Τ.Ε.Ι. ΗΠΕΙΡΟΥ

T.E.I. OF EPIRUS

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ (Σ.Δ.Ο)
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ

SCHOOL OF MANAGEMENT AND ECONOMICS
DEPARTMENT OF COMMUNICATIONS, INFORMATICS AND MANAGEMENT

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ:

ΥΛΟΠΟΙΗΣΗ ΤΟΥ ACTIVE DIRECTORY ΣΕ ΠΕΡΙΒΑΛΛΟΝ WINDOWS 2003

ΨΑΡΡΑΣ ΒΑΣΙΛΕΙΟΣ

Πρόλογος

Το παρών έγγραφο αποτελεί εκπόνηση της διπλωματικής εργασίας του φοιτητή Ψαρρά Βασίλειο με τίτλο : *Υλοποίηση του Active Directory σε Περιβάλλον Windows 2003.* Στόχος αυτού του εγγράφου είναι να εισάγει το αναγνώστη στα μυστικά του Active Directory, στις δυνατότητες του και στην πληθώρα εφαρμογών που έχει αυτό με επίκεντρο της δικτυακές του δυνατότητες. Η δομή του εγγράφου ξεκινά ιεραρχικά με το να εισάγει τον αναγνώστη στον τρόπο λειτουργίας και διεκπεραίωσης των εργασιών από το Active Directory και αργότερα να εντρυφήσει στους τρόπους υλοποίησης δικτυακών μοντέλων και υπηρεσιών που μπορούν να παραχθούν με την χρησιμοποίηση του.

Το παρών σύγγραμμα υλοποιήθηκε υπό την επίβλεψη του Κου Γεώργιου Ρίζου , μόνιμου διαχειριστή δικτύου στο Τ.Ε.Ι. Ηπείρου και καθηγητή του τμήματος Τηλεπληροφορικής και Διοίκησης στην Άρτα. Σας ευχαριστούμε εκ τον προτέρων για την διάθεση σας να αναγνώσετε το έγγραφο και ελπίζουμε στην κατανόηση ενός νέου αλλά πολλά υποσχόμενου λειτουργικού στον χώρο των δικτυακών εφαρμογών.

ΠΕΡΙΕΧΌΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

Έχετε ακούσει πληθώρα πραγμάτων για το Active Directory. Μερικοί λένε ότι το Active Directory είναι το καλύτερο προϊόν που η Microsoft έχει παράγει – άλλοι πάλι λένε ότι το Active Directory είναι σε πρώιμο στάδιο ακόμα και πρέπει να ωριμάσει. Ανεξαρτήτως με την θέση σας, μπορούμε όλοι να συμφωνήσουμε ότι το Active Directory είναι προϊόν ναυαρχίδα για την Microsoft, προς το παρόν, και ότι ήρθε για να μείνει. Το Active Directory είναι το θεμελιώδες στοιχείο δικτύωσης στα Windows 2000 και συνεπώς αναπόσπαστο κομμάτι από τα Windows 2003. Το Active Directory βελτιώνει εντελώς τον τρόπο δικτύωσης της Microsoft από τις ημέρες των NT και τον φέρνει σε ένα ιεραρχικό, μοντέλο υπηρεσιών καταλόγου. Αυτό το μοντέλο εκσυγχρονίζει τα NT και προετοιμάζει το έδαφος για το μέλλον. Με το Active Directory, έχουμε περισσότερη ευχρηστία , περισσότερη υποστήριξη για τους πόρους δικτύων, τυποποιημένη ονομασία, και άριστες ικανότητες ερώτησης. Εν ολίγοις, το Active Directory ανοίγει έναν ολόκληρο νέο κόσμο για τα Windows.

1.1 Ιστορία του Directory Service

Στο κοντινό παρελθόν, τα δίκτυα ήταν server-κεντρικά. Κάθε server είχε το δικό του σύστημα ασφάλειάς, το όποιος αποτελούταν από τους λογαριασμούς χρηστών, λογαριασμούς ομάδας, και πόρους του δικτύου. Θα συσχέτιζε εκείνους τους λογαριασμούς χρηστών στα αρχεία, κατάλογους εκτυπωτές, άλλες υπηρεσίες ή πόρους που είχε να προσφέρει. Αυτές οι συσχετίσεις είχαν αξία για τους servers, έτσι ώστε ένα άτομο να μπορεί να έχει περισσότερη πρόσβαση σε πόρους του δικτύου από ένα άλλο πρόσωπο, απλά λόγω των δικαιωμάτων που ανατίθενται στους λογαριασμούς χρηστών και ομάδας. Κατά κάποιο τρόπο, αυτό το server -κεντρικό σύστημα ήταν μια από τις πρώτες υπηρεσίες καταλόγου αρχείων, αλλά ενός ο ρόλος του οποίου υπήρξε μόνο σε έναν server.

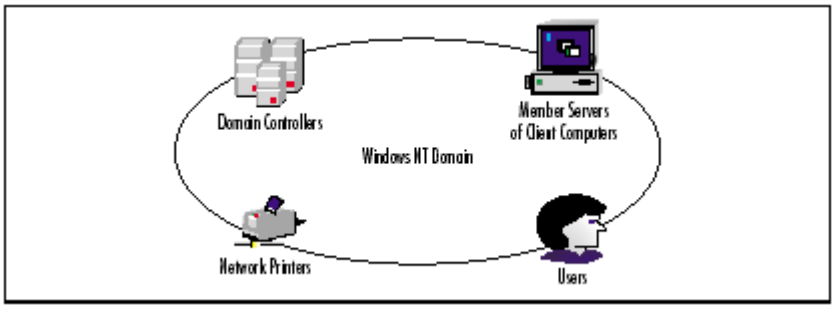
Τα δίκτυα εμφανίστηκαν αρχικά στο στρατό ως μέθοδος διαμοίρασης δεδομένων γρήγορα σε μεγάλες αποστάσεις. Πρόσφεραν ένα σημαντικό πλεονέκτημα σε περιόδους πολέμου. Τα χρήματα ήταν ένας από τους βασικούς λόγους που η δικτύωση επικράτησε στις επιχειρήσεις. Οι σκληροί δίσκοι ήταν εξαιρετικά ακριβοί, όπως ήταν οι εκτυπωτές. Πολλά από τα πρώτα εταιρικά δίκτυα είχαν την ανάγκη να μοιράζονται εκτυπωτές και το πολύτιμο χώρο από τους σκληρούς δίσκους μεταξύ των πολλών υπολογιστών. Σύντομα, οι σκληροί δίσκοι αυτών των servers θα γέμιζαν. Θα τελείωναν οι θύρες των εκτυπωτών. Σε κάποιο χρονικό σημείο, ένας άλλος server θα προστιθόταν στο δίκτυο για να επιτρέψει την περαιτέρω αποθήκευση των κοινών αρχείων ή για την πρόσθεση νέων εκτυπωτών.

Μόλις ένας διαχειριστής εγκαθιστούσε έναν server για να μοιραστεί τα αρχεία και τους εκτυπωτές, ήταν αντιμέτωπος με ένα ζήτημα-πώς να προστατεύσει τα ευαίσθητα αρχεία και τους εκτυπωτές από τους αναρμόδιους χρήστες επιτρέποντας τη

χρήση των υπόλοιπων αρχείων και των εκτυπωτών. Σε μερικές περιπτώσεις, ο διαχειριστής ήθελε να επιτρέψει σε κάποιους χρήστες να έχουν περιορισμένη πρόσβαση σε ένα αρχείο ή έναν εκτυπωτή. Τα δικαιώματα πρόσβασης προστέθηκαν στο σύστημα, και δόθηκαν τους χρήστες συγκεκριμένα στοιχεία σύνδεσης (logon IDs). Ο server θα μπορούσε έπειτα εύκολα να μοιραστεί τα αρχεία και τους εκτυπωτές στους σωστούς χρήστες, ανάλογα με τις ρυθμίσεις του διαχειριστή.

Όταν ένα δίκτυο περιείχε περισσότερους από έναν servers, η διαχείριση έγινε δύσκολη. Εάν ένας χρήστης έπρεπε να έχει πρόσβαση στα αρχεία ή τους εκτυπωτές που βρίσκονταν σε δύο ή περισσότερους servers, εκείνος ο χρήστης έπρεπε να ξέρει πώς να έχει πρόσβαση σε κάθε συγκεκριμένο server. Επιπλέον ο χρήστης χρειαζόταν ξεχωριστό λογαριασμό για κάθε server. Μερικοί διαχειριστές χρησιμοποιούσαν τυποποιημένα ονόματα για να εξασφαλίσουν ότι ένας χρήστης δεν χρειαζόταν να έχει περισσότερους από ένα μοναδικό λογαριασμό. Μερικές φορές, ένα δίκτυο είχε τους πολλούς διαχειριστές με διαφορετικά τυποποιημένα ονόματα, παρέχοντας στους χρήστες δύο ή περισσότερους μοναδικούς λογαριασμούς. Για τους διαχειριστές, ήταν δύσκολο να κρατηθούν οι κωδικοί πρόσβασης συγχρονισμένοι δεδομένου ότι κάθε server είχε έναν διαφορετικό μηχανισμό συγχρονισμού για να επιβάλει τις αλλαγές κωδικού πρόσβασης. Για τους χρήστες, το τελικό αποτέλεσμα σε ένα multiserver περιβάλλον ήταν μια μπερδεμένη και δύσκολη διαδικασία να θυμούνται τη θέση των πόρων, τα σωστά στοιχεία του λογαριασμού του, όλα για να είναι σε θέση να έχει πρόσβαση στους πόρους του δικτύου.

Τα λειτουργικά συστήματα δικτύων σύντομα ανέπτυξαν ποικίλους τρόπους να χρησιμοποιηθεί ένας ενιαίος λογαριασμός για να έχουν οι χρήστες πρόσβαση σε πολλούς servers. Παραδείγματος χάριν, τα WINDOWS 2003 χρησιμοποιούν την αρχιτεκτονική των domain. Ένα domain σε windows 2003 είναι ομάδα από servers που συμμετέχουν σε ένα ενιαίο σύστημα ασφάλειας που περιέχει χρήστες, ομάδες, και πόρους δικτύων. Αποτελείται από διάφορους domain controllers και διάφορους servers μέλη και υπολογιστών χρηστών. Οι servers μέλη και οι υπολογιστές χρηστών έρχονται σε επαφή με τον domain controller (DC) για να έχουν πρόσβαση σους πόρους των δικτύων.



Προκειμένου να αρχίσω να μιλάω για το Active Directory, θα είναι φρόνιμο να καθορίσω πρώτα τον όρο Directory (κατάλογος αρχείων)

1.2 Τι είναι ένα Directory (κατάλογος αρχείων)?

Ένας κατάλογος αρχείων είναι, στο πιο θεμελιώδες επίπεδό του, μια συλλογή πληροφοριών που οργανώνεται με έναν ιδιαίτερο τρόπο. Η οργανωτική μέθοδος κάνει

ταξινόμηση μέσω των πληροφοριών γρήγορα και εύκολα έτσι μπορούμε να βρούμε τα επιθυμητά στοιχεία. Οι υπηρεσίες καταλόγου αρχείων συγκρίνονται συχνά με έναν τηλεφωνικό κατάλογο. Ένας τηλεφωνικός κατάλογος είναι μια συλλογή των στοιχείων που οργανώνεται σύμφωνα με το επίθετο, όνομα, τηλεφωνικός αριθμός, πόλη, και κράτος. Επειδή οι πληροφορίες οργανώνονται με έναν ιδιαίτερο τρόπο, μπορούμε γρήγορα να βρούμε ένα ιδιαίτερο πρόσωπο και να πάρουμε τον αριθμό τηλεφώνου του/της. Οι κατάλογοι αρχείων, φυσικά, δεν είναι τίποτα καινούργιο- έχουν χρησιμοποιηθεί όσο είναι διαθέσιμα τα βιβλία αλλά από την άποψη της δικτύωσης, οι κατάλογοι αρχείων είναι ακόμα στην ακμή της τεχνολογίας των δικτύων.

1.2.1 Τι είναι η υπηρεσία καταλόγου αρχείων (Directory services)?

Το Active Directory δεν είναι η πρώτη υπηρεσία καταλόγου αρχείων για να χτυπήσει την αγορά. Στην πραγματικότητα, οι υπηρεσίες καταλόγου αρχείων υπήρχαν εδώ και κάποιο καιρό. Εντούτοις, η έκδοση των Windows 2000 και το Active Directory από τη Microsoft και η ύπαρξη του NDS από Novell σταθεροποιούν την ιδέα ότι τα δίκτυα θα πρέπει να είναι βασισμένα σε καταλόγους αρχείων. Μόλις πριν λίγα χρόνια, η δικτύωση δεν ήταν τόσο σημαντική όπως είναι σήμερα. Υπήρχαν, φυσικά, μεγάλες επιχειρήσεις με μεγάλους mainframes και πολλά στοιχεία. Αλλά, ήταν μέχρι που το PC πήρε τη λαβή που ο υπολογισμός άρχισε να αλλάζει και τα δίκτυα άρχισαν να αυξάνονται σε ένα ανησυχητικό ποσοστό. Στα περισσότερα σημαντικά δίκτυα σήμερα, κάθε χρήστης έχει έναν υπολογιστή, δημόσια και προσωπικά στοιχεία, και πολλά είδη διαφορετικών αναγκών υπολογισμού. Λόγω των καθαρών αριθμών, τα δίκτυα μπορούν σήμερα εύκολα να βγουν εκτός ελέγχου- πολλοί servers, πολλοί πόροι, πάρα πολλή μαζική σύγχυση. Στην πραγματικότητα, η εύρεση των αναγκαίων πληροφοριών για το δίκτυο μπορεί να είναι ένα σοβαρό ζήτημα χρόνος-απώλειας και μια κοινή καταγγελία μεταξύ των χρηστών. Εισάγουμε τις υπηρεσίες καταλόγου αρχείων. Ο στόχος των υπηρεσιών καταλόγου αρχείων είναι να φέρουν την τάξη και στα μεγάλα και μικρά δίκτυα. Οι υπηρεσίες καταλόγου αρχείων παρέχουν μια βελτιωμένη προσέγγιση στην ανακάλυψη δικτύων και των στοιχείων συμπεριφοράς. Με έναν κατάλογο αρχείων, οι χρήστες μπορούν να πραγματοποιήσουν τις ερωτήσεις αναζήτησης και να βρουν τις πληροφορίες δικτύων γρήγορα και εύκολα. Το Active Directory είναι απάντηση της Microsoft στις ανάγκες υπηρεσιών καταλόγου αρχείων των σημερινών δικτύων.

1.2.2 Τι είναι το Active Directory?

Το Active Directory είναι μια αληθινή υπηρεσία καταλόγου αρχείων δικτύων - παρέχει διάφορες υπηρεσίες σχετικά με την οργανωμένη αποθήκευση των στοιχείων συμπεριφοράς δικτύων και περιλαμβάνει χαρακτηριστικά γνωρίσματα και οφέλη μη διαθέσιμα στις παραδοσιακές υπηρεσίες καταλόγου αρχείων.

Το Active Directory είναι η βάση για τα domains διοικούμενα από domain controllers (επίσης καλείται Active Directory servers) και «τρέχει» Windows 2000 ή/και Windows 2003. Ένα domain είναι μια ομάδα λογικά συνδεμένων υπολογιστών και

χρηστών που δουλεύουν σε αυτούς και ενώνονται από μια ιδέα συγκεντρωμένης διαχείρισης.

1.3 Χαρακτηριστικά του Active Directory

Τα ακόλουθα σημεία δίνουν έμφαση σε μερικά από τα χαρακτηριστικά γνωρίσματα του Active Directory:

- **Οργανική προσέγγιση** – το Active Directory φέρνει την τάξη στο δίκτυό μας με την οργάνωση των πηγών του δικτύου, όπως οι λογαριασμοί χρηστών, λογαριασμοί ομάδας, κοινόχρηστοι φάκελοι, εκτυπωτές, και τα λοιπά. Με το Active Directory, οι χρήστες μπορούν να βρουν γρήγορα τις πληροφορίες που χρειάζονται.
- **ευκολία διαχείρισης** – τα δίκτυα Windows 2000 και 2003 δεν χρησιμοποιούν πλέον τους primary domain controllers (PDCs) και τους backup domain controllers (BDCs). Όλοι οι domain controllers είναι απλά peers, παρέχοντας ένα ενιαίο σημείο διαχείρισης και άριστης ανοχής βλαβών.
- **Αφαιρεί την τοπολογία από τους χρήστες** – το Active Directory βοηθά στα να αφαιρεθεί η γνώση της τοπολογίας δικτύων από τους τελικούς χρήστες. Οι τελικοί χρήστες δεν είναι απαραίτητο να ξέρουν ποιος κεντρικός υπολογιστής κρατά ποιον πόρο και που βρίσκεται στο δίκτυο. Το Active Directory περιέχει τις ισχυρές ικανότητες ερώτησης έτσι οι χρήστες μπορούν να εκτελέσουν πλήρεις αναζητήσεις κειμένων για να βρουν ποιους πόρους χρειάζονται.
- **Μείωση των NT Domains** – Ένας σημαντικός στόχος του Active Directory είναι να καταστούν τα μεγάλα δίκτυα περισσότερο εύχρηστα-και μέρος εκείνου του υψηλού στόχου είναι να μειωθεί ο αριθμός δικτυακών γειτονιών NT Domains. Το Active Directory δεν έχει ένα domain χρήστη/περιορισμό λογαριασμού ομάδας , και εξαιτίας της σχεδίασης του, πολλά δίκτυα που έχουν αυτήν την περίοδο διάφορα υπάρχον NT Domains να χρειαστούν τώρα μόνο ένα Windows 2000 Domain.
- **Η δυνατότητα αύξησης** - δύο λέξεις που μπορούν να ειπωθούν για το Active Directory είναι εξελιξιμότητα και επεκτασιμότητα. Η εξελιξιμότητα σημαίνει ότι μια υπηρεσία μπορεί να αυξηθεί με τις ανάγκες του δικτύου. Το Active Directory είναι ένα εξελικτικό προϊόν επειδή μπορεί να επεκταθεί για να ικανοποιήσει τις ανάγκες του δικτύου. Το Active Directory λειτουργεί σε ένα δίκτυο με μερικές εκατοντάδες υπολογιστών ή σε ένα δίκτυο χιλιάδων υπολογιστών. Επεκτασιμότητα σημαίνει ότι η υπηρεσία μπορεί να διευρυνθεί. Το Active Directory μπορεί να επεκταθεί από την άποψη του namespace του και μέσω των πόρων που περιέχει.
- **Επεκτασιμότητα -** το Active Directory παρέχει τις πολλές κλάσεις αντικειμένου και εκατοντάδες ιδιότητες. Κάθε κλάση, όπως ο υπολογιστής, χρήστης, ή εκτυπωτής, αντιπροσωπεύει ένα αντικείμενο στοιχείων. Η κλάση προσδιορίζει επίσης ποιες ιδιότητες είναι διαθέσιμες στα αντικείμενα εκείνης της κλάσης. Οι υπεύθυνοι για την ανάπτυξη μπορούν να προσθέσουν τις

κλάσεις αντικειμένου τους και να προσθέσουν ακόμη και τις νέες ιδιότητες στις υπάρχουσες κλάσεις.

- **Τυποποίηση** - το Active Directory στηρίζεται εντελώς στα πρότυπα δικτύωσης και πρωτοκόλλου που υπάρχουν αυτήν την περίοδο και χρησιμοποιούνται ευρέως. Με άλλα λόγια, δεν υπάρχει κανένα συνολικά νέο πρότυπο που πρέπει να κυριαρχηθεί το Active Directory στηρίζεται σε ένα TCP/ IP Δίκτυο, που είναι το πρωτόκολλο δικτύωσης της επιλογής αυτές τις μέρες, και είναι εντελώς ενσωματωμένο με στο Domain Name System (DNS) και το Lightweight Directory Access Protocol (LDAP).
- **Διαλειτουργικότητα (Interoperability)** - Η χρήση του LDAP ως πρωτόκολλο πρόσβασης καταλόγου αρχείων εξασφαλίζει ότι ένα ευρύ φάσμα των χρηστών μπορεί να χρησιμοποιήσει τις πληροφορίες που καταχωρούνται στον κατάλογο αρχείων. Οι ενεργές διαπροσωπείες υπηρεσιών καταλόγου αρχείων (Active Directory Service Interfaces ADSI) χρησιμοποιούν το LDAP για να πάρουν τις πληροφορίες σε και από τον κατάλογο αρχείων. Το ADSI είναι βασισμένο στο μοντέλο συστατικού αντικειμένου (Component Object Model COM) και επιτρέπει το scripting.
- **Έλεγχος δικτύου** - το Active Directory προσφέρει ένα πολύ καλό επίπεδο διαχείρισης δικτύων, και από την άποψη της διαχείρισης κεντρικών υπολογιστών και της διαχείρισης υπολογιστών γραφείου. Μέσω του Group Policy των Windows 2000 και 2003, μπορούμε να διαχειριστούμε τις ρυθμίσεις υπολογιστών γραφείου χρηστών δικτύων ευκολότερα και αποτελεσματικά.
- **Ασφάλεια** - Μέσω του Active Directory, μπορούμε να ελέγξουμε την ασφάλεια των πόρων και ακόμη και τις διοικητικές στοιχειώδεις εργασίες σε άλλους ανθρώπους μέσω της αντιπροσωπείας του ελέγχου. (Delegation of Control). Κάθε αντικείμενο μέσα στο Active Directory μπορεί να ασφαλιστεί χωριστά για να ελέγξει την πρόσβαση. Τα αντικείμενα καταλόγου αρχείων μπορούν να έχουν πολλαπλάσια επίπεδα ασφάλειας, επιτρέποντας σε ορισμένους χρήστες τη δυνατότητα να ενημερώσουν κάποιες πληροφορίες, αλλά όχι όλα. Η ασφάλεια στο Active Directory είναι στενά ενσωματωμένη με στο πρότυπο της γενικής ασφάλειας στα Windows 2000, το οποίο χρησιμοποιεί το πρωτόκολλο πιστοποίησης Kerberos v5.
- **Ενοποίηση (Integration)** το Active Directory είναι ενσωματωμένο στην ίδια την ουσία των Windows 2003. Τα εργαλεία διαχείρισης ενός server εξαρτώνται από το Active Directory, και οι τελικοί χρήστες θα παρατηρήσουν ότι όλες οι εφαρμογές που χρησιμοποιούν τα κοινά στοιχεία αλληλεπίδρασης με τον χρήστη βασισμένα στο λειτουργικό σύστημα περιέχουν τις αναφορές για την πρόσβαση και τη χρησιμοποίηση των πληροφοριών από το Active Directory.
- **Ευκολότερη διαχείριση WAN** - μόλις στήσουμε το Active Directory σωστά, αυτό διαχειρίζεται την τοπολογία του replication του. Το Active Directory περιλαμβάνει περισσότερες εσωτερικές υπηρεσίες που το βοηθούν να διαχειριστεί και να ελέγξει τις διαδικασίες του, συμπεριλαμβάνοντας του replication. Αυτό το χαρακτηριστικό γνώρισμα κρατά τους διαχειριστές έξω από τέτοιες λεπτομέρειες και επιτρέπει στο λογισμικό να φροντιστεί και να

κάνει replicate τα στοιχεία μεταξύ των domain controllers και των sites όπως απαιτούνται.

- **Replication -** οι πληροφορίες που περιλαμβάνονται στο Active Directory γίνονται replicate σε όλους τους domain controllers μέσα στην οργάνωση. Κάθε domain μπορεί να έχει πολλαπλάσιους DCs για την ανοχή βλαβών και την εξισορρόπηση φορτίου

Η Microsoft κατευθύνεται σαφώς στη σωστή κατεύθυνση με το Active Directory. Η επεκτασιμότητα, η ασφάλεια, και τα χαρακτηριστικά γνωρίσματα ενοποίησης είναι αρκετά να επιτρέψουν μια προσεκτική εξέταση των δυνατοτήτων στους υπεύθυνους για την ανάπτυξη και τους διαχειριστές δικτύων.

1.4 Λογική οργάνωση

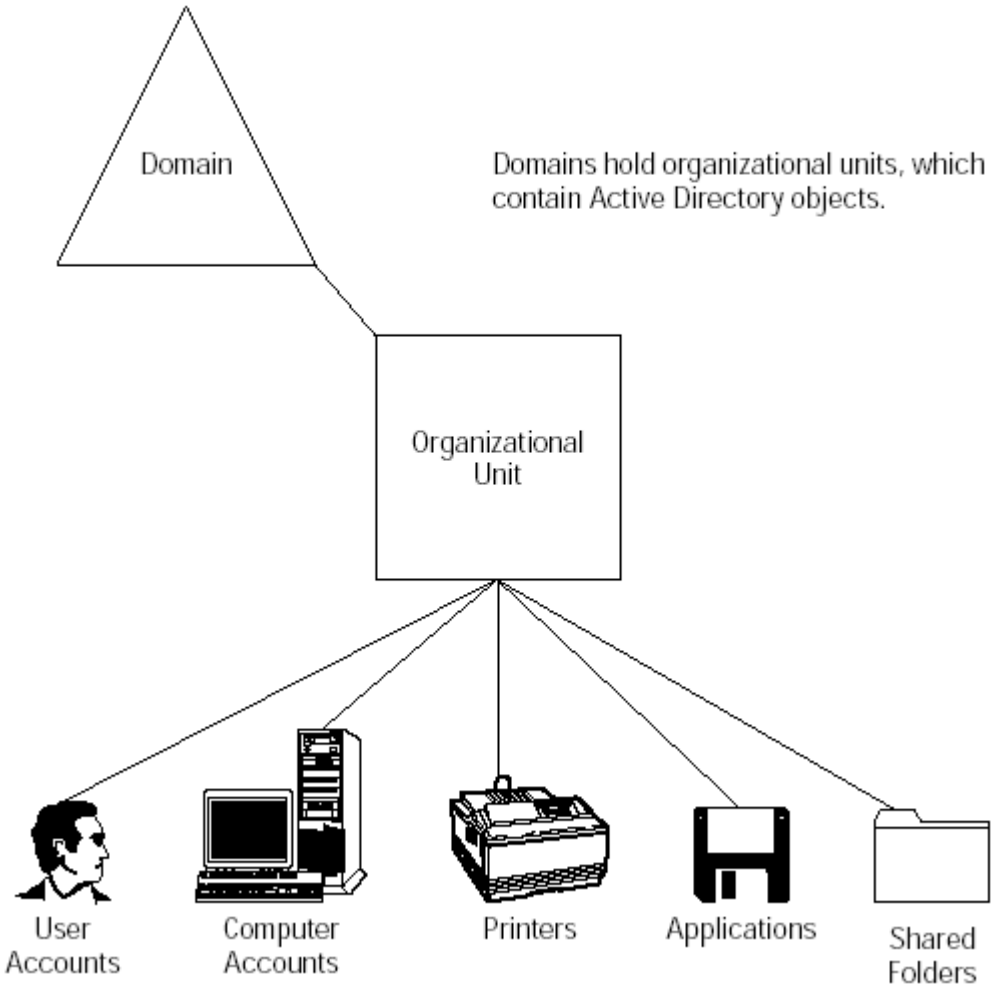
Για να αρχίσει την εξερεύνηση του Active Directory, θέλω να ρίξω μια ματιά στη λογική δομή του. Προκειμένου να σχεδιάσουμε αποτελεσματικά, να εφαρμόσουμε, και να διαχειριστούμε το Active Directory, αυτή η λογική δομή θα πρέπει να γίνει δεύτερη φύση.

