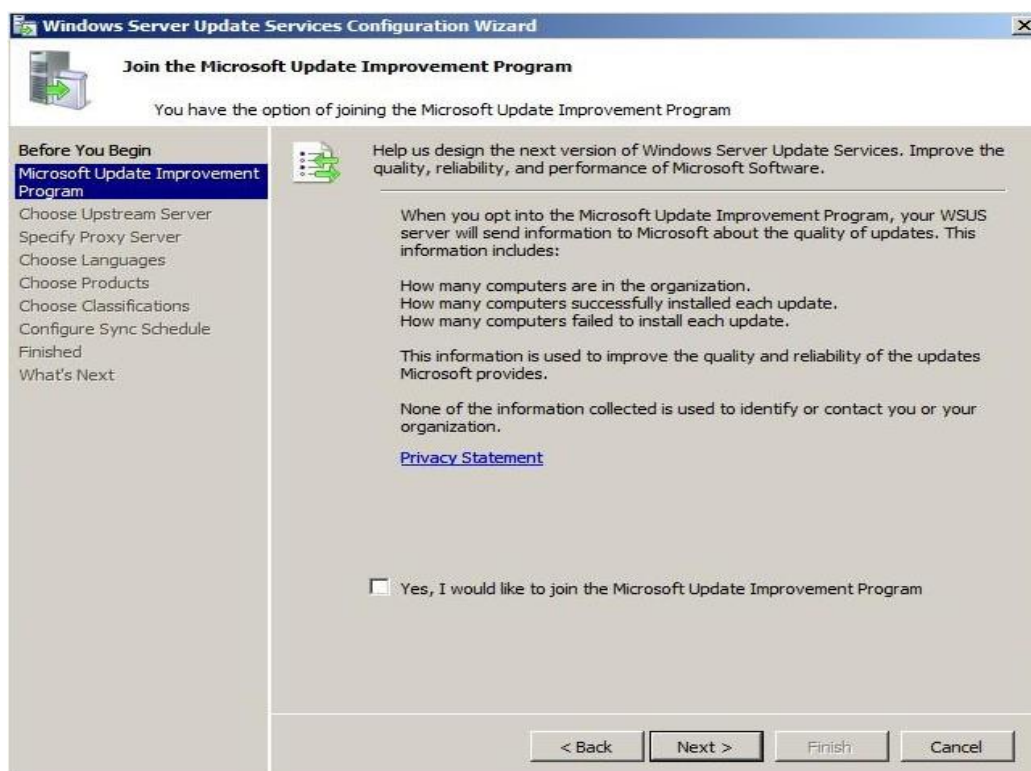
Σημείωση: Οι οδηγίες αυτές αφορούν την παραμετροποίηση ενός firewall που βρίσκεται ανάμεσα στον WSUS server και στο Internet. Επειδή ο WSUS ξεκινάει όλη τη σχετική κίνηση, δεν χρειάζεται να παραμετροποιήσετε το Windows Firewall στον WSUS server.

Αν και η σύνδεση μεταξύ του Microsoft Update και του WSUS χρειάζεται τις πόρτες 80 και 443, μπορείτε να ρυθμίσετε πολλούς WSUS servers (του δικτύου σας) να συγχρονίζονται με έναν WSUS server (επίσης του δικτύου σας) σε οποιαδήποτε πόρτα.

Στις επόμενες διαδικασίες υποθέτουμε ότι χρησιμοποιείτε τον οδηγό παραμετροποίησης. Παρακάτω θα δείτε πως μπορείτε να παραμετροποιήσετε τον server και μέσα από την σελίδα «Options».

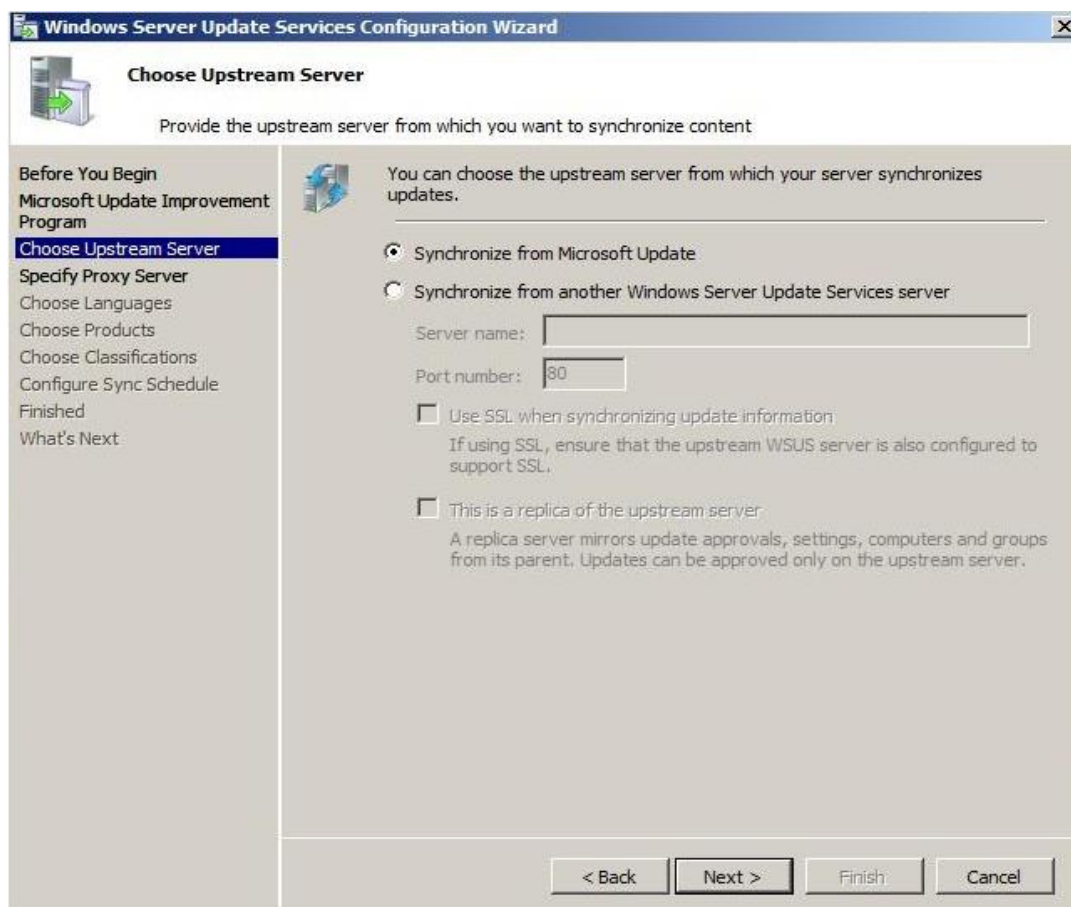
Διαδικασία επιλογής τρόπου λήψης ενημερώσεων από το server

1. Στον οδηγό παραμετροποίησης, μετά τη σελίδα «Microsoft Improvement Program», επιλέξτε **Next** και διαλέξτε τον server από τον οποίο θα λαμβάνει ενημερώσεις (upstream server).



Εικ. 17.12. Συμμετοχή στο Microsoft Improvement Program

2. Εάν διαλέξετε ως upstream server το Microsoft Update, έχετε τελειώσει με τις ρυθμίσεις αυτές και μπορείτε να επιλέξετε **Next** ή **Specify Proxy Server** προκειμένου να δώσετε τις σχετικές με τον proxy server ρυθμίσεις.
3. Εάν επιλέξατε να συγχρονίζεται αυτός ο WSUS server με κάποιον άλλο, δηλώστε το όνομα και την πόρτα με την οποία θα επικοινωνούν οι servers μεταξύ τους.
4. Για να χρησιμοποιήσετε SSL, επιλέξτε **Use SSL when synchronizing update information**. Σε αυτή την περίπτωση οι servers θα χρησιμοποιούν την πόρτα 443 για το συγχρονισμό. Σιγουρευτείτε ότι αυτός ο server καθώς και ο upstream server υποστηρίζουν SSL.
5. Εάν αυτός είναι ένας server-αντίγραφο (replica server), επιλέξτε the **This is a replica of the upstream server**.
6. Εδώ φτάσατε στο τέλος της παραμετροποίησης του upstream server. Επιλέξτε **Next** ή **Specify proxy server**.



Εικ. 17.13. Επιλογή του Microsoft Update ως upstream server

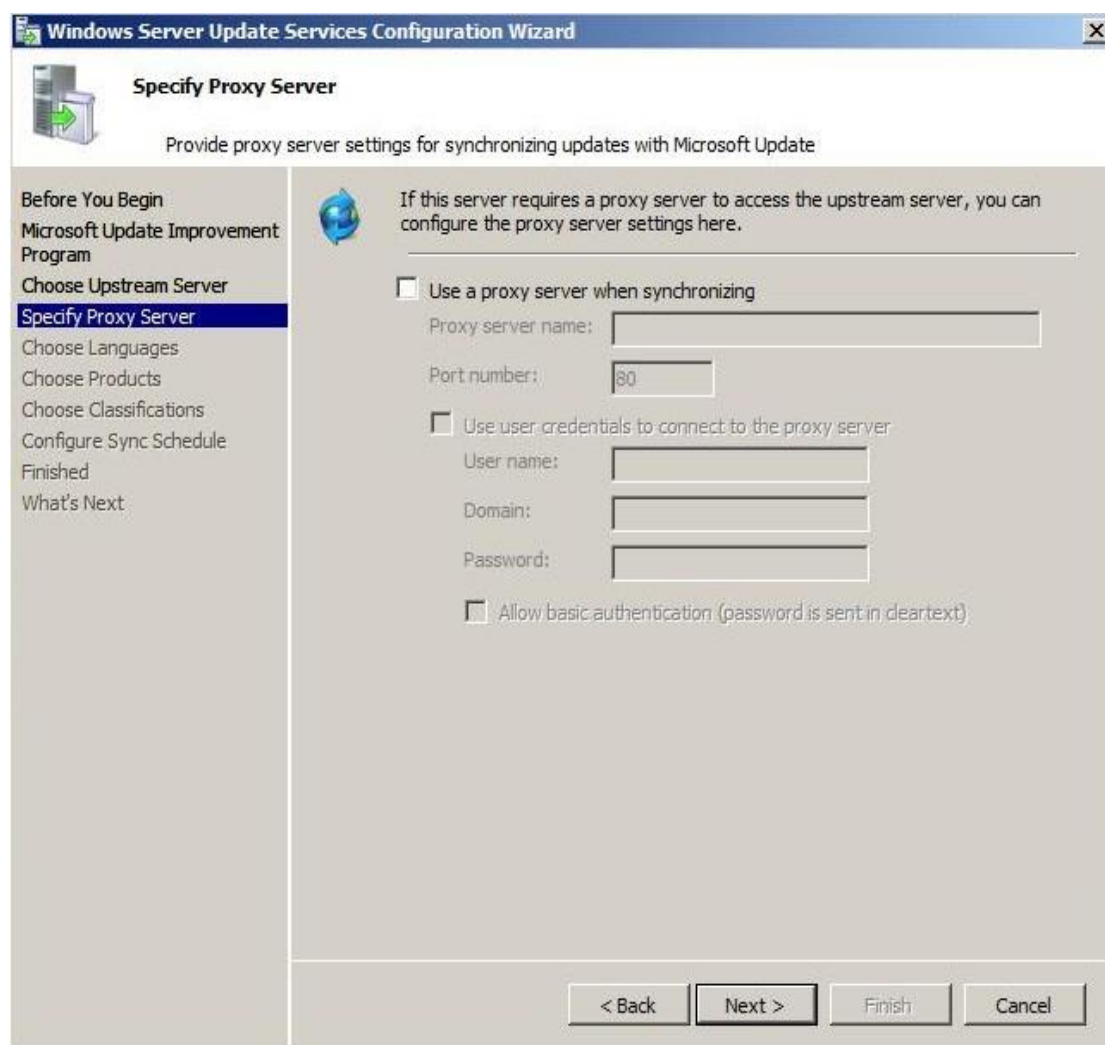
Διαδικασία ρυθμίσεων proxy server

1. Στη σελίδα «Specify Proxy Server» του οδηγού παραμετροποίησης, επιλέξτε

Use a proxy server when synchronizing, ακολούθως δηλώστε το όνομα του proxy server και την πόρτα του [80] στα αντίστοιχα πλαίσια.

2. Εάν θέλετε να συνδέεστε σε έναν proxy server χρησιμοποιώντας τα στοιχεία (user credentials) ενός συγκεκριμένου χρήστη, επιλέξτε **Use user credentials to connect to the proxy server**, κατόπιν συμπληρώστε το όνομα χρήστη, το domain και το συνθηματικό του χρήστη στα αντίστοιχα πλαίσια. Εάν θέλετε, επιλέξτε **Allow basic authentication (password is sent in cleartext)**.

3. Εδώ τελειώσατε με την παραμετροποίηση του proxy server. Επιλέξτε **Next** για να πάτε στην επόμενη σελίδα, όπου θα μπορέσετε να ρυθμίσετε τη διαδικασία συγχρονισμού.



Εικ. 17.14. Ρυθμίσεις proxy server

Στις επόμενες διαδικασίες υποθέτουμε ότι χρησιμοποιείτε τον οδηγό παραμετροποίησης. Στις διαδικασίες αυτές θα μάθετε πώς να ξεκινάτε την εφαρμογή διαχείρισης του WSUS (WSUS Administration MMC snap-in) και πώς να ρυθμίζετε

τον proxy server και τον upstream server από την επιλογή **Options**.

Διαδικασία εκκίνησης της κονσόλας διαχείρισης του WSUS

1. Για να εκκινήσετε την κονσόλα διαχείρισης του WSUS, επιλέξτε **Start, All Programs, Administrative Tools** και τέλος **Windows Server Update Services 3.0**.

Σημείωση: Προκειμένου να χρησιμοποιήσετε όλες τις δυνατότητες της κονσόλας διαχείρισης, πρέπει να έχετε κάνει login ως χρήστης που είναι μέλος της ομάδας WSUS Administrators ή της ομάδας Local Administrators (στο server που είναι εγκατεστημένος ο WSUS). Τα μέλη της ομάδας WSUS Reporters έχουν πρόσβαση στην κονσόλα διαχείρισης αλλά μόνο για ανάγνωση.