Όλες οι στοιχειώδεις εργασίες "οικοκυρικής" εκτελούνται στους domain controllers που κρατούν την βάση δεδομένων του Active Directory που περιέχει τις πληροφορίες για τα διοικούμενα αντικείμενα όπως οι χρήστες, υπολογιστές, ομάδες, και τα λοιπά. Αυτές οι πληροφορίες καταχωρούνται ως αντικείμενα καταλόγου αρχείων των αντίστοιχων τύπων. Χρήστης, ομάδα, και υπολογιστής (και InetOrgPerson - στα Windows.NET) τα αντικείμενα (αποκαλούμενοι λογαριασμοί) αντιπροσωπεύουν τις αρχές ασφάλειας που μπορούν να χορηγηθούν τα προνόμια για να εκτελέσουν συγκεκριμένες υπολογιστικές - domain, ή forest – wide στοιχειώδεις εργασίες ή δικαιοδοσίες για την πρόσβαση στους κοινούς πόρους δικτύων (όπως τα αρχεία, φάκελοι, και εκτυπωτές). Κατά συνέπεια, ένας χρήστης κάποιου domain που συνδέεται στο domain μόλις χρησιμοποιήσει έναν λογαριασμό μπορεί να έχει πρόσβαση σε όλους τους επιτρεπτούς πόρους χωρίς να πρέπει να πρέπει να κάνει log in κάθε φορά σε ξεχωριστό server που έχει κάποιον πόρο του δικτύου. Ένας διαχειριστής domain μπορεί να αλλάξει τα αντικείμενα του Active Directory σε οποιοδήποτε domain controller και, κατά συνέπεια, να ελέγξει όλες τις προαιρετικές δυνατότητες που επιτρέπονται στα μέλη του domain. Επομένως, ένα domain είναι ένα όριο διαχειριστικής ισχύος.

Εν ολίγοις, για να αναπτυχθεί ένα Active Directory domain, πρέπει πρώτα να σχεδιαστεί, εγκαθιστούμε τον domain controller(s), προσθέτουμε τους υπολογιστές χρηστών του domain, και δημιουργούμε τους λογαριασμούς χρηστών (και ομάδας). Κατόπιν μπορούμε να μοιραστούμε τους πόρους στα μέλη του domain και να αναθέσούμε τα απαραίτητα προνόμια και τις δικαιοδοσίες στους χρήστες (και στις ομάδες)

Ένα Active Directory domain μπορεί να περιέχει τα σύνολα αντικειμένων καταλόγου αρχείων που καλούνται οργανωτικές μονάδες (organizational units OU), και αυτό περιέχει συνήθως τους λογαριασμούς χρηστών ή υπολογιστών. Κάθε OU μπορεί να έχει τον δικό του διαχειριστή και ένα Group Policy Object (GPO)(s) με το αντικείμενο OU. Η τεχνολογία πολιτικής ομάδας προορίζεται για τη συγκεντρωτική ρύθμιση του

περιβάλλοντος χρηστών και ρυθμίσεις υπολογιστικών συστημάτων . Τα GPOs μπορούν να συνδεθούν τοπικά ή με ένα site, domain, ή αντικείμενα OU.



Σχήμα 1.1

Τα Active Directory domains διαμορφώνουν ένα δάσος (ένα δάσος μπορεί να περιλάβει ένα ή περισσότερα domains), όπου όλα τα domains συνδέονται από διπλής κατεύθυνσης, μεταβατικά trusts. Τα trusts επιτρέπουν στους χρήστες που συνδέονται σε ένα domain για να έχουν πρόσβαση στους πόρους που βρίσκονται σε οποιαδήποτε θέση στο δάσος, ή για να έχει τα προνόμια σε οποιοδήποτε domain. Ο διαχειριστής – δημιουργημένα trusts μπορεί να καθιερωθεί με ξένα Active Directory δάση ή domains των WINDOWS NT 4.0

Όσοι έχουν εργαστεί σε ένα πολλαπλάσιο δίκτυο domain NT, ξέρουν μερικά πράγματα για τις σχέσεις εμπιστοσύνης. Οι σχέσεις εμπιστοσύνης επιτρέπουν σε έναν χρήστη στο Domain A για να έχει πρόσβαση στους πόρους στο Domain B. Οι σχέσεις εμπιστοσύνης πρέπει να καθιερωθούν για να επιτρέψουν την απομακρυσμένη πρόσβαση των πόρων των domains, και στα WINDOWS NT, έπρεπε να ρυθμίσουμε κάθε πλευρά του trust –καθορίζοντας ποιος εμπιστεύθηκε και ποιος εμπιστευόταν. Στα σύνθετα

περιβάλλοντα, η σχέση εμπιστοσύνης έγινε πολύ σύνθετη και δύσκολο να διαμορφωθεί και να διαχειριστεί. Πέστε αντίο στη σύνθετη εμπιστοσύνη τις σχέσεις στα Windows 2003. Στα Windows 2003 περιβάλλοντα που χρειάζονται περισσότερα από ένα domain ,οι αυτόματες μεταβατικές εμπιστοσύνες Kerberos καθιερώνονται όταν δημιουργούμε τα νέα domainsστο δασικό δέντρο. Το Kerberos είναι το πρωτόκολλο ασφάλειας στα Windows 2000 και 2003, που αντικαθιστά το NTLM στα WINDOWS NT. Το Kerberos παρέχει την ανώτερη τεχνολογία ασφάλειας και πολλά νέα χαρακτηριστικά γνωρίσματα ασφάλειας, όπως τις μεταβατικές σχέσεις εμπιστοσύνης. Μια μεταβατική εμπιστοσύνη απλά σημαίνει ότι εάν το Domain A εμπιστεύεται το Domain B, και το Domain Γ εμπιστεύεται το Domain B, κατόπιν το Domain A εμπιστεύεται αυτόματα το Domain Γ. Οι μεταβατικές σχέσεις εμπιστοσύνης ρυθμίζονται αυτόματα με όλα τα άλλα το domains και domain trees μέσα στο δάσος. Το δάσος χρησιμεύει ως το όριό μας, και όλα τα domains εμπιστεύονται αυτόματα το ένα το άλλο – από εμάς δεν απαιτείται καμία ρύθμιση!

1.5 Φυσική οργάνωση

Ολόκληρη η βάση δεδομένων του Active Directory διαιρείται λογικά σε χωρίσματα (partitions) καταλόγου αρχείων, τα οποία είναι μονάδες του replication (π.χ., κάθε χώρισμα γίνεται replicated ανεξάρτητα, αν και οι μηχανισμοί του replication, όπως το scheduled replication ή η διαδικασία ανακοίνωσης, μπορεί να έχει επιπτώσεις σε όλα τα χωρίσματα). Δεδομένου ότι Active Directory είναι μια διανεμημένη βάση δεδομένων δικτύων, οποιοσδήποτε domain controller κρατά ένα αντίγραφο ολόκληρης της βάσης δεδομένων.

Κάθε αντίγραφο μετρά τουλάχιστον τρία χωρίσματα: το Schema και Configuration που μοιράζονται από όλα τα domains σε ένα δάσος και καταχωρούνται σε κάθε domain controller και ένα domain partition που περιέχει τα αντικείμενα ενός συγκεκριμένου domain και καταχωρείται στους domain controllers που ανήκουν σε εκείνο το domain. Κάθε δάσος έχει ένα παραπάνω χώρισμα, τον Global Catalog (GC), ο όποιος περιέχει ένα περιορισμένο σύνολο ιδιοτήτων όλων των αντικειμένων του Active Directory. Το GC επιτρέπει στους χρήστες να βρουν γρήγορα οποιοδήποτε αντικείμενο καταλόγου αρχείων στο δάσος. Το GC είναι ένα μέρος της βάσης δεδομένων του Active Directory και μπορεί να καταχωρηθεί σε οποιοδήποτε domain controller.

Το Active Directory μπορεί να λάβει υπόψη το γεγονός ότι ένα μεγάλο επιχειρηματικό δίκτυο (ένα δάσος) συνήθως περιέχει διάφορα υποδίκτυα που συνδέονται από γρήγορα και αργά κανάλια. Ένα σύνολο υποδικτύων που συνδέονται με τα γρήγορα κανάλια μπορεί να αναφερθεί ως site. Τα sites, στη συνέχεια, συνδέονται με τα αργά κανάλια (dial-up). Εξ ορισμού, όλα τα domains τοποθετούνται στο ίδιο Default-First-Site (που μπορεί να μετονομαστεί ακίνδυνα).

Οι απαιτήσεις χωρισμάτων καταλόγου αρχείων καθώς επίσης και η υποδομή του/ων site θα καθορίσουν την τοπολογία του replication που, εξ ορισμού, παράγεται αυτόματα από την υπηρεσία Knowledge Consistency Checker (KCC) που τρέχει σε κάθε domain controller. Αυτή η υπηρεσία διαχειρίζεται τις συνδέσεις replication μεταξύ των domain controllers ανάλογα με τις οποίες τα χωρίσματα καταλόγου αρχείων αυτοί

αποθηκεύουν. Το Replication εκτελείται σύμφωνα με τους κανόνες, διαστήματα, και προγράμματα που καθορίζονται για inter- και intra-site replication τύπους.

1.6 DNS και LDAP

Ανέφερα νωρίτερα ότι το Active Directory είναι πλήρως συμβατό με το Domain Name System (DNS) και το Lightweight Directory Access Protocol (LDAP). Ο DNS είναι μια μέθοδος επίλυσης ονομάτων που επιλύει τα host names σε διευθύνσεις IP. Ο DNS χρησιμοποιείται στα TCP/IP δίκτυα και είναι το σύστημα επίλυσης ονομάτων που χρησιμοποιείται το σε ολόκληρο διαδίκτυο. Ο DNS επιτρέπει ένα host name όπως το www.Microsoft.com να επιλυθεί σε ένα TCP/IP διεύθυνση όπως 131.107.2.200. Οι υπολογιστές επικοινωνούν χρησιμοποιώντας μια διεύθυνση IP. Είναι δύσκολο για τους ανθρώπους να θυμηθούν IP διευθύνσεις επειδή είμαστε πλάσματα βασισμένα στη γλώσσα. Ο DNS μας επιτρέπει να δώσουμε φιλικά, γλωσσικά ονόματα, όπως Microsoft.com, στους hosts αντί να πρέπει να αναφερθεί η αριθμητική του διεύθυνση IP. Η δουλειά του DNS είναι να επιλύσει και τα δύο. Όταν ένας χρήστης κάνει αίτηση στο site www.Microsoft.com, ο DNS χρησιμοποιεί διάφορους name servers για να βρει την πραγματική IP διεύθυνση της Microsoft.com. Μόλις βρεθεί, η διεύθυνση IP επιστρέφει στο χρήστη έτσι ο χρήστης μπορεί να χρησιμοποιήσει τη διεύθυνση IP για να έρθει σε επαφή με τη Microsoft.com. Όλο αυτό είναι αόρατο στους χρήστες και πολύ γρήγορο.

Έτσι, τι από όλα αυτά έχουν να κάνουν με το Active Directory; Ο DNS είναι ένα namespace, που σημαίνει ότι είναι μια περιοχή που μπορεί να επιλυθεί. Ένας τηλεφωνικός κατάλογος είναι ένα namespace επειδή περιέχει ορισμένα στοιχεία που επιλύονται (όνομα στον τηλεφωνικό αριθμό) με έναν ορισμένο τρόπο. Ονόματα Διαδικτύου, όπως η Microsoft.com, yahoo.com, amazon.com, και ούτω καθ'εξής, όλοι ακολουθούν αυτό το naming scheme προκειμένου να επιλυθούν. το Active Directory έχει χτιστεί πάνω στον DNS - στην ουσία, τα ονόματα του Active Directory είναι DNS ονόματα. Στις προηγούμενες εκδόσεις των Windows, Το NetBIOS χρησιμοποιήθηκε για να παρέχει φιλικά ονόματα στους υπολογιστές, και η Windows Internet Name Service (WINS) χρησιμοποιήθηκε για την υπηρεσία εντοπιστών (locator service). Στα καθαρά Windows 2000 δίκτυα, ο DNS χρησιμοποιείται τώρα για την υπηρεσία εντοπιστών.

Είναι σημαντικό να αναφέρουμε ότι η ονοματολογία του Active Directory δεν είναι αυτή του DNS. Η ονοματολογία του DNS χρησιμοποιείται στο internet ενώ αυτή του Active Directory χρησιμοποιείται σε ιδιωτικά δίκτυα. Όμως η ονοματολογία του Active Directory βασίζεται στον DNS και συνδέεται σε αυτήν. Με άλλα λόγια ο DNS είναι ένας γενικός χώρος διευθύνσεων που φτιάχνει ολόκληρο το internet και η ονοματολογία του Active Directory είναι χτισμένη πάνω στην ιεραρχική δομή του DNS έτσι ώστε να συνδέεται στην γενική ονοματολογία του. Συνοπτικά, δεν μπορούμε να υλοποιήσουμε ένα Active Directory χωρίς DNS και όλα τα ονόματα του Active Directory είναι ονόματα του DNS.

Το Active Directory είναι επίσης συμβατό με την υπηρεσία καταλόγου LDAP. Για να καταλάβουμε γιατί αυτό είναι σημαντικό πρέπει πρώτα να κατανοήσουμε μερικά πράγματα σχετικά με το LDAP. Το LDAP είναι βασισμένο στο Directory Access Protocol (DAP) που ήταν μια υλοποίηση των δικτύων X.500. Το X.500 είναι μια αρκετά

ευρεία υπηρεσία καταλόγου που είναι χτισμένη σε ιεραρχική δομή αρκετά ίδια με αυτή του DNS. Οι κατάλογοι του X.500 είναι ερευνήσιμοι και το DAP χρησιμοποιείται στα δίκτυα X.500 για να κάνει ερωτήματα στη βάση με σκοπό να εντοπίσει διάφορες πληροφορίες καταλόγου. Το πρόβλημα με το DAP είναι ότι μεγάλο μέρος του βάρους της διεργασίας πηγαίνει στον υπολογιστή του χρήστη και έτσι απέκτησε την φήμη για την μεγάλη του κίνηση. Το LDAP αναπτύχθηκε από το DAP (RFC 1777) αλλά δεν κληρονόμησε το μεγάλο βάρος του DAP και δεν χρειάζεται την υλοποίηση των X.500 δικτύων. Το LDAP διατηρεί την λειτουργικότητα του DAP χωρίς το βάρος του X.500.

Από τότε που αναπτύχθηκε το LDAP έχει γίνει ένα standard του Internet. Το χρησιμοποιούμε σε μηχανές αναζήτησης και newsgroups. Δουλεύει θαυμάσια και χρησιμοποιείται στο Active Directory για ερωτήματα χρηστών. Όλη η πρόσβαση στα αντικείμενα του Active Directory γίνεται μέσω του LDAP και χρησιμοποιείται όταν οι διαχειριστές μετατρέπουν κάποιο αντικείμενο του Active Directory.

Για να παρέχονται οι ισχυρές δυνατότητες ερώτησης που κάνουν το LDAP τόσο διάσημο, αυτό ορίζει στα αντικείμενα του Active Directory διάφορα ονόματα. Αυτά τα διαφορετικά ονόματα παρέχουν πληροφορίες σχετικά με το αντικείμενο που μπορεί να χρησιμοποιηθεί για ταίριασμα ερωτημάτων.

Πρώτα το LDAP δίνει στα αντικείμενα ένα distinguished name (DN) και ένα relative distinguished name (RDN). Το DN δείχνει την διαδρομή προς το αντικείμενο ή το που βρίσκεται μέσα στο Active Directory. Το Active Directory ιεραρχικά ξεκινάει από το domain level, και μετά πάει στο OU, και τελικώς στο επίπεδο του αντικειμένου. Το DN δείχνει ολόκληρη την διαδρομή. Το RDN παρέχει το όνομα του αντικειμένου. Π.χ. Cn=vpsarras, ou=epirgreece, dc=teiep dc=gr

Εδώ βλέπουμε το DN και το RDN ενός λογαριασμού. Το RDN είναι vpsarras το όνομα για το λογαριασμό κάποιου χρήστη. Το DN παρέχει ολόκληρη την διαδρομή στο λογαριασμό αυτό, που βρίσκεται σε ένα OU που λέγεται epirgreece που με την σειρά του βρίσκεται στο domain teiep.gr. Το RDN πάντα εμφανίζεται πρώτο ακολουθούμενο από το DN.

Συνεχίζοντας για το DN και το RDN, το LDAP επίσης χρησιμοποιεί το user principal name (UPN) για τον εντοπισμό αντικειμένων. Το UPN είναι ένα φιλικό όνομα ορισμένο σε ένα αντικείμενο που έχει την μορφή objectname@domainname. Για παράδειγμα ένας λογαριασμός ενός χρήστη που είναι vpsarras στο domain teiep.gr εμφανίζεται σαν vpsarras@teiep.gr. Για το LDAP αυτό είναι ένα τοπικό όνομα σε ένα τοπικό δίκτυο. Το UPN χρησιμοποιείται και από το LDAP για να κάνει το windows logon Πιο εύκολο. Οι διαχειριστές μπορούν να παράγουν UPN προθέματα για να κάνουν το logon πιο εύκολο.

1.7 Windows 2003 domain controllers

Οι domain controllers στα windows 2003 λειτουργούν ως peers. Αυτό σημαίνει ότι δεν υπάρχει Primary Domain Controller. Όλοι οι domain controllers είναι απλά domain controllers και είναι όλοι ισοδύναμοι. Επειδή μπορούμε να χρησιμοποιήσουμε οποιοδήποτε domain controller για να κάνουμε αλλαγές στο Active Directory και η ανεκτικότητα λαθών είναι ενσωματωμένη, αυτό μας δίνει ένα εξαιρετικό χαρακτηριστικό διαχείρισης. Εάν πέσει ένας domain controller δεν υπάρχει πρόβλημα, οι άλλοι domain

controllers λειτουργούν κανονικά και η κίνηση στο δίκτυο λειτουργεί όπως συνήθως. Στα δίκτυα με Windows 2003 όλοι οι domain controllers κρατούν ένα εγγράψιμο αντίγραφο της βάσης.

Αν και οι domain controllers είναι peers μερικοί από αυτούς έχουν συγκεκριμένους ρόλους. Αυτοί οι συγκεκριμένοι ρόλοι υπάρχουν γιατί αν λειτουργούν σε όλους τους domain controllers ταυτόχρονα δεν δουλεύουν καλά. Παρακάτω παρατίθενται αυτοί οι συγκεκριμένοι ρόλοι.

1.8 Global catalog servers

Μερικοί domain controllers είναι global catalog servers. Αναλόγως με το configuration του δικτύου μπορούμε να έχουμε διάφορους global catalog servers. Οι global catalog servers εκτελούν δύο βασικές λειτουργίες.

1. Έχουν ένα πλήρες αντίγραφο όλων των αντικειμένων του Active Directory στο domain τους και μερικό αντίγραφο όλων των αντικειμένων του Active Directory σε άλλα domains στο δάσος.
2. Χρειάζονται για τις συνδέσεις χρηστών. Οι global catalog servers είναι απαραίτητοι για τις συνδέσεις χρηστών εάν το domain τρέχει σε native mode -όχι mixed mode- επειδή τα universal groups υποστηρίζονται μόνο σε native mode

Όταν εγκαθιστούμε για πρώτη φορά το Active Directory ο πρώτος domain controller γίνεται global catalog server για το domain. Μπορούμε να αλλάξουμε αυτό το ρόλο σε κάποιον άλλο server εφόσον χρειαστεί.

1.9 Multimaster roles

Εκτός του global catalog server μερικοί domain controllers έχουν και τον ρόλο του FSMO (Flexible Single Master Role). Για να γίνει κατανοητός ο ρόλος αυτός πρέπει πρώτα να αναφερθούν μερικά πράγματα για το replication των Windows 2003. Replication ονομάζεται η διαδικασία που στέλνει πληροφορίες ανανέωσης σε άλλους domain controllers. Τα windows 2003 χρησιμοποιούν multimaster replication. Όπως με την απουσία ενός PDC δεν υπάρχει single master replicator. Αυτό σημαίνει ότι αλλαγές στη βάση μπορούν να γίνουν από οποιοδήποτε domain controller που επομένως είναι υπεύθυνος για την ενημέρωση όλων των domain controllers για τις αλλαγές στη βάση.

Το multimaster replication δουλεύει υπέροχα, αλλά για μερικές αλλαγές στη βάση η διαδικασία δεν δουλεύει καλά. Για να λυθεί το πρόβλημα συγκεκριμένοι domain controllers κρατούν τον ρόλο του FSMO. Αυτό σημαίνει ότι μόνο αυτοί οι domain controllers δέχονται συγκεκριμένους τύπους αλλαγών στη βάση και εκτελούν συγκεκριμένες λειτουργίες. Υπάρχουν πέντε (5) διαφορετικοί ρόλοι FSMO που καλύπτουν τις εξαιρέσεις του replication και τη διαδικασία χειρισμού εξαιρέσεων του multimaster replication.

1.10 Ρόλοι FSMO

Ρόλος FSMO	Επεξήγηση
Schema master	Ο ρόλος του schema master ανήκει σε έναν μόνο domain controller σε ολόκληρο το δάσος. Το schema είναι απλά ένα διάγραμμα των αντικειμένων του active directory και των ιδιοτήτων του. Το schema καθορίζει τι είδους αντικείμενα μπορούν να αποθηκευτούν στον κατάλογο και τι ιδιότητες ορίζουν αυτά τα αντικείμενα. Όποιες αλλαγές γίνουν στο schema πρέπει να γίνουν από τον domain controller που έχει τον ρόλο του schema master
Domain naming master	Ο ρόλος του domain naming master ανήκει σε έναν domain controller στο δάσος. Ο domain naming master ελέγχει την πρόσθεση και αφαίρεση διαφόρων domains στο δάσος.
Relative ID (RID) master	Ο RID Master χειρίζεται την διανομή αριθμών RID σε άλλους domain controllers και βεβαιώνει ότι δύο domain controllers δεν θα έχουν τους ίδιους ή υπέρθετους αριθμούς RID. Κάθε domain στο δάσος έχει έναν RID master
PDC emulator	Ο PDC emulator υπάρχει σε έναν domain controller σε κάθε domain για να ενεργεί σαν Windows NT PDC
Infrastructure master	Ο ρόλος του Infrastructure master ο οποίος κρατείται σε έναν domain controller σε κάθε domain, ανανεώνει τα μέλη μιας ομάδας όπου είναι απαραίτητο.

1.11 SCHEMA

Το σχήμα είναι απλά ένα πλαίσιο ορισμών που καθιερώνει τον τύπο διαθέσιμων αντικειμένων στο active directory. Αυτοί οι ορισμοί διαιρούνται σε κλάσεις αντικειμένου, και οι πληροφορίες που περιγράφουν το αντικείμενο είναι γνωστές ως οι ιδιότητές του. Υπάρχουν δύο τύποι ιδιοτήτων: εκείνοι που πρέπει να υπάρχουν και εκείνοι που μπορούν να υπάρχουν. Παραδείγματος χάριν, το σχήμα καθορίζει μια κλάση αντικειμένου χρηστών όπως έχοντας το όνομα του χρήστη ως απαραίτητη ιδιότητα η φυσική θέση του χρήστη ή η περιγραφή εργασίας είναι προαιρετική. Οι ιδιότητες

χρησιμοποιούνται για να διακρίνουν περαιτέρω ένα αντικείμενο από ένα άλλο. Περιλαμβάνουν το όνομα αντικειμένου, το προσδιοριστικό του αντικειμένου (OID), σύνταξη, και προαιρετικές πληροφορίες.

Το σχήμα καταχωρείται στο αρχείο βάσεων δεδομένων Ntds.dit του Active Directory. Οι ορισμοί αντικειμένου καταχωρούνται ως μεμονωμένα αντικείμενα, έτσι ο κατάλογος αρχείων μπορεί να μεταχειριστεί τους ορισμούς σχημάτων με τον ίδιο τρόπο που μεταχειρίζεται άλλα αντικείμενα. Το προκαθορισμένο σχήμα δημιουργείται με την πρώτη εγκατάσταση του Active Directory. Περιέχει κοινά αντικείμενα και ιδιότητες για τέτοια αντικείμενα όπως τους χρήστες, ομάδες, υπολογιστές, εκτυπωτές, και συσκευές δικτύων. Επίσης καθιερώνει τη προκαθορισμένη δομή του Active Directory που χρησιμοποιείται εσωτερικά.

Επειδή το σχήμα είναι ένα επεκτάσιμο συστατικό, οι νέες κλάσεις αντικειμένου μπορούν να προστεθούν δυναμικά στο παρόν σχήμα και οι παλαιές κλάσεις αντικειμένου μπορούν να τροποποιηθούν. Δεν ήταν δυνατό να τροποποιηθούν ή να απενεργοποιηθούν οι κλάσεις συστημάτων και οι ιδιότητες κάτω από τα Windows 2000, αλλά είναι τώρα δυνατό με τα Windows Server 2003

Τα στοιχεία σχημάτων δεν πρέπει να συγχέονται με τα στοιχεία διαμόρφωσης, τα οποία παρέχουν τις δομικές πληροφορίες για το Active Directory. Το σχήμα παρέχει πληροφορίες για το ποια αντικείμενα και ιδιότητες είναι διαθέσιμα στον κατάλογο αρχείων. Οι πληροφορίες διαμόρφωσης διατηρούν τη δομή καταλόγου αρχείων που αντιπροσωπεύει τη σχέση μεταξύ των πραγματικών αντικειμένων και προσδιορίζει πώς να κάνει replicate αυτήν την δομή μεταξύ των domain controllers.

Το σχήμα είναι προσιτό μόνο στις ομάδες χρηστών Enterprise Administrators και Schema Admins εξ ορισμού. Ρυθμίζεται μέσω του εργαλείου Active Directory Schema. (Το Active Directory Schema snap-in διατίθεται μόνο αφού εγκαθίσταται η εφαρμογή adminpak από το CD των Windows Server 2003 μέσα στο φάκελο I386.) Τα στοιχεία σχημάτων του Active Directory είναι δυναμικά και διαθέσιμα στις εφαρμογές μετά από το αρχικό ξεκίνημα του συστήματος. Ιδιότητες και κλάσεις μπορούν να προστεθούν στο σχήμα για να παρέχουν τη δυναμική επεκτασιμότητα στο Active Directory.
Η χρησιμοποίηση του Schema Active Directory Service Interface (SADS) είναι μια άλλη μέθοδος για να διευκολύνει την περιοδεία και να επεκταθεί των λειτουργιών και τις σχέσεις ενός αντικειμένου ή μιας ιδιότητας σχημάτων.

Το κοντέϊνερ αντικειμένου σχημάτων συνδέει τους ορισμούς με το δέντρο καταλόγου αρχείων. Αντιπροσωπεύεται χαρακτηριστικά ως παιδί της ρίζας καταλόγου αρχείων. Στη συνέχεια, κάθε περίπτωση έχει ένα μοναδικό μεμονωμένο σχήμα.
Ο κύριος domain controller διαδικασιών σχημάτων διαχειρίζεται τη δομή και το περιεχόμενο του σχήματος. Κάνει replicate τις πληροφορίες σχημάτων στους domain controllers στο δάσος. Κάθε domain controller φορτώνει ένα αντίγραφο του σχήματος σε μια RAM-based cache, εξασφαλίζοντας άμεση πρόσβαση στους παρόντες ορισμούς αντικειμένου και ιδιοτήτων. Εάν αλλαγές εμφανίζονται στο σχήμα, η cache ανανεώνεται.

1.12 ΝΕΑ ΧΑΡΑΚΤΗΣΤΙΣΤΙΚΑ ΤΟΥ ACTIVE DIRECTORY ΣΕ WINDOWS 2003

Σε αυτό το κομμάτι θα αναφερθούν τα πιο σημαντικά και ενημερωμένα χαρακτηριστικά του active directory που είναι διαθέσιμα στους domain controllers της οικογένειας windows 2003 server και δίνουν την δυνατότητα στους admins να τα διαχειριστούν πιο αποτελεσματικά.

1.12.1 DOMAIN MODES ΚΑΙ ΛΕΙΤΟΥΡΓΙΚΑ ΕΠΙΠΕΔΑ (FUNCTIONAL LEVELS)

Ας δούμε πρώτα κάποιες γενικές λειτουργίες για τα domains και το δάσος, που μέχρι κάποιο σημείο είναι ίδια για τα windows 2000 όπως και για τα windows 2003. Τα domains σε windows 2000 είτε σε προκαθορισμένο mixed mode (όταν ένα domain περιέχει Windows NT BDC) ή σε native mode (όταν ένα domain περιέχει μόνο Windows 2000 – based domain controller)

Όταν η κατάσταση ενός domain αλλάζει σε native πρέπει να ληφθούν υπόψιν οι παρακάτω παράγοντες.

- Οι domain controllers δεν υποστηρίζουν πλέον NTLM replication. Σαν αποτέλεσμα ο PDC Emulator του domain δεν μπορεί να κάνει replicate δεδομένα σε κάποιον BDC κάτω από Windows NT, και δεν μπορούν να προστεθούν domain controllers βασισμένοι σε windows NT.
- Οι domain controllers παρέχουν pass-through πιστοποίηση που επιτρέπει στους χρήστες και domain controllers που χρησιμοποιούν παλαιότερες εκδόσεις από windows 2000 να πιστοποιηθούν σε οποιοδήποτε domain στο δάσος (παρόλο που αυτά τα συστήματα δεν υποστηρίζουν το πρωτόκολλο Kerberos v5). Όμως μπορούν να χρησιμοποιήσουν μεταβατικές σχέσεις εμπιστοσύνης (trusts) που υπάρχουν στο δάσος ενός active directory έχοντας πρόσβαση σε πόρους σε οποιουδήποτε domain.

Στα domains των windows 2003 έχει εισαχθεί ο όρος functional level. Τα λειτουργικά επίπεδα έχουν οριστεί για ένα domain όπως και για ένα δάσος. Ο παρακάτω πίνακας καταγράφει τρία διαθέσιμα domain functional levels και τύπους από domain controllers που υποστηρίζονται σε αυτά τα επίπεδα.

Domain Functional Level	**Υποστηριζόμενοι domain controllers**
Windows 2000 mixed (default)	Windows NT, windows 2000, windows 2003
Windows 2000 native	windows 2000, windows 2003
Windows 2003	windows 2003 μόνο

Τα πρώτα δύο επίπεδα αντιστοιχούν σε περιβάλλοντα windows 2000 και προαναφερθείς παράγοντες για τα native mode domains είναι εφαρμόσιμοι στα windows 2000 native functional level επίσης.

Μεταξύ άλλων χαρακτηριστικών που χρειάζεται το λειτουργικό επίπεδο των domains σε windows 2003 είναι η επιλογή της μετονομασίας του domain controller. Τα windows 2000 και windows 2003 υποστηρίζουν τα παρακάτω χαρακτηριστικά: universal groups, φώλιασμα ομάδων (group nesting), μετατροπή των τύπων των ομάδων, και η επιλογή του ιστορικού SID.

Τα λειτουργικά επίπεδα ορίζουν κάποια χαρακτηριστικά που είναι διαθέσιμα σε όλα τα domains σε ένα δάσος. Ο παρακάτω πίνακας αναφέρει δυο διαθέσιμα λειτουργικά επίπεδα στ δάσος όπως και τους τύπους των domain controllers που υποστηρίζονται σε αυτά τα επίπεδα.

Λειτουργικό επίπεδο δάσους	**Υποστηριζόμενοι domain controllers**	**Επιτρεπτά υπαρκτά επίπεδα του domain ή νέα domains**
Windows 2000 (default)	Windows NT, windows 2000, windows 2003	Οποιοδήποτε επίπεδο
Windows 2003	windows 2003	Windows 2003 μόνο.

Υπάρχει επίσης ένα προσωρινό λειτουργικό επίπεδο στο δάσος κάτω από windows 2003 που είναι διαθέσιμο μόνο όταν ένα domain σε windows NT αναβαθμίζεται σε δάσος στα windows 2003, και δεν περιέχει domain controllers Που τρέχουν σε windows 2000.

Ας έχουμε υπόψιν τις παρακάτω πληροφορίες που αφορούν την κατάσταση του domain ή τα λειτουργικά επίπεδα του δάσους/domain

- Μπορούμε να αλλάξουμε την κατάσταση του domain από native σε mixed ή να μειώσουμε ένα λειτουργικό επίπεδο χωρίς να χρειαστεί να ξαναεγκαταστήσουμε το active directory στο domain ή σε ολόκληρο το δάσος.
- Τα domains σε ένα δάσος δεν χρειάζεται να λειτουργούν στην ίδια κατάσταση ή στο ίδιο λειτουργικό επίπεδο.
- Η κατάσταση native ή ένα λειτουργικό επίπεδο υψηλότερο από τα windows 2000 mixed level δεν έχει καμία επίπτωση σε χρήστες χαμηλότερου επιπέδου όπως windows 9x/ME (με ή χωρίς την επέκταση του active directory client). Αυτή επίσης είναι η περίπτωση με trusts μεταξύ του τοπικού domain και οποιωνδήποτε εξωτερικών domains. Ωστόσο οποιοδήποτε εξωτερικό trust είναι πάντα αναμφίβολο, μιας κατεύθυνσης και όχι μεταβατικό (εκτός τα trusts του δάσους).

1.13 ΝΕΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ DOMAIN CONTROLLERS ΣΕ WINDOWS 2003

Κάθε domain controller που τρέχει σε windows 2003 παρέχει νέα χαρακτηριστικά που περιγράφονται παρακάτω.

ΕΜΠΛΟΥΤΙΣΜΟΣ ΣΤΑ ΕΡΓΑΛΕΙΑ ΔΙΑΧΕΙΡΗΣΗΣ

Στα windows 2003 τα στάνταρ εργαλεία διαχείρισης παρέχουν πρόσθετες επιλογές που δίνουν στους διαχειριστές την δυνατότητα να διαχειρίζονται τα domains πιο αποτελεσματικά. Μεταξύ αυτών των επιλογών είναι οι παρακάτω:

- Αποθηκευμένα ερωτήματα καταλόγου στο active directory users and computers
- Επιλογή και μετατροπή πολλαπλών αντικειμένων καταλόγου.
- Εργασίες drag and drop
- Αποτελεσματικές εργασίες αναζήτησης που περιλαμβάνουν νέα φίλτρα και επιλογές εύρεσης.

ΕΡΓΑΛΕΙΑ ΓΡΑΜΜΗΣ ΕΝΤΟΛΩΝ ΓΙΑ ΤΟ ACTIVE DIRECTORY

Νέα εργαλεία ευπειθή με το LDAP όπως DsQuery.exe DsAdd.exe DsMod.exe κτλ παρέχουν την δυνατότητα στους admins να εκτελέσουν batch και στερεότυπες διαδικασίες με τα αντικείμενα καταλόγου.

ΠΡΟΣΘΕΤΟΝΤΑΣ ΕΝΑΝ DOMAIN CONTROLLER ΑΠΟ ΑΡΧΕΙΑ BACKUP

Ένας επιπρόσθετος domain controller σε ένα domain μπορεί να εγκατασταθεί από τα backup αρχεία ενός υπάρχον domain controller. Αυτό μειώνει τον χρόνο προώθησης όπως και την κίνηση του replication στο δίκτυο.

UNIVERSAL GROUP MEMBERSHIP CACHING

Όλες οι προσπάθειες πιστοποίησης χρηστών ελέγχονται από έναν Global Catalog server που ελέγχει την ιδιότητα του χρήστη-μέλους στα universal groups. Αυτή η διαδικασία παράγει πρόσθετη κυκλοφορία δια μέσου ενός WAN σε έναν απομακρυσμένο GC server. Για να εξαλείψουμε την ανάγκη να έχουμε έναν GC server για κάθε site μπορούμε να υποδείξουμε έναν domain controller να κάνει cache το universal group membership και να ενημερώνει εκείνες τις πληροφορίες από ένα συγκεκριμένο site.

APPLICATION DIRECTORY PARTITIONS

Ένα application directory partition μπορεί να δημιουργηθεί από μια εφαρμογή ή από έναν admin που επίσης ορίζει τον σκοπό του διαμερίσματος του replication. Αυτή είναι η βασική διάκριση μεταξύ του τύπου του partition και των άλλων partitions του active directory, (των οποίων η τοπολογία του replication, σαν κανόνας, δημιουργείται αυτόματα από το Knowledge Consistency Checker, KCC). Η έννοια του replication για μια εφαρμογή ενός partition μπορεί να συμπεριλαμβάνει οποιοδήποτε σετ από domain controllers στο δάσος.

Ένα application partition μπορεί να αποθηκεύσει κάθε αντικείμενο καταλόγου (εκτός των αρχών ασφαλείας) που είναι ορισμένα στο schema (συμπεριλαμβανομένου και δυναμικά αντικείμενα). Αντικείμενα στα application partitions δεν γίνονται replicate στο Global Catalog. Παρόλα αυτά υπάρχουν δύο ενσωματωμένα application partitions που μπορούν να χρησιμοποιηθούν από τους windows 2003 DNS servers που τρέχουν σε domain controllers.

InetOrgPerson Object Class

Η κλάση αντικειμένου inetOrgPerson που καθορίζεται στο RFC 2798 έχει προστεθεί στο schema του active directory για να καταστήσει τη μετανάστευση (migration)από τους καταλόγους LDAP τρίτων στο active directory αποδοτικότερη. Τα αντικείμενα εκείνης της κλάσης είναι οι αρχές ασφάλειας και μπορούν να χρησιμοποιηθούν ως πρότυπα αντικείμενα χρηστών

1.14 ΝΕΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΓΙΑ ΑΓΝΑ WINDOWS 2003 DOMAINS ΚΑΙ ΔΑΣΗ

Αυτό το τμήμα περιγράφει τα νέα χαρακτηριστικά γνωρίσματα που είναι διαθέσιμα μόνο όταν το λειτουργικό επίπεδο του domain/δάσους έχει ανεβεί σε Windows 2003.

Επιλογές μετονομασίας

Μπορούμε να μετονομάσουμε έναν domain controller χωρίς πρώτα να τον υποβιβάσουμε ή να αλλάξουμε το όνομα του dns ή του NetBIOS οποιουδήποτε domain. Η μετονομασία ενός domain μπορεί να προκαλέσει την μετακίνησή του σε άλλη θέση στη δασική υποδομή.

Σχέσεις εμπιστοσύνης δάσους

Οι σχέσεις εμπιστοσύνης του δάσους καθιερώνονται μεταξύ των root domains του δάσους που δουλεύουν στο λειτουργικό επίπεδο των Windows 2003 και μπορούν να έχουν μια μονόδρομη καθώς επίσης αμφίδρομη κατεύθυνση. Αντίθετα από τις συνηθισμένες εξωτερικές εμπιστοσύνες, οι δασικές εμπιστοσύνες είναι μεταβατικές, πχ,

επιτρέπουν σε έναν χρήστη που επικυρώνεται σε ένα δάσος να έχει πρόσβαση σε πόρους που βρίσκονται σε οποιοδήποτε domain σε ένα άλλο δάσος.

Defunct Objects

Το active directory δεν μας επιτρέπει να διαγράψουμε μια κλάση αντικειμένου καταλόγου ή ένα χαρακτηριστικό γνώρισμα: μπορούμε μόνο να το απενεργοποιήσουμε. Μια απενεργοποιημένη κλάση ή μια ιδιότητα καλείται defunct. Είναι δυνατό να ενεργοποιηθεί μια απενεργοποιημένη κλάση ή μια ιδιότητα και να επαναπροσδιοριστεί, εάν υπήρξε ένα σφάλμα όταν δημιουργήθηκε αρχικά η κλάση ή η ιδιότητα.

Replication Enhancements

Μερικά προβλήματα σχετικά με το replication που υπάρχουν στα Windows 2000 έχουν εξεταστεί στα Windows 2003. Πρώτιστα, αυτό αφορά την ενισχυμένη συνδεμένη αξία και το Global Catalog replication καθώς επίσης και τους αλγορίθμους που χρησιμοποιούνται από το *Knowledge Consistency Checker* (KCC) για την παραγωγή της τοπολογίας του replication στα δάση με το μεγάλο αριθμό από sites.

Η συνδεμένη αξία του replication μειώνει την κυκλοφορία δικτύου όταν αλλάζει η ιδιότητα μέλους ομάδας: μόνο τα νέα ή διαγραμμένα μέλη ομάδας γίνονται replicate αντί του ολόκληρου καταλόγου μελών ομάδας που καταχωρείται στις ιδιότητες μελών. Αυτό είναι ουσιαστικό για τις ομάδες με μεγάλο αριθμό μελών.

Στα Windows 2000, όταν μια νέα ιδιότητα προστίθεται στο Global Catalog, ένας πλήρης συγχρονισμός των μερικών αντιγράφων απαιτείται, και αυτή η διαδικασία έχει επιπτώσεις σε όλα τα domains στο δάσος. Στα windows 2003, μόνο η νέα ιδιότητα γίνεται replicate στους Global Catalog servers.

Δυναμικές βοηθητικές κλάσεις και δυναμικά αντικείμενα

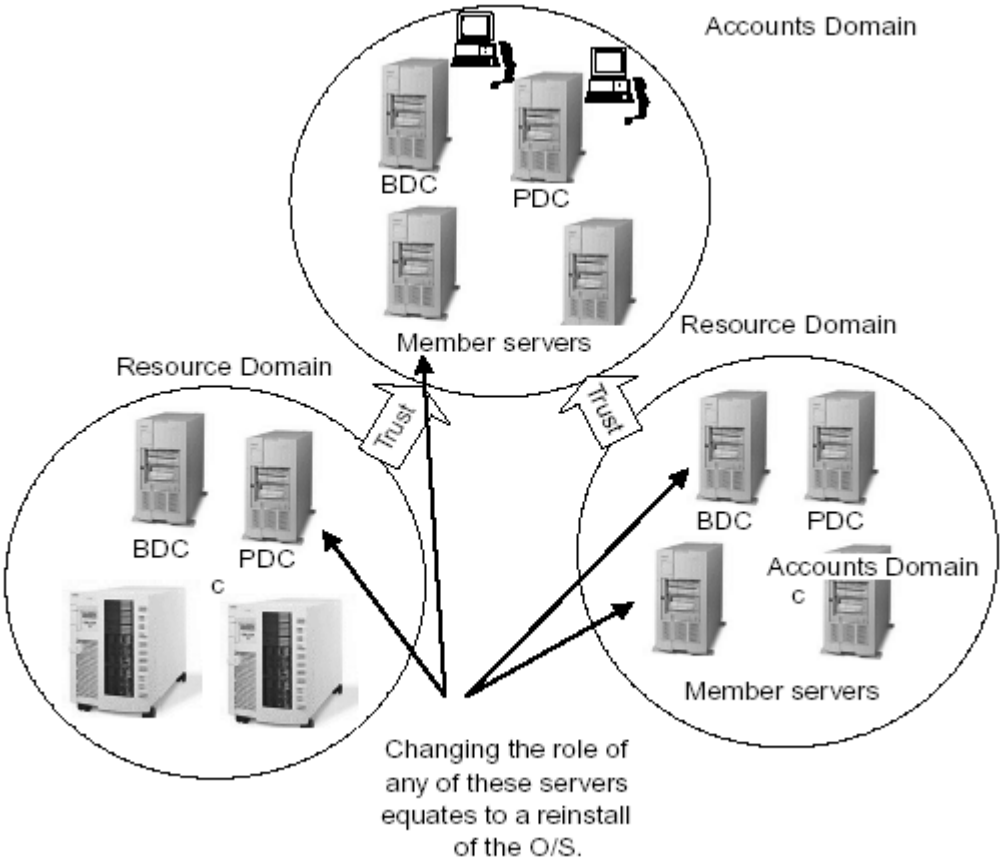
Είναι δυνατό να συνδεθούν δυναμικά ή να αφαιρεθούν οι βοηθητικές κλάσεις στις περιπτώσεις αντικειμένου καθώς επίσης και στις κλάσεις αντικειμένου.

Τα δυναμικά αντικείμενα επείγονται από μια κλάση αντικειμένου που έχει τη βοηθητική κλάση dynamicObject. Αυτή η κλάση μπορεί επίσης να προστεθεί σε μια περίπτωση αντικειμένου με τη χρησιμοποίηση ενός προγράμματος ή ενός script. Κατά συνέπεια, ένα δυναμικό αντικείμενο υπάρχει κατά τη διάρκεια που καθορίζεται από μια *Time-to-Live* (TTL) αξία που ανατίθεται στη δημιουργία αντικειμένου και μπορεί να ανανεωθεί από έναν χρήστη ή μια εφαρμογή.

Κατά τη διάρκεια της διαδικασίας της εγκατάστασης, τα Windows 2003 Server, δεν έχουν καμία προαιρετική δυνατότητα να επιλεχτεί ο ρόλος θα παίξει που ο κεντρικός υπολογιστής. Στα WINDOWS NT, κατά τη διάρκεια της διαδικασίας της εγκατάστασης, μας ρωτάει εάν ο κεντρικός υπολογιστής θα ενεργήσει ως Primary Domain Controller (PDC), Backup Domain Controller (BDC), ή σαν Standalone server (Member server).

Αυτό ήταν ένας περιορισμός στις προηγούμενες εκδόσεις, καθώς η απόφαση μεταξύ του Domain Controller και του Member server δεν μπορούσε να αλλάξει. Μόλις επιλεγόταν ένας Domain Controller, εάν ο κεντρικός υπολογιστής έπρεπε να αναδιαρθρωθεί ως κεντρικός υπολογιστής σε έναν άλλο ρόλο, ας πούμε έναν Member

server, ο κεντρικός υπολογιστής θα απαιτούσε μια επανεγκατάσταση του λειτουργικού συστήματος. Αυτό ήταν επίσης αληθινό εάν ο κεντρικός υπολογιστής λειτουργούσε ως Domain Controller και έπρεπε να μετακινηθεί σε ένα άλλο Domain. Αυτή η συγκεκριμένη φύση των ρόλων κεντρικών υπολογιστών είναι πολύ άκαμπτη, που με την σειρά της μεταφράζεται σε κόστος που χρειάζεται για την αναδιάρθρωση των servers. Το σχήμα 1.1 περιγράφει μια χαρακτηριστική επέκταση των WINDOWS NT και σχετική ακαμψία.



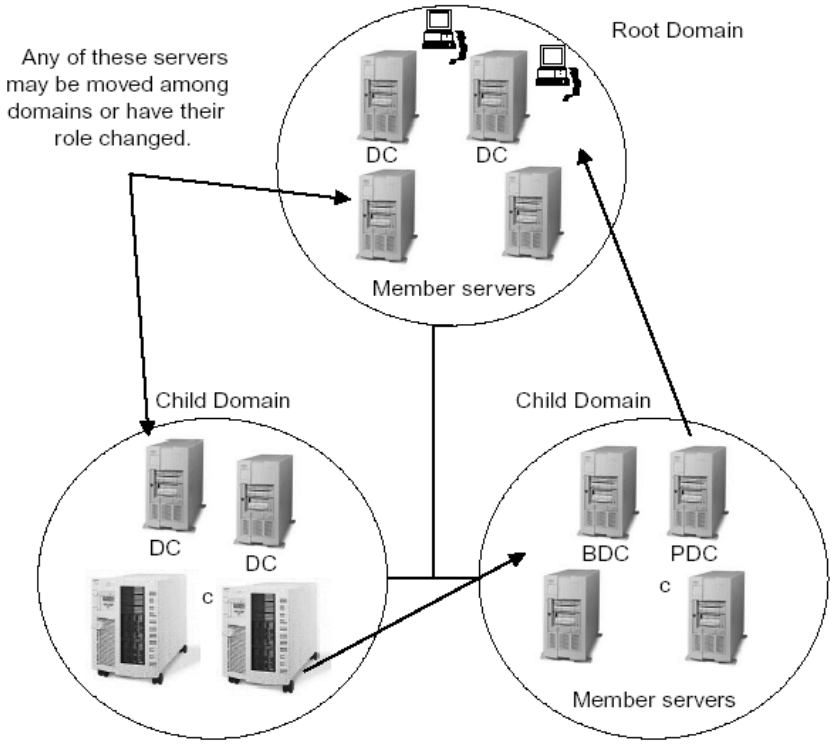
Σχήμα 1.2

Μια από τις πιο ευπρόσδεκτες αλλαγές σε αυτό το νέο λειτουργικό σύστημα, τα Windows 2003 Server, είναι η δυνατότητα να κινηθούν οι κεντρικοί υπολογιστές ελεύθερα από έναν ρόλο προς έναν άλλο, μέλος στον Domain Controller, και αντίστροφα. Κατά την εγκατάσταση των Windows 2003, δεν ρωτιέστε για το ρόλο του κεντρικού υπολογιστή, όπως ο κεντρικός υπολογιστής παρουσιάζεται στον κόσμο του ως μόνος Member server χωρίς καμία δέσμευση σε κάποιο Domain. Ένα συνειδητό, δευτεροβάθμιο βήμα πρέπει να εκτελεσθεί προκειμένου να προαχθεί ο κεντρικός υπολογιστής σε έναν Domain Controller. Αυτή η προώθηση ολοκληρώνεται μέσω ενός βοηθήματος γραμμής εντολών, το DCPROMO, το οποίο καλεί έναν βοηθό εγκατάστασης για να μας καθοδηγήσει μέσω της διαδικασίας αυτής. Το πρώτο βήμα στη δημιουργία ενός Windows 2003 δικτύου είναι η δημιουργία της ρίζας του domain από το οποίο όλα τα άλλα domains ή τα οργανωτικά ή δομικά στοιχεία θα ακολουθήσουν. Είναι αυτό το πρώτο κρίσιμο βήμα που καθορίζει την επιτυχία του υπολοίπου του δικτύου, σαν

όλα τα άλλα domains είναι εξαρτήσεις (από φόβο μήπως έχετε αποφασίσει να πάρετε μια ανορθόδοξη προσέγγιση στη δικτυακή αρχιτεκτονική σας).

Η πράξη της κλήσης του βοηθήματος DCPROMO και της μετατροπής του Member Server σε έναν domain controller θα δημιουργήσει επίσης είτε τη ρίζα του Active Directory, εάν αυτός είναι ο πρώτος κεντρικός υπολογιστής, ή επόμενα χωρίσματα από την ιεραρχία του Active Directory. Οι Domain controllers παρέχουν υπηρεσίες καταλόγου αρχείων και είναι τα μέρη αποθήκευσης της βάσης δεδομένων καταλόγου αρχείων και συσκευών αντιγράφων. Με τις υπηρεσίες καταλόγου αρχείων σε ισχύ, οι χρήστες είναι έπειτα ικανοί να επικυρώσουν στο domain. Όταν ένας κεντρικός υπολογιστής προάγεται σε Domain controller, γίνεται η ρίζα του Domain ενός δέντρου ή ένα λειτουργικό μέλος του δέντρου υπηρεσιών καταλόγου αρχείων. Ομοίως, όταν ο κεντρικός υπολογιστής υποβιβάζεται από Domain controller σε έναν member server, χάνει τις λειτουργίες του Active Directory και διατηρεί μόνο τις τοπικές λειτουργίες. Το σχήμα 1.3 εμφανίζει τις μεταβλητές ιδιότητες των Windows 2003 server.

Όπως με την εγκατάσταση των υπηρεσιών dns, οι οποίες θα δείτε ότι είναι επίσης ίσως ενσωματωμένες σε αυτήν την διαδικασία επίσης, είναι επιτακτικό να υπάρχει η τεκμηρίωση του προσχεδιασμού εύκαιρη σε αυτή τη φάση για να χρησιμοποιηθεί ως οδηγός ονομασίας του domain controller ή των επόμενων domain controllers. Ας εξετάσουμε τι είναι απαραίτητο για να προάγουμε έναν κεντρικό υπολογιστή σε έναν domain controller/Active Directory server.



Σχήμα 1.3

2. ΕΓΚΑΤΑΣΤΑΣΗ ΤΟΥ ACTIVE DIRECTORY

2.1 ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΤΟΥ DOMAIN CONTROLLER ΚΑΙ ΤΟΥ ACTIVE DIRECTORY

Υπάρχουν ορισμένες απαιτήσεις που πρέπει να ικανοποιηθούν πριν από την εγκατάσταση του Active Directory. Ας προσπαθήσουμε να μην συγχέουμε αυτό με την εγκατάσταση ενός domain controller, αν και τα δύο είναι συνώνυμα. Τι σημαίνει αυτό? Η ιδέα της συνύπαρξης των dns υπηρεσιών στον ίδιο κεντρικό υπολογιστή με τον domain controller προτείνεται ως συνιστώμενη προσέγγιση. Για να λειτουργήσει σωστά το Active Directory, οι υπηρεσίες εξάρτησης του dns πρέπει να είναι παρών, ακόμη και κατά τη διάρκεια της διαδικασίας εγκατάστασης. Στις μεγαλύτερες εφαρμογές, ή σε περιπτώσεις όπου μια μεγάλη υποδομή dns υπάρχει ήδη, ο Dns σίγουρα δεν θα υπάρξει στον ίδιο κεντρικό υπολογιστή με το Active Directory.

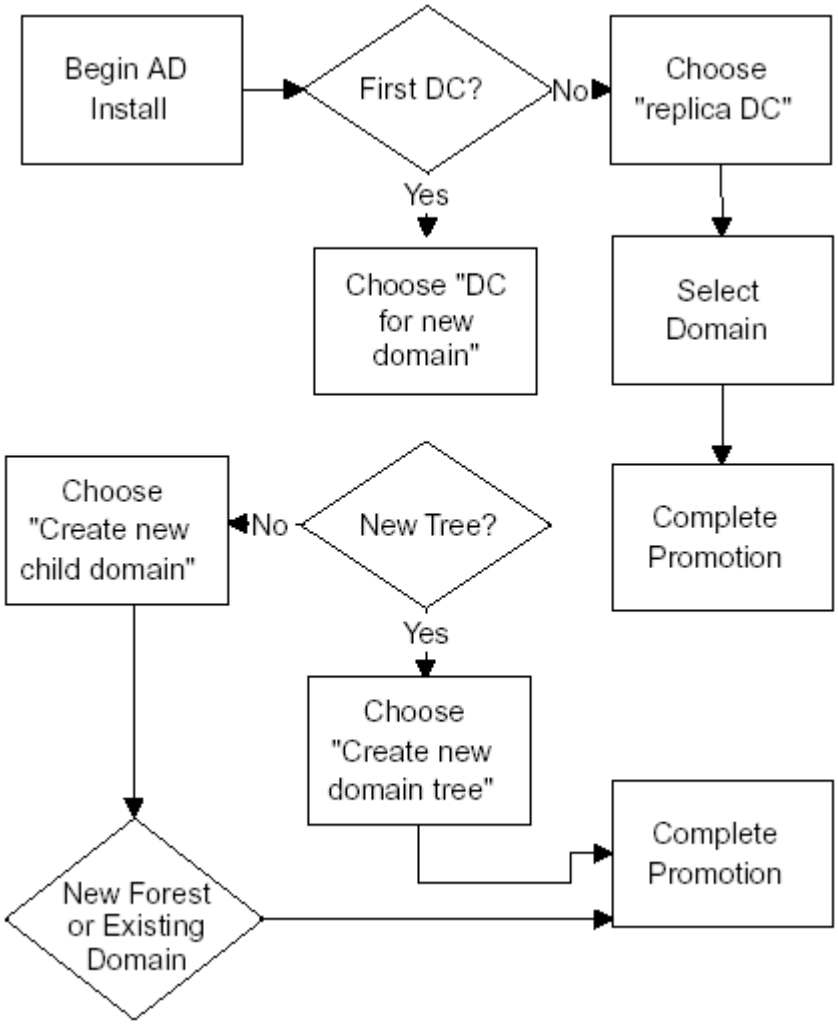
Στις καταστάσεις όπου αυτό δεν ισχύει, ή εάν αρχίζουμε από μια καθαρή κατάσταση, η συνιστώμενη δυνατότητα συνύπαρξης του dns και του Active Directory είναι ελκυστική προσέγγιση για να οργανωθεί ένα δίκτυο Windows 2003 καθαρά χωρίς την αυτοματοποίηση της εγκατάστασης του dns και του Active Directory. Μέρος της διαδικασίας εγκατάστασης για την προαγωγή ενός κεντρικού υπολογιστή σε domain controller και η εγκατάσταση του Active Directory ελέγχουν για την ύπαρξη ενός dns server. Εάν δεν βρεθεί καμία dns υπηρεσία, το πρόγραμμα εγκατάστασης "αυτόματα" θα εγκαταστήσει και θα παραμετροποιήσει τον dns στον ίδιο κεντρικό υπολογιστή επίσης.