Διαδικασία ορισμού upstream και proxy server

1. Στην κονσόλα διαχείρισης του WSUS, επιλέξτε από το αριστερό πλαίσιο **Options**, και στη συνέχεια **Update Source and Proxy Server** στο μεσαίο πλαίσιο. Θα εμφανιστεί ένας διάλογος με τις καρτέλες (tabs) **Update Source** και **Proxy Server**.
2. Στην καρτέλα **Update Source**, επιλέξτε τη θέση από την οποία αυτός ο server θα προμηθεύεται ενημερώσεις. Εάν επιλέξατε να συγχρονίζεται με το Microsoft Update (προκαθορισμένη τιμή), έχετε τελειώσει με αυτή την καρτέλα.
3. Εάν επιλέξετε να συγχρονίζεται από έναν άλλο WSUS server, πρέπει να δηλώσετε την πόρτα [80] στην οποία θα επικοινωνούν οι servers. Εάν επιλέξετε κάποια άλλη πόρτα, πρέπει να βεβαιωθείτε ότι και οι δύο servers μπορούν να χρησιμοποιούν αυτή την πόρτα.
4. Μπορείτε επίσης να επιλέξετε αν θα χρησιμοποιείται SSL για τον συγχρονισμό από τον upstream WSUS server. Σε αυτή την περίπτωση οι servers θα χρησιμοποιούν την πόρτα 443.
5. Εάν αυτός ο server είναι replica κάποιου άλλου WSUS server, επιλέξτε **This is a replica of the upstream server**. Σε αυτή την περίπτωση, όλες οι ενημερώσεις χρειάζεται να εγκρίνονται μόνο στον upstream WSUS server.
6. Στην καρτέλα **Proxy server**, επιλέξτε **Use a proxy server when synchronizing**, δηλώστε το όνομα του proxy server και την πόρτα [80] στα αντίστοιχα πλαίσια.
7. Εάν θέλετε να συνδέσετε σε έναν proxy server χρησιμοποιώντας τα στοιχεία (user credentials) ενός συγκεκριμένου χρήστη, επιλέξτε **Use user credentials to connect to the proxy server**, κατόπιν συμπληρώστε το όνομα χρήστη, το domain και

το συνθηματικό του χρήστη στα αντίστοιχα πλαίσια. Εάν θέλετε, επιλέξτε **Allow basic authentication (password is sent in cleartext)**.

8. Επιλέξτε **OK** για να αποθηκεύσετε αυτές τις ρυθμίσεις.

17.3.2 Παραμετροποίηση ενημερώσεων και συγχρονισμού

Οι ακόλουθες διαδικασίες μπορούν να εκτελεστούν είτε με χρήση του οδηγού παραμετροποίησης του WSUS είτε με χρήση της κονσόλας διαχείρισης του WSUS.

- Αποθήκευση και κατέβασμα (download) πληροφοριών σχετικά με τον upstream server και τον proxy server.
- Επιλογή γλωσσών για τις ενημερώσεις.
- Επιλογή προϊόντων για τα οποία θα λαμβάνονται ενημερώσεις.
- Επιλογή κατηγοριών των ενημερώσεων.
- Προσδιορισμός του προγράμματος συγχρονισμού του WSUS server.

Αφού παραμετροποιήσετε τη σύνδεση του WSUS στο δίκτυο, μπορείτε να κατεβάσετε ενημερώσεις επιλέγοντας συγχρονισμό του WSUS server. Ο συγχρονισμός ξεκινάει όταν ο server επικοινωνήσει με το Microsoft Update. Όταν ο WSUS επικοινωνήσει με το Microsoft Update, ο WSUS προσδιορίζει εάν υπάρχουν διαθέσιμες νέες ενημερώσεις (από την τελευταία φορά που έγινε συγχρονισμός). Την πρώτη φορά που συγχρονίζει ο WSUS, όλες οι ενημερώσεις είναι διαθέσιμες και περιμένουν την έγκριση για εγκατάσταση. Ο αρχικός (πρώτος) συγχρονισμός μπορεί να διαρκέσει αρκετή ώρα.

Οι διαδικασίες σε αυτό το τμήμα περιγράφουν συγχρονισμό με τις προκαθορισμένες ρυθμίσεις.

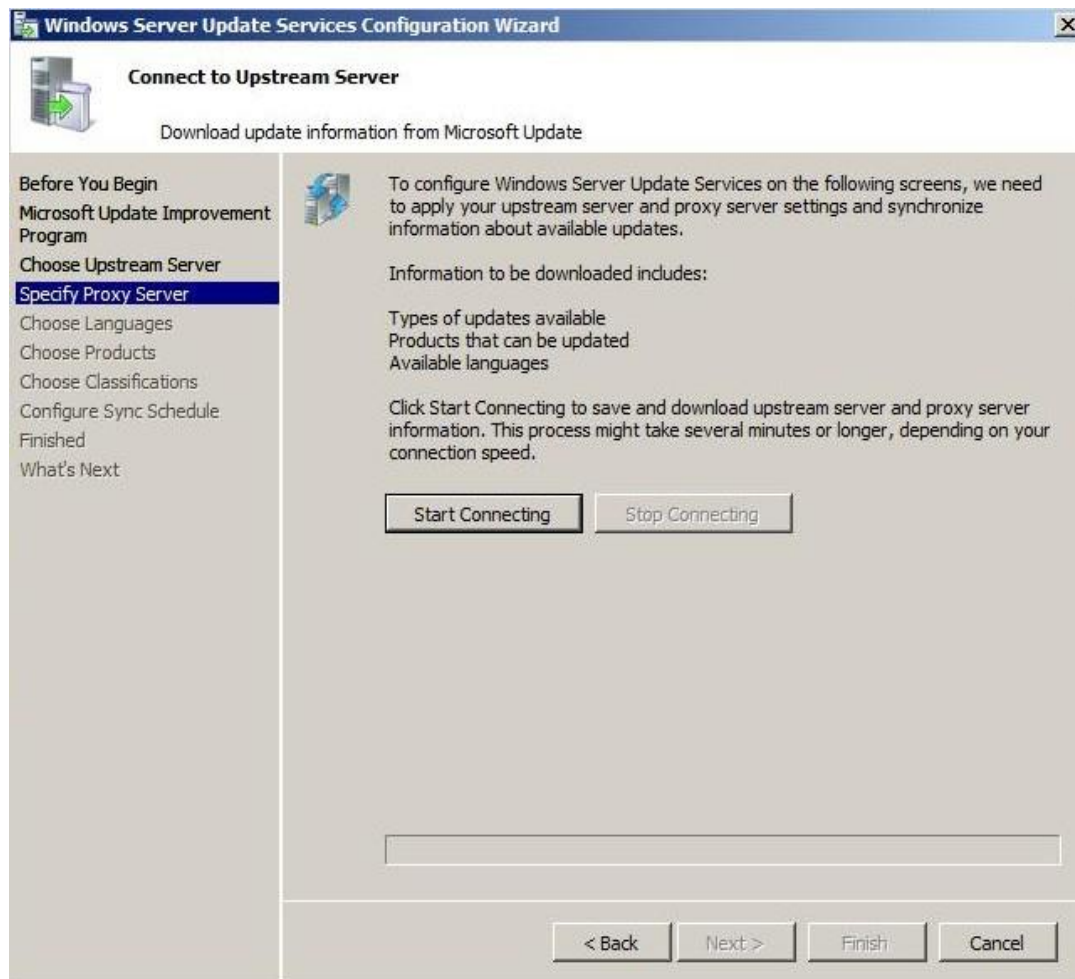
1. Με χρήση του οδηγού παραμετροποίησης του WSUS

Με τις διαδικασίες της προηγούμενης παραγράφου, ολοκληρώθηκε η παραμετροποίηση του upstream server και του proxy server. Οι ακόλουθες διαδικασίες ξεκινούν από τη σελίδα **Connect to Upstream Server** του οδηγού παραμετροποίησης.

Διαδικασία αποθήκευσης και κατεβάσματος (download) πληροφοριών για τους upstream και proxy server

1. Στη σελίδα «Connect to Upstream Server» του οδηγού παραμετροποίησης, επιλέξτε **Start Connecting**. Αυτό σώζει και ανεβάζει (upload) τις ρυθμίσεις σας και συλλέγει πληροφορίες σχετικά με τις διαθέσιμες ενημερώσεις.

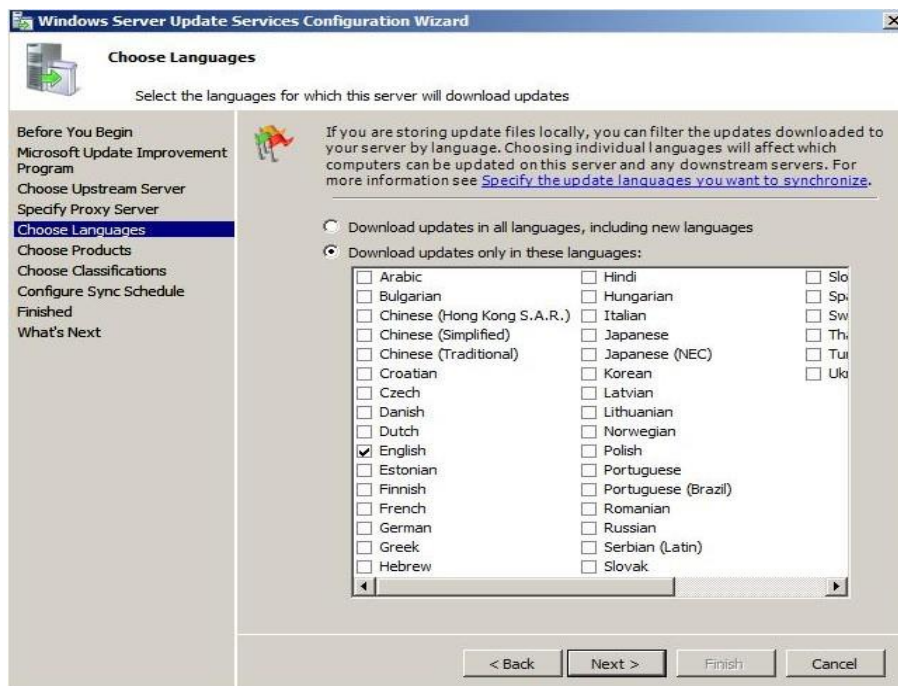
2. Ενώ γίνεται η σύνδεση, η επιλογή **Stop Connecting** είναι διαθέσιμη. Εάν υπάρχουν προβλήματα σύνδεσης, επιλέξτε, διορθώστε τα προβλήματα σύνδεσης και ξεκινήστε πάλι την σύνδεση.
3. Αφού τελειώσει το κατέβασμα, επιλέξτε **Next**.



Εικ. 17.15. Πρώτη σύνδεση στον upstream server

Διαδικασία επιλογής γλωσσών ενημερώσεων

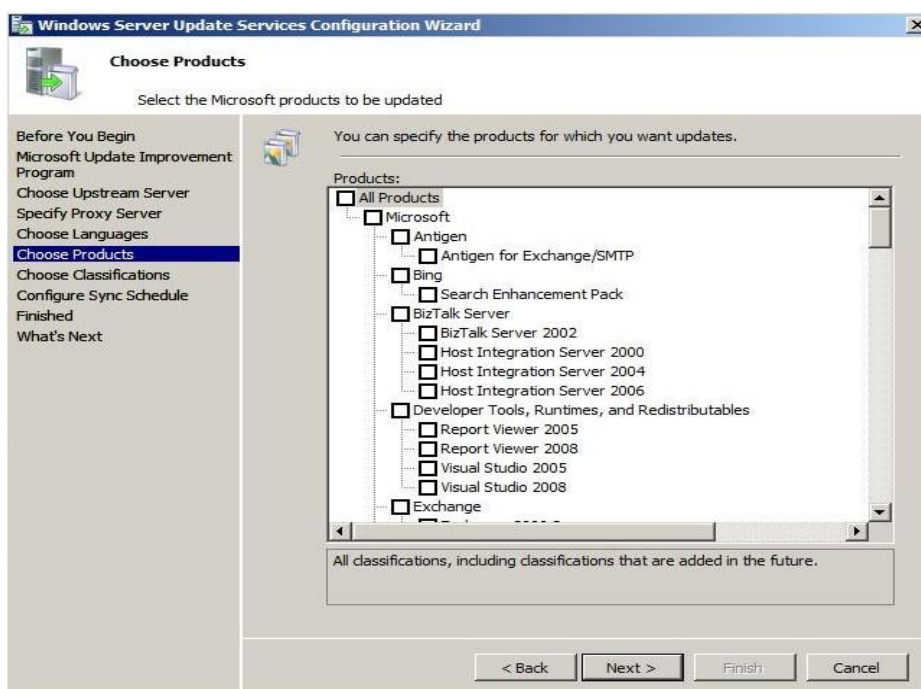
1. Στη σελίδα «Choose Languages» ρυθμίζετε αν θα λαμβάνετε ενημερώσεις για όλες τις γλώσσες ή για το υποσύνολο των γλωσσών που επιθυμείτε. Εάν επιλέξετε ένα υποσύνολο των γλωσσών, θα κάνετε οικονομία στον αποθηκευτικό χώρο του δίσκου σας, όμως είναι σημαντικό να επιλέξετε όλες τις γλώσσες που θα χρειαστούν οι clients του WSUS. Εάν θέλετε να λαμβάνετε ενημερώσεις μόνο για συγκεκριμένες γλώσσες, επιλέξτε **Download updates only in these languages** και επιλέξτε τις γλώσσες που επιθυμείτε.
2. Επιλέξτε **Next**.