Επιπρόσθετα στην απαίτηση για dns, η προαγωγή απαιτεί επίσης την ύπαρξη ενός χωρίσματος NTFS 5 προκειμένου να εγκατασταθούν και να ασφαλιστούν τα μέρη του καταλόγου αρχείων και της βάσης δεδομένων. Αυτό το χώρισμα εξαρτάται αν μπορεί ή δεν μπορεί να υπάρξει από τις επιλογές που γίνονται κατά τη διάρκεια της εγκατάστασης του κεντρικού υπολογιστή. Ελέγχουμε ότι ο κεντρικός υπολογιστής έχει τουλάχιστον ένα χώρισμα NTFS και ότι είναι αρκετά μεγάλο για να προσαρμόσει ένα κόσμιο ποσό στοιχείων. Δύο gigabytes για αυτά τα δεδομένα που είναι το χαμηλό όριο ανά domain controller πρέπει να αρκεί. Αυτές οι πληροφορίες μπορούν να εδρεύουν στο χώρισμα του λειτουργικού συστήματος ή αλλού.

Επιπλέον, πρέπει να κάνουμε log in στον κεντρικό υπολογιστή ως τοπικός administrator ή να έχει έναν λογαριασμό με δικαιώματα administrator προκειμένου να τρέξει το DCPROMO. Εάν αυτός είναι domain controller αντιγράφου (εκτός από τον αρχικό domain controller) για το domain, απαιτείται ο λογαριασμός του administrator για το domain . Ο κατάλογος ονομάτων για το domain(s) που δημιουργείται στο στάδιο προγραμματισμού πρέπει επίσης να είναι παρών. Η εγκατάσταση του Active Directory μπορεί επίσης να τρέξει από το εργαλείο Configure Your Server που εμφανίζεται στο ξεκίνημα του κεντρικού υπολογιστή. Η τελευταία διαδικασία είναι εντελώς αυτοματοποιημένη με εξαίρεση μερικές ερωτήσεις, και πολύ απλούστερη να εκτελέσει. Θα ρίξουμε μια ματιά σε εκείνη την διαδικασία σε μια στιγμή αφού πάρουμε την “χειροκίνητη” διαδικασία του DCPROMO, αυστηρά ως βοήθημα στην προαγωγή ενός κεντρικού υπολογιστή.

2.2 Η Εφαρμογή DCPROMO

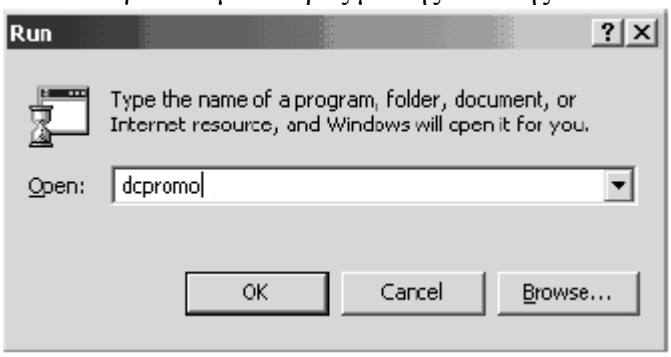
Δεδομένου ότι συζητήσαμε νωρίτερα, η έναρξη του βοηθήματος DCPROMO είναι απαραίτητη στην προαγωγή του κεντρικού υπολογιστή από έναν Member server σε έναν domain controller. Το πρόγραμμα καλείται από γραμμή εντολών, ή από την επιλογή Run στα Windows 2003 στο Start μενού.
Μόλις τρέξει η εντολή, καλείται ο βοηθός της εγκατάστασης του Active Directory, και μια ευπρόσδεκτη οθόνη δίνει τις πληροφορίες για τη διαδικασία. Έπειτα, θα υποβληθούμε στη βαθμιαία διαδικασία εγκατάστασης του Active Directory. Το πρώτο τμήμα εγκατάστασης του Active Directory υποθέτει ότι αυτό είναι αρχική εγκατάσταση του Active Directory στο δίκτυο, ή ακριβέστερα, ότι ένα νέο δέντρο δημιουργείται που δεν συμμετέχει σε ένα δάσος. Τα επόμενα τμήματα περιέχουν τα σενάρια για τη δημιουργία replica domain controllers και child domains. Το σχήμα 2.1 εμφανίζει ένα διάγραμμα ροής από τη διαδικασία εγκατάστασης και τα μονοπάτια που μπορούν να ληφθούν στο δρόμο στη δημιουργία μιας ιεραρχίας του Active Directory χρησιμοποιώντας τον βοηθό εγκατάστασης του Active Directory (DCPROMO).



Σχήμα 2.1

2.3 Βήμα προς Βήμα Εγκατάσταση του Πρώτου Domain Controller

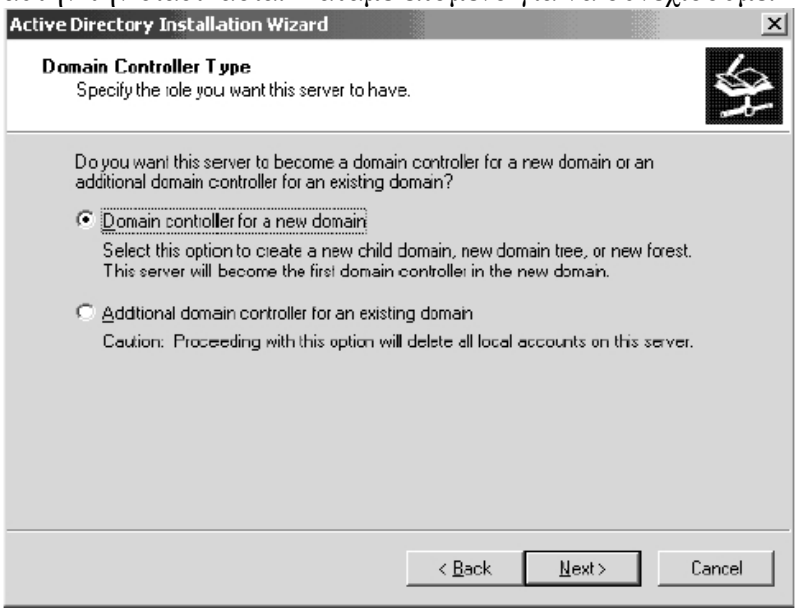
Το πρώτο βήμα στην εγκατάσταση του Active Directory μέσω της μεθόδου DCPROMO είναι δια μέσου της κλήσης του βοηθού εγκατάστασης του Active Directory, το οποίο γίνεται με το τρέξιμο της εντολής DCPROMO όπως φαίνεται στο σχήμα 2.2.



Σχήμα 2.2

Από την οθόνη καλωσορίσματος, κάνουμε κλικ στο 'επόμενο' για να αρχίσει η διαδικασία εγκατάστασης των υπηρεσιών καταλόγου αρχείων. Τα έπειτα διάφορα παράθυρα περιέχουν κάποιο είδος ερωτηματολογίου. Αυτές οι ερωτήσεις βοηθούν την εγκατάσταση να καθορίσει τον τύπο του domain controller που εγκαθίσταται και όπου θα καθίσει στην ιεραρχία δέντρων του domain.

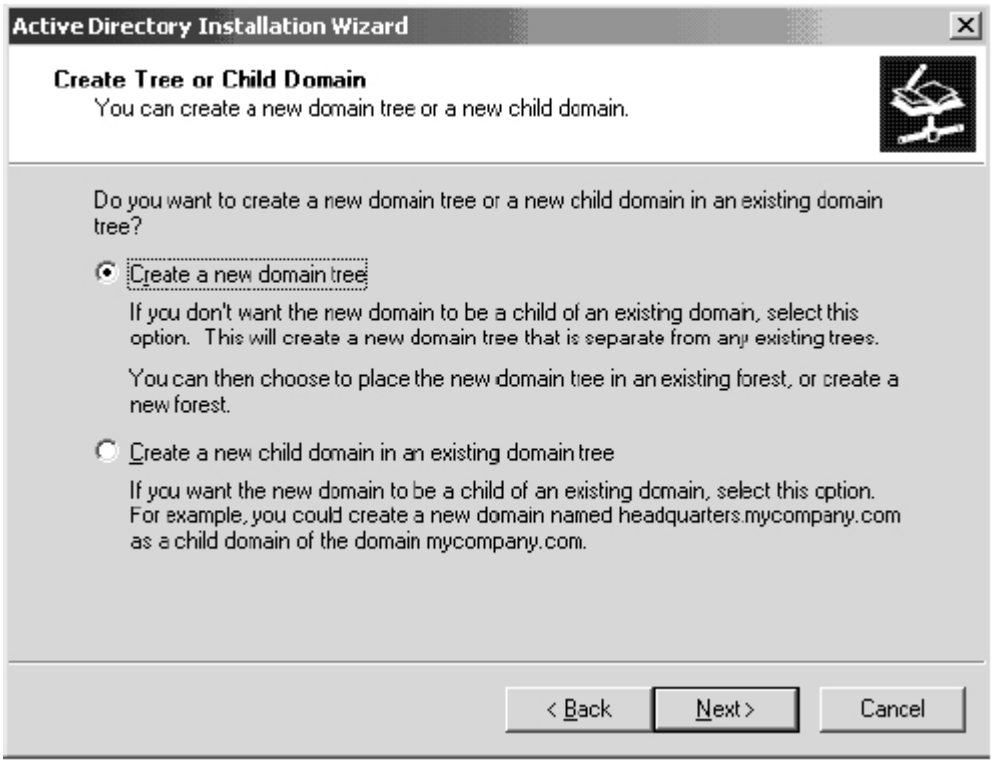
Τώρα είμαστε στο παράθυρο με τους τύπους των domain controllers, όπου ρωτά εάν θέλουμε αυτόν τον domain controller να είναι νέος domain controller για ένα νέο domain ή έναν domain controller αντιγράφου για ένα υπάρχων domain. Δεδομένου ότι υποθέτουμε ότι αυτό είναι ο πρώτος domain controller στο πρώτο domain, επιλέγουμε την πρώτη επιλογή, " domain controller για ένα νέο domain". Το σχήμα 2.3 εμφανίζει αυτήν την διαδικασία. Πατάμε επόμενο για να συνεχίσουμε.



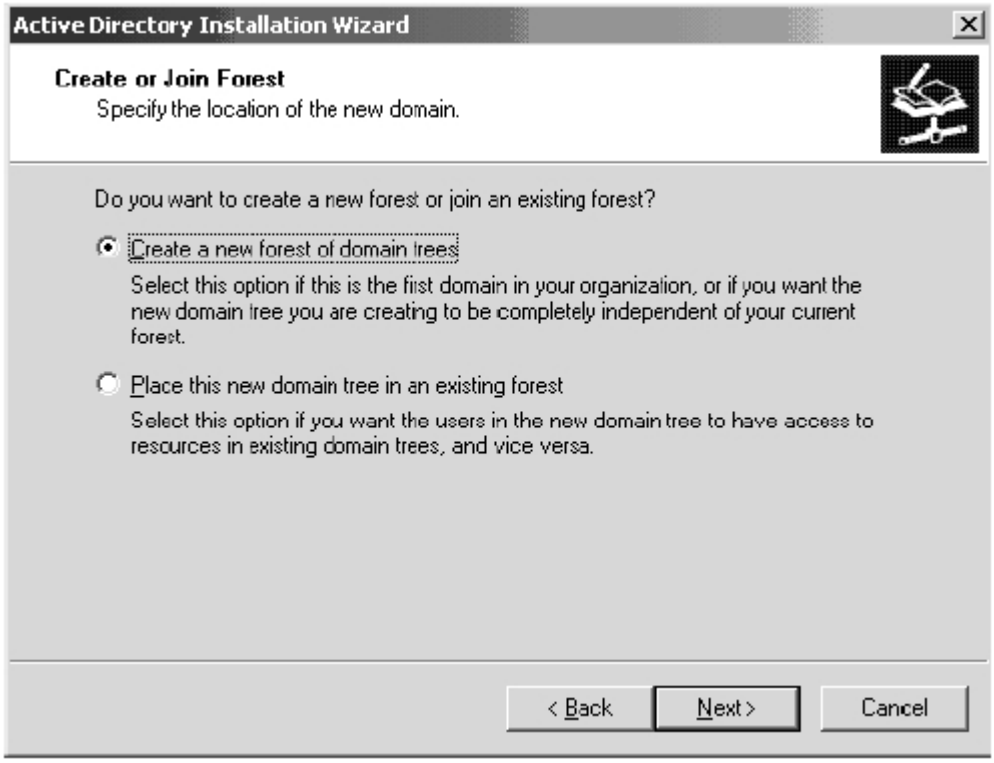
Σχήμα 2.3

Η επόμενη οθόνη, Create Tree or Child Domain, προσφέρει την επιλογή είτε για να δημιουργήσουμε ένα νέο δέντρο για κάποιο domain χρησιμοποιώντας αυτόν τον

domain controller ως κεντρικό υπολογιστή ρίζας (που, δεδομένου ότι θα αναφερθεί αργότερα, μπορούμε επίσης να χρησιμοποιηθεί για να δημιουργηθεί ένα δάσος από δέντρα), ή ένα child domain που χρησιμοποιεί αυτόν τον κεντρικό υπολογιστή ως πρώτο domain controller στο παρακλάδι (αυτό είναι όπου θα δημιουργούσε first-level domains). Το σχήμα 2.4 εμφανίζει τις επιλογές σε αυτήν την φόρμα. Επιλέγουμε την επιλογή "Create a new domain tree" και πατάμε επόμενο για να συνεχίσουμε.

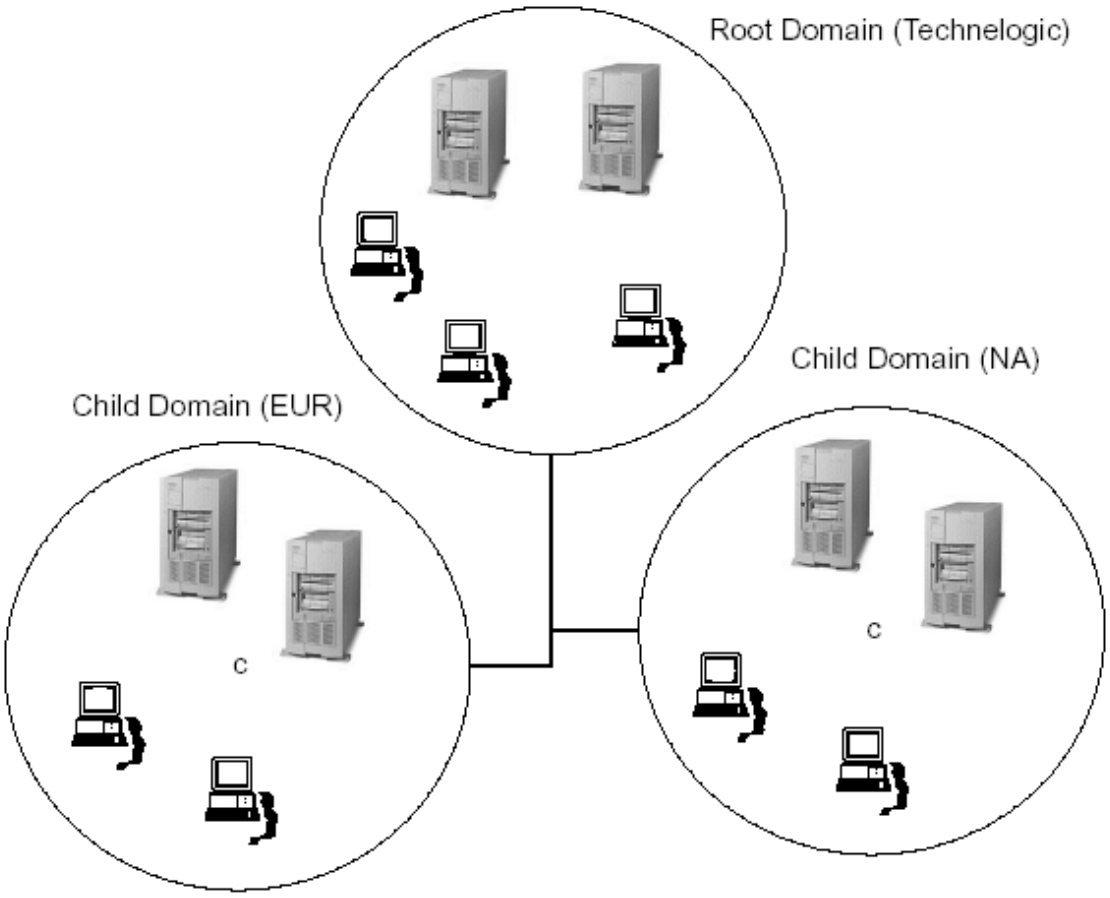


Σχήμα 2.4



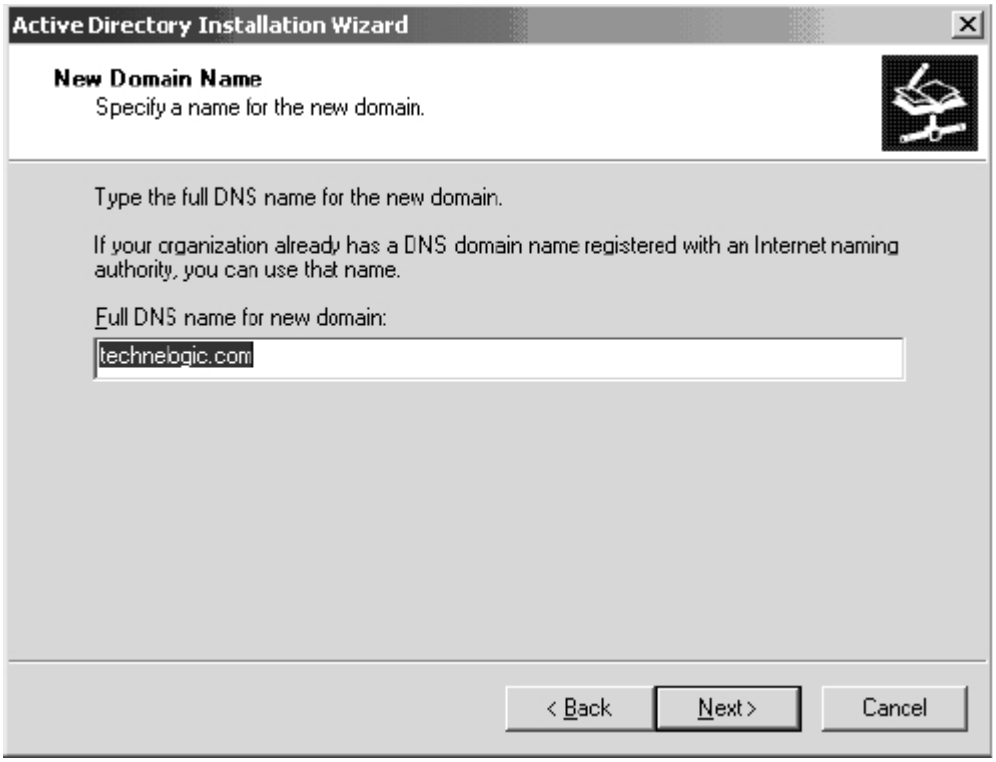
Σχήμα 2.5

Το σχήμα 2.5 εμφανίζει την επιλογή Create or Join Forest. Εδώ ρωτόμαστε εάν το δέντρο θα υπάρξει σε ένα υπάρχον δάσος ή εάν αυτό είναι ένα νέο δάσος συνολικά. Επειδή αυτό είναι το πρώτο δέντρο στο δάσος, επιλέξτε "Create a new forest of domain trees", και συνεχίζουμε. Έπειτα ρωτόμαστε για το όνομα του domain. Αυτό πρέπει να προέλθει από την τεκμηρίωση του προσχεδιασμού και θα απεικονίσει το πρώτο επίπεδο του domain που έχουμε επιλέξει για την επιχείρηση.



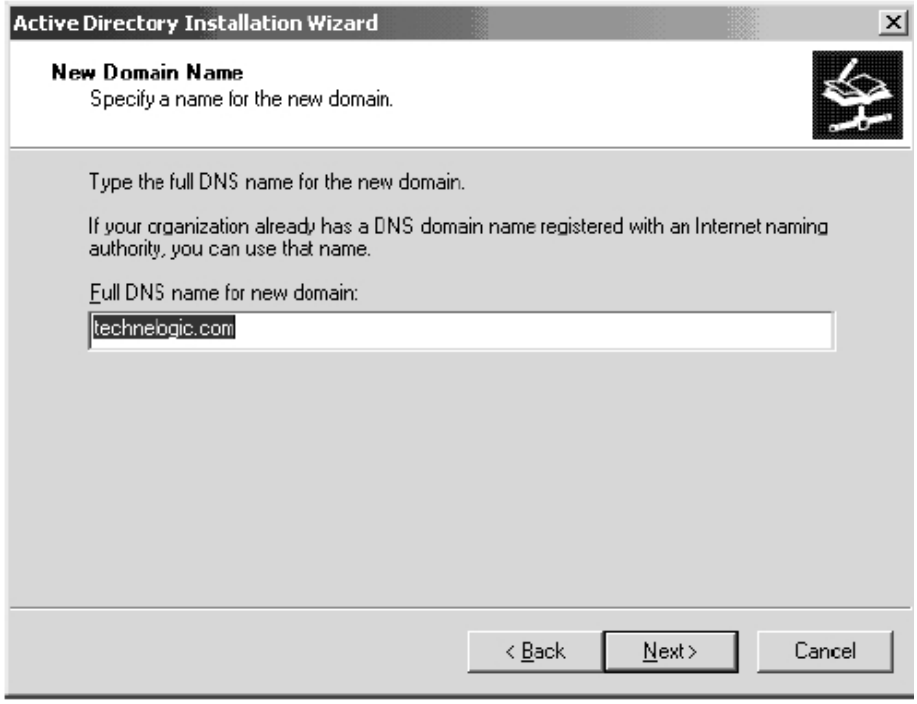
Σχήμα 2.6

Στο παράδειγμα που εμφανίζεται στο σχήμα 2.6, είναι το domain name για την επιχείρηση που εγγράφεται με μια αρχή Διαδικτύου. Αυτό οργανώνει τη δυνατότητα για ένα γεωπολιτικό μοντέλο όπου οι ακόλουθες first-level child domains μπορούν να οργανωθούν ως γεωγραφικά domains, και περαιτέρω υποδιαιρεμένα σε τμήματα.
Το σχήμα 2.6 παρουσιάζει αυτόν τον τύπο οργάνωσης στο δέντρο technologic.com.
Έπειτα, επιλέγουμε τον πλήρες dns για το νέο domain, και επιλέγουμε επόμενο όπως στο Σχήμα 2.7.

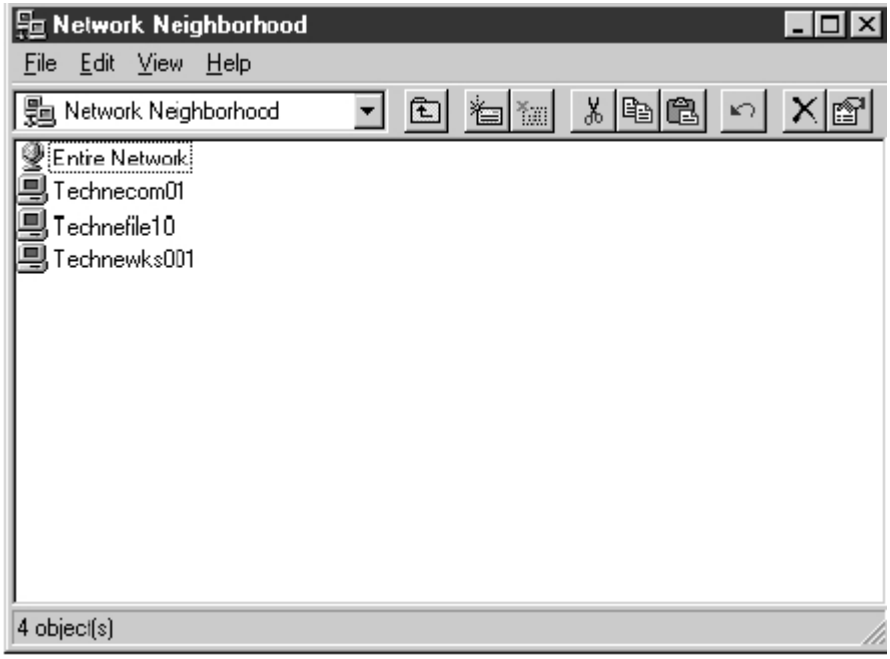


Σχήμα 2.7

Ένα όνομα NetBIOS απαιτείται στην επόμενη οθόνη για την υποστήριξη κληρονομιών. Αυτό θα είναι το όνομα NetBIOS του domain.



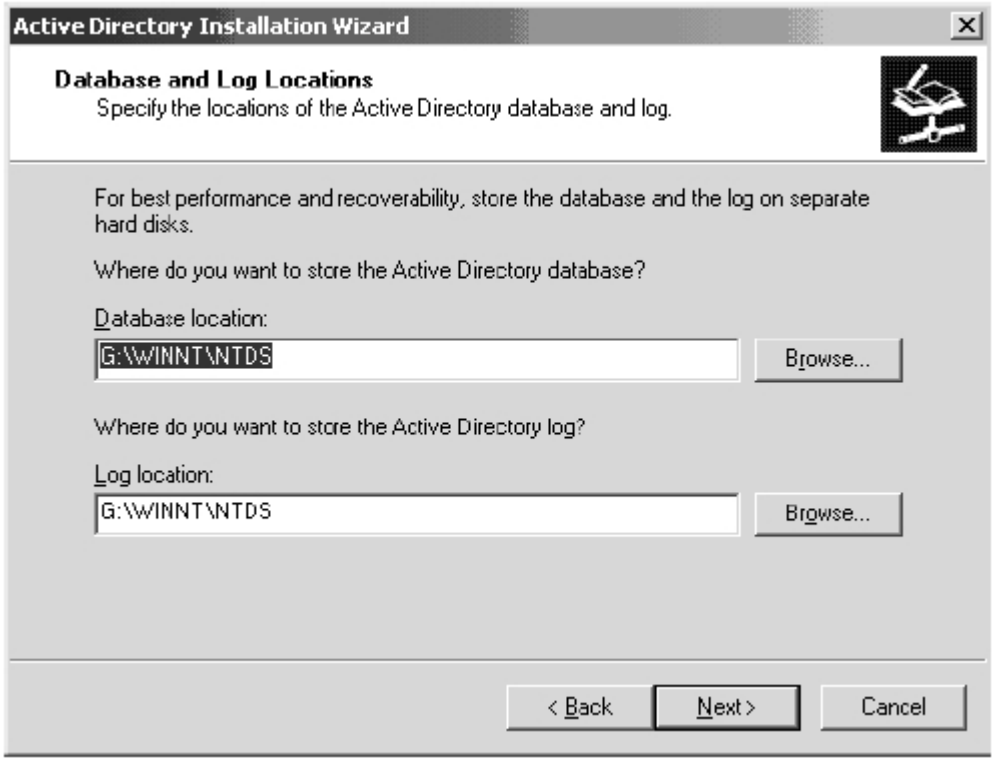
Σχήμα 2.8



Σχήμα 2.9

Το σχήμα 2.9 ανοίγει το δρόμο ότι αυτό θα εμφανιζόταν στην browse list ενός χρήστη τερματικών σταθμών των WINDOWS NT 4.0. Τα ονόματα NetBIOS επιτρέπουν σε αυτούς τους χρήστες για να λειτουργήσουν στο δίκτυο των Windows 2003.

Ο βοηθός της εγκατάστασης ζητά τώρα να ελεγχθεί η θέση των βάσεων δεδομένων καταλόγου αρχείων και των αρχείων καταγραφής γεγονότων. Το προκαθορισμένο πρέπει να είναι αποδεκτό στις περισσότερες καταστάσεις. Στην περίπτωση των πολύ μεγάλων επιχειρηματικών εγκαταστάσεων όπου οι domain controllers θα χειρίζονται ένα πολύ μεγάλο ποσό αντικειμένων στη βάση δεδομένων, θα ήταν καλύτερα να επανεντοπίσει αυτά τα αρχεία στον αφιερωμένο δίσκο ή το χώρισμα (όπως με οποιοδήποτε κεντρικό υπολογιστή βάσεων δεδομένων). Το σχήμα 2.10 εμφανίζει μια απεικόνιση αυτής της οθόνης.



Σχήμα 2.10

Το επόμενο αντικείμενο που παρουσιάζεται είναι η θέση του "shared system volume," συνώνυμο με τον κατάλογο αρχείων Netlogon, όπου τα συνδεδεμένα και τα αντεγραμένα αντικείμενα καταχωρούνται προς χρήση από όλους τους χρήστες του δικτύου. Πάλι, το προκαθορισμένο πρέπει να είναι αποδεκτό εδώ. Το σχήμα 2.10 εμφανίζει το παράθυρο Shared System Volume. Η τελευταία οθόνη που παρουσιάζεται στο βοηθό επιβεβαιώνει όλες τις επιλογές. Είναι μια καλή ιδέα να αναθεωρηθούν αυτά για σφάλματα πριν συνεχίσουμε για να αποφύγουμε να τρέξουμε το DCPROMO δύο φορές, μία φορά για να υποβιβαστεί ο κεντρικός υπολογιστής, και κατόπιν να προαγθεί και πάλι. Τουλάχιστον εκείνη η επιλογή είναι διαθέσιμη εάν πήγαινε κάτι στραβά, και είναι μια καλή ιδέα για να εξοικειωθούμε με την διαδικασία δεδομένου ότι θα χρησιμοποιηθεί στο μέλλον.

2.4 Εγκατάσταση Replica Domain Controllers

Υπάρχουν όροι που υπαγορεύουν τη χρήση των πολλαπλών domain controllers σε ένα domain, ιδιαίτερα για την ανοχή βλαβών. Εάν ο μόνος domain controller στη ρίζα υποστεί κάποια καταστροφή χωρίς έναν εφεδρικό ελεγκτή σε ισχύ, το καθαρό αποτέλεσμα είναι ο υποβιβασμός όλων των child domains και επαναδημιουργία ολόκληρης της δομής του καταλόγου αρχείων. Εκτός από την ανοχή βλαβών, οι μεγαλύτερες εφαρμογές θα απαιτήσουν βεβαίως πολλαπλάσιους domain controllers για να διευκολύνουν έναν μεγάλο αριθμό logons μέσα στο domain. Ενώ είναι αλήθεια ότι με την εφαρμογή των περιοχών εκείνοι οι χρήστες θα επαναπροσανατολιστούν σε άλλους domain controllers (ενδεχομένως μέσα στην ίδια περιοχή εάν υπάρχουν άλλοι domain controllers) σε περίπτωση μιας κατάστασης όπου ο τοπικός κεντρικός υπολογιστής δεν

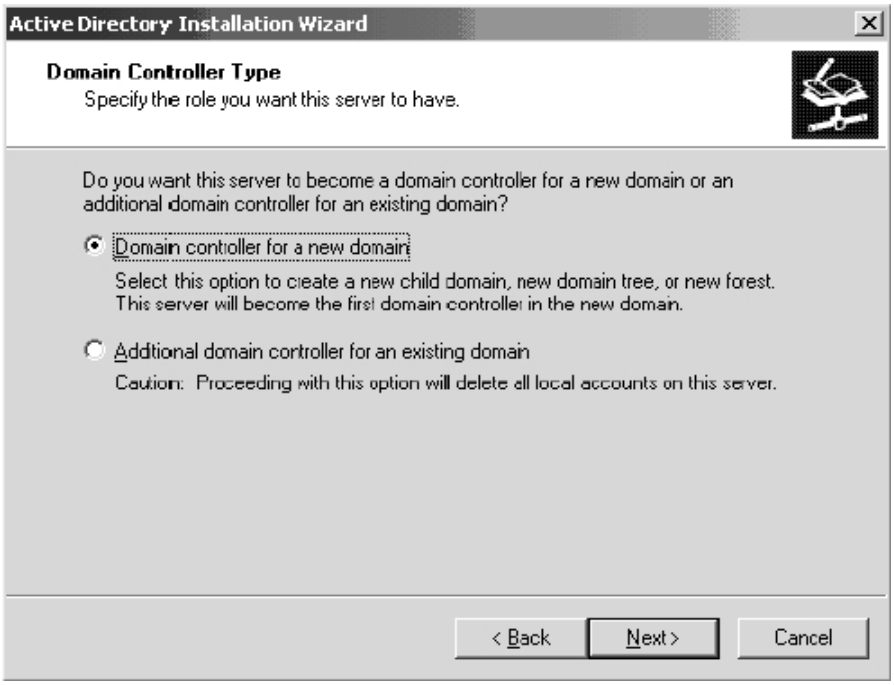
μπορεί να παρέχει μια απάντηση, αυτό μπορεί να σημάνει ότι τα αιτήματα για επόμενες συνδέσεις μπορούν να υπερβούν τις WAN συνδέσεις για να βρουν έναν κεντρικό υπολογιστή σύνδεσης.

Ο αριθμός logons που μπορεί να διαχειριστεί ένας κεντρικός υπολογιστής εξαρτάται από την πολυπλοκότητα του υλικού του, φυσικά, αλλά οι παλαιοί κανόνες των Windows NT είναι καλά πρότυπα για να χρησιμοποιηθούν όπου εκεί πρέπει(κατά προσέγγιση) να είναι ένας domain controller ανά 2500 χρήστες (dedicated). Σε όλες τις περιπτώσεις, προτείνεται ότι ένας δευτεροβάθμιος domain controller υπάρχει για να περιέχει το αντίγραφο του καταλόγου αρχείων της βάσης δεδομένων του κεντρικού υπολογιστή της ρίζας.

2.5 Βήμα Προς Βήμα Εγκατάσταση Των Replica Domain Controllers

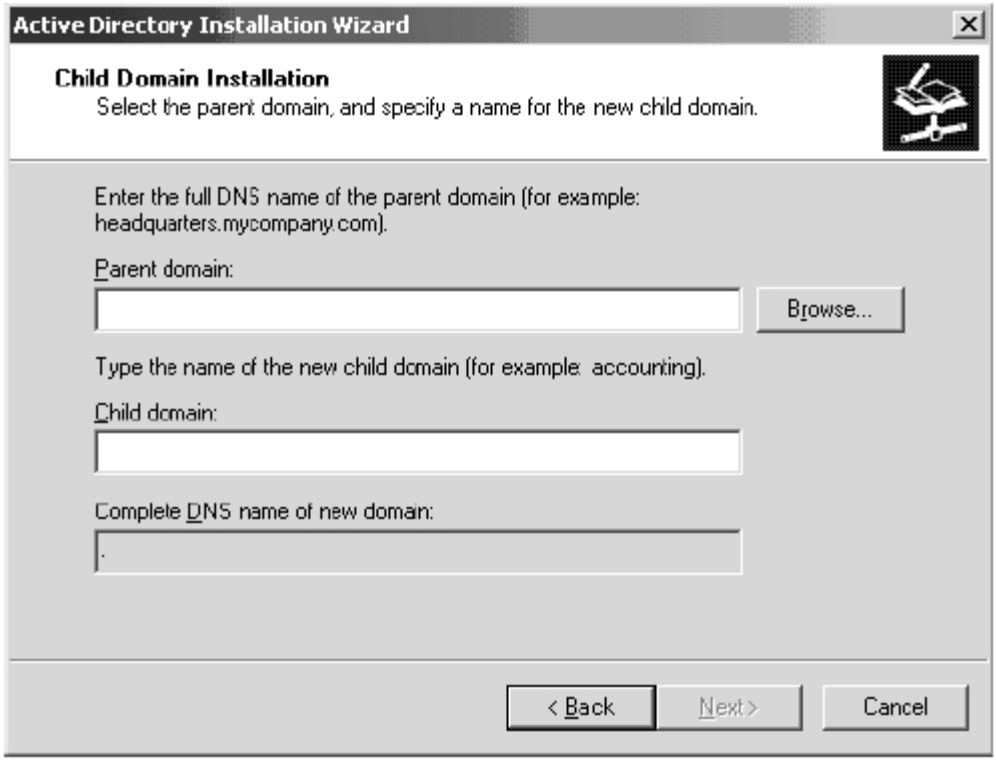
Η εγκατάσταση των domain controllers αντιγράφου δεν απέχει τόσο πολύ από τη διαδικασία της εγκατάστασης του αρχικού domain controller. Η σύλληψη είναι ότι πρέπει έχουμε ένα λογαριασμό στο domain που να έχει την αρμοδιότητα να προσθέσει έναν κεντρικό υπολογιστή στο domain. Αυτός μπορεί να είναι ο λογαριασμός του administrator, εν τούτοις οποιοσδήποτε λογαριασμός με δικαιώματα administrator στο domain θα λειτουργήσει.

Από τον κεντρικό υπολογιστή που μετατρέπεται, τρέχουμε το βοήθημα DCPROMO για να αρχίσει ο βοηθός εγκατάστασης του Active Directory, και πατάμε επόμενο για να συνεχίσουμε στην οθόνη Domain Controller Type. Πατάμε στην επιλογή για πρόσθετο Domain Controller και πατάμε επόμενο όπως φαίνεται στο σχήμα 2.11.



Σχήμα 2.11

Θα χρειαστούμε το πλήρες dns όνομα για το domain στο οποίο θα συμμετάσχει ο domain controller. Αυτό πρέπει να είναι κάτι σαν το domain_name .COM. Αυτό εμφανίζεται στο σχήμα 2.12 χρησιμοποιώντας το technologic σαν παράδειγμα.



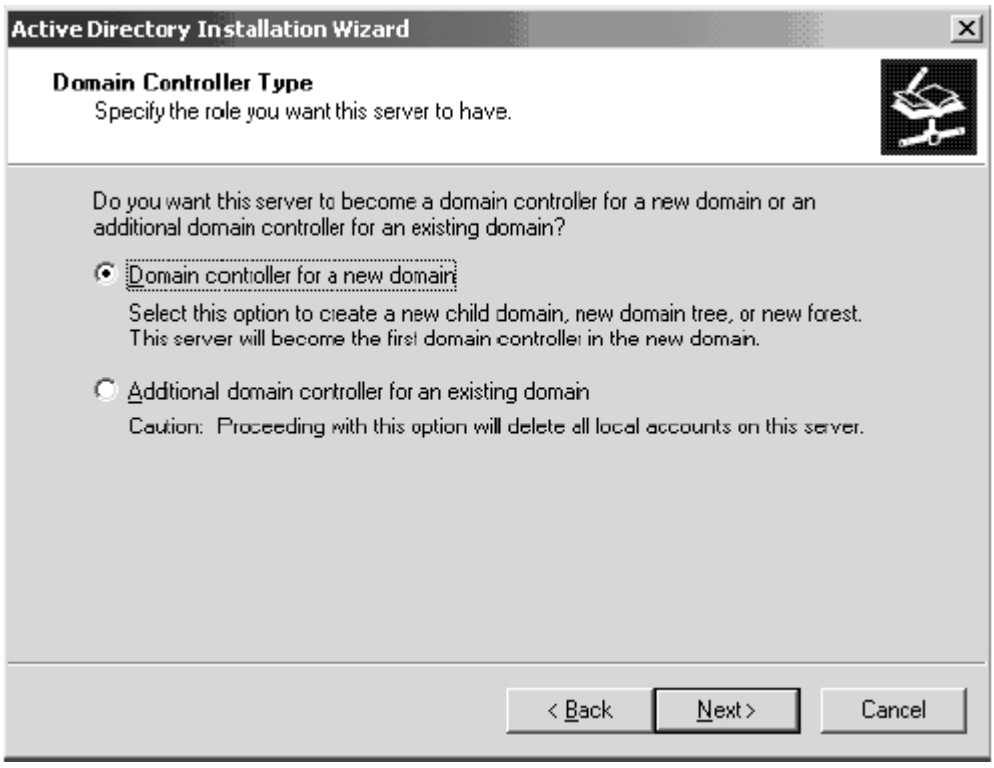
Σχήμα 2.12

Πατάμε επόμενο και εισάγουμε τα απαραίτητα διοικητικά πιστοποιητικά για να ενωθεί ο κεντρικός υπολογιστής στη δικτυακή γειτονιά και να συμμετέχει στον κατάλογο αρχείων. Οι ακόλουθες επιλογές είναι για τα μονοπάτια βάσεων δεδομένων και την επιβεβαίωση των επιλογών που γίνονται. Μόλις επικυρωθούν, ο βοηθός θα αρχίσει την εγκατάσταση των στοιχείων του καταλόγου αρχείων και έπειτα θα ζητήσει μια επανεκκίνηση.

2.6 Δημιουργώντας Child Domains Στην Ιεραρχία

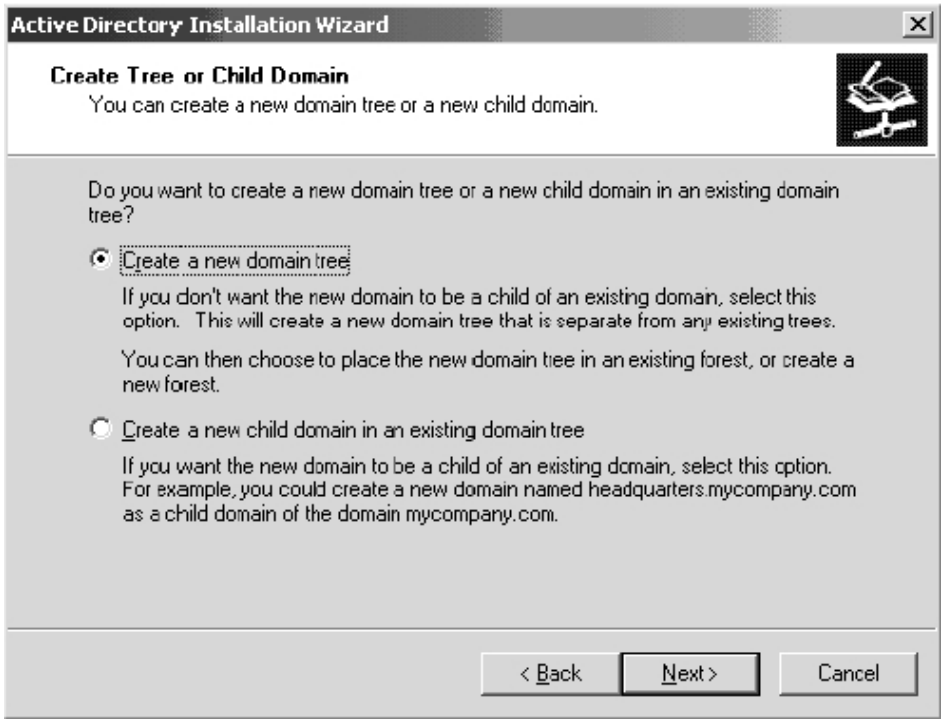
Μέχρι τώρα, η συζήτηση της δημιουργίας των domain controllers έχει λειτουργήσει μέσα στα όρια ενός ενιαίου domain. Προκειμένου να δημιουργηθούν first-level domains και να χτιστεί μια σύνθετη ιεραρχία για το Active Directory, τα child domains πρέπει να παραχθούν. Αυτό ολοκληρώνεται με τον ίδιο τρόπο με τις προηγούμενες εγκαταστάσεις, με μερικές συστροφές.

Αρχίζουμε με το τρέξιμο του βοηθού εγκατάστασης του Active Directory μέσω του DCPROMO. Στη σελίδα Domain Controller Type, επιλέξτε “Domain controller for a new domain” και πατάμε επόμενο όπως στο σχήμα 2.13.



Σχήμα 2.13

Στη σελίδα Create Tree or Child Domain, επιλέγουμε την επιλογή "Create a new child domain in an existing domain tree," έπειτα πατάμε επόμενο όπως στο σχήμα 2.14

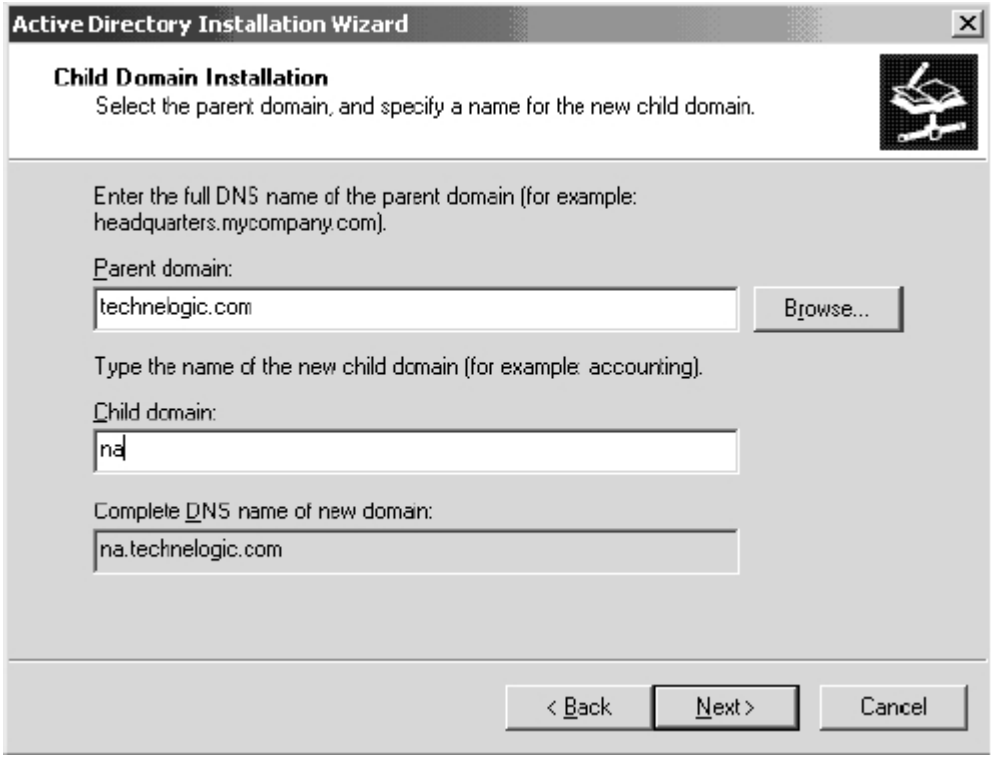


Σχήμα 2.14

Το επόμενο σύνολο επιλογών στο Child Domain Installation δεν έχει οριστεί ακόμα. Πατάμε στο κουμπί Browse αριστερά του παραθύρου κειμένου Parent domain για να ελέγξει για την ύπαρξη του domain στην οποία τοποθετούμε αυτό το domain. Το Parent domain πρέπει να εμφανιστεί σε ένα παράθυρο σαν αυτό που παρουσιάζεται στο σχήμα 2.15.

Σχήμα 2.15

Επιλέγουμε το Parent Domain και πατάμε OK. Το παράθυρο κειμένου του Parent Domain πρέπει τώρα να έχει το όνομα του Parent Domain που εμφανίζεται στη λίστα. Προσθέτουμε το όνομα από του Child Domain στο παράθυρο κειμένου Child Domain. Αυτό πρέπει να είναι γεωγραφική περιοχή εάν αυτό είναι ένα first-level Domain (που παρέχει το γεωπολιτικό το μοντέλο που χρησιμοποιείται). Διαπιστώνουμε ότι το όνομα του πλήρους dns ονόματος συμπληρώνεται παρακάτω για μας. Το σχήμα 2.16 εμφανίζει ένα παράδειγμα αυτού. Πατάμε επόμενο για να συνεχίσουμε.



Σχήμα 2.16

Επιλέγουμε το όνομα NetBIOS και επιλέγουμε τις διαδρομές των βάσεων δεδομένων και των αρχείων καταγραφής γεγονότων. Επιβεβαιώνουμε τις απαντήσεις και πατάμε επόμενο για να εγκαταστήσουμε το Active Directory.

2.7 Χρησιμοποιώντας τα Εργαλεία Διαχείρισης του Active Directory

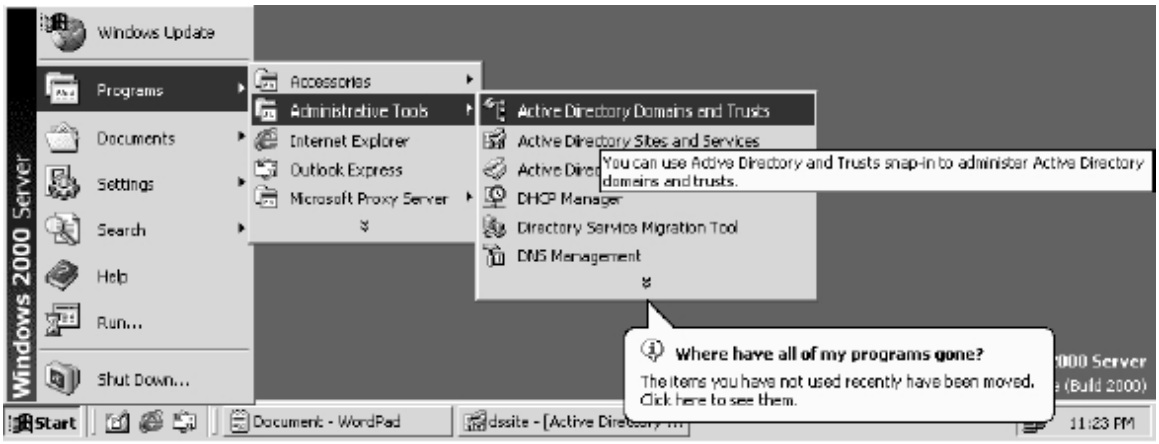
Τώρα που η επιχείρηση διαμορφώνεται και τα Child Domains είναι σε ισχύ, είναι ώρα να αναφερθώ στα εργαλεία διαχείρισης των Windows 2003 που χρησιμοποιούνται στο συντονισμό, διαμόρφωση, και διαχείριση του καταλόγου αρχείων και τα αντικείμενα του καταλόγου αρχείων. Αυτά τα εργαλεία είναι σχετικά σε αυτήν την συμβολή ως δημιουργία των αντικειμένων καταλόγου αρχείων όπως οι λογαριασμοί χρηστών και, το πιο σημαντικό, οι Organizational Units (OUs) πρέπει να πραγματοποιηθούν στην περαιτέρω κατασκευή του δικτύου. Όπως πάντα, έχουμε το κείμενο προσχεδιασμού σε ετοιμότητα σαν αναφορά πριν συνεχίσουμε.

Υπάρχουν διάφορα εργαλεία διαχείρισης που παρέχονται ως κονσόλες MMC που χρησιμοποιούνται στην καθημερινή επιτήρηση του καταλόγου αρχείων:

- Το εργαλείο Active Directory Domains and Trusts (ADDT)
- Το εργαλείο Directory Sites and Services (ADSS)
- Το εργαλείο Directory Users and Computers (ADUC)

Επιπλέον, πρέπει να έχουμε μια καλή γνώση της κονσόλας dns προκειμένου να ελεγχθούν τα αρχεία των στοιχείων συμπεριφοράς (RRs) στην περίπτωση των αποτυχιών.

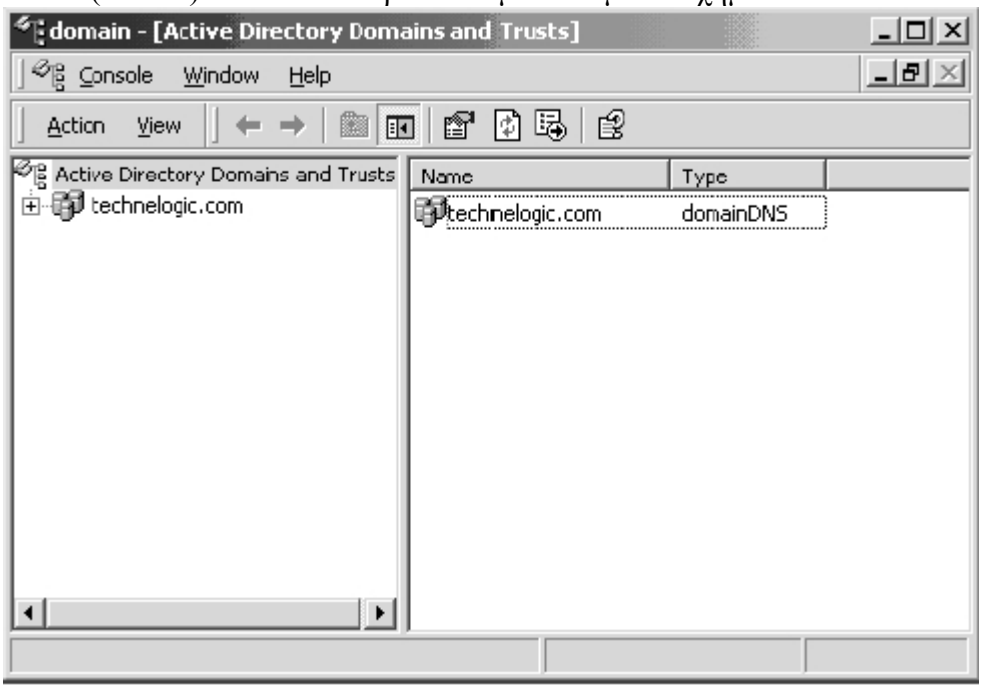
Τα εργαλεία υπηρεσιών καταλόγου αρχείων βρίσκονται από το Start, Programs και έπειτα κάτω από το Administrative Tools παρόμοια με το σχήμα 2.17. Παρατηρούμε και τα τρία από τα εργαλεία αναφερθέντα.



Σχήμα 2.17

Τεχνικά, υπάρχουν άλλα εργαλεία που χρησιμοποιούνται για να διαχειρίζονται υπηρεσίες καταλόγου αρχείων. Οποιοδήποτε εργαλείο που χρησιμοποιείται για να χειριστεί τα αντικείμενα μέσα στον κατάλογο αρχείων είναι κατάλληλο ως εργαλείο διαχείρισης καταλόγου αρχείων. Εντούτοις, προκειμένου να εστιάσουμε σε υψηλού επιπέδου διαχείριση καταλόγου αρχείων και για να περιοριστεί η σύγχυση στο ελάχιστο, με αυτά τα πρώτα τρία εργαλεία θα ασχοληθούμε.

Αρχίζοντας με το άνοιγμα της κονσόλας του Active Directory Domains and Trusts (ADDT). Η κονσόλα πρέπει να μοιάσει με το σχήμα 2.18.



Σχήμα 2.18

Σε κάθε περίπτωση συζήτησης του συνόλου εργαλείων του Active Directory, καλύπτουμε αρχικά τι είναι τα αντικείμενα της κονσόλα, ακολουθούμενα από έναν λειτουργικό γύρο. Πρέπει να έχουμε δικαιοδοσίες πρόσβασης να προσεγγιστούν αυτά τα εργαλεία.