Εικ. 17.16. Επιλογή γλωσσών για τις ενημερώσεις

Διαδικασία επιλογής προϊόντων για τα οποία θα λαμβάνονται ενημερώσεις

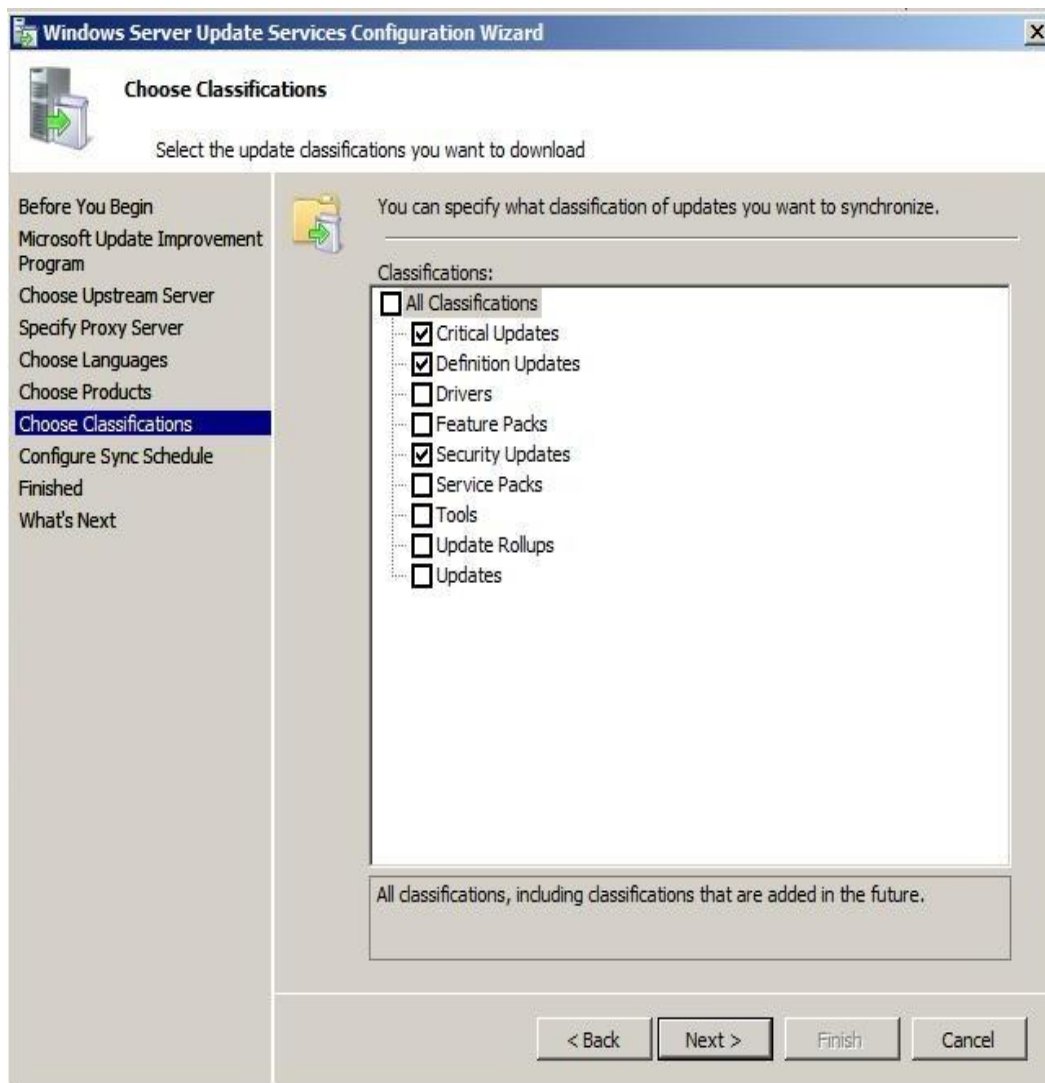
1. Στη σελίδα «Choose Products» μπορείτε να επιλέξετε τα προϊόντα για τα οποία θέλετε να λαμβάνετε ενημερώσεις. Επιλέξτε κατηγορίες προϊόντων (π.χ. Windows) ή συγκεκριμένα προϊόντα (π.χ. Windows Server 2008). Επιλογή μίας κατηγορίας συνεπάγεται επιλογή όλων των προϊόντων της κατηγορίας.
2. Επιλέξτε **Next**.



Εικ. 17.17. Επιλογή προϊόντων για τα οποία θα λαμβάνονται ενημερώσεις

Διαδικασία επιλογής κατηγοριών ενημερώσεων

1. Στη σελίδα «Choose Classifications» μπορείτε να επιλέξετε ποιες κατηγορίες ενημερώσεων θέλετε να λαμβάνετε. Μπορείτε να επιλέξετε όλες τις ενημερώσεις ή ένα υποσύνολο αυτών.
2. Επιλέξτε **Next**.



Εικ. 17.18. Επιλογή κατηγοριών ενημερώσεων

Διαδικασία παραμετροποίησης του προγράμματος συγχρονισμού του WSUS

1. Στη σελίδα «Set Sync Schedule», επιλέγετε αν θέλετε ο συγχρονισμός να γίνεται αυτόματα ή όχι.

Εάν επιλέξετε **Synchronize manually**, πρέπει να εκκινείτε την διαδικασία συγχρονισμού από την κονσόλα διαχείρισης του WSUS.

Εάν επιλέξετε **Synchronize automatically**, ο WSUS server θα συγχρονίζει ανά τακτά χρονικά διαστήματα. Αφού θέσετε την ώρα του πρώτου συγχρονισμού, **First synchronization**, προσδιορίστε τον αριθμό των ημερήσιων συγχρονισμών,

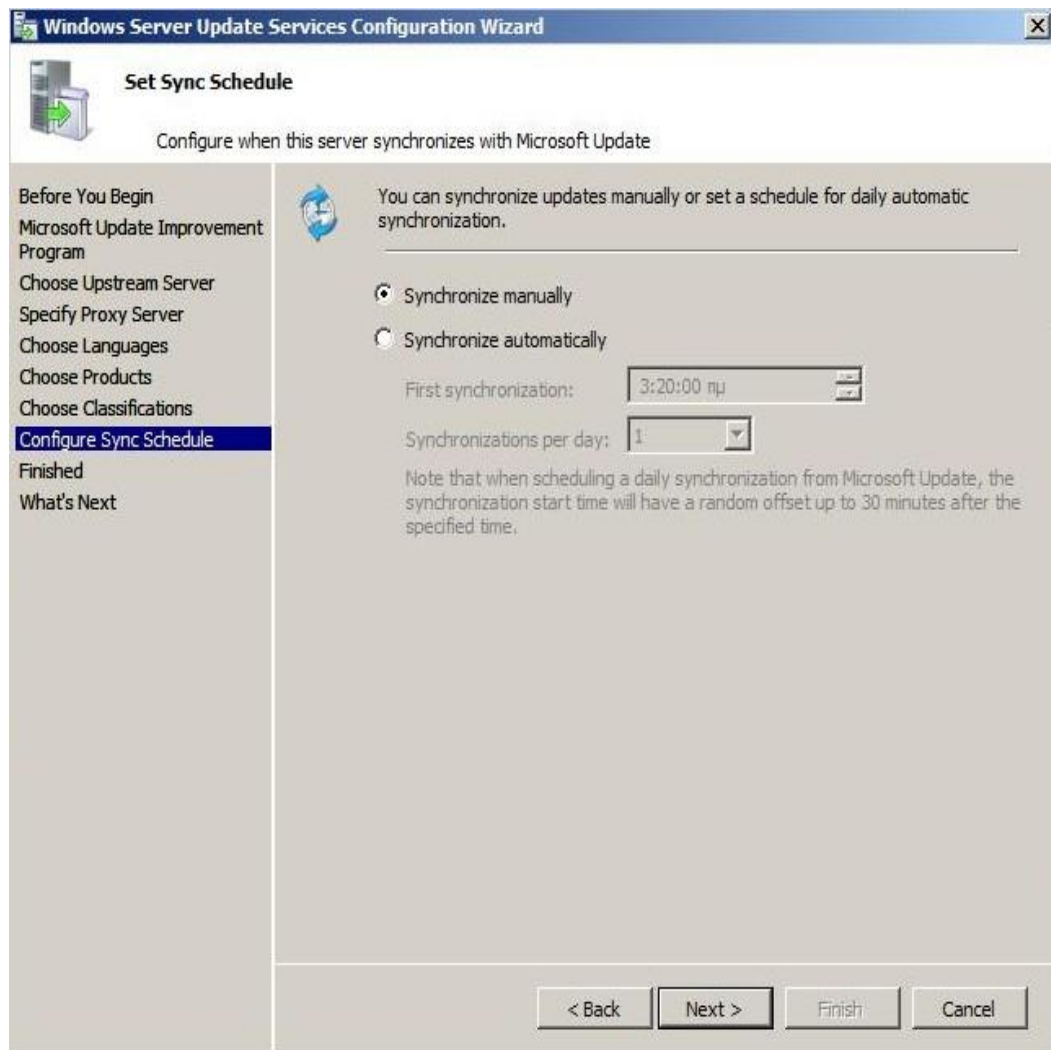
Synchronizations per day. Για παράδειγμα, εάν θέλετε τέσσερις συγχρονισμούς ανά ημέρα που να ξεκινούν στις 3 π.μ. (3:00 A.M.), οι επόμενοι συγχρονισμοί θα γίνουν στις 9:00 A.M., 3:00 P.M., και 9:00 P.M.

2. Επιλέξτε **Next**.

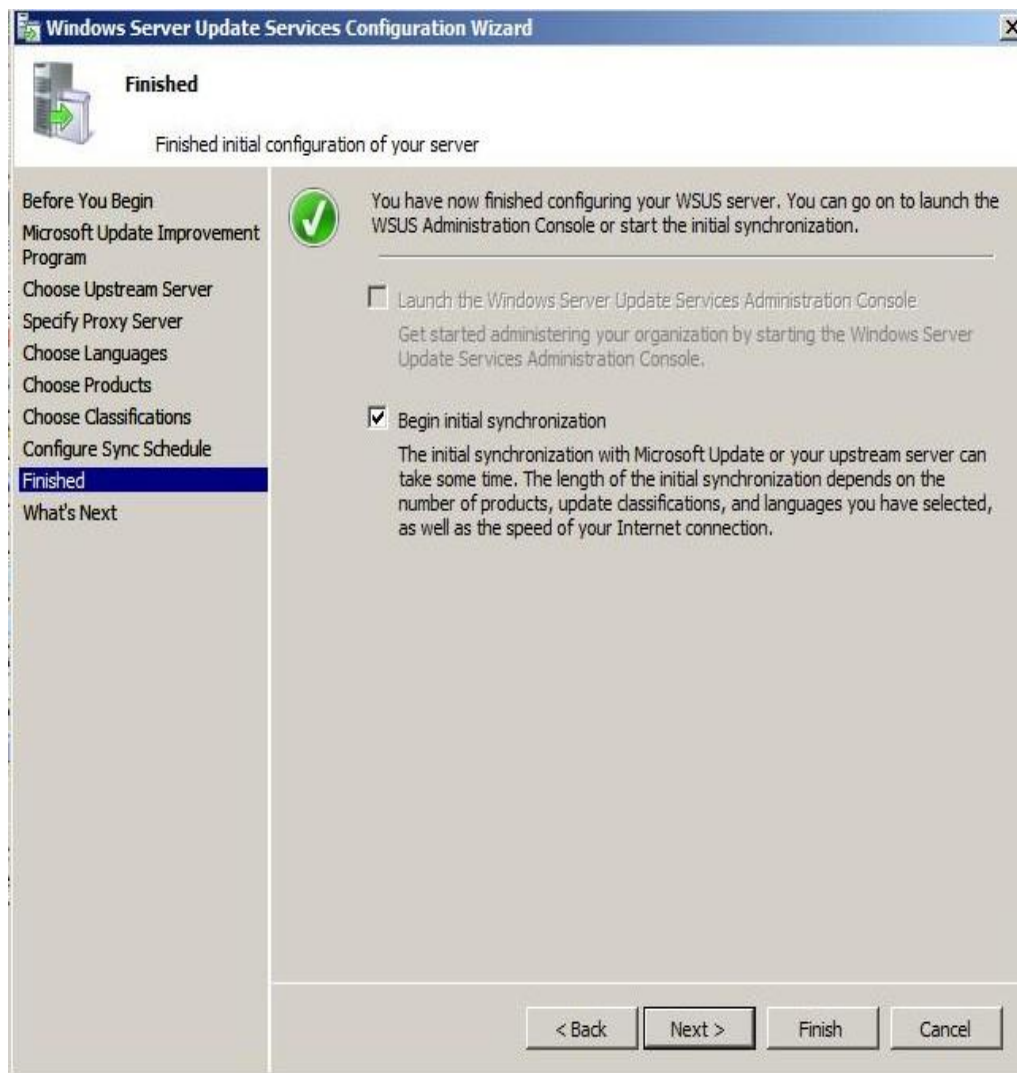
Στη σελίδα «Finished», μπορείτε να ξεκινήσετε την κονσόλα διαχείρισης του WSUS, επιλέγοντας **Launch the Windows Server Update Services Administrations snap-in** και μπορείτε να εκκινήσετε τον αρχικό συγχρονισμό αφήνοντας την επιλογή **Begin initial synchronization** επιλεγμένη.

3. Επιλέξτε **Finish**.

Σημείωση: Δε μπορείτε να αποθηκεύσετε αλλαγές στις ρυθμίσεις κατά τη διάρκεια του συγχρονισμού. Περιμένετε να τελειώσει ο συγχρονισμός και μετά κάνετε τις αλλαγές που θέλετε.



Εικ. 17.19. Επιλογή ρυθμίσεων συγχρονισμού



Εικ. 17.20. Αρχικός συγχρονισμός

17.3.3 Με χρήση της κονσόλας διαχείρισης του WSUS

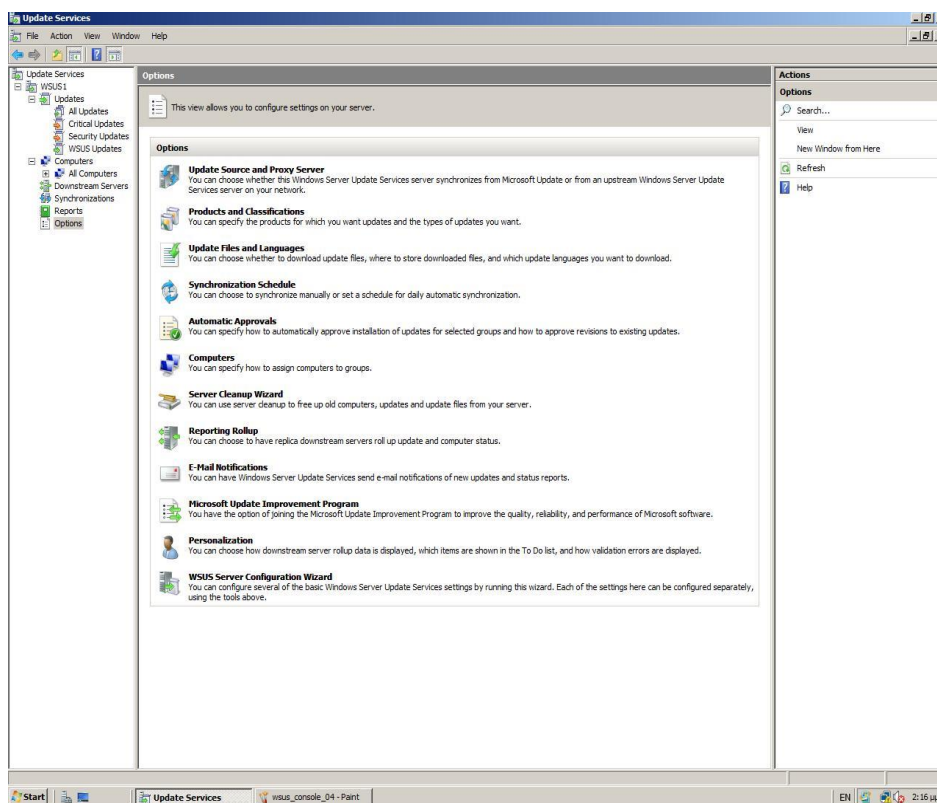
Οι παρακάτω διαδικασίες εξηγούν πώς να διενεργήσετε την παραμετροποίηση με χρήση της κονσόλας διαχείρισης του WSUS.

Διαδικασία επιλογής προϊόντων και κατηγοριών ενημερώσεων

1. Στον πίνακα (panel) **Options**, επιλέξτε **Products and Classifications**. Θα εμφανιστεί ένας διάλογος με τις καρτέλες **Products** και **Classifications**.
2. Στην καρτέλα **Products**, επιλέξτε την κατηγορία προϊόντων ή μεμονωμένα προϊόντα για τα οποία θέλετε να λαμβάνετε ενημερώσεις, αλλιώς επιλέξτε **All Products**.
3. Στην καρτέλα **Classifications**, επιλέξτε τις κατηγορίες ενημερώσεων που θέλετε, αλλιώς **All Classifications**.
4. Επιλέξτε **OK** για να αποθηκεύσετε τις ρυθμίσεις σας,

Διαδικασία επιλογής αποθήκευσης ενημερώσεων και επιλογής γλωσσών

1. Στον πίνακα **Options**, επιλέξτε **Update Files and Languages**. Θα εμφανιστεί ένας διάλογος με τις καρτέλες **Update Files** και **Update Languages**.
2. Στην καρτέλα **Update Files**, επιλέξτε εάν θα αποθηκεύονται τοπικά (στο WSUS server) τα αρχεία των ενημερώσεων, **Store update files locally on this server** ή αν όλοι οι clients θα κατεβάζουν τις ενημερώσεις απευθείας από το Microsoft Update. Εάν επιλέξετε να αποθηκεύονται οι ενημερώσεις τοπικά, πρέπει επίσης να αποφασίσετε αν θα κατεβάζετε μόνο τις ενημερώσεις που έχετε εγκρίνει και αν θα κατεβάζετε τα αρχεία για express εγκατάσταση.
3. Στην καρτέλα **Update Languages**, εάν αποθηκεύονται οι ενημερώσεις τοπικά, επιλέγετε αν θα κατεβάζετε τις ενημερώσεις για όλες τις γλώσσες, **Download updates for all languages** (το προκαθορισμένο) ή μόνο για τις επιλεγμένες γλώσσες, **Download updates only in the specified languages**. Εάν ο WSUS server έχει και downstream servers, αυτοί θα λαμβάνουν ενημερώσεις μόνο για τις γλώσσες που έχουν επιλεγεί στον upstream server. **Σημείωση:** Αν έχετε επιλέξει να μην αποθηκεύονται οι ενημερώσεις τοπικά, η συγκεκριμένη ρύθμιση δεν έχει νόημα και μπορείτε να την αγνοήσετε.
4. Επιλέξτε **OK** για να αποθηκεύσετε τις ρυθμίσεις σας.



Εικ. 17.21. Ο πίνακας Options

Διαδικασία παραμετροποίησης του προγράμματος συγχρονισμού του WSUS

1. Στον πίνακα **Options**, επιλέξτε **Synchronization Schedule**.
2. Στην καρτέλα **Synchronization Schedule** tab, επιλέγετε αν θέλετε ο συγχρονισμός να γίνεται αυτόματα ή όχι.

Εάν επιλέξετε **Synchronize manually**, πρέπει να εκκινείτε την διαδικασία συγχρονισμού από την κονσόλα διαχείρισης του WSUS.

Εάν επιλέξετε **Synchronize automatically**, ο WSUS server θα συγχρονίζει ανά τακτά χρονικά διαστήματα. Αφού θέσετε την ώρα του πρώτου συγχρονισμού, **First synchronization** προσδιορίστε τον αριθμό των ημερήσιων συγχρονισμών, **Synchronizations per day**. Για παράδειγμα, εάν θέλετε τέσσερις συγχρονισμούς ανά ημέρα που να ξεκινούν στις 3 π.μ. (3:00 A.M.), οι επόμενοι συγχρονισμοί θα γίνουν στις 9:00 A.M., 3:00 P.M., και 9:00 P.M.

3. Επιλέξτε **OK** για να αποθηκεύσετε τις ρυθμίσεις σας.
4. Στην κονσόλα διαχείρισης του WSUS, επιλέξτε **Synchronizations**.
5. Στο τμήμα **Actions**, επιλέξτε **Synchronize Now**.

Εάν δεν βλέπετε το τμήμα **Actions**, στην γραμμή εργαλείων της κονσόλας επιλέξτε **View, Customize** και βεβαιωθείτε ότι η επιλογή **Action pane** είναι επιλεγμένη.

6. Αφού ολοκληρωθεί ο συγχρονισμός, επιλέξτε στο αριστερό τμήμα **Updates** για να δείτε τον κατάλογο των ενημερώσεων.

17.3.4 Παραμετροποίηση ομάδων υπολογιστών

Οι ομάδες υπολογιστών (computer groups) έχουν ιδιαίτερη σημασία για τη λειτουργία του WSUS. Μεταξύ άλλων, η χρήση ομάδων υπολογιστών σας επιτρέπει να ελέγχετε τις ενημερώσεις και να κατευθύνετε συγκεκριμένες ενημερώσεις σε συγκεκριμένους υπολογιστές. Υπάρχουν δύο προκαθορισμένες ομάδες: All Computers και Unassigned Computers. Όταν ένας client επικοινωνεί για πρώτη φορά με τον WSUS Server, ο server τον προσθέτει και στις δύο παραπάνω ομάδες.

Μπορείτε να δημιουργήσετε όσες ομάδες υπολογιστών νομίζετε ότι χρειάζονται για να διαχειρίζεστε τις ενημερώσεις στο δίκτυό σας. Καλό είναι να δημιουργήσετε τουλάχιστον μία ομάδα υπολογιστών, στην οποία θα μπορείτε να δοκιμάζετε τις ενημερώσεις, προτού τις εφαρμόσετε σε ολόκληρο το δίκτυό σας.

Διαδικασία δημιουργίας ομάδας υπολογιστών

1. Στην κονσόλα διαχείρισης του WSUS, αναπτύξτε **Computers** και επιλέξτε **All Computers**.
2. Δεξί κλικ **All Computers** και επιλέξτε **Add Computer Group**.

3. Στο διάλογο **Add Computer Group**, δώστε το όνομα **Name** της νέας ομάδας και επιλέξτε **Add**.

Στην επόμενη διαδικασία, θα βάλετε έναν client στην ομάδα υπολογιστών test. Ο υπολογιστής αυτός είναι οποιοσδήποτε υπολογιστής έχει υλικό και λογισμικό ίδιο με αυτό που έχουν οι περισσότεροι υπολογιστές του δικτύου σας. Μπορείτε, αν θέλετε, να χρησιμοποιήσετε ακόμα και virtual machines. Αφού βεβαιωθείτε ότι οι δοκιμαστικές εγκαταστάσεις των ενημερώσεων ολοκληρώθηκαν με επιτυχία μπορείτε να εγκρίνετε τις ενημερώσεις και για τους υπόλοιπους υπολογιστές.

Διαδικασία μεταφοράς υπολογιστή σε άλλη ομάδα

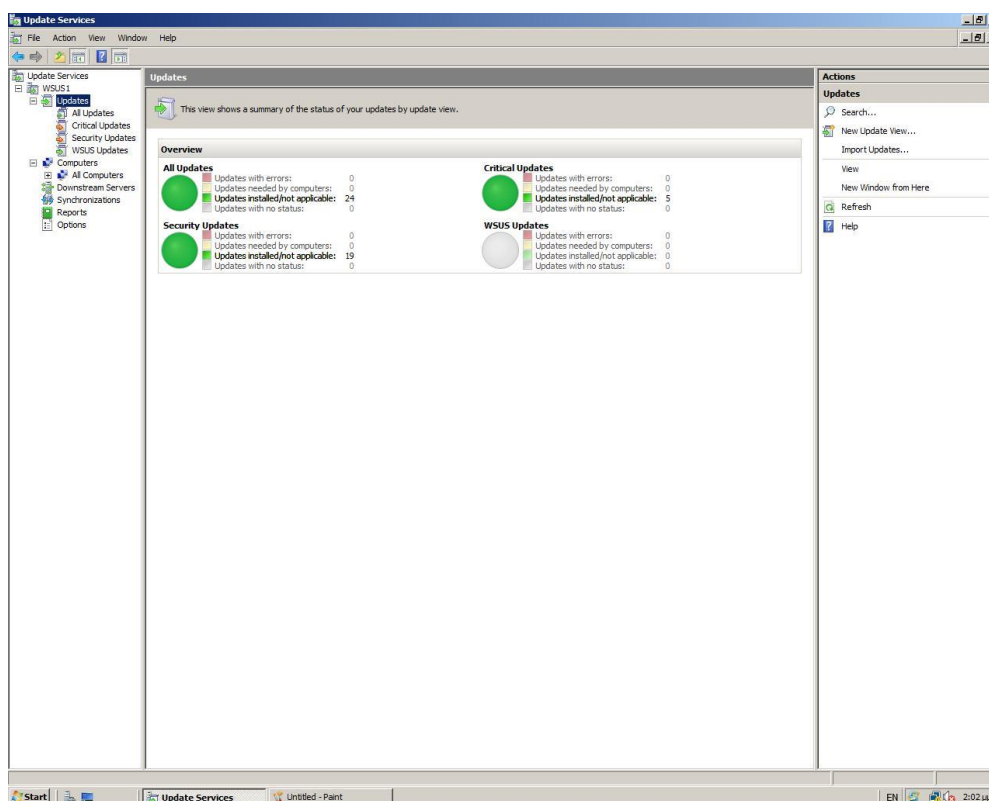
1. Στην κονσόλα διαχείρισης του WSUS, επιλέξτε **Computers**.
2. Επιλέξτε την ομάδα υπολογιστών στην οποία ανήκει ο υπολογιστής που θέλετε να μεταφέρετε στην ομάδα test.
3. Στον κατάλογο των υπολογιστών, επιλέξτε τον υπολογιστή ή τους υπολογιστές που θέλετε να μεταφέρετε.
4. Δεξί κλικ **Change Membership**.
5. Στο διάλογο **Set Computer Group Membership**, επιλέξτε την ομάδα test και επιλέξτε **OK**.

Επαναλάβετε τις παραπάνω δύο διαδικασίες για να δημιουργήσετε όσες ομάδες υπολογιστών χρειάζεστε και να τοποθετήσετε τους υπολογιστές στις ομάδες αυτές.

17.4 Έγκριση και διάθεση ενημερώσεων

Στην παράγραφο αυτή, θα βρείτε διαδικασίες σχετικά με την έγκριση των ενημερώσεων. Οι υπολογιστές της ομάδας, αυτόματα, εντός των επόμενων 24 ωρών, θα επικοινωνήσουν με τον WSUS server για να αποκτήσουν την ενημέρωση. Μπορείτε να χρησιμοποιήσετε τα εργαλεία αναφοράς του WSUS για να δείτε ποιες ενημερώσεις πράγματι διατέθηκαν στους υπολογιστές της ομάδας test. Όταν οι δοκιμές ολοκληρωθούν με επιτυχία, μπορείτε να εγκρίνετε τη διάθεση των ενημερώσεων και για τους υπόλοιπους υπολογιστές του δικτύου σας.

Σημειώνουμε εδώ πως εκτός από την επιλογή έγκρισης (approve), μπορείτε ακόμα να απορρίψετε την εγκατάσταση μίας ενημέρωσης (decline), να αναιρέσετε την έγκρισή σας (disapprove) ή να εγκρίνετε την ανάγκη εγκατάστασης μίας ενημέρωσης αλλά όχι την ίδια την εγκατάστασή της (detect only).



Εικ. 17.22. Σύνοψη της κατάστασης των ενημερώσεων στο δίκτυό σας

Διαδικασία έγκρισης (approval) και διαθέσης (deployment) μία ενημέρωση

1. Στην κονσόλα διαχείρισης του WSUS, επιλέξτε **Updates**. Εμφανίζεται αναφορά για την κατάσταση των ενημερώσεων **All Updates**, **Critical Updates**, **Security Updates**, και **WSUS Updates**.
2. Στο τμήμα **All Updates**, επιλέξτε **Updates needed by computers**.

3. Στον κατάλογο των ενημερώσεων, επιλέξτε τις ενημερώσεις που θέλετε να εγκρίνετε για εγκατάσταση στους υπολογιστές που ανήκουν στην ομάδα test. Πληροφορίες για την επιλεγμένη ενημέρωση βλέπετε στο κάτω μέρος της οθόνης. Μπορείτε να επιλέξετε περισσότερες από μία ενημερώσεις κρατώντας πατημένα τα πλήκτρα **SHIFT** ή/και **CTRL**.
4. Δεξί κλικ και επιλέξτε **Approve**.
5. Στο διάλογο **Approve Updates**, επιλέξτε την ομάδα test, και πατήστε το κάτω βέλος.
6. Επιλέξτε **Approved for Install** και **OK**.
7. Εμφανίζεται το παράθυρο «Approval Progress» στο οποίο βλέπετε την πρόοδο των εργασιών που γίνονται ως συνέπεια της έγκρισης που μόλις κάνατε. Όταν τελειώσει η έγκριση, επιλέξτε **Close**.

Μετά από 24 ώρες, το αργότερο, μπορείτε να χρησιμοποιήσετε τον WSUS για να δείτε τις αναφορές σχετικά με την επιτυχία των εγκαταστάσεων στην ομάδα υπολογιστών test.

Διαδικασία ελέγχου κατάστασης ενημέρωσης

1. Στην κονσόλα διαχείρισης του WSUS, επιλέξτε **Reports**.
2. Στη σελίδα **Reports**, επιλέξτε **Update Status Summary**. Εμφανίζεται το παράθυρο «**Updates Report**».
3. Εάν θέλετε να φιλτράρετε τον κατάλογο των ενημερώσεων, επιλέξτε τα κριτήρια που θέλετε να χρησιμοποιήσετε, π.χ. **Include updates in these classifications**, και μετά επιλέξτε **Run Report** από τη γραμμή εργαλείων του παραθύρου.
4. Θα δείτε το τμήμα **Updates Report** και μπορείτε να ελέγξετε την κατάσταση των ενημερώσεων. Στο τελευταίο μέρος της αναφοράς μπορείτε να δείτε την περίληψη της αναφοράς.
5. Μπορείτε να αποθηκεύσετε ή να εκτυπώσετε την αναφορά από το αντίστοιχο κουμπί στη γραμμή εργαλείων.
6. Αφού ελέγξετε την κατάσταση των ενημερώσεων, μπορείτε να εγκρίνετε την εγκατάσταση και για τους υπόλοιπους υπολογιστές του δικτύου σας.

17.4.1 Αυτόματη έγκριση ενημερώσεων

Μπορείτε να παραμετροποιήσετε τον WSUS server, με τέτοιο τρόπο, ώστε αυτός να εγκρίνει αυτόματα ορισμένες ενημερώσεις. Μπορείτε ακόμα να εγκρίνετε αυτόματα αναθεωρήσεις (revisions) ενημερώσεων που ήδη έχουν εγκριθεί. Εάν επιλέξετε να

μην εγκρίνονται αυτόματα οι αναθεωρήσεις ήδη εγκατεστημένων ενημερώσεων, θα πρέπει να τις εγκρίνετε ξεχωριστά την κάθε μία προτού διανεμηθούν.