2.8 Η Κονσόλα Active Directory Domains and Trusts

Η κονσόλα ADDT παρέχει το interface στον χρήστη από το οποίο ρυθμίζονται τα παρακλάδια των δέντρων. Το εργαλείο παρέχει έναν μηχανισμό για να διαχειριστεί κάθε Domain στο Active Directory από ένα απλό σημείο. Οι λειτουργίες που εκτελούνται από το εργαλείο ADDT είναι υψηλού επιπέδου διαχειριστικές στοιχειώδεις εργασίες, όπως η διαχείριση των σχέσεων εμπιστοσύνης, η παραμετροποίηση του τρόπου λειτουργίας των κεντρικών υπολογιστών (μικτός τρόπος ή εγγενής τρόπος), η αλλαγή του ρόλου ενός Domain Controller για να λειτουργεί σαν Operations Master, και προσθέτοντας τα επιθήματα UPN για τη χρήση σε ένα δάσος.
Το σχήμα 2.18 εμφανίζει την κονσόλα ADDT με το πλαίσιο διατομής που συμπεριλαμβάνει το αντικείμενο του καταλόγου ρίζας και το παιδί αντικειμένου. Τα αντικείμενα που αντιπροσωπεύονται εδώ είναι φυσικά αντικείμενα από domains που αποτελούν τον κατάλογο αρχείων. Παρατηρούμε το σχέδιο με το domain ρίζας που βρίσκεται στην κορυφή του δέντρου και του first-level child domains που αντιπροσωπεύουν τις γεωγραφικές περιοχές κάτω. Το πλαίσιο διατομής είναι η βασική εστίαση της κονσόλας ADDT, και το πλαίσιο αποτελεσμάτων παρουσιάζει ελάχιστες ή καμία πληροφορία. Ο χειρισμός αντικειμένου, όπως στα περισσότερα εργαλεία κονσόλων, επιτυγχάνεται μέσω της λειτουργίας δεξί-κλικ και των επιλογών των προκυπτουσών μενού. Ας κάνουμε δεξί κλικ στο αντικείμενο ρίζας για να βρούμε τις ακόλουθες επιλογές:

- Διαχείριση
- Όψη
- Νέο παράθυρο από εδώ
- Κατάλογος εξαγωγής...
- Ιδιότητες
- Οδηγίες

Οι δύο σημαντικές επιλογές του μενού είναι το Manage και το Properties. Κάνοντας κλικ στο αντικείμενο Manage ενός επιλεγμένου αντικειμένου ενός domain ενεργοποιείται η κονσόλα Active Directory Users and Computers για αυτό το domain. Στο μενού, το αντικείμενο Properties χρησιμοποιείται για να διαμορφώσει τον τρόπο η το domain και διαχειρίζεται τις σχέσεις εμπιστοσύνης. Υπάρχουν τρεις ετικέτες στη σελίδα ιδιοτήτων:

- General
- Trusts
- Managed By

Η ετικέτα General εμφανίζει το όνομα του down-level domain και έχει μια θέση για να εισάγουμε μια περιγραφή του ίδιου του domain. Κάτω από αυτές τις επιλογές είναι η επιλογή Change Domain Modes.

Η λειτουργία Mixed-Mode domain επιτρέπει στους down-level domain controllers σε WINDOWS NT να υπάρχουν στο domain και να επικυρώνουν τα logons των χρηστών. Ο μικτός τρόπος (mixed mode) είναι ο προκαθορισμένος τρόπος στην εγκατάσταση, η μεταπήδηση στο native mode πρέπει να είναι μια συνειδητή απόφαση. Εάν η εγκατάσταση των Windows 2003 ξεκινάει από την αρχή, και δεν υπάρχει κανένα κληρονομικό domain ή ζητήματα που θα συνυπάρξουν, τότε η μετατροπή σε native mode είναι απόλυτα αποδεκτή. Πρέπει να σημειωθεί ότι αυτή η αλλαγή είναι μη αναστρέψιμη, έτσι η απόφαση πρέπει να έχει ερευνηθεί πριν από το πάτημα του διακόπτη.

Η ετικέτα Trusts εμφανίζει τις πληροφορίες εμπιστοσύνης (εάν περισσότερα από ένα domain υπάρχει στο δέντρο) και επιτρέπει την προσθήκη ή την αφαίρεση σχέσεων εμπιστοσύνης. Οι εμπιστοσύνες Kerberos χτίζονται αυτόματα μεταξύ του parent και του child domains επάνω στη δημιουργία της δομής δέντρων. Η σχέση εμφανίζεται στην οθόνη. Είναι δυνατό να δημιουργηθούν οι παράλληλες εμπιστοσύνες ή "συντομεύσεις" για εμπιστοσύνες μεταξύ όμοιων domains δηλαδή domains που είναι στο ίδιο επίπεδο. Αυτή η ενέργεια μπορεί να χρησιμοποιηθεί για να επιταχύνει τα κανάλια πιστοποίησης ταυτότητας μεταξύ των domains αντί της χρησιμοποίησης της μεταβατικής εμπιστοσύνης για την επικύρωση χρηστών ή υπηρεσιών στα αντικείμενα, αν και αυτό μπορεί να μην είναι απαραίτητο σε πολλές εφαρμογές.

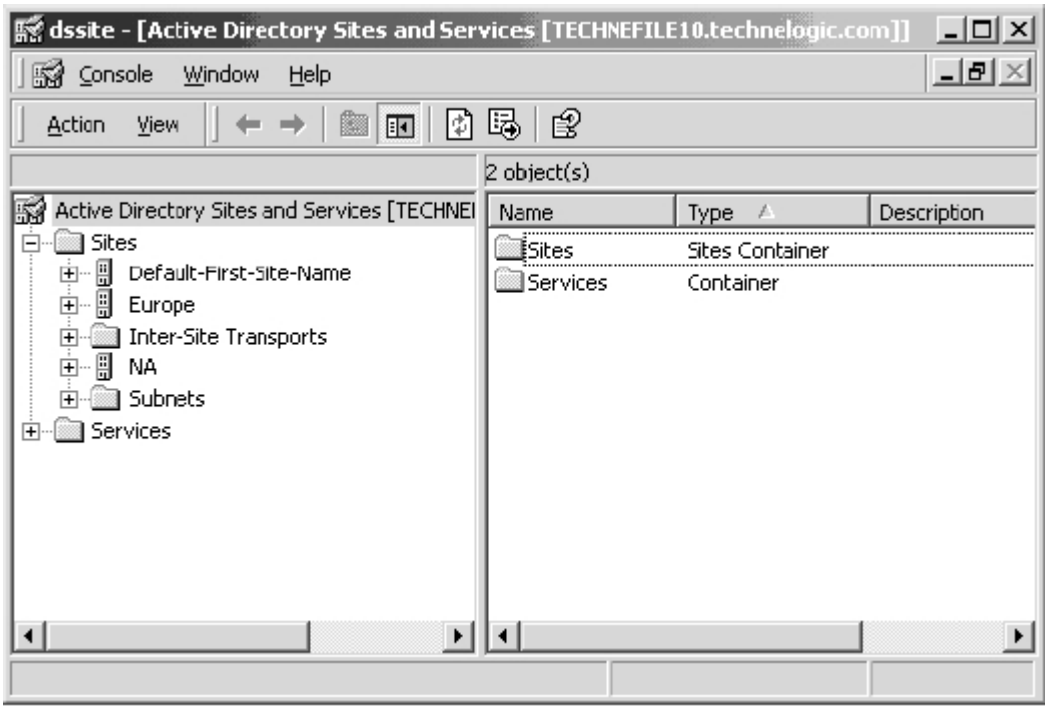
Η τελευταία ετικέτα είναι μια ετικέτα πληροφοριών που προσφέρει την είσοδο για το συμβαλλόμενο μέρος της διαχείριση του domain. Η είσοδος στην ομάδα των top – level Domain Administrators επιτρέπει στους root administrators να διαχειριστούν αυτό το domain. Η ομάδα ή το πρόσωπο που εισάγεται εδώ θα εξαρτηθεί από τη δομή της ιεραρχίας και το διοικητικό μοντέλο που χρησιμοποιείται.

2.9 Η Κονσόλα Active Directory Sites and Services

Η διαμόρφωση των σελίδων και των υποδικτύων είναι ένα αναπόσπαστο κομμάτι από την συνολική στρατηγική του domain. Το εργαλείο Active Directory Sites and Services (ADSS) επιτρέπει την δημιουργία σελίδων και υποδικτύων για την παραμετροποίηση του domain replication. Το πλαίσιο διαλόγου περιέχει τα παρακάτω αντικείμενα:

- Sites
- Inter-Site Transports
- Services

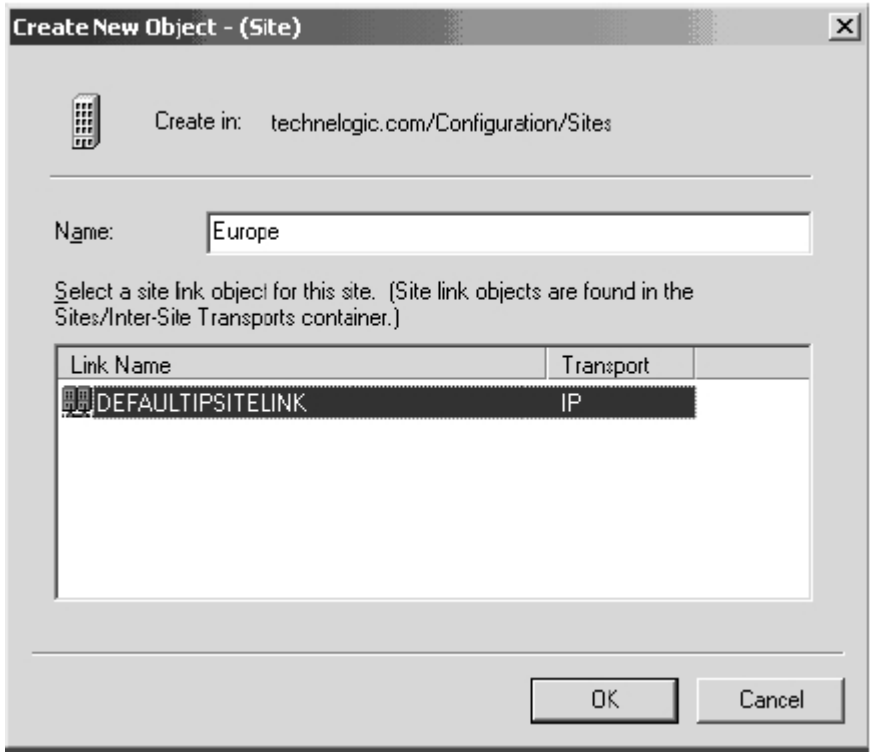
Το σχήμα 2.19 εμφανίζει την κονσόλα ADSS με κάθε ένα από τα αντικείμενα που επεκτείνονται στην περαιτέρω παρουσίαση των αντικείμενα child που περιλαμβάνονται. Αντίθετα με την κονσόλα ADDT, το πλαίσιο αποτελεσμάτων παρέχει συμπληρωματικές πληροφορίες των αντικειμένων κονσόλων.



Σχήμα 2.19

Το αντικείμενο Sites φιλοξενεί όλες τα sitesπου δημιουργούνται αυτόματα ή με την επέμβαση χρηστών. Το βασικό ενδιαφέρον του μενού του δεξιού κλικ στο επίπεδο του Site folder είναι το New Site, το όποιο είναι το εργαλείο που χρησιμοποιείται για τη δημιουργία Sites για να ελέγξει την κυκλοφορία των domain controller replication. Στο παράδειγμα του Technologic , έχει δημιουργηθεί ένα domain από την επιχείρηση που αντιπροσωπεύει τον ευρωπαϊκό κλάδο. Η φυσική θέση αυτών των κεντρικών υπολογιστών είναι συνδεμένοι με το root domain μέσω μιας σύνδεσης T1, η οποία για το μέγεθος του domain και όλους τους χρήστες μπορεί να προτρέψει ενέργεια για να δημιουργηθεί ένα χωριστό site για να ελέγχει την κυκλοφορία του replication πέρα από την WAN σύνδεση. Τα ακόλουθα περιγράμματα δείχνουν πώς αυτό είναι πραγματοποιείται.

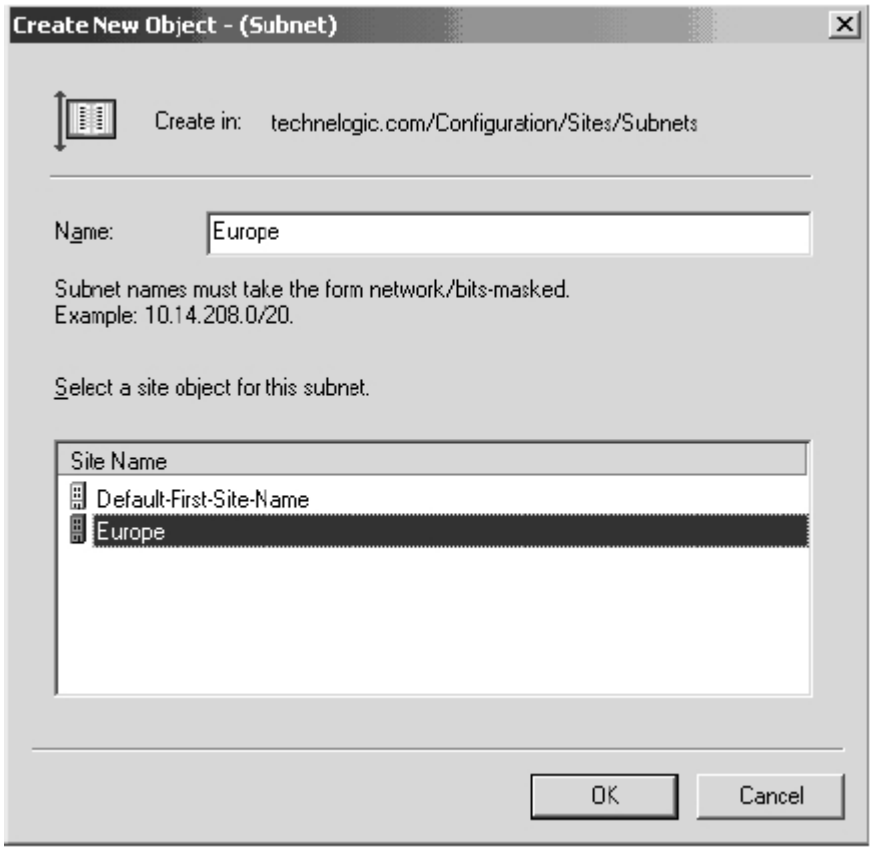
Για την δημιουργία ενός νέου site, κάνουμε δεξί κλικ στον κατάλογο Sites και κάνουμε κλικ στο New Site. Στο παράθυρο Create New Object-(Site), εισάγουμε το όνομα του νέου site όπως παρουσιάζεται στο σχήμα 2.20.



Σχήμα 2.20

Επιλέγουμε ένα αντικείμενο συνδέσεων περιοχών (Site Link Object) στο πλαίσιο και πατάμε OK για να συνεχίσουμε. Η πρόσφατα δημιουργημένη περιοχή εμφανίζεται στο πλαίσιο αποτελεσμάτων κάτω από τον κατάλογο Site parent. Τώρα για να δημιουργήσουμε ένα υποδίκτυο για το νέο site.

Μόλις δημιουργηθεί το site, ένα υποδίκτυο ή πολλαπλάσια υποδίκτυα πρέπει να συνδεθούν σε αυτό. Κάνουμε δεξί κλικ στον κατάλογο Subnet και επιλέγουμε το New Subnet. Συμπληρώνουμε το όνομα του υποδικτύου, στο όποιο είναι το προσδιοριστικό network/bit-masked, όπως φαίνεται στο σχήμα 2.21.

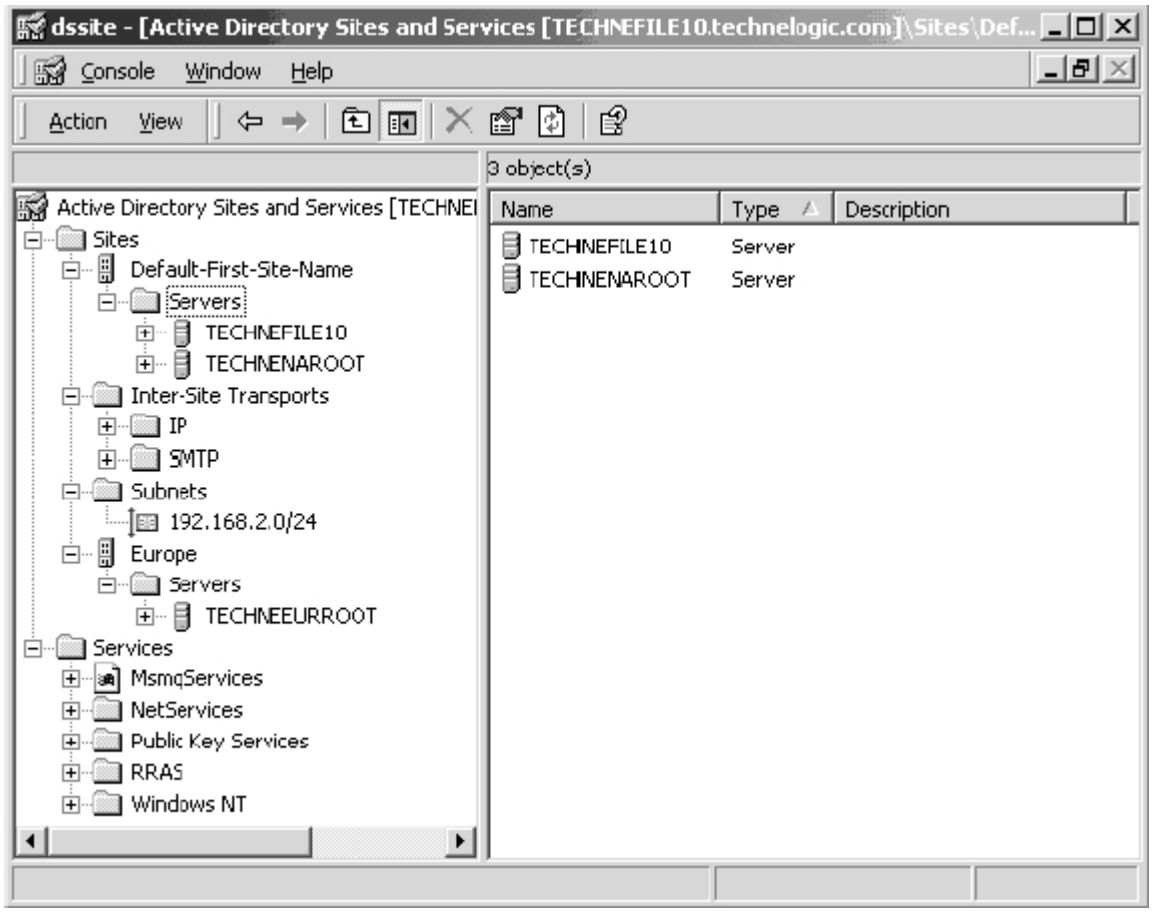


Σχήμα 2.21

Αυτή είναι η διεύθυνση δικτύου του υποδικτύου και ο αριθμός δυαδικών ψηφίων στη μάσκα δικτύου. Η χρήση είναι εδώ ως εξής:
<network address>/<bits masked> ή192.168.5.0/24 που αντιπροσωπεύει το υποδίκτυο 192.168.5.χ κλάσης C με τα πρώτα τρία octets να είναι masked.

Πατάμε OK για να συνεχίσουμε. Το νέο υποδίκτυο εμφανίζεται στο πλαίσιο αποτελεσμάτων.

Το επόμενο και τελικό βήμα είναι να κινηθεί το domain σε ένα πρόσφατα δημιουργημένο αντικείμενο περιοχών (site object). Κάνουμε δεξί κλικ στο domain που πρόκειται να μετακινηθεί και επιλέγουμε το Move. Το ακόλουθο παράθυρο εμφανίζει έναν κατάλογο από sites για να επιλέξουμε. Αυτή η διαδικασία εμφανίζεται στα σχήματα 2.22 και 2.23.



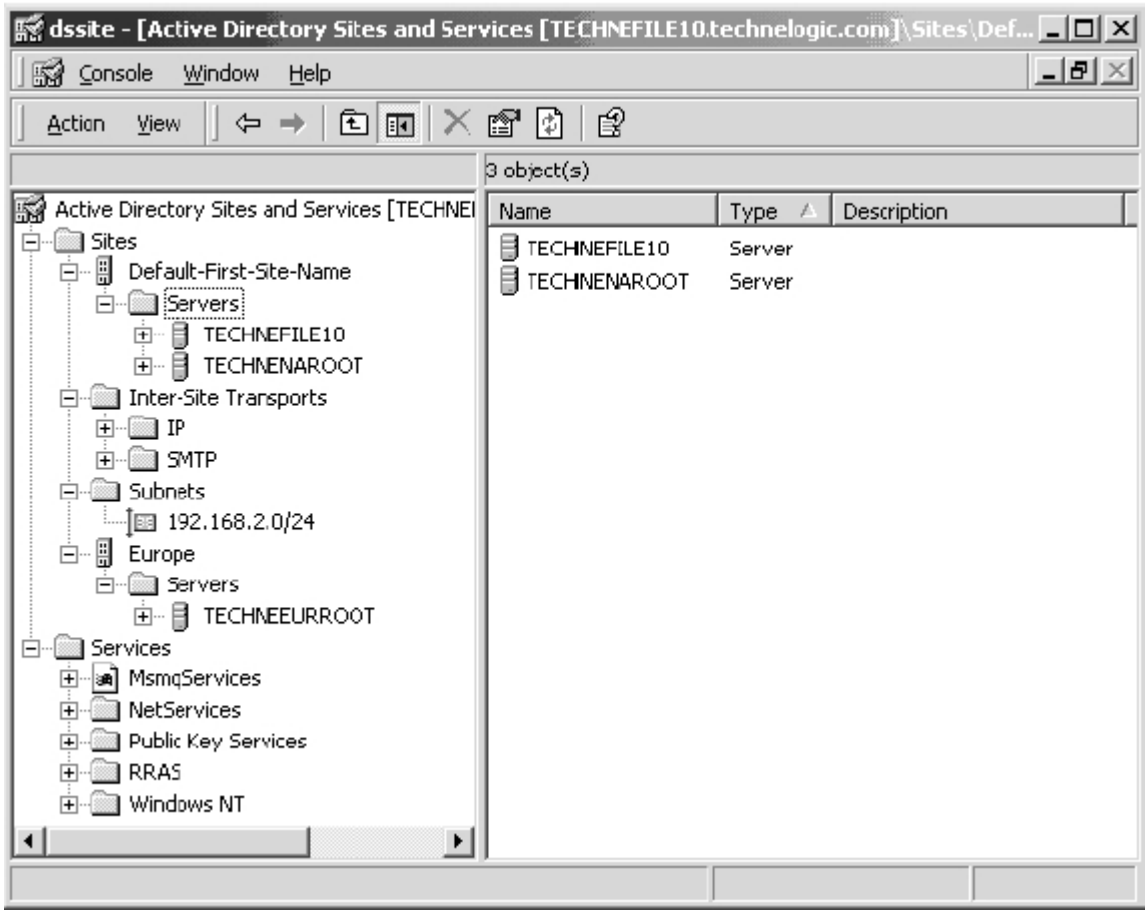
Σχήμα 2.22

Στο παραδειγματικό μας δίκτυο, το domain Technenaroot μετακινείται προς το πρόσφατα δημιουργημένο site της Ευρώπης. Επιλέγουμε το site και πατάμε OK για να συνεχίσουμε.

Το νέο site έχει δημιουργηθεί και οι πόροι καταμερίσθηκαν. Το Site replication μεταξύ των sites δεν είναι αυτόματο ως εκ τούτου, θα υπερνικούσε το σκοπό της δημιουργίας όλων μαζί των sites, η όποια είναι να ελέγχεται η κυκλοφορία του replication πέρα από τα links ευρείας περιοχής. Λογικά, το επόμενο βήμα είναι να εγκαθιδρυθεί ένα Site Link Connector έτσι ώστε τις πληροφορίες καταλόγου αρχείων να μπορούν να περάσουν μεταξύ των πρόσφατα δημιουργημένων sites και να καταλήξουν μέσα στους domain controllers. Μόλις δημιουργηθεί, μπορούν να οριστούν τα χρονοδιαγράμματα του replication του Site Connector.

Για να δημιουργήσουμε ένα Site Connector, αρχικά επεκτείνουμε τον κατάλογο Inter-Site Transports για να αποκαλυφθούν οι υποκατάλογοι IP και SMTP. Οι πληροφορίες καταλόγου μπορούν να περάσουν δια μέσου οποιουδήποτε πρωτοκόλλου μεταφορών.

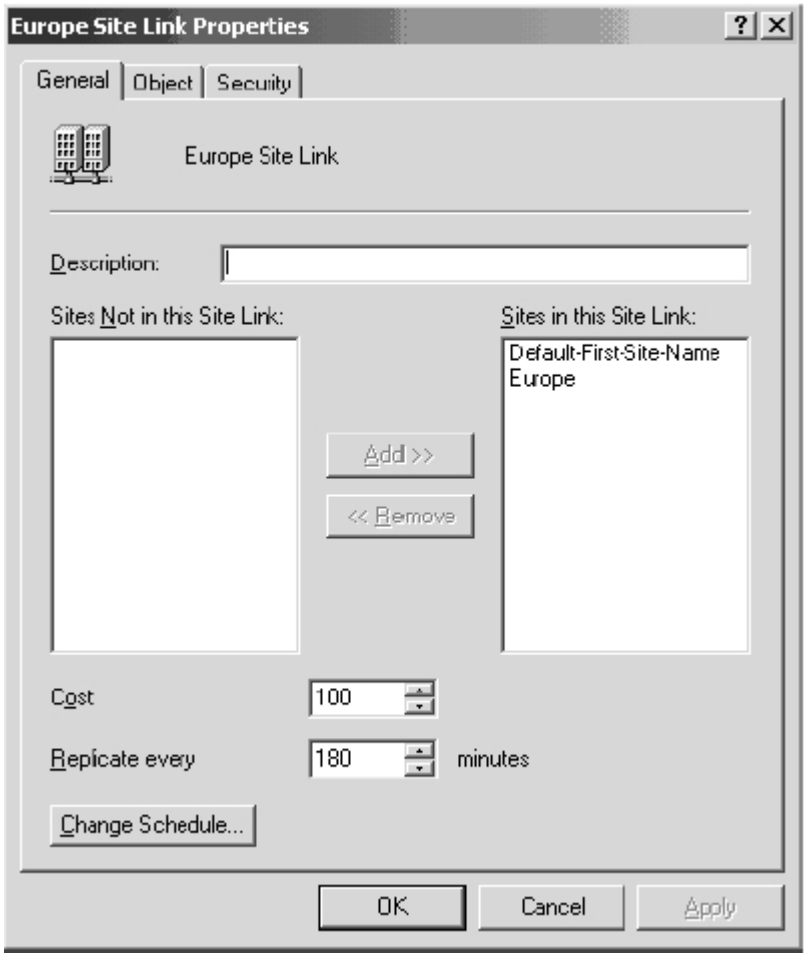
Κάνοντας δεξί κλικ στον κατάλογο IP και επιλέγοντας New Site Link όπως φαίνεται στο σχήμα 2.23.