Μπορείτε να δημιουργήσετε κανόνες, οι οποίοι θα εφαρμόζονται αυτόματα από το WSUS κατά τη διάρκεια του συγχρονισμού. Μπορείτε να επιλέξετε ποιες ενημερώσεις θα εγκρίνονται αυτόματα, χρησιμοποιώντας ως κριτήρια την κατηγορία των ενημερώσεων, το προϊόν και την ομάδα υπολογιστών. Αυτοί οι κανόνες ισχύουν μόνο για νέες ενημερώσεις και όχι για αναθεωρήσεις ενημερώσεων. Μπορείτε ακόμα να ορίσετε μία προθεσμία, μέχρι τη λήξη της οποίας πρέπει να έχει ολοκληρωθεί η εγκατάσταση των ενημερώσεων. Αυτές οι επιλογές είναι διαθέσιμες στο τμήμα **Options, Automatic Approvals**.

Διαδικασία δημιουργίας νέου κανόνα αυτόματης έγκρισης

1. Στην κονσόλα διαχείρισης του WSUS, επιλέξτε **Options, Automatic Approvals**.
2. Στο **Update Rules**, επιλέξτε **New Rule**.
3. Στο διάλογο **Add Rule**, κάτω από το **Step 1: Select properties**, επιλέξτε εάν θέλετε να χρησιμοποιήσετε ως κριτήριο **When an update is in a specific classification** ή **When an update is in a specific product** ή και τα δύο. Εάν θέλετε, μπορείτε να θέσετε και προθεσμία **Set a deadline for the approval**.
4. Στο **Step 2: Edit the properties** κάντε κλικ στις υπογραμμισμένες ιδιότητες για να επιλέξετε ποια από τα παρακάτω: **Classifications**, **Products**, και **Computer groups** θέλετε να χρησιμοποιήσετε ως κριτήρια αυτόματης έγκρισης. Εάν θέλετε, επιλέξτε προθεσμία για την εγκατάσταση των ενημερώσεων, συμπληρώνοντας **Day** και **Time**.
5. Στο **Step 3: Specify a name**, δώστε ένα όνομα στον κανόνα αυτό.
6. Επιλέξτε **OK**.

Σημείωση: Οι κανόνες αυτόματης έγκρισης δεν εφαρμόζονται στις ενημερώσεις που έχουν End User License Agreement (EULA). Εάν παρατηρήσετε ότι η εφαρμογή κάποιου κανόνα αυτόματης έγκρισης δεν έχει σαν αποτέλεσμα την εγκατάσταση μίας ενημέρωσης (ενώ θα έπρεπε), πρέπει να εγκρίνετε αυτές τις ενημερώσεις μόνοι σας.

Διαδικασία έγκρισης αυτόματης αναθεώρησης και ενημερώσεων και απόρριψης ενημερώσεων που έχουν λήξει (expired updates)

1. Στην κονσόλα διαχείρισης του WSUS, επιλέξτε **Options, Automatic Approvals**.

2. Στην καρτέλα **Advanced**, σιγουρευτείτε ότι και οι ρυθμίσεις **Automatically approve new revisions of approved updates** και **Automatically decline updates when a new revision causes them to expire** είναι ενεργές.

3. Επιλέξτε **OK**.

Σημείωση: Οι προκαθορισμένες ρυθμίσεις για αυτές τις επιλογές εξασφαλίζουν την ορθή λειτουργία και απόδοση του WSUS. Εάν δεν θέλετε οι ενημερώσεις που έχουν λήξει να απορρίπτονται αυτόματα, θα πρέπει περιοδικά να το κάνετε μόνοι σας.

17.4.2 Έγκριση αντικαταστάτριας ενημέρωσης

Μία ενημέρωση μπορεί να διαδέχεται μία άλλη. Αυτό σημαίνει ότι η νεώτερη ενημέρωση περιέχει επιπλέον χαρακτηριστικά που ουσιαστικά ακυρώνουν την ανάγκη εγκατάστασης της παλαιότερης ενημέρωσης. Στην ορολογία του WSUS, η παλαιότερη ενημέρωση λέγεται *superseded* (διαδεχόμενη, αντικαθιστώμενη) και η νεώτερη *superseding* (διάδοχη, αντικαταστάτρια). Στις ιδιότητες κάθε ενημέρωσης ξεχωριστά, μπορείτε να δείτε μία εικόνα και ένα μήνυμα που δηλώνει ότι είναι αντικαταστάτρια ή αντικαθιστώμενη ή ακόμα να δείτε ότι η συγκεκριμένη ενημέρωση αντικαθιστά κάποια άλλη, αλλά και αυτήν την ίδια την αντικαθιστά μία τρίτη έτσι μία ενημέρωση μπορεί να είναι συγχρόνως *superseding* και *superseded*. Μπορείτε επίσης να δείτε ποιες ενημερώσεις αντικαθιστούν αυτή την ενημέρωση (**Updates superseding this update**) και ποιες ενημερώσεις αντικαθιστά αυτή η ενημέρωση (**Updates superseded by this update**). Ο WSUS δεν απορρίπτει αυτόματα τις αντικαθιστώμενες (*superseded*) ενημερώσεις και συνιστάται να μην τις απορρίψετε και εσείς «μηχανικά». Προτού απορρίψετε μία *superseded* ενημέρωση, σιγουρευτείτε ότι δεν την χρειάζεται πλέον κανένας από τους clients σας.

Διαδικασία έγκρισης αντικαταστάτριας ενημέρωσης

1. Ελέγξτε την κατάσταση μίας ενημέρωσης στους clients. Σημειώστε ποιοι υπολογιστές έχουν κατάσταση **Not applicable** για την ενημέρωση και, κατόπιν, συγκρίνετε τα χαρακτηριστικά αυτών των υπολογιστών με αυτά της ενημέρωσης.

2. Χρησιμοποιήστε τις πληροφορίες που είναι διαθέσιμες στις ιδιότητες (properties) της ενημέρωσης για να προσδιορίσετε ποια προηγούμενη έκδοση είναι διαθέσιμη. Μπορείτε να συμβουλευτείτε το **Updates superseded by this update** στις ιδιότητες της ενημέρωσης, και να ελέγξετε την **Description** και το **KB article number**.

3. Δείτε τις ιδιότητες της αντικαθιστώμενης ενημέρωσης.

4. Εάν βρείτε μία αντικαθιστώμενη ενημέρωση που νομίζετε ότι την χρειάζονται κάποιοι από τους υπολογιστές σας, δώστε την έγκρισή σας για την εγκατάσταση.

17.4.3 Κατηγορίες ενημερώσεων WSUS

Κάθε ενημέρωση ανήκει σε μία από τις ακόλουθες κατηγορίες.

- ☐ Critical Updates
- ☐ Definition Updates
- ☐ Drivers
- ☐ Feature Packs
- ☐ Security Updates
- ☐ Service Packs
- ☐ Tools
- ☐ Update Rollups
- ☐ Updates

17.5 Παραμετροποίηση WSUS clients με χρήση πολιτικών σε Active Directory

Κατά την εγκατάσταση του WSUS3.0 SP2, ο IIS ρυθμίζεται αυτόματα, ώστε να διανέμει την τελευταία έκδοση του Automatic Updates σε κάθε client που επικοινωνεί με τον WSUS server.

Ο καλύτερος τρόπος να παραμετροποιήσετε το Automatic Updates είναι με χρήση της δικτυακής σας υποδομής. Σε ένα δίκτυο με Active Directory, μπορείτε να χρησιμοποιήσετε μία ήδη υπάρχουσα πολιτική του domain (GPO) ή να δημιουργήσετε μία νέα. Η Microsoft δεν συνιστά τη χρήση των πολιτικών Default Domain και Default Domain Controller για την προσθήκη ρυθμίσεων του WSUS, αλλά αντίθετα, συνιστά τη χρήση μίας ξεχωριστής πολιτικής για αυτή τη δουλειά. Σε ένα σύνθετο δικτυακό περιβάλλον, μπορεί να χρειαστεί να δημιουργήσετε περισσότερες από μία GPO για να εφαρμόζετε διαφορετικές ρυθμίσεις WSUS σε διαφορετικές ομάδες υπολογιστών.

Σε ένα δικτυακό περιβάλλον χωρίς Active Directory, χρησιμοποιήστε τις τοπικές GPO. Εδώ θα βρείτε διαδικασίες ώστε και θα μάθετε πώς να παραμετροποιείτε το Automatic Updates και να ρυθμίζετε τη λειτουργία του με χρήση GPOs. Για τις ακόλουθες διαδικασίες, απαραίτητη προϋπόθεση είναι η ύπαρξη του Active Directory. Για περισσότερες πληροφορίες σχετικά με Group Policy, επισκεφθείτε το Group Policy Tech Center Web, στη διεύθυνση <http://go.microsoft.com/fwlink/?LinkID=47375>.



Εικ. 17.23. Ρυθμίσεις πολιτικών Windows Update

17.5.1 Παραμετροποίηση Automatic Updates

Διαδικασία παραμετροποίησης Automatic Updates

1. Στην κονσόλα Group Policy Management Console (GPMC), πλοηγηθείτε σε μία GPO στην οποία θέλετε να συμπεριληφθεί η παραμετροποίηση του WSUS και επιλέξτε **Edit**.
2. Στο GPMC, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, Windows Components**, και επιλέξτε **Windows Update**.
3. Στο τμήμα details, κάντε διπλό κλικ στο **Configure Automatic Updates**.
4. Επιλέξτε **Enabled**, και μετά κάντε μία από τις ακόλουθες επιλογές:
 - **Notify for download and notify for install**. Ειδοποιείται ο χρήστης που είναι μέσα στο σύστημα (εφόσον ο χρήστης αυτός έχει δικαιώματα διαχείρισης του συγκεκριμένου υπολογιστή) πριν από το κατέβασμα της ενημέρωσης στον client και πριν από την εγκατάσταση της ενημέρωσης.
 - **Auto download and notify for install**. Ξεκινά αυτόματα το κατέβασμα των ενημερώσεων και κατόπιν ειδοποιείται ο χρήστης που είναι μέσα στο σύστημα (εφόσον ο χρήστης αυτός έχει δικαιώματα διαχείρισης του συγκεκριμένου υπολογιστή) πριν από την εγκατάσταση των ενημερώσεων.
 - **Auto download and schedule the install**. Ξεκινά αυτόματα το κατέβασμα των ενημερώσεων και κατόπιν εγκαθίστανται οι ενημερώσεις την ημέρα και ώρα που ορίζετε.
 - **Allow local admin to choose setting**. Με αυτή την επιλογή, οι τοπικοί διαχειριστές μπορούν να χρησιμοποιήσουν το Automatic Updates (στο Control Panel) για να επιλέξουν ρυθμίσεις κατά την κρίση τους, π.χ. ώρα εγκατάστασης των ενημερώσεων. Οι τοπικοί διαχειριστές δεν μπορούν να απενεργοποιήσουν το Automatic Updates.
5. Επιλέξτε **OK**.

17.5.2 Προσδιορισμός του WSUS server με GPO

Η πολιτική αυτή σάς δίνει τη δυνατότητα να ορίζετε με ποιον WSUS server θα επικοινωνούν τα Automatic Updates προκειμένου να προμηθευτούν τις ενημερώσεις. Είναι απαραίτητο να ενεργοποιήσετε αυτή την πολιτική προκειμένου η εφαρμογή Automatic Updates να κατεβάζει από τον WSUS server τις ενημερώσεις.

Διαδικασία ανακατεύθυνσης Automatic Updates σε WSUS server

1. Στο Group Policy Object Editor, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, Windows Components** και επιλέξτε **Windows Update**.
2. Στις λεπτομέρειες, επιλέξτε **Specify Intranet Microsoft update service location**.
3. Επιλέξτε **Enabled** και γράψτε τη διεύθυνση HTTP(S) του WSUS server στα πλαίσια **Set the intranet update service for detecting updates** και **Set the intranet statistics server**. Π.χ. γράψτε *http://wsus_server* και στα δύο πλαίσια. Εάν δεν χρησιμοποιείται την πόρτα 80 (HTTP) ή 443 (HTTPS) θα πρέπει να γράψετε και την πόρτα, **https://servername:portnumber**.
4. Επιλέξτε **OK**.

Αφού ρυθμίσετε έναν client, θα χρειαστούν αρκετά λεπτά προτού ο υπολογιστής εμφανιστεί στη σελίδα **Computers** της κονσόλας διαχείρισης του WSUS. Για τους clients που έχουν παραμετροποιηθεί μέσω domain GPO, μπορεί να χρειαστούν μέχρι και 20 λεπτά μετά την εφαρμογή της πολιτικής στον client. Θυμίζουμε ότι, σύμφωνα με τις προκαθορισμένες τιμές, οι πολιτικές ασφαλείας ενημερώνονται ανά 90 λεπτά πλέον κάποιου τυχαίου χρονικού διαστήματος που κυμαίνεται από 0–30 λεπτά. Αν επιθυμείτε την ταχύτερη ενημέρωση των GPO's μπορείτε στη γραμμή εντολών του client να δώσετε την εντολή **gpupdate /force**.

Εάν οι clients παραμετροποιούνται με χρήση τοπικής GPO, η πολιτική εφαρμόζεται άμεσα και η ενημέρωση χρειάζεται περίπου 20 λεπτά.

Εάν ξεκινήσετε αναζήτηση δε χρειάζεται να περιμένετε 20 λεπτά μέχρι να επικοινωνήσουν οι clients με τον WSUS.

Διαδικασία αναζήτησης του WSUS server από client

1. Στον client, ανοίξτε τη γραμμή εντολών.
2. Στη γραμμή εντολών, τρέξτε την εντολή **wuauctl /detectnow**. Αυτή η εντολή αναγκάζει το Automatic Updates να επικοινωνήσει με το WSUS server αμέσως.
3. Ένταξη clients σε ομάδες υπολογιστών μέσω GPO -Enable client-side targeting

Η πολιτική αυτή δίνει τη δυνατότητα στους clients να συμμετάσχουν σε μία ομάδα υπολογιστών του WSUS, όταν η εφαρμογή Automatic Updates βλέπει έναν WSUS server αντί του Windows Update.

Όταν είναι ενεργοποιημένη, **Enabled**, ο client θα αναγνωρίζεται από το WSUS ως μέλος μίας συγκεκριμένης ομάδας υπολογιστών, έτσι ώστε ο WSUS να του στέλνει τις κατάλληλες ενημερώσεις. Αυτή η πολιτική δείχνει στον WSUS σε ποια ομάδα υπολογιστών πρέπει να εντάξει τον client. Η ομάδα υπολογιστών δεν δημιουργείται αυτόματα, αλλά πρέπει να δημιουργηθεί από εσάς.

Εάν η πολιτική είναι **Disabled** ή **Not Configured**, τότε οι clients δεν στέλνουν στον WSUS πληροφορίες σχετικές με την ομάδα υπολογιστών που ανήκουν. Σε αυτή την περίπτωση η ένταξη σε ομάδες υπολογιστών γίνεται από το διαχειριστή, μέσω της κονσόλας διαχείρισης του WSUS.

Διαδικασία ένταξης υπολογιστών σε ομάδες

1. Στο Group Policy Object Editor, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, Windows Components** και επιλέξτε **Windows Update**.
2. Στις λεπτομέρειες, επιλέξτε **Enable client-side targeting**.
3. Επιλέξτε **Enabled** και στο πλαίσιο **Target group name for this computer box** γράψτε το όνομα της ομάδας υπολογιστών στην οποία θέλετε να ανήκουν οι clients στους οποίους εφαρμόζεται αυτή η πολιτική.
4. Επιλέξτε **OK**.

Σημείωση: Εάν θέλετε να εντάξετε έναν client σε περισσότερες από μία ομάδες, θα πρέπει να χωρίσετε τα ονόματα των ομάδων με το ελληνικό ερωτηματικό ακολουθούμενο από ένα κενό χαρακτήρα: *Group1; Group2*.

17.5.3 Επαναπρογραμματισμός προγραμματισμένων εγκαταστάσεων - Reschedule Automatic Updates scheduled installations

Αυτή η πολιτική ρυθμίζει το χρονικό διάστημα που πρέπει να περιμένει η εφαρμογή Automatic Updates μετά την επανεκκίνηση ενός client προκειμένου να προχωρήσει στην εγκατάσταση ενημερώσεων που δεν ολοκληρώθηκαν πριν την επανεκκίνηση του client.

Αν αυτή η πολιτική είναι **Enabled**, μία εγκατάσταση που δεν έγινε (π.χ. επειδή ο client ήταν κλειστός εκείνη την ώρα), θα ξεκινήσει μερικά λεπτά μετά την επόμενη επανεκκίνηση του client.

Αν αυτή η πολιτική είναι **Disabled**, μία εγκατάσταση που δεν έγινε, θα γίνει την ώρα της επόμενης προγραμματισμένης εγκατάστασης.

Αν αυτή η πολιτική είναι **Not Configured**, μία εγκατάσταση που δεν έγινε, θα ξεκινήσει ένα λεπτό μετά την επόμενη επανεκκίνηση του client.

Αυτή η πολιτική εφαρμόζεται μόνο όταν η εφαρμογή Automatic Updates είναι ρυθμισμένη να εκτελεί προγραμματισμένες εγκαταστάσεις ενημερώσεων. Αν η πολιτική Configure Automatic Updates είναι απενεργοποιημένη, τότε αυτή η πολιτική δεν έχει καμία επίδραση.

Διαδικασία επαναπρογραμματισμού αυτόματης εγκατάστασης ενημέρωσης

1. Στο Group Policy Object Editor, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, Windows Components** και επιλέξτε **Windows Update**.
2. Στις λεπτομέρειες, επιλέξτε **Reschedule Automatic Update scheduled installations, Enabled** και δώστε τον αριθμό των λεπτών που θέλετε να μεσολαβούν από την επανεκκίνηση του client μέχρι την έναρξη της εγκατάστασης.
3. Επιλέξτε **OK**.

17.5.4 Μη αυτόματη επανεκκίνηση για ολοκλήρωση εγκαταστάσεων - No auto-restart for scheduled Automatic Update installation options

Αυτή η πολιτική καθορίζει το εάν, για να ολοκληρωθεί μία προγραμματισμένη εγκατάσταση ενημέρωσης, η εφαρμογή Automatic Updates θα περιμένει τον υπολογιστή να επανεκκινήσει αντί να ζητήσει την επανεκκίνηση του client. Εάν η πολιτική αυτή είναι **Enabled**, η εφαρμογή Automatic Updates δεν θα επανεκκινεί τον client κατά τη διάρκεια μίας προγραμματισμένης ενημέρωσης εφόσον υπάρχει ενεργός (logged in) χρήστης. Αντί αυτού, ο χρήστης θα ενημερώνεται ότι πρέπει να γίνει επανεκκίνηση προκειμένου να ολοκληρωθεί η εγκατάσταση. Να έχετε υπόψη σας, ότι μέχρι να γίνει επανεκκίνηση η εφαρμογή Automatic Updates δεν μπορεί να προσδιορίσει αν χρειάζονται επιπλέον ενημερώσεις.

Εάν η πολιτική αυτή είναι **Disabled** ή **Not Configured**, τότε η εφαρμογή Automatic Updates θα ενημερώνει το χρήστη ότι ο client πρέπει να επανεκκινήσει αυτόματα σε 5 λεπτά. Αυτή η πολιτική εφαρμόζεται μόνο όταν η εφαρμογή Automatic Updates είναι ρυθμισμένη να εκτελεί προγραμματισμένες εγκαταστάσεις ενημερώσεων. Αν η πολιτική Configure Automatic Updates είναι απενεργοποιημένη, τότε αυτή η πολιτική δεν έχει καμία επίδραση.

Σημείωση: Αυτή η πολιτική δεν εφαρμόζεται σε χρήστες των Terminal Services που δεν έχουν δικαιώματα διαχείρισης του server. Αυτό γίνεται, διότι οι χρήστες των Terminal Services δεν έχουν το δικαίωμα επανεκκίνησης του server.

Διαδικασία αποτροπής αυτόματης επανεκκίνησης του client για προγραμματισμένες εγκαταστάσεις ενημερώσεων

1. Στο Group Policy Object Editor, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, Windows Components** και επιλέξτε **Windows Update**.
2. Στις λεπτομέρειες, επιλέξτε **No auto-restart for scheduled Automatic Update installation options, Enabled**.
3. Επιλέξτε **OK**.

17.5.5 Συχνότητα ελέγχου νέων ενημερώσεων - Automatic Updates detection frequency

Η πολιτική αυτή προσδιορίζει το χρονικό διάστημα που θα μεσολαβεί μεταξύ δύο διαδοχικών αιτήσεων του client για λήψη νέων ενημερώσεων. Ορίζετε τον αριθμό των ωρών που πρέπει να μεσολαβεί μεταξύ διαδοχικών αιτήσεων, π.χ. 20 ώρες. Από αυτό τον αριθμό αφαιρείται ένα τυχαίο χρονικό διάστημα που κυμαίνεται από 0 μέχρι 20% του διαστήματος που ορίσατε (εδώ δηλαδή, 0-4 ώρες). Έτσι, όλοι οι υπολογιστές πάνω στους οποίους εφαρμόζεται η πολιτική αυτή θα επικοινωνούν με το WSUS ζητώντας νέες ενημερώσεις σε ένα χρονικό διάστημα που κυμαίνεται από 16-20 ώρες. Εάν η πολιτική αυτή είναι **Enabled**, η εφαρμογή Automatic Updates θα ελέγχει για νέες ενημερώσεις στο χρονικό διάστημα που προσδιορίστηκε.

Εάν η πολιτική αυτή είναι **Disabled** ή **Not Configured**, η εφαρμογή Automatic Updates θα ελέγχει για νέες ενημερώσεις στο προκαθορισμένο διάστημα [22 ώρες].

Διαδικασία καθορισμού συχνότητας ελέγχου ύπαρξης νέων ενημερώσεων

1. Στο Group Policy Object Editor, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, Windows Components** και επιλέξτε **Windows Update**.
2. Στις λεπτομέρειες, επιλέξτε **Automatic Update detection frequency, Enabled** και γράψτε τον αριθμό των ωρών που θέλετε να μεσολαβεί μεταξύ διαδοχικών ελέγχων.
3. Επιλέξτε **OK**.

17.5.6 Άμεση εγκατάσταση ενημερώσεων - Allow Automatic Update immediate installation

Η πολιτική αυτή προσδιορίζει το εάν η εφαρμογή Automatic Updates πρέπει να εγκαθιστά αυτόματα ενημερώσεις που δεν χρειάζεται να σταματήσουν υπηρεσίες των

Windows για να εγκατασταθούν ή που δεν ζητούν επανεκκίνηση των clients για να ολοκληρωθούν.

Εάν η πολιτική είναι **Enabled**, η εφαρμογή Automatic Updates θα εγκαταστήσει τις ενημερώσεις αμέσως μόλις είναι διαθέσιμες.

Εάν η πολιτική είναι **Disabled**, αυτές οι ενημερώσεις δεν θα εγκαθίστανται αμέσως, αλλά αργότερα, μαζί με άλλες τυχόν ενημερώσεις.

Διαδικασία άμεσης εγκατάστασης ενημερώσεων

1. Στο Group Policy Object Editor, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, Windows Components** και επιλέξτε **Windows Update**.
2. Στις λεπτομέρειες, επιλέξτε **Allow Automatic Update immediate installation** και **Enabled**.
3. Επιλέξτε **OK**.

17.5.7 Καθυστέρηση επανεκκίνησης - Delay restart for scheduled installations

Η πολιτική αυτή προσδιορίζει το χρονικό διάστημα που η εφαρμογή Automatic Updates θα περιμένει, μετά από την εγκατάσταση μίας ενημέρωσης που χρειάζεται επανεκκίνηση για την ολοκλήρωσή της, πριν ζητήσει την επανεκκίνηση του client. Εάν η πολιτική είναι **Enabled**, η επανεκκίνηση θα γίνει μετά από όσο χρονικό διάστημα προσδιορίσετε.

Εάν η πολιτική είναι **Disabled** ή **Not Configured**, τότε η επανεκκίνηση θα γίνεται μετά από 5 λεπτά.

Διαδικασία καθυστέρησης επανεκκίνησης των clients

1. Στο Group Policy Object Editor, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, Windows Components** και επιλέξτε **Windows Update**.
2. Στις λεπτομέρειες, επιλέξτε **Delay restart for scheduled installations, Enabled** και γράψτε τον αριθμό των λεπτών που θέλετε να καθυστερήσει η επανεκκίνηση του client.
3. Επιλέξτε **OK**.

17.5.8 Επανάληψη υπενθύμισης για επανεκκίνηση - Re-prompt for restart with scheduled installations

Η πολιτική αυτή ορίζει το χρονικό διάστημα το οποίο θα μεσολαβεί μεταξύ των υπενθυμίσεων της εφαρμογής Automatic Updates προς το χρήστη για επανεκκίνηση.

Εάν η πολιτική είναι **Enabled**, η υπενθύμιση προς το χρήστη θα γίνεται ανά τακτά χρονικά διαστήματα, την διάρκεια των οποίων ορίζετε εσείς.

Εάν η πολιτική είναι **Disabled** ή **Not Configured**, η υπενθύμιση προς το χρήστη θα γίνεται ανά 10 λεπτά.

Διαδικασία υπενθύμισης επανεκκίνησης

1. Στο Group Policy Object Editor, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, Windows Components** και επιλέξτε **Windows Update**.
2. Στις λεπτομέρειες, επιλέξτε **Re-prompt for restart with scheduled installations, Enabled** και γράψτε τον αριθμό των λεπτών που θέλετε να μεσολαβούν μεταξύ διαδοχικών υπενθυμίσεων.
3. Επιλέξτε **OK**.

17.5.9 Ειδοποιήσεις προς χρήστες που δεν έχουν δικαιώματα διαχείρισης - Allow non-administrators to receive update notifications

Η πολιτική αυτή προσδιορίζει το εάν θα λαμβάνουν οι χρήστες, που είναι logged-on στους clients και δεν έχουν δικαιώματα διαχείρισης, ειδοποιήσεις σχετικές με τις ενημερώσεις. Εάν η εφαρμογή Automatic Updates είναι ρυθμισμένη να ειδοποιεί το χρήστη πριν από το κατέβασμα ή/και πριν την εγκατάσταση ενημερώσεων, αυτές οι ειδοποιήσεις θα απευθύνονται προς όλους τους χρήστες, διαχειριστές και μη.

Εάν η πολιτική είναι **Enabled**, η εφαρμογή Automatic Updates θα ειδοποιεί όλους τους χρήστες (διαχειριστές και μη), εφόσον είναι συνδεδεμένοι (logged-on).

Εάν η πολιτική είναι **Disabled** ή **Not Configured**, η εφαρμογή Automatic Updates θα ειδοποιεί μόνο τους διαχειριστές, εφόσον είναι συνδεδεμένοι (logged-on).

Διαδικασία λήψης ειδοποιήσεων από μη διαχειριστές

1. Στο Group Policy Object Editor, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, Windows Components** και επιλέξτε **Windows Update**.
2. Στις λεπτομέρειες, επιλέξτε **Allow non-administrators to receive update notifications** και **Enabled**.
3. Επιλέξτε **OK**.

Σημείωση: Αυτή η πολιτική δεν εφαρμόζεται σε χρήστες των Terminal Services που δεν έχουν δικαιώματα διαχείρισης του server. Αυτό γίνεται, διότι οι χρήστες των Terminal Services δεν έχουν το δικαίωμα επανεκκίνησης του server.

17.5.10 Να επιτρέπεται η λήψη ενημερώσεων και από τρίτους κατασκευαστές -**Allow signed content from the intranet Microsoft update service location**

Εάν αυτή η πολιτική είναι ενεργή, η εφαρμογή Automatic Updates θα λαμβάνει ενημερώσεις (που τις έχει εγκρίνει και τις διανέμει η Microsoft) τρίτων κατασκευαστών. Αν η πολιτική αυτή δεν είναι ενεργή, θα μπορείτε να λαμβάνετε ενημερώσεις μόνο από την Microsoft.

Διαδικασία λήψης ενημερώσεων τρίτων κατασκευαστών

1. Στο Group Policy Object Editor, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, Windows Components** και επιλέξτε **Windows Update**.
2. Στις λεπτομέρειες, επιλέξτε **Allow signed content from intranet Microsoft update service location** και **Enabled**.
3. Επιλέξτε **OK**.

17.5.11 Αφαίρεση συνδέσμων και πρόσβασης στο Windows Update - Remove links and access to Windows Update

Εάν αυτή η πολιτική είναι ενεργοποιημένη, η εφαρμογή Automatic Updates λαμβάνει ενημερώσεις από τον WSUS server. Οι χρήστες που έχουν ενεργοποιημένη αυτή τη πολιτική δεν μπορούν να λαμβάνουν ενημερώσεις από το Windows Update που δεν έχουν εγκριθεί από εσάς. Εάν αυτή η πολιτική δεν είναι ενεργοποιημένη, οι τοπικοί διαχειριστές εξακολουθούν να βλέπουν σύνδεσμο προς το Windows Update και να μπορούν να επισκέπτονται το Windows Update, από το οποίο μπορούν να εγκαθιστούν μη εγκεκριμένες από εσάς ενημερώσεις.

Διαδικασία αφαίρεσης συνδέσμων και πρόσβασης στο Windows Update

1. Στο Group Policy Object Editor, αναπτύξτε **User Configuration, Policies, Administrative Templates** και επιλέξτε **Start Menu and Taskbar**.
2. Στις λεπτομέρειες, επιλέξτε **Remove links and access to Windows Update** και **Enabled**.
3. Επιλέξτε **OK**.