Σχήμα 2.23

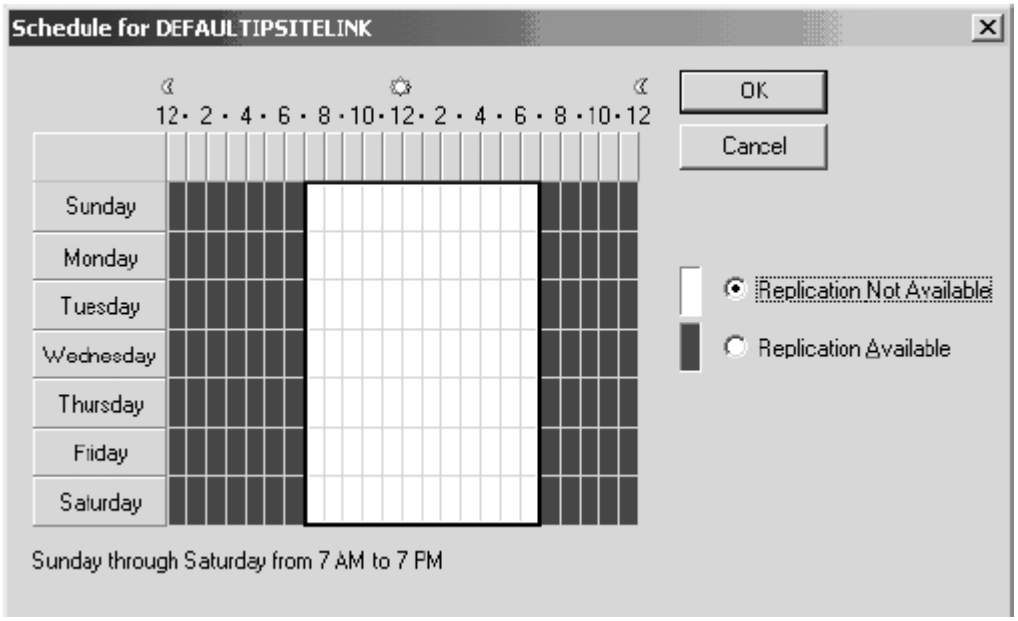
Αυτό ανοίγει το παράθυρο Create New Object-(Site Link) όπου επιλέγονται δύο αντικείμενα περιοχών που συνδέονται. Στο παράδειγμά μας, η περιοχή της Ευρώπης και το Default First Site είναι τα αντικείμενα συνδέσεων, και δεδομένου ότι υπάρχει μόνο άλλο ένα site, η επιλογή γίνεται για μας εξ ορισμού. Πατάμε OK για να συνεχίσουμε. Το Site Link είναι τώρα σε ισχύ, και το replication θα εμφανιστεί. Ένα πρόγραμμα πρέπει να εφαρμοστεί προκειμένου να χειριστούμε πραγματικά την κυκλοφορία του replication.

Κάνουμε δεξί κλικ στο πρόσφατα δημιουργημένο Site Link και επιλέγουμε τις ιδιότητες για το αντικείμενο. Η σελίδα Site Link Properties παρουσιάζεται με δυνατότητα να αλλάξουν οι παράμετροι συνεργατών του replication, σχεδιάζοντας τη συχνότητα του replication, και αλλάζοντας την ώρα και ημέρα της εβδομάδας. Το σχήμα 2.24 εμφανίζει τις ιδιότητες για τη σύνδεση περιοχών της Ευρώπης του παραδείγματος εταιριών Technologic.



Σχήμα 2.24

Ρυθμίζουμε τη συχνότητα του replication ανάλογα με τις ανάγκες και αναθέτουμε ένα κόστος στον σύνδεσμο εάν υπάρχουν περισσότεροι από ένα σύνδεσμοι ή μονοπάτια για replication. Για να αλλάξει η ώρα και η ημέρα του εβδομαδιαίου προγραμματισμού, πατάμε το κουμπί Change Schedule για να εμφανίζουμε το ημερολόγιο όπως εμφανίζεται στο σχήμα 2.25.

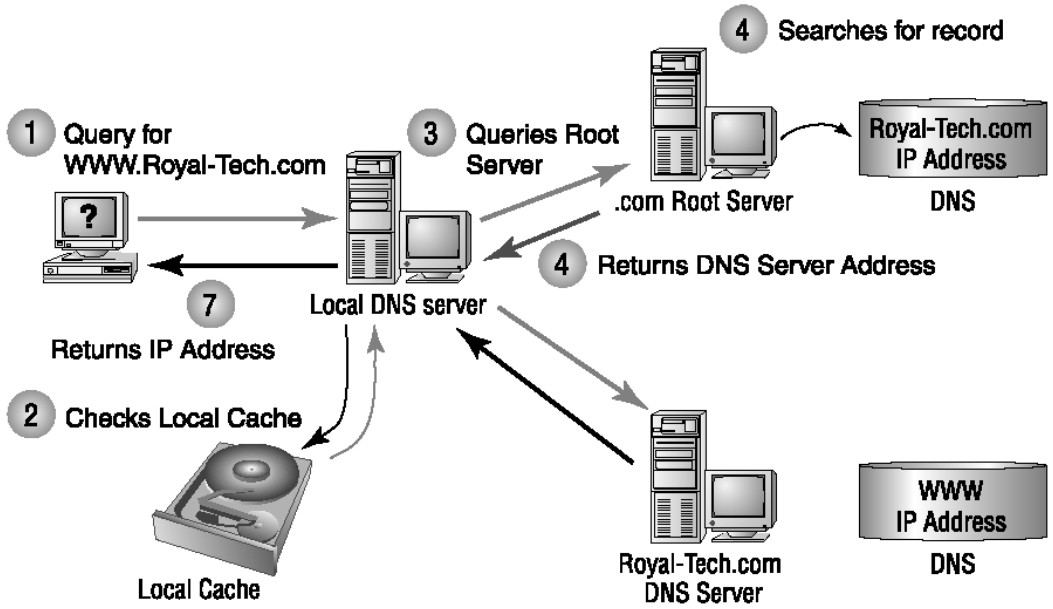


Σχήμα 2.25

Δίνουμε έμφαση στις μερίδες του ημερολογίου στις οποίες θέλουμε να απαγορεύσουμε το replication και πατάμε στο κουμπί Replication Not Available για να αλλάξει την παράμετρο.

Στο παράδειγμα Technelogic, το replication καταλόγου αρχείων πρέπει να επιτραπεί για να γίνει μόνο κατά τη διάρκεια των εκτός των ωρών αιχμής για να κρατήσει την κυκλοφορία χαμηλά στη σύνδεση T1. Δεδομένου ότι η άλλη περιοχή βρίσκεται σε μια χρονική ζώνη που έχουν κατά προσέγγιση έξι έως οκτώ ώρες διαφορά, υπάρχει ένα επικαλυπτόμενο χρονικό πλαίσιο όπου οι δύο περιοχές μπορούν να ανταλλάξουν ένα μεγάλο ποσό πληροφοριών (ώρες γραφείου). Κατά συνέπεια, το replication πρέπει να εμποδιστεί κατά τη διάρκεια αυτού του χρονικού πλαισίου για να ελαχιστοποιήσει σύγκρουση στο WAN link.

Η διαμόρφωση του site replication βοηθά να αποτραπούν οι αποτυχίες που προκαλούνται από υπερφορτωμένες συνδέσεις. Οι πληροφορίες καταλόγου αρχείων επιτρέπονται να περάσουν δια μέσου αφιερωμένων links τα οποία είναι τόσο μικρά όσο εκείνα που βρίσκονται σε αναλογικές γραμμές dial-on-demand διατηρώντας ένα συνεπές κατάλογο αρχείων σε όλη την ιεραρχία. Ο προγραμματισμός του site replication είναι το κλειδί στην υγεία του γενικού συστήματος και πρέπει να μελετηθεί προσεκτικά και με την ενίσχυση των υλικών προσχεδιασμού που έχουν αναπτυγθεί πριν από την εγκατάσταση.



Σχήμα 2.26

3. Κοινές Διαχειριστικές Εργασίες

Αυτό το κεφάλαιο εξετάζει μερικές χαρακτηριστικές διαχειριστικές εργασίες σχετικά με το Active Directory. Αυτοί οι στόχοι σε καμία περίπτωση δεν καλύπτουν όλες τις εργασίες που ένας διαχειριστής διεκπεραιώνει κάθε ημέρα.

Οι εργασίες που συζητούνται κατωτέρω εκτελούνται χρησιμοποιώντας διαχειριστικά snap-ins ή τα διαφορετικά εργαλεία από τα Windows .NET Support Tools

3.1 Χρησιμοποιώντας την Εντολή RunAs

Λόγω των απαιτήσεων ασφαλείας, δεν συνιστάται να συνδεόμαστε μόνιμα στο σύστημα (domain) με έναν λογαριασμό χρήστη που έχει πλήρη διαχειριστικά προνόμια. Τα Windows 2000/XP/NET προσφέρουν μια πολύ χρήσιμη εντολή, την RunAs. Αυτή η εντολή επιτρέπει σε έναν διαχειριστή συστημάτων να εκτελέσει τους κοινές εργασίες χρησιμοποιώντας έναν λογαριασμό με περιορισμένα (ή "κανονικού" χρήστη) δικαιώματα, και για να αρχίσει μια συγκεκριμένη εντολή εξ ονόματος ενός "power" user

(αυτό μπορεί να είναι ένας λογαριασμός διαχειριστή ή ένας λογαριασμός με μερικά πρόσθετα δικαιώματα). Κατά συνέπεια, δεν είναι απαραίτητη η επανειλημμένη επανασύνδεση στο σύστημα.

Ας εξετάσουμε πώς να χρησιμοποιήσουμε αυτήν την εντολή με τα διαχειριστικά snap-ins.

3.1.1 Λειτουργώντας τα Διαχειριστικά Εργαλεία (Administrative Tools) από τις Επιλογές Πλαισίου

Μπορείτε να επιλέξετε ένα διαχειριστικό εργαλείο με έναν από τους ακόλουθους τρόπους:

- Επιλέξτε το εργαλείο στο **Start | Programs | Administrative Tools**.
- Ανοίξτε το παράθυρο που περιέχει όλα τα εργαλεία. Επιλέξτε **Start | Programs | Administrative Tools** και επιλέξτε είτε **Open** ή **Open All Users** στις επιλογές πλαισίου. (Η προηγούμενη εντολή θα ανοίξει το παράθυρο που περιέχει μόνο τα εργαλεία που δημιουργούνται από το χρήστη, ενώ το τελευταίο ανοίγει το παράθυρο που περιέχει όλα τα εργαλεία εγκατεστημένα εξ ορισμού.) Επιλέξτε το εργαλείο στο ανοικτό παράθυρο.
- Αντιγράψτε τα εικονίδια (drag and drop) των απαραίτητων εργαλείων στην επιφάνεια εργασίας. (Μπορείτε επίσης να δημιουργήσετε έναν ή περισσότερους φακέλους στην επιφάνεια εργασίας, και αντιγράψτε τα εικονίδια σε αυτούς.)

Κατόπιν, για καθένα διαχειριστικό snap-in,, μπορείτε να ανοίξετε τις επιλογές πλαισίου και να επιλέξετε την εντολή **Run as**. (Υπάρχουν μερικοί περιορισμοί στους υπολογιστές που τρέχουν τα Windows 2000.) Θα δείτε ένα παράθυρο παρόμοιο με αυτό που παρουσιάζεται στην εικόνα. 3.1.

εικόνα. 3.1: Με την είσοδο των κατάλληλων πιστοποιητικών σε αυτό το παράθυρο, μπορείτε να αρχίσετε ένα πρόγραμμα εξ ονόματος ενός άλλου χρήστη

Ο ανώτερος διακόπτης (προεπιλογή) σας επιτρέπει να αρχίσετε το εργαλείο εξ ονόματος του τρέχοντος λογαριασμού σας (Π.χ., με τα τρέχοντα προνόμιά σας). Η άλλη επιλογή (εμφάνιση) – **τον ακόλουθο χρήστη** – σας επιτρέπει να εισάγετε τα διαχειριστικά διαπιστευτήρια, και να ξεκινήσετε το εργαλείο σε " προνομιούχα" κατάσταση.

Σημειώστε ότι η διαδικασία που περιγράφεται ανωτέρω μπορεί να χρησιμοποιηθεί με οποιοδήποτε EXE - ή Msc-αρχείο, και όχι μόνο με τα διαχειριστικά εργαλεία.

Επιπλέον, μπορείτε να ανοίξετε το παράθυρο ιδιοτήτων οποιουδήποτε διαχειριστικού εργαλείου, κάνοντας κλικ στην ετικέτα συντόμευση, και θέτοντας τη σημαία **Run with different credentials**. Αφού αυτή η λειτουργία εκτελεστεί, το σύστημα πάντα θα προτείνει ότι αρχίζετε το εργαλείο ως έναν άλλο χρήστη.

3.1.2 Ξεκινώντας Ένα Εργαλείο Από Την Γραμμή Εντολών

Χρησιμοποιώντας την εντολή RunAs, είναι δυνατό να αρχίσει οποιοδήποτε εκτελέσιμο αρχείο - EXE, COM, CMD, BAT, MSC συντομεύσεις για προγράμματα (LNK) και στοιχεία του πίνακα ελέγχου (CPL) - εξ ονόματος ενός διαφορετικού χρήστη. Ας δούμε μερικά παραδείγματα. (Μπορείτε να πάρετε πλήρεις πληροφορίες για το RunAs στο κέντρο βοήθειας και υποστήριξης ή τρέχοντας το runas /?)

Το RunAs δεν μπορεί να χρησιμοποιηθεί με μερικά στοιχεία, όπως ο Windows Explorer, ο φάκελος εκτυπωτών, και στοιχεία της επιφάνειας εργασίας.

Συνήθως, είναι καταλληλότερο να ξεκινήσουν τα εργαλεία MMC με RunAs από την γραμμή εντολών παρά από το παράθυρο **Run**, επειδή στην πρώτη περίπτωση, θα είστε σε θέση να δείτε τα πιθανά λάθη. Για τις συχνά χρησιμοποιημένες εντολές, μπορείτε να θελήσετε να δημιουργήσετε τους συντομεύσεις στην επιφάνεια εργασίας.

3.1.2.1 Παράδειγμα 1. Δουλεύοντας Στο Ίδιο Domain

Υποθέστε ότι συνδέεστε αυτήν την περίοδο στο *net.dom* domain με έναν "κανονικό" λογαριασμό χρήστη, και θέλετε να διαμορφώσετε τις ρυθμίσεις ασφάλειας του domain controller, ο όποιος απαιτεί τα διαχειριστικά δικαιώματα (δείτε τον πίνακα 3.1). Στο παράθυρο **Run** ή στην γραμμή εντολών εισάγετε την εντολή:

Πίνακας 3.1: Μερικά Διαχειριστικά Εργαλεία και τα Απαραίτητα Δικαιώματα για την Χρήση τους

Όνομα Εργαλείου	**Όνομα Snap-in**	**Απαραίτητα Δικαιώματα**
Active Directory Domains and Trusts	domain.msc	User

Πίνακας 3.1: Μερικά Διαχειριστικά Εργαλεία και τα Απαραίτητα Δικαιώματα για την Χρήση τους

Όνομα Εργαλείου	**Όνομα Snap-in**	**Απαραίτητα Δικαιώματα**
Active Directory Schema	*userCreatedName*.msc	User
Active Directory Sites and Services	dssite.msc	User
Active Directory Users and Computers	dsa.msc	User
Computer Management	compmgmt.msc	User
Distributed File System	dfsgui.msc	User
DNS	dnsmgmt.msc	User
Domain Controller Security Settings	dcpol.msc	Administrator
Domain Security Settings	dompol.msc	Administrator
Group Policy (see below)	gpedit.msc	Administrator
Local Security Settings	secpol.msc	Administrator
Routing and Remote Access	rrasmgmt.msc	Administrator
Services	services.msc	User
Snap-ins που δεν εμφανίζονται στο μενού *Administrative Tools*		
Device Manager	devmgmt.msc	User
Disk Management	diskmgmt.msc	User
Local Users and Groups	lusrmgr.msc	User
Shared Folders	fsmgmt.msc	Administrator

```
runas /user:administrator@net.dom "mmc dcpol.msc"
```

Ο διαχειριστής είναι το όνομα ενός χρήστη που είναι μέλος της ομάδας Domain Admins. Πληκτρολογείστε τον προσωπικό κωδικό του διαχειριστή όταν προτρέπεται

3.1.2.2 Παράδειγμα 2. Διαχειρίζοντας Ένα Αλλο Domain

Τώρα θέλετε να δημιουργήσετε έναν χρήστη στο domain *subdom.net.dom* που χρησιμοποιεί το snap-in **Active Directory Users and Computers** (Π.χ., θα επιθυμούσατε να εργαστείτε σε ένα domain, άλλο από το domain όπου συνδέεστε). Εισάγετε την ακόλουθη σειρά:

```
runas /netonly /user:SUBDOM\administrator "mmc dsa.msc"
```

Οπως μπορείτε να δείτε, είναι δυνατό να χρησιμοποιηθούν δύο σχήματα για την αντιπροσώπευση ενός λογαριασμού χρήστη: ένα σχήμα UPN, και ένα τυποποιημένο

σχήμα SAM - DOMAIN\USER. Και τα δύο σχήματα είναι αποδεκτά, αλλά στην τελευταία περίπτωση, πρέπει να χρησιμοποιήσετε το σχήμα SAM, ή το snap-in θα τρέχει για τον domain στο οποίο συνδέεστε αυτήν την περίοδο.

3.1.2.3 Παράδειγμα 3. Πιστοποιώντας Τα Δικαιώματα Χρήστη

Το RunAs μπορεί να είναι πολύ χρήσιμο για την οργάνωση των δικαιωμάτων των χρηστών σε ένα αρχείο ή σε αντικείμενα του Active Directory. Για να θέσετε τις απαραίτητες άδειες για έναν χρήστη, μπορείτε να αρχίσετε ένα εργαλείο χρησιμοποιώντας διαχειριστικά δικαιώματα. Συγχρόνως, είναι δυνατό να ανοιχτεί η γραμμή εντολών ή να αρχίσει ένα πρόγραμμα εξ ονόματος αυτού του χρήστη και να ελεγχθούν οι προκύπτουσες άδειες. Δεν χρειάζεστε είτε επανειλημμένα να συνδέεστε στο σύστημα χρησιμοποιώντας διαφορετικούς λογαριασμούς είτε να χρησιμοποιείτε διάφορους υπολογιστές

3.1.3 Ονόματα Αρχείων Των Διαχειριστικών Snap-ins

Για να χρησιμοποιήσετε τα διαχειριστικά εργαλεία με RunAs, πρέπει να ξέρετε τα ονόματα των αντίστοιχων snap-ins. Επίσης, μερικά εργαλεία μπορούν μόνο να χρησιμοποιηθούν με διαχειριστικά δικαιώματα. Ο πίνακας 3.1 περιέχει τις πληροφορίες για μερικά σημαντικά εργαλεία.

Όλα τα εγκατεστημένα snap-ins μπορούν να βρεθούν στον φάκελο %SystemRoot%/system32.

3.1.4 Τρέχοντας τον GPO Editor

Εξ ορισμού (όταν αρχίζει χωρίς οποιεσδήποτε παραμέτρους), το **Group Policy Object Editor** snap-in στρέφεται στο τοπικό GPO που αποθηκεύεται στον υπολογιστή. Γενικά, έχετε δύο επιλογές:

- Τρέξτε αυτό το snap-in με ένα προδιαμορφωμένο GPO. Μπορείτε να χρησιμοποιήσετε είτε το τυποποιημένο snap-in (gpedit.Msc, dompol.Msc, και dcpol.msc) ή διάφορες MMC κονσόλες με το **Group Policy Object Editor** snap-in
- Διευκρινίστε ένα GPO όταν το snap-in τρέχει.

Στην πρώτη περίπτωση, μπορείτε να δημιουργήσετε μια MMC κονσόλα, προσθέστε το **Group Policy Object Editor** snap-in σε αυτό, συνδέστε το snap-in με ένα απαραίτητο GPO (αποθηκευμένο σε έναν απομακρυσμένο υπολογιστή ή στο Active Directory), και σώστε την κονσόλα με οποιοδήποτε όνομα που θέλετε. Κατόπιν μπορείτε να αρχίσετε την κονσόλα από το όνομά της. Αυτό είναι η "στατική" προσέγγιση.

Με τη χρησιμοποίηση της δεύτερης μεθόδου, εκμεταλλεύεστε το γεγονός ότι το **Group Policy Object Editor** snap-in (το αρχείο gpedit.Msc) σας επιτρέπει να αλλάξετε την εστίασή του (η "δυναμική" προσέγγιση). Παραδείγματος χάριν, η ακόλουθη εντολή σας επιτρέπει να ανοίξετε ένα GPO που αποθηκεύεται σε έναν μακρινό υπολογιστή

(ακόμη και ο τοπικός υπολογιστής που διευκρινίζεται με την παράμετρο /gpcomputer θεωρείται "απομακρυσμένος"):

```
C:\>gpedit.msc /gpcomputer:"netdcl.net.dom"
```

Εσείς δεν μπορείτε να δείτε και να διαχειριστείτε την επέκταση τοποθετήσεων ασφάλειας (εκτός από τις πολιτικές ασφάλειας IP) του GPO ενός μακρινού υπολογιστή. Οι επεκτάσεις εγκατάστασης λογισμικού (Software Installation) και επαναπροσανατολισμού φακέλων (Folder Redirection)δεν επιδεικνύονται ποτέ για τοπικό GPOs.

Μπορείτε επίσης να τρέξετε το gpedit.msc και να διευκρινίσετε το διακεκριμένο όνομα οποιουδήποτε GPO που αποθηκεύεται στο Active Directory. Η ακόλουθη προσέγγιση θα βοηθήσει το χρήστη για να το κάνει αυτό αποτελεσματικότερα.

Στην γραμμή εντολών, διενεργήστε μια λειτουργία αναζήτησης με τη χρησιμοποίηση του script Search.vbs (Ldp.exe και DsQuery.exe μπορούν επίσης να χρησιμοποιηθούν) με τις παραμέτρους παρόμοιες με:

```
C:\>search "LDAP: //DC=net, DC=dom"
     /C: (objectCategory=GroupPolicyContainer)
     /S: subtree /P:AdsPath, displayName
```

Στην οθόνη θα δείτε την λίστα όλων των αποθηκευμένων GPOs στο domain, για παράδειγμα:

```
<LDAP://DC=net, DC=dom>; ((objectCategory=GroupPolicyContainer));
AdsPath,displayName;subtree
Finished the query.
Found 5 objects.
AdsPath 1 = LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},
  CN=Policies,CN=System,DC=net,DC=dom
displayName 1 = Default Domain Policy
AdsPath 2 = LDAP://CN={6AC1786C-016F-11D2-945F-00C04fB984F9},
  CN=Policies, CN=System, DC=net, DC=dom
displayName 2 = Default Domain Controllers Policy
...
```

Η εντολή DsQuery που εμφανίζεται παρακάτω θα παράγει το ίδιο αποτέλεσμα:

```
C:\>dsquery * -filter (objectCategory=GroupPolicyContainer) -attr
distinguishedName displayName
```

Μπορείτε εύκολα να επιλέξετε μια απαραίτητη πολιτική από το φιλικό όνομά της και να χρησιμοποιήσετε το DN της ως παράμετρο. Παραδείγματος χάριν, για να ανοίξει το *Default Domain Policy* που παρουσιάζεται ανωτέρω, χρησιμοποιήστε την ακόλουθη εντολή (τα εισαγωγικά είναι υποχρεωτικά):

```
C:\>gpedit.msc /gpobject:"LDAP://
     CN= {31B2F340-016D-11D2-945F-00C04FB984F9},
     CN=Policies, CN=System, DC=net, DC=dom"
Η εντολή που χρησιμοποιείται με το RunAs θα έχει την ακόλουθη σύνταξη:
   C:\>runas /user:net\administrator "mmc gpedit.msc
     /gpobject:\"LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},
```

```
CN=Policies, CN=System, DC=net, DC=dom\""
```

3.2 Διαχείριση Εξ΄Αποστάσεως

Για να διαχειριστείτε το Active Directory από έναν υπολογιστή πελάτη του domain, έχετε τις ακόλουθες τυποποιημένες επιλογές (η σειρά δεν είναι σημαντική):

- Οι τερματικές υπηρεσίες επιτρέπουν σε έναν διαχειριστή να εργαστεί σε έναν υπολογιστή πελατών με τον ίδιο τρόπο όπως μπορεί στην κονσόλα του domain controller. Αυτή είναι η μόνη τυποποιημένη επιλογή για τους υποβαθμισμένους υπολογιστές πελατών (Windows NT, Windows 9x) για να τρέξουν τα διαχειριστικά εργαλεία, και η μόνη επιλογή για τις αργόστροφες συνδέσεις (dial-up). Αν και πολλά διαχειριστικά εργαλεία γραμμής εντολών μπορούν να συνδεθούν άμεσα με τους μακρινούς υπολογιστές, θα χρειαστείτε τις τερματικές υπηρεσίες για να πάρετε την πλήρη λειτουργία της γραμμής εντολών σε ένα DC.

Στους υπολογιστές που είναι βασισμένοι στα Windows.NET, οι τερματικές υπηρεσίες εγκαθίστανται εξ ορισμού. Αυτοί οι υπολογιστές έχουν ένα ενσωματωμένο χαρακτηριστικό γνώρισμα, το *Remote Desktop*, που είναι ενεργοποιημένο στην ετικέτα **Remote** στο παράθυρο **System Properties** και παρέχει σε έναν διαχειριστή με single-user πρόσβαση στην επιφάνεια εργασίας του υπολογιστή.

- Το *Windows .NET Administration Tools Pack* περιέχει σχεδόν όλα τα διαχειριστικά snap-ins (δείτε τον πίνακα 3.2). Αυτό το πακέτο εγκαθίσταται από το αρχείο *%SystemRoot*%\system32\adminpak.msi διαθέσιμο σε κάθε domain controller βασισμένο σε Windows.NET. Μπορείτε να εγκαταστήσετε τα εργαλεία διαχείρισης σε οποιοδήποτε υπολογιστή με Windows XP/.NET, αλλά για να τα χρησιμοποιήσετε, πρέπει να συνδεθείτε ως χρήστης με διαχειριστικά δικαιώματα του domain.

Πίνακας 3.2: Τα Snap-ins που περιλαμβάνονται στο Windows.NET Administration Tools Pack

Active Directory Domains and Trusts	Internet Information Services
Active Directory Schema Manager	Network Load Balancing Manager
Active Directory Sites and Services	Remote Desktops
Active Directory Users and Computers	Remote Storage
Certification Authority	Routing and Remote Access
Cluster Administrator	Server Extensions Administrator
Connection Manger Administration Kit	Telephony
DHCP	Terminal Services Licensing
Distributed File System	Terminal Services Manager
DNS	WINS

Το Windows.NET Administration Tools Pack δεν μπορεί να εγκατασταθεί στους υπολογιστές που τρέχουν τα Windows 2000! Γενικά, τα εργαλεία διαχείρισης των Windows 2000 θα μπορούσαν να χρησιμοποιηθούν για τη διαχείριση των domains που είναι βασισμένα στα Windows.NET, εντούτοις, υπάρχουν μερικοί περιορισμοί σε εκείνη την περίπτωση. Μια καλύτερη επιλογή θα ήταν να εγκατασταθεί το Windows.NET Administration Tools Pack και να χρησιμοποιηθεί για τη διαχείριση των domain controllers που τρέχουν και σε Windows 2000 και σε Windows.NET συστήματα

- Μπορείτε με το χέρι να εγκαταστήσετε τα επιλεγμένα διαχειριστικά snap-ins σε έναν υπολογιστή πελάτη.

3.2.1 Εγκαθιστώντας τα Διαχειριστικά Snap-ins Επιλεκτικά

Για κάποιους λόγους, μπορεί να θελήσετε να εγκαταστήσετε μόνο ένα ή μερικά ξεχωριστά διαχειριστικά εργαλεία σε έναν υπολογιστή πελάτη αντί του ολόκληρου πακέτου εργαλείων διαχείρισης. Αυτό μπορεί να γίνει αρκετά εύκολα. (Αλλά μην ξεχάστε για τις απαιτήσεις ασφάλειας!) Θα πρέπει να πραγματοποιήσετε τα ακόλουθα βήματα:

1. Αντιγράψτε τα απαραίτητα snap-ins (αρχεία με την επέκταση MSC) από το φάκελο %SystemRoot%\system32 σε ένα DC σε οποιοδήποτε τοπικό φάκελο που επιθυμείτε.
2. Αντιγράψτε το κατάλληλο DLL(s) στο τοπικό φάκελο %SystemRoot%\system32 ή σε οποιοδήποτε τοπικό φάκελο.
3. Εάν το DLL έχει αντιγραφεί σε έναν φάκελο εκτός από SystemRoot%\system32, πρέπει πρώτα να αλλάξετε το φάκελο ανάλογα με τις ανάγκες. Για να καταχωρήσετε το DLL, εισάγετε την ακόλουθη σειρά στην γραμμή εντολών:
4. regsvr32 < DLLname >
5. Παραδείγματος χάριν, για να καταχωρήσετε το DLL για το snap-in **Active Directory Users and Computers**, εισάγετε το regsvr32 dsadmin.dll

Τώρα μπορείτε να δημιουργήσετε συντομεύσεις για νέα snap-ins, και έπειτα να τα τρέξετε. Φυσικά, πρέπει να συνδεθείτε στο domain με τα κατάλληλα (διαχειριστικά) προνόμια.