17.5.12 Απαγόρευση πρόσβασης στο Windows Update - Disable access to Windows Update

Εάν αυτή η πολιτική είναι ενεργοποιημένη, η πρόσβαση προς το Windows Update αφαιρείται ή απενεργοποιείται. Οι υπολογιστές που υπόκεινται σε αυτή τη πολιτική δε μπορούν να λάβουν ενημερώσεις από το Windows Update ή το Microsoft Update, αλλά μπορούν να αντλούν ενημερώσεις από τον WSUS server. Αυτή η πολιτική

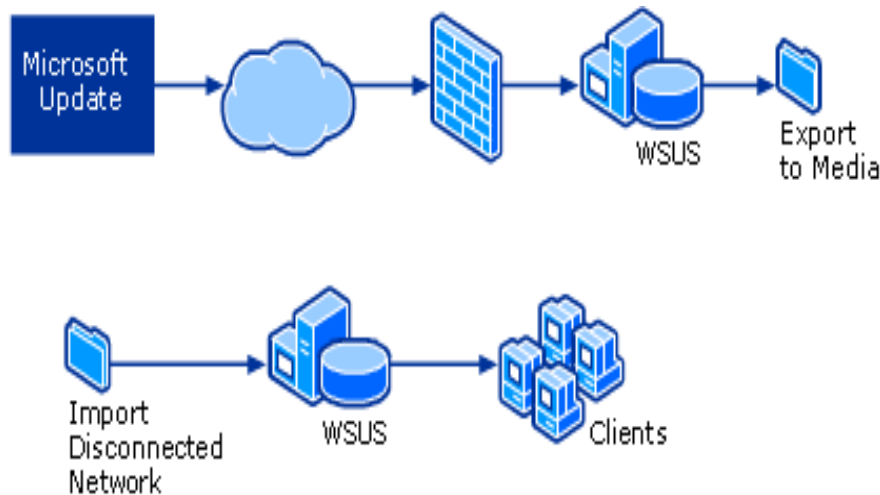
υπερισχύει των ρυθμίσεων **Remove links and access to Windows Update** και **Remove access to use all Windows Update features**.

Διαδικασία απαγόρευσης πρόσβασης στο Windows Update

1. Στο Group Policy Object Editor, αναπτύξτε **Computer Configuration, Policies, Administrative Templates, System, Internet Communication Management** και επιλέξτε **Internet Communication settings**.
2. Στις λεπτομέρειες, επιλέξτε **Turn off access to all Windows Update features** και **Enabled**.
3. Επιλέξτε **OK**.

17.6 WSUS για απομονωμένα δίκτυα

Η διαχείριση του WSUS σε ένα μη συνδεδεμένο (στο Internet) δίκτυο περιλαμβάνει (πλέον όσων έχουμε ήδη αναφέρει) την εξαγωγή ενημερώσεων και metadata από έναν WSUS server που βρίσκεται συνδεδεμένος στο Internet και την εισαγωγή τους στον WSUS server του απομονωμένου δικτύου.



Εικ. 17.24. Διάθεση ενημερώσεων σε απομονωμένο δίκτυο

Για την εξαγωγή και εισαγωγή των ενημερώσεων και των metadata πρέπει να γίνουν τα ακόλουθα.

- Να σιγουρευτείτε ότι οι επιλογές σχετικά με τα αρχεία express εγκατάστασης και γλώσσες ενημερώσεων στους δύο servers είναι οι ίδιες. Αυτό εξασφαλίζει ότι συλλέγετε πράγματι τις ενημερώσεις που σκοπεύετε να διαθέσετε στο απομονωμένο δίκτυο.
- Να αντιγράψετε τις ενημερώσεις από τον server από τον οποίο κάνετε την εξαγωγή στον απομονωμένο server.
- Να εξάγετε τα metadata από τη βάση του server εξαγωγής και να τα εισάγετε στη βάση του απομονωμένου server.

Σημείωση: Για λόγους συντομίας, στο εξής, αναφερόμαστε στον WSUS server από τον οποίο γίνεται η εξαγωγή ως WSUS_e (e: export) και στον απομονωμένο WSUS ως WSUS_i (i: import).

17.6.1 Επιλογές για αρχεία και γλώσσες

Σιγουρευτείτε ότι οι επιλογές σχετικά με τα αρχεία για εγκατάσταση με αρχεία express εγκατάστασης και γλώσσες ενημερώσεων στους δύο servers είναι οι ίδιες. Δε χρειάζεται να συμβαίνει το ίδιο με τις ρυθμίσεις σχετικά με το πρόγραμμα συγχρονισμού, προϊόντα και κατηγορίες ενημερώσεων, upstream και proxy server.

Διαδικασία ρυθμίσεων για αρχεία express εγκατάστασης και γλώσσες μεταξύ δύο WSUS servers

1. Στην κονσόλα διαχείρισης του WSUS_e, επιλέξτε **Options** (στο αριστερό τμήμα) και μετά **Update Files and Languages**.
2. Στην καρτέλα **Update Files**, ελέγξτε τη ρύθμιση **Download express installation files**.
3. Στην καρτέλα **Update Languages**, ελέγξτε τις ρυθμίσεις για τις γλώσσες των ενημερώσεων.
4. Στην κονσόλα διαχείρισης του WSUS_i, επιλέξτε **Options** (στο αριστερό τμήμα) και μετά **Update Files and Languages**.
5. Σιγουρευτείτε ότι οι ρυθμίσεις για **Download express installation files and Update Languages** είναι οι ίδιες με αυτές του WSUS_e.

17.6.2 Μεταφορά αρχείων στον απομονωμένο server

Η αντιγραφή των ενημερώσεων από τον WSUS_e στον WSUS_i μπορεί να γίνει με οποιοδήποτε πρόσφορο τρόπο (π.χ αντιγραφή φακέλου, με χρήση της εντολής xcopy ή με όποιον άλλο σας βολεύει). Κατά τη διαδικασία αυτή χρειάζεται να διατηρείται η δομή των φακέλων που περιέχουν τις ενημερώσεις.

Στις ακόλουθες διαδικασίες χρησιμοποιούμε την εφαρμογή backup που περιλαμβάνεται στο λειτουργικό σύστημα. Καλό είναι επίσης να χρησιμοποιείται incremental backup ώστε να περιορίζετε ο όγκος των δεδομένων που μεταφέρεται κάθε φορά που ενημερώνετε τον WSUS_i.

Διαδικασία εξαγωγής ενημερώσεων

1. Στον WSUS_e, επιλέξτε **Start, Run**.
2. Στο διάλογο **Run**, γράψτε **ntbackup**. Ο οδηγός **Backup or Restore Wizard** ξεκινά, εκτός αν είναι απενεργοποιημένος. Σε αυτή την περίπτωση επιλέξτε **Advanced Mode**.
3. Επιλέξτε **Backup**, και μετά επιλέξτε το φάκελο στον οποίο αποθηκεύονται οι ενημερώσεις. Ο προκαθορισμένος φάκελος είναι ο *WSUSInstallationDrive\WSUS\WSUSContent*, όπου *WSUSInstallationDrive* είναι ο δίσκος στον οποίο έχει γίνει η εγκατάσταση του WSUS.
4. Στο **Backup media or file name**, γράψτε τη θέση που θα αποθηκευτεί το αρχείο του backup (.bkf).
5. Επιλέξτε **Start Backup**. Θα εμφανιστεί ο διάλογος **Backup Job Information**.
6. Επιλέξτε **Advanced** και κάτω από το **Backup Type**, επιλέξτε **Incremental**.

7. Στο διάλογο **Backup Job Information**, επιλέξτε **Start Backup**.
8. Αντιγράψτε το αρχείο του backup στον WSUS_i.

Διαδικασία εισαγωγής ενημερώσεων

1. Στον WSUS_i, επιλέξτε **Start, Run**.
2. Στο διάλογο **Run**, γράψτε **ntbackup**. Ο οδηγός **Backup or Restore Wizard** ξεκινά, εκτός αν είναι απενεργοποιημένος. Σε αυτή την περίπτωση επιλέξτε **Advanced Mode**.
3. Επιλέξτε την καρτέλα **Restore and Manage Media**, και επιλέξτε το αρχείο που δημιουργήσατε στον WSUS_e.
4. Στο **Restore files to**, επιλέξτε **Alternate location**. Με αυτή την επιλογή διατηρείται η δομή των φακέλων των ενημερώσεων. Θυμίζουμε ότι πρέπει να διατηρείτε τη δομή όλων των φακέλων κάτω από το φάκελο \WSUSContent.
5. Κάτω από το **Alternate location**, προσδιορίστε το φάκελο που αποθηκεύονται οι ενημερώσεις στον WSUS_i. Ο προκαθορισμένος φάκελος είναι ο *WSUSInstallationDrive\WSUS\WSUSContent*, όπου *WSUSInstallationDrive* είναι ο δίσκος στον οποίο έχει γίνει η εγκατάσταση του WSUS.
6. Επιλέξτε **Start Restore**. Όταν εμφανιστεί ο διάλογος **Confirm Restore**, επιλέξτε **OK**.

17.6.3 Μεταφορά metadata στον απομονωμένο server

Η εξαγωγή και η εισαγωγή των metadata γίνεται με χρήση της εντολής WSUSUtil.exe.

Σημείωση: Πρέπει να είσαστε μέλος της ομάδας Local Administrators στον WSUS server για να εξάγετε ή εισάγετε στοιχεία στη βάση. Και οι δύο διαδικασίες εκτελούνται μόνο σε WSUS server και όχι απομακρυσμένα.

Η αντιγραφή των ενημερώσεων στον WSUS_i, πρέπει να έχει ολοκληρωθεί πριν από την εισαγωγή των metadata. Σε περίπτωση που ο WSUS βρει metadata για μία ενημέρωση που δεν βρίσκεται στο σύστημα αρχείων του, τότε η κονσόλα του WSUS δείχνει ότι απέτυχε να κατεβάσει την ενημέρωση. Αυτό το πρόβλημα διορθώνεται αντιγράφοντας την ενημέρωση στον WSUS_i και διαθέτοντας (deploy) την ενημέρωση εκ νέου.

Αν και μπορείτε να χρησιμοποιήσετε incremental backup για να μεταφέρετε τα αρχεία των ενημερώσεων, δε μπορείτε να μεταφέρετε τα metadata με αυτό τον τρόπο. Η WSUSUtil.exe εξάγει όλα τα metadata από τη βάση του WSUS.

Σημείωση: Μην εισάγετε ποτέ δεδομένα από πηγή που δεν εμπιστεύεστε. Η

εισαγωγή δεδομένων από μη έμπιστο server μπορεί να θέσει σε κίνδυνο την ασφάλεια του WSUS server.

Σημείωση: Κατά τη διάρκεια της εισαγωγής ή της εξαγωγής η υπηρεσία Update Service, που στηρίζει το WSUS, σταματά να λειτουργεί.

Διαδικασία εξαγωγής metadata

1. Στη γραμμή εντολών του WSUS_e, πηγαίνετε στο φάκελο που περιέχει την εντολή WSUSutil.exe (τυπικά...\Program Files\Update Services\Tools).

2. Δώστε την εντολή: **wsusutil.exe export packagename logfile**

Για παράδειγμα: **wsusutil.exe export export.cab export.log**

Η εντολή WSUSutil.exe δημιουργεί τα αρχεία export.cab και export.log καθώς εξάγει στοιχεία από τη βάση του WSUS.

3. Μεταφέρετε το αρχείο τύπου cab στον WSUS_i.

Διαδικασία εισαγωγής metadata

1. Στη γραμμή εντολών του WSUS_e, πηγαίνετε στο φάκελο που περιέχει την εντολή WSUSutil.exe (τυπικά...\Program Files\Update Services\Tools).

2. Δώστε την εντολή: **wsusutil.exe import packagename logfile**

Για παράδειγμα: **wsusutil.exe import export.cab import.log**

Η εντολή WSUSutil.exe εισάγει τα metadata από τον WSUS_e και δημιουργεί ένα αρχείο log.

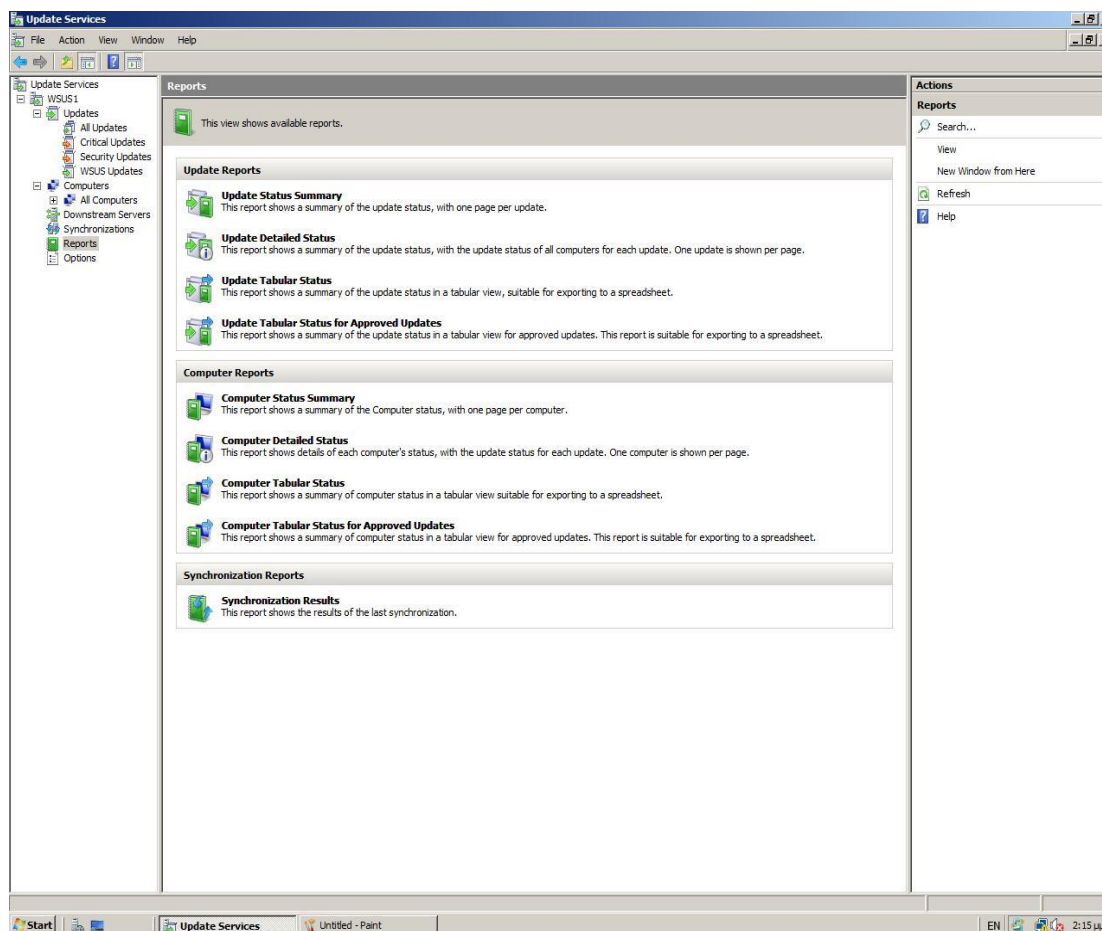
Σημείωση: Μπορεί να χρειαστούν μερικές ώρες μέχρι η βάση να επιβεβαιώσει ότι η εισαγωγή του περιεχομένου ολοκληρώθηκε.

17.7 Διαχείριση αναφορών στο WSUS

Οι αναφορές αποτελούν ένα σημαντικό κομμάτι της διαχείρισης του WSUS.

Μπορείτε να δείτε τις ακόλουθες αναφορές:

- Συνοπτική αναφορά, που περιλαμβάνει τον αριθμό των υπολογιστών που πρέπει να εγκαταστήσουν ενημερώσεις και τον αριθμό των ενημερώσεων που λείπουν από τους υπολογιστές. Αυτές οι αναφορές είναι διαθέσιμες στον αρχικό κόμβο του αριστερού τμήματος της κονσόλας διαχείρισης του WSUS.
- Αναφορά για συγκεκριμένο υπολογιστή, στο αριστερό τμήμα της κονσόλας διαχείρισης του WSUS κάντε δεξί κλικ πάνω στο **Computers**.
- Αναφορά για συγκεκριμένη ενημέρωση, στο αριστερό τμήμα της κονσόλας διαχείρισης του WSUS κάντε δεξί κλικ πάνω στο **Updates**.
- Συνοπτική αναφορά downstream server, στο αριστερό τμήμα της κονσόλας διαχείρισης του WSUS κάντε δεξί κλικ πάνω στο **Downstream Servers**.
- Αναφορές συγχρονισμού, στο αριστερό τμήμα της κονσόλας διαχείρισης του WSUS κάντε δεξί κλικ πάνω στο **Synchronizations**.



Εικ. 17.25. Αναφορές στο WSUS

17.7.1 Κατάσταση εγκατάστασης ενημέρωσης

Η πρόσβαση στις αναφορές είναι εφικτή από διάφορα σημεία της κονσόλας διαχείρισης του WSUS. Οι καταστάσεις που αναφέρει ο WSUS για μία ενημέρωση είναι οι ακόλουθες.

- **Installed:** Η ενημέρωση έχει εγκατασταθεί στον client.
- **Needed:** Όταν αναφέρεται στην κατάσταση ενός client, σημαίνει ότι η ενημέρωση είναι συμβατή με τον client και ότι πρέπει να εγκατασταθεί. Όταν αναφέρεται σε ομάδα υπολογιστών δείχνει τον αριθμό των υπολογιστών που χρειάζονται την ενημέρωση.
- **Installed/Not Applicable:** Όταν αναφέρεται σε έναν client, σημαίνει ότι η ενημέρωση δεν χρειάζεται να εγκατασταθεί στον client ή έχει ήδη εγκατασταθεί σε αυτόν. Όταν αναφέρεται σε ομάδα υπολογιστών, δείχνει τον αριθμό των clients που δεν χρειάζονται αυτή την ενημέρωση ή την έχουν ήδη εγκατεστημένη.
- **No status:** Συνήθως αυτή η κατάσταση σημαίνει ότι από την ώρα που η ενημέρωση κατέβηκε στον WSUS, ο client δεν έχει επικοινωνήσει με τον WSUS server.
- **Failed:** Κάποιο πρόβλημα προέκυψε κατά την ανίχνευση ή την εγκατάσταση της ενημέρωσης.
- **Last contacted:** Ημερομηνία τελευταίας επικοινωνίας μεταξύ του client και του WSUS server.

17.7.2 Δημιουργία αναφορών

Οι αναφορές σάς βοηθούν να παρακολουθείτε διάφορες πτυχές της δραστηριότητας του WSUS, όπως: ενημερώσεις, clients και downstream servers. Αν ένας WSUS server έχει replica servers, τότε και αυτοί μπορούν να αναφέρουν την κατάσταση των ενημερώσεων των clients τους στον upstream server.

17.8 Χρήση των αναφορών

Μπορείτε να δημιουργήσετε τρία είδη αναφορών.

- **Update Reports:** Για να δείτε την κατάσταση των ενημερώσεων.
- **Computer Reports:** Για να δείτε την κατάσταση των υπολογιστών.
- **Synchronization Reports:** Για να δείτε τα αποτελέσματα των συγχρονισμών.

17.8.1 Αναφορές ενημερώσεων

Οι αναφορές ενημερώσεων δείχνουν την κατάσταση των ενημερώσεων. Οι αναφορές ενημερώσεων εμφανίζουν τα δεδομένα με έναν από τους ακόλουθους τρόπους: (α)

περιληπτικά, (β) λεπτομερώς, (γ) σε πίνακα, και (δ) σε πίνακα για εγκεκριμένες ενημερώσεις. Μπορείτε ακόμα να χρησιμοποιήσετε ως φίλτρο την κατηγορία ενημέρωσης, το προϊόν, ομάδα υπολογιστών και την κατάσταση εγκατάστασης της ενημέρωσης.

Διαδικασία εκτέλεσης αναφοράς ενημερώσεων

1. Στην κονσόλα διαχείρισης του WSUS, επιλέξτε **Reports**
2. Στο τμήμα **Reports**, επιλέξτε μία από τις ακόλουθες επιλογές για το **Update Reports: Update Status Summary, Update Detailed Status, Update Tabular Status**, ή **Update Tabular Status for Approved Updates**.
3. Στο παράθυρο **Updates Report** μπορείτε να επιλέξετε τις ενημερώσεις που θέλετε να εμφανιστούν με κριτήριο την κατηγορία, το προϊόν, την ομάδα υπολογιστών και την κατάσταση εγκατάστασης της ενημέρωσης.
4. Επιλέξτε **Run Report**.
5. Μπορείτε να αλλάξετε την προβολή της αναφοράς σε λεπτομερειακή, περιληπτική ή σε πίνακα επιλέγοντας **Report View** στη γραμμή εργαλείων **Updates Report**.

17.8.2 Αναφορές υπολογιστών

Οι αναφορές υπολογιστών δείχνουν την κατάσταση των υπολογιστών. Και εδώ υπάρχουν διαθέσιμες οι ίδιες προβολές, (α) περιληπτικά, (β) λεπτομερώς, (γ) σε πίνακα, και (δ) σε πίνακα για εγκεκριμένες ενημερώσεις. Μπορείτε ακόμα να χρησιμοποιήσετε ως φίλτρο την κατηγορία ενημέρωσης, το προϊόν, ομάδα υπολογιστών και την κατάσταση εγκατάστασης της ενημέρωσης.

Διαδικασία εκτέλεσης αναφοράς υπολογιστών

1. Στην κονσόλα διαχείρισης του WSUS, επιλέξτε **Reports**.
2. Στο τμήμα **Reports**, επιλέξτε μία από τις ακόλουθες επιλογές για το **Update Reports: Update Status Summary, Update Detailed Status, Update Tabular Status**, ή **Update Tabular Status for Approved Updates**.
3. Στο παράθυρο **Computers Report**, να επιλέξετε τις ενημερώσεις που θέλετε να εμφανιστούν με κριτήριο την κατηγορία, το προϊόν, την ομάδα υπολογιστών και την κατάσταση εγκατάστασης της ενημέρωσης.
4. Επιλέξτε **Run Report**.
5. Μπορείτε να αλλάξετε την προβολή της αναφοράς σε λεπτομερειακή, περιληπτική ή σε πίνακα επιλέγοντας **Report View** στη γραμμή εργαλείων **Updates**

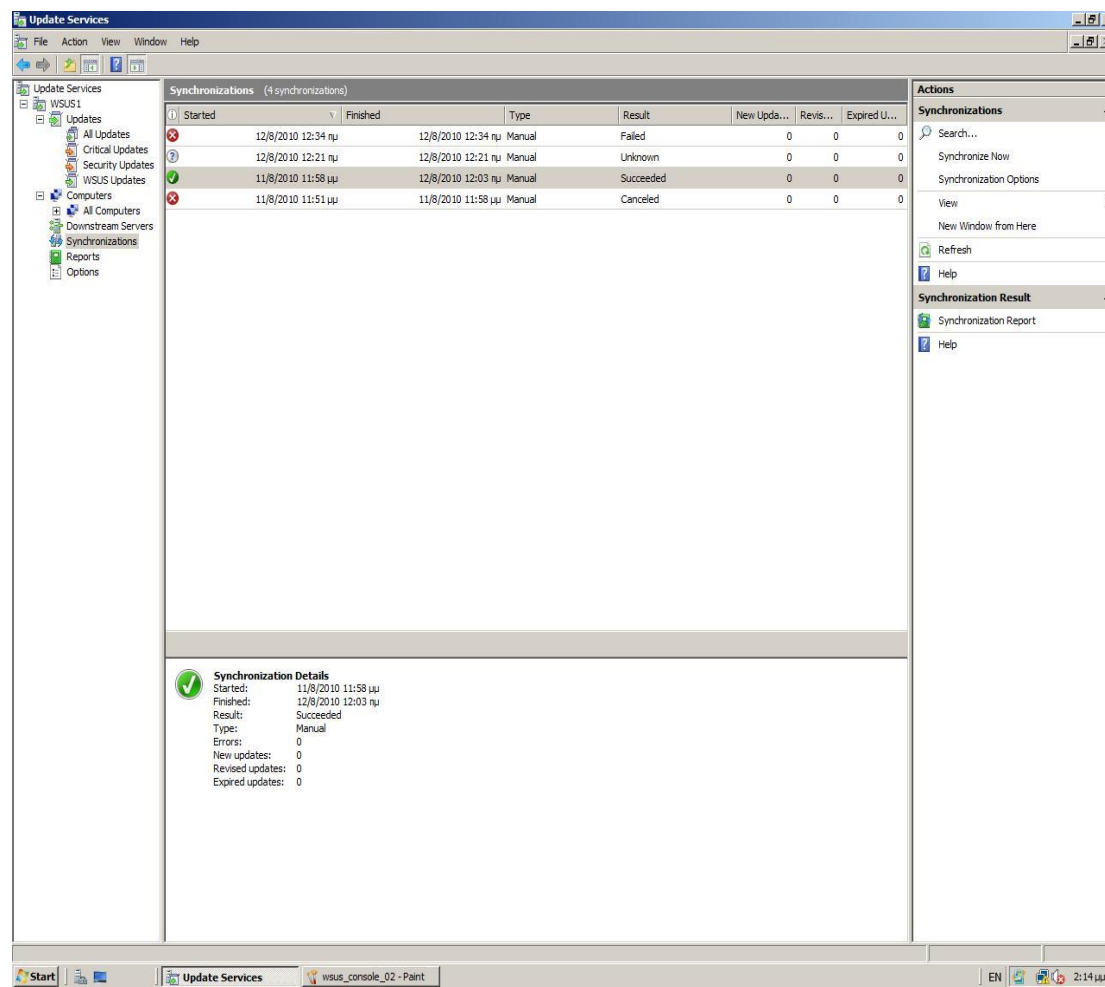
Report.

17.8.3 Αναφορές συγχρονισμού

Οι αναφορές συγχρονισμού σάς δίνουν τη δυνατότητα να δείτε πληροφορίες σχετικά με το συγχρονισμό του WSUS server για ένα συγκεκριμένο διάστημα. Στις πληροφορίες αυτές συμπεριλαμβάνονται τυχόν λάθη που συνέβησαν κατά τη διάρκεια των συγχρονισμών και λίστα νέων ενημερώσεων.

Διαδικασία εκτέλεσης αναφοράς συγχρονισμού

1. Στην κονσόλα διαχείρισης του WSUS, επιλέξτε **Reports**.
2. Στο τμήμα **Reports**, επιλέξτε **Synchronization Results**. Η προκαθορισμένη ρύθμιση είναι η εμφάνιση των συγχρονισμών που έγιναν την ίδια ημέρα.
3. Για να αλλάξετε το χρονικό διάστημα για το οποίο θα εμφανίζονται αποτελέσματα στην αναφορά, στο παράθυρο **Synchronization Report**, επιλέξτε **Between these dates** και προσδιορίστε τις ημέρες που θέλετε να συμπεριληφθούν στην αναφορά.
4. Επιλέξτε **Run Report**.



Εικ. 17.26. Αναφορά συγχρονισμού στο WSUS

17.9 Βέλτιστες πρακτικές WSUS

Για διευκόλυνσή σας, παραθέτονται εδώ βέλτιστες πρακτικές σχετικά με τη ρύθμιση και τη χρήση του WSUS. Όλες είναι απλές και λογικές επιλογές, συνεπώς η χρήση τους δεν θα πρέπει να σας προβληματίσει. Φυσικά θα πρέπει να εφαρμόσετε μόνο εκείνες που σας εξυπηρετούν και ταιριάζουν στο δίκτυό σας.

- Να μην χρησιμοποιείτε τις πολιτικές Default Domain ή Default Domain Controller για να ρυθμίζετε τους clients, αλλά μία άλλη πολιτική.
- Να χρησιμοποιείτε τουλάχιστον τρεις διαφορετικές πολιτικές (άρα και Organizational Units) για να εφαρμόζετε διαφορετικές ρυθμίσεις στους servers, στους WSUS servers και στους clients.
- Να βάλετε τους WSUS servers σας σε μία ξεχωριστή ομάδα υπολογιστών. Η διάθεση των ενημερώσεων σε αυτή την ομάδα υπολογιστών θα πρέπει να γίνεται με προθεσμία. Η προθεσμία όμως θα πρέπει να λήγει σε ώρα που να είναι αποδεκτή η έλλειψη διαθεσιμότητας των WSUS servers, π.χ. Κυριακή πρωί στις 3:00 π.μ.
- Να εφαρμόζετε τη ρύθμιση «Download the updates automatically and notify when they are ready to be installed» στις ομάδες υπολογιστών που περιέχουν servers, ώστε να έχετε εσείς την επιλογή του χρόνου της επανεκκίνησης.
- Να διαθέτετε ενημερώσεις με χρήση προθεσμίας. Η προθεσμία για κάθε ομάδα υπολογιστών πρέπει να είναι τέτοια ώστε να είναι αποδεκτό το διάστημα μη λειτουργίας (downtime) που μπορεί να υπάρξει.
- Να χρησιμοποιείτε ομάδες υπολογιστών για δοκιμαστικές εγκαταστάσεις.
- Να ρυθμίσετε τους clients σας ώστε να εγκαθιστούν αμέσως τις ενημερώσεις που δεν απαιτούν σταμάτημα υπηρεσιών ή επανεκκίνηση υπολογιστών.
- Να αποφεύγετε την αυτόματη επανεκκίνηση στους clients που θα κάνουν ούτως ή άλλως (π.χ. σε μία υπηρεσία με πρωινή βάρδια μόνο) μία επανεκκίνηση μέσα σε ένα 24ώρο, να την επιβάλλετε όμως για υπολογιστές που δουλεύουν συνεχώς.
- Να συνδέονται όλοι οι downstream servers σε έναν μόνο upstream server.
- Να χρησιμοποιείτε για κάθε downstream server διαφορετικό πρόγραμμα συγχρονισμού με τον upstream server.
- Να εξασφαλίσετε ότι όλοι οι WSUS servers του δικτύου σας έχουν την ίδια ώρα συστήματος.