Πίνακας 3.3: περιέχει ονόματα DLL για κάποια διαχειριστικά snap-ins.

Όνομα εργαλείου	**Όνομα Snap-in**	**Όνομα DLL**
Active Directory Domain and Trusts	domain.msc	domadmin.dll
Active Directory Sites and Services	dssite.msc	dsadmin.dll
Active Directory Schema	*userCreatedName*.msc	schmmgmt.dll
Active Directory Users and Computers	dsa.msc	dsadmin.dll

Αφού το schmmgmt.dll έχει αντιγραφεί σε έναν τοπικό υπολογιστή, θα είστε σε θέση να προσθέσετε το snap-in σε οποιαδήποτε MMC κονσόλα (δεδομένου ότι δεν υπάρχει κανένα schema snap-in διαμορφωμένο εξ ορισμού).

Εξ ορισμού, το **Group Policy Object Editor** snap-in είναι παρών σε οποιονδήποτε υπολογιστή που τρέχει Windows 2000/XP/.NET. Επομένως, για να χρησιμοποιήσετε αυτό το εργαλείο και να το συνδέσετε με οποιοδήποτε domain GPO, πρέπει μόνο να έχετε τα προνόμια του διαχειριστή στο domain.

Παρατηρήστε ότι το **Active Directory Users and Computers** όπως και το **Active Directory Sites and Services** snap-ins χρησιμοποιούν το ίδιο dsadmin.dll αρχείο. Και τα δύο snap-ins παρέχουν πραγματικά παρόμοιες λειτουργίες (ιδιότητες φυλλομετρήματος και επέμβασης) με τα αντικείμενα καταλόγου. Το πρώτο σας επιτρέπει να εργαστείτε με ολόκληρο το χώρισμα ονομασίας περιοχών του Active Directory. Το τελευταίο παρέχει την πρόσβαση σε δύο containers στο χώρισμα ρυθμίσεων, δηλαδή *Sites* and *Services* (μπορείτε επίσης να τα δείτε με το **ADSI Edit** snap-in).

3.3 Ρωτώντας το Active Directory

Η ερώτηση είναι μια λειτουργία που χρησιμοποιείται συχνά στους καταλόγους δικτύων, και το Active Directory δεν είναι μια εξαίρεση. Το Active Directory μπορεί να περιέχει έναν τεράστιο αριθμό αντικειμένων, των οποίων οι ακριβείς θέσεις είναι συχνά άγνωστες. Η ερώτηση του καταλόγου είναι προτιμητέα παρά το ξεφύλλισμα του δέντρου του καταλόγου και για τους χρήστες και για τους διαχειριστές. Οι χρήστες των AD-based domains έχουν τα ακόλουθα εργαλεία (μερικά από αυτά είναι διαθέσιμα σε όλους τους πελάτες, συμπεριλαμβάνοντας υποδιέστερα συστήματα, και άλλα που λειτουργούν μόνο σε συστήματα Windows 2000/XP/.NET) τα οποία βοηθούν το χρήστη στην εύρεση ενός ή περισσότερων αντικειμένων στο Active Directory:

- Το χαρακτηριστικό της ενσωματωμένης αναζήτησης - ο καταλληλότερος τρόπος για έναν χρήστη να βρει έναν κοινό φάκελο ή έναν εκτυπωτή, χρήστη, ομάδα, ή άλλο κοινό αντικείμενο καταλόγου. Όλα τα άλλα εργαλεία προορίζονται για τους διαχειριστές.
- DsQuery.exe και Dsget.exe - τα τυποποιημένα εργαλεία αναζήτησης από γραμμή εντολών στα Windows.NET
- Το **ADSI Edit** snap-in (από τα εργαλεία υποστήριξης) - χρησιμοποιώντας αυτό το εργαλείο, ένας διαχειριστής μπορεί να δημιουργήσει ισχυρές ερωτήσεις και να τροποποιήσει αντικείμενα σε όλα τα χωρίσματα καταλόγου.
- Το script *Search.vbs* (από τα εργαλεία υποστήριξης) - το απλούστερο εργαλείο ερώτησης που χρησιμοποιεί το πρωτόκολλο LDAP. Μπορεί να χρησιμοποιηθεί σε οποιεσδήποτε πλατφόρμες Windows.
- Το *Active Directory Administration Tool* (Ldp.exe από τα εργαλεία υποστήριξης) και το *Active Directory Browser* (AdsVw.exe από το ADSI SDK) - περίπλοκα διαχειριστικά εργαλεία που επιτρέπουν επίσης σε έναν διαχειριστή να περιηγηθεί μέσα στο δέντρο του καταλόγου και να τροποποιήσει αντικείμενα. Το Ldp.exe χρησιμοποιεί το πρωτόκολλο LDAP και είναι το μόνο εργαλείο που μπορεί να ανακτήσει τα διαγραμμένα αντικείμενα. Το AdsVw.exe χρησιμοποιεί τα

πρωτόκολλα LDAP και WinNT, και λειτουργεί με AD-based (Windows 2000 and Windows .NET) και Window NT domains.

- Το εργαλείο Guid2obj.exe (από το *Windows 2000 Resource Kit*) - ένα εξειδικευμένο εργαλείο που μπορεί να καθορίσει το διακεκριμένο όνομα ενός αντικειμένου από το GUID του.

Τα περισσότερα από τα απαριθμημένα εργαλεία απαιτούν μια καλή κατανόηση της σύνταξης φίλτρων LDAP. Μόνο τότε θα είστε σε θέση γρήγορα και ακριβώς να βρείτε ή να επιλέξετε τα απαραίτητα αντικείμενα.

3.3.1 Παραμετροποιώντας την Επιλογή *Search* για τους Υπολογιστές Πελατών.

Εξ ορισμού, οι χρήστες - εκείνοι που γνωρίζουν αυτήν την επιλογή – μπορούν να ψάξουν το Active Directory για διάφορα αντικείμενα με τη χρήση της εντολής **Find** από τις επιλογές πλαισίου ενός domain που φαίνεται στο φάκελο **Directory** (στο **My Network Places**). Αυτή η επιλογή είναι διαθέσιμη στους υπολογιστές που τρέχουν τα Windows 2000 και έχει αφαιρεθεί από τα Windows XP/.NET. (Κάποιος μπορεί επίσης να χρησιμοποιήσει το **Active Directory Users and Computer** snap-in που είναι εγκατεστημένο σε έναν υπολογιστή πελάτη.) Υπάρχουν δύο ειδικευμένες εντολές που καλούνται από το μενού **Start | Search**: **For printers** και **For People**.

Είναι δυνατό να παρασχεθούν στους χρήστες τα ισχυρά χαρακτηριστικά γνωρίσματα αναζήτησης και να προστεθεί μια συντόμευση για αυτές τις διαδικασίες στην επιφάνεια εργασίας ή σε οποιοδήποτε φάκελο. Πρέπει να εκτελέσετε τα ακόλουθα βήματα:

1. Δεξί κλικ στην επιφάνεια εργασίας και επιλέξτε **New | Shortcut** από τις επιλογές του μενού.
2. Εισάγετε την ακόλουθη σειρά (διακρίνουσα κεφαλαία και μικρά!) στο **Type the location of the item**, και πατήστε **Επόμενο**:
3. rundll32.exe dsquery,OpenQueryWindow
4. Στο επόμενο παράθυρο, εισάγετε ένα όνομα για την συντόμευση και πατήστε στο **Τέλος**.
5. Επίσης μπορεί να επιθυμήσετε να κινήσετε την δημιουργημένη συντόμευση σε κάποιο φάκελο ή μενού.

Αφού κάνετε κλικ στην συντόμευση, ο χρήστης θα δει το παράθυρο αναζήτησης. Από εκείνο το παράθυρο, είναι δυνατό να βρεθούν οι χρήστες, επαφές, ομάδες, εκτυπωτές, OUs, κ.λπ....

3.4 Τροποποίηση Αντικειμένων Καταλόγου. Εξαγωγή και Εισαγωγή.

Υπάρχουν, στην πραγματικότητα, αρκετά διάφορα εργαλεία που επιτρέπουν σε έναν διαχειριστή να δημιουργήσει, διαγράψει, και να τροποποιήσει ένα ή περισσότερα αντικείμενα του Active Directory. Πρέπει να εξοικειωθείτε με όλα (ή τουλάχιστον τα περισσότερα) από αυτά για να είστε σε θέση να επιλέξετε το αποτελεσματικότερο εργαλείο για έναν συγκεκριμένο στόχο. Απαριθμίζονται όλες τις κύριες εγκαταστάσεις που παρέχονται στα Windows 2000 και στα Windows .NET:

- Τυποποιημένα snap-ins εγκατεστημένα εξ ορισμού - καθολικά εργαλεία GUI που λειτουργούν με ένα αντικείμενο μόνο, και στα Windows 2000, έχουν μέτρια υποστήριξη για τις λειτουργίες ομάδας.
    - Το **Active Directory Users and Computers** snap-in δημιουργεί χρήστες, επαφές, ομάδες, υπολογιστές, εκτυπωτές, κοινοί φάκελοι, και OUs.
    - Το **Active Directory Sites and Services** snap-in δημιουργεί περιοχές, υποδίκτυα, συνδέσεις, και συνδέσεις.
    - Το **Active Directory Domains and Trusts** snap-in δημιουργεί τις inter-Domain εμπιστοσύνες.
- Τυποποιημένες εφαρμογές γραμμής εντολών για τα Windows.NET που εκτελούν εξειδικευμένες εργασίες και μπορούν να χρησιμοποιηθούν για τη διαχείριση αντικειμένων του Active Directory από την γραμμή εντολών
    - DsAdd.exe δημιουργεί συγκεκριμένους τύπους αντικειμένων. DsMod.exe τροποποιεί τις ιδιότητες συγκεκριμένων τύπων αντικειμένου.
    - DsRm.exe αφαιρεί οποιαδήποτε αντικείμενα.
    - DsMove.exe κινεί οποιαδήποτε αντικείμενα προς ένα άλλο container καθώς επίσης και τα μετονομάζει.

Προσοχή στο γεγονός ότι το DsMod.exe μπορεί να διοχετεύσει αποτελέσματα από το DsQuery.exe, το όποιο ενισχύει σημαντικά την ευελιξία και την αποτελεσματικότητα της εφαρμογής.

- Εξειδικευμένα διαχειριστικά εργαλεία GUI που χρησιμοποιούνται για συγκεκριμένες διαδικασίες για ρύθμισμα και ανίχνευσης λαθών του Active Directory.
    - Το **Active Directory Schema** snap-in δημιουργεί τις ιδιότητες και τις κατηγορίες.
    - Το **ADSI Edit** snap-in, Ldp.exe και AdsVw.exe δημιουργούν αντικείμενα οποιουδήποτε τύπου (συμπεριλαμβανομένων των αντικειμένων που δεν μπορούν να δημιουργηθούν από οποιαδήποτε άλλα εργαλεία), αλλά είναι πρώτιστα χρήσιμα για τις αλλαγές ιδιοτήτων
- Εργαλεία για εισαγωγή/εξαγωγή – εργαλεία γραμμής εντολών που θα μπορούσαν (και πρέπει) να χρησιμεύσουν ως τα ισχυρά εργαλεία για τη διαχείριση μεγάλης κλίμακας εγκατάστασης του Active Directory. Το LDIFDE μπορεί επίσης να χρησιμοποιηθεί για την αλλαγή των ιδιοτήτων διάφορων παρόμοιων αντικειμένων. Στους υπολογιστές που τρέχουν τα Windows.NET, εφαρμογές από

την "οικογένεια" Ds*.exe μπορεί να είναι μια καλή επιλογή σε πολλές περιπτώσεις.
    - LDIFDE
    - CSVDE
- Εφαρμογές προοριζόμενες για τους συγκεκριμένους στόχους
    - AddUsers.exe, CreateUsers.vbs, και άλλα (π.χ., το NetDom.exe μπορεί να χρησιμοποιηθεί για τη δημιουργία των λογαριασμών μηχανών στα domains)
- ADSI scripts - ο πιο εύκαμπτος των επιλογών και, στην πραγματικότητα, ένας αρκετά απλός τρόπος να χειριστείτε τα αντικείμενα τουActive Directory (ειδικά για τους περιοδικούς στερεότυπους στόχους και όταν ένας μεγάλος αριθμός αντικειμένων πρόκειται να υποβληθεί σε επεξεργασία).

3.4.1 Χρησιμοποιώντας το *Active Directory Users and Computers* Snap-in

Το **Active Directory Users and Computers** snap-in είναι, ίσως, το κύριο εργαλείο που ένας διαχειριστής θα χρησιμοποιεί καθημερινά για να διαχειριστεί τους διάφορους πόρους του domain. Η διαδικασία της δημιουργίας και διαγραφής αντικειμένων του Active Directory είναι βασικά η ίδια για όλους τους τύπους αντικειμένων. Υπάρχουν κουμπιά στην τυποποιημένη γραμμή εργαλείων για μερικά από τα συνηθισμένα αντικείμενα:

- **Create a new user in the current container**
- **Create a new group in the current container**
- **Create a new organizational unit in the current container**

Μπορείτε να επιλέξετε ένα, αρκετά, ή όλα τα δημιουργημένα αντικείμενα και τα κινήσετε σε οποιοδήποτε container ή OU στο τρέχων domain. Όπως συνήθως στα Windows, χρησιμοποιήστε τα πλήκτρα < Shift > ή < CTRL > για την επιλογή των πολλαπλάσιων αντικειμένων.

Η έκδοση Windows.NET του **Active Directory Users and Computers** snap-in προσφέρει μερικές βελτιώσεις στην διεπαφή με τον χρήστη: μπορείτε να χρησιμοποιήσετε τις διαδικασίες drag-and-drop, και να τροποποιήσετε τις ιδιότητες διάφορων αντικειμένων που επιλέγονται.

Είναι δυνατό να επιλέξετε ένα λογαριασμό χρήστη ως πρότυπο, και να δημιουργήσετε χρήστες με τις ίδιες ιδιότητες (μέλη ομάδας, ρυθμίσεις προφίλ, κ.λπ....) Για να αρχίσει αυτή η διαδικασία, επιλέξτε έναν χρήστη "πρότυπο" και κάντε κλικ στο **Copy** στις επιλογές πλαισίου του.

3.4.2 Προσθέτωντας Χρήστες Και Ομάδες στο Domain

Υπάρχουν μερικές εφαρμογές (εκτός από τα εργαλεία εισαγωγών batch LDIFDE και τα CSVDE scripts) που απλοποιούν τη δημιουργία διάφορων λογαριασμών χρηστών σε έναν τομέα ή περιβάλλοντα δοκιμής.

3.4.3 Η Εφαρμογή Των Windows.NET — DsAdd

Μια ολοκαίνουργια εφαρμογή των Windows.NET, η DsAdd.exe, μπορεί να δημιουργήσει έναν ξεχωριστό υπολογιστή, επαφή, ομάδα, OU, και αντικείμενα χρηστών σε AD-based domains. Χρησιμοποιεί το πρωτόκολλο LDAP μόνο.

Με το DsAdd, μπορείτε να δημιουργήσετε μια τοπική, σφαιρική, ή καθολική (εάν επιτρέπεται) ομάδα και να προσθέσετε τα διευκρινισμένα μέλη σε αυτήν συγχρόνως (όχι αργότερα!). Παραδείγματος χάριν:

```
C:\>dsadd group CN=Admins, OU=Staff, DC=net, DC=dom -members
     "CN=John, OU=Staff, DC=net, DC=dom" "CN=Tim, OU=Personnel, DC=net,
DC=dom"
```

Ένα παράδειγμα του πώς να χρησιμοποιήσετε την DsAdd για να δημιουργήσετε έναν χρήστη και να τον προσθέσετε σε συγκεκριμένη ομάδα:

```
   C:\>dsadd user CN=Alice, OU=Staff, DC=net, DC=dom -memberof
     xg312
"CN=Admins, OU=Staff, DC=net, DC=dom"
     "CN=Account Operators, CN=Builtin, DC=net, DC=dom"
```

3.4.4 To Script CreateUsers.vbs

Αυτό το script μπορεί μόνο να δημιουργήσει τους χρήστες. Λειτουργεί και με τους διακομιστές WinNT και LDAP. Οι δημιουργημένοι λογαριασμοί θα επιτραπούν. Οι ακόλουθες ιδιότητες απαιτούνται (το ελάχιστο σύνολο ιδιοτήτων):

- WinNT - όνομα και κωδικός πρόσβασης
- LDAP *cn, samAccountName*, και κωδικός πρόσβασης

Μπορείτε να διευκρινίσετε πολλές άλλες ιδιότητες, επίσης εντούτοις, δεν είναι επιτρεπτή κάθε διαθέσιμη ιδιότητα για ένα αντικείμενο χρηστών. Προσεκτικά εξετάστε την εντολή σας (και το αρχείο εισαγωγής, εάν υπάρχει). Να είστε βέβαιος ότι όλες οι διευκρινισμένες ιδιότητες είναι συνεπείς διαφορετικά, θα μπορούσατε εύκολα να λάβετε ένα μήνυμα λάθους παρόμοιο με:

Error 0X80072035 occurred in settings properties for user cn=...

Αυτό το λάθος (8245) σημαίνει ότι "ο κεντρικός υπολογιστής είναι απρόθυμος να επεξεργαστεί το αίτημα". Μια από τις πιθανές πηγές αυτού του λάθους είναι οι ανακριβείς "ονομαστικές" ιδιότητες: *cn, name, sn, distinguishedName*, κ.λπ.... Μην

ξεχάστε να εσωκλείσετε τις τιμές οποιωνδήποτε ιδιοτήτων που περιέχουν τα διαστήματα στα διπλά εισαγωγικά.

Εδώ είναι το απλούστερο παράδειγμα για το πώς να δημιουργήσει έναν χρήστη με CreateUsers.vbs:

```
C:\>createusers WinNT://NET name:user01 password:psw1
```

Το script πρέπει να έχει έξοδο το ακόλουθο:

```
Working ...
Getting domain WinNT://NET ...
Creating user user01
Succeeded in creating user user01 in NET.
```

Για να θέσετε εκτός λειτουργίας την παραγωγή των πληροφοριακών μηνυμάτων, χρησιμοποιήστε την παράμετρος /q.

Οι νέοι χρήστες θα δημιουργούνται πάντα στο *Users* container. Θα μπορούσατε να τους κινήσετε προς άλλα containers (πιθανότατα, οργανωτικές μονάδες), αλλά ένας καλύτερος τρόπος θα ήταν να χρησιμοποιηθεί η " LDAP -έκδοση" του CreateUsers.vbs, το οποίο "καταλαβαίνει" την δομή του Active Directory:

```
C:\>createusers LDAP: //OU=Staff, DC=net, DC=dom cn: "User User01"
     samAccountName: user-ldap01 password:psw1
```

Ίσως το πιο ενδιαφέρων ζήτημα είναι πώς να δημιουργήσετε πολλούς χρήστες με τη μία. Είναι πραγματικά πολύ εύκολο. Δημιουργήστε ένα αρχείο με τις επιθυμητές ιδιότητες χρηστών και χρησιμοποιήστε τον αρμόδιο προμηθευτή (WinNT ή LDAP). Παραδείγματος χάριν, η ακόλουθη εντολή θα δημιουργήσει τους χρήστες που διευκρινίζονται σε ένα αρχείο στο OU προσωπικού:

```
createusers LDAP://OU=Staff, DC=net, DC=dom /i:newUsers.txt
```

Το αρχείο με τις περιγραφές μπορεί να είναι όμοιο με το ακόλουθο:

```
cn: "User01" samAccountName:user01 password:psw1
cn: "User02" samAccountName:user02 password:psw2
```

3.4.5 AddUsers.exe

Σε σύγκριση με το CreateUsers.vbs, το AddUsers.exe έχει μερικά πρόσθετα χαρακτηριστικά γνωρίσματα. Εκτός από την προσθήκη των χρηστών και των ομάδων σε μια περιοχή, σας επιτρέπει:

- Να απορρίψετε πληροφορίες λογαριασμού (χρήστες και ομάδες) σε ένα αρχείο.
- Να διευκρινίσετε τον έλεγχο των επιλογών λογαριασμού-δημιουργίας. Εξ ορισμού, ένας νέος χρήστης πρέπει να αλλάξει τον κωδικό πρόσβασής του/της στη σύνδεση.

- Να διαγράψετε χρήστες ή ομάδες. Τα ονόματα λογαριασμού μπορούν μόνο να διευκρινιστούν στο αρχείο εισαγωγής.
- Να δημιουργήσετε ένα αρχείο εισαγωγής σε ένα πρόγραμμα υπολογισμών με λογιστικό φύλλο (spreadsheet), όπως το Microsoft Excel, και το σώστε με το κόμμα-οριοθετημένο format, που μπορεί να χρησιμοποιήσει το εργαλείο. Ένας διαχωριστικός χαρακτήρας εκτός από ένα κόμμα μπορεί να διευκρινιστεί.

Μια αρνητική πτυχή του AddUsers.exe είναι ότι το εργαλείο "δεν βλέπει" την δομή του Active Directory.

Χρησιμοποιώντας το AddUsers.exe, μπορείτε επιτυχώς να προσθέσετε χρήστες στις υπάρχουσες ομάδες, παρά το μήνυμα λάθους " ομάδα υπάρχει ήδη". Οι ομάδες μπορούν να βρεθούν σε οποιοδήποτε container στο Active Directory, όχι μόνο στο "προεπιλεγμένο"container χρηστών.

Ένα δείγμα αρχείου απορρίψεως που παράγεται από το AddUsers.exe τοποθετείται κατωτέρω (τα ονόματα των ιδιοτήτων είναι σε έντονες παρενθέσεις και δεν συμπεριλαμβάνονται πραγματικά στο αρχείο). Ένα τέτοιο αρχείο μπορεί εύκολα να εισαχθεί σε ένα λογιστικό φύλλο (spreadsheet).

```
[User]
    {samAccountName, name, password, description, homeDrive,
homeDirectory, profilePath, scriptPath}
    Administrator,,,Built-in account for administering the
      computer/domain,,,,
    Guest,,,Built-in account for guest access to the
computer/domain,,,,
    JSmith,John Smith,,A test user,Z:,\\netdcl\UserData\JSmith,
      \\netdcl\Profiles\JSmith,Users\Welcome.vbs...
    [Global]
    {samAccountName, description, member's account names...}
    Domain Admins,Designated administrators of the
domain,Administrator,
    Domain Controllers,All domain controllers in the
      domain,NETDC1$,NETDC4$,
    Domain Users,All domain users,Administrator,HelpAssistant_67861b,
    SUPPORT_388945a0, krbtgt,SUBDOM$,Bob,John,Pam,...
    ...
    [Local]
    {samAccountName, description, member's account names...}
    Administrators,Administrators have complete and unrestricted
      access to the computer/domain,NET\Administrator,NET\Enterprise
      Admins,NET\Domain Admins,

DC1Loca1Group,NET\John,NET\Lee,NET\Jessica,NET\Globa1Gr1,NET\UniGr2,
      NET\DC1LocGr1,
    ...
```

Παρατηρείστε ότι στην τελευταία γραμμή οι ομάδες μπορούν να περιέχουν άλλες ομάδες (τα ονόματα ομάδας παρουσιάζονται με έντονους χαρακτήρες) συμπεριλαμβανομένων των τοπικών ομάδων.

Όπως μπορείτε να δείτε, το απορριπτόμενο αρχείο περιέχει τρία τμήματα: *User, Global,* και *Local*. Το ίδιο σχήμα μπορεί να χρησιμοποιηθεί για τη δημιουργία νέων χρηστών και ομάδων. Τα άσχετα συρόμενα κόμματα, όπως και τα αχρησιμοποίητα τμήματα, μπορείτε να τα παραλείψετε στο αρχείο εισαγωγής. Οι νέες ομάδες μπορούν είτε να είναι κενές είτε να περιέχουν τα ονόματα των μελών τους.

3.4.6 Τροποποιώντας Την Ιδιότητα Μέλους Ομάδας

Το **Active Directory Users and Computers** snap-in έχει ένα χαρακτηριστικό γνώρισμα για τις "μεμονωμένες" διαδικασίες που σας επιτρέπει για να προσθέσετε διάφορους επιλεγμένους χρήστες και επαφές σε μια ομάδα. Πηγαίνετε σε έναν λογαριασμό (ή επιλέξτε μερικούς λογαριασμούς) και επιλέξτε την εντολή **Add to a group** από τις επιλογές πλαισίου ή από το μενού **Action**, ή πατήστε το κουμπί **Add the selected objects to a group you specify** στη γραμμή εργαλείων. Κατόπιν διευκρινίστε μια ομάδα στο παράθυρο **Select Group**. Στα Windows .NET, μπορείτε επίσης να διενεργήσετε τις διαδικασίες *drag-and-drop*.

Εάν επιλέγετε αρχικά ένα OU, το σύστημα ρωτά εάν θέλετε να προσθέσετε όλους τους χρήστες και τις επαφές από αυτό το container στη διευκρινισμένη ομάδα. Αυτό το χαρακτηριστικό γνώρισμα είναι πολύ χρήσιμο για τη διαχείριση των OUs (αλλά στα Windows.NET, είναι ελλιπής).

Για να εποικήσουν οι ομάδες, μπορείτε να χρησιμοποιήσετε τα εργαλεία LDIFDE και CSVDE, όπως και το AddUsers.exe. Το LDIFDE είναι επίσης ικανό να διαγράψει τα μέλη από τις ομάδες.

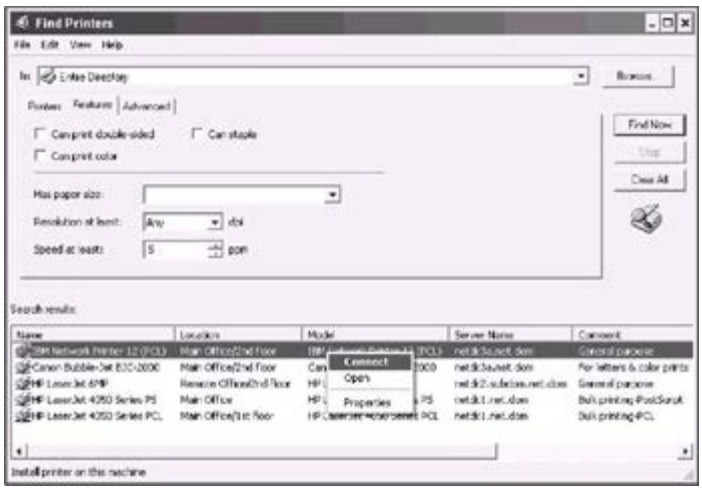
Στους υπολογιστές που τρέχουν τα Windows.NET, μπορείτε να χρησιμοποιήσετε το τυποποιημένο DsMod.exe που εκτελεί όλες τις τροποποιήσεις των ομάδων. Παραδείγματος χάριν, η ακόλουθη εντολή προσθέτει δύο νέα μέλη στην ομάδα Schema Admins:

```
C:\>dsmod group "CN=Schema Admins,CN=Users,DC=net,DC=dom" -addmbr
     "CN=John Smith,OU=Staff,DC=net,DC=dom"
     "CN=Pamela,OU=Staff,DC=net,DC=dom"
```

Η παράμετρος `-rmmbr` απομακρύνει τα διευκρινισμένα μέλη, και η παράμετρος `'-chmbr` αντικαθιστά όλα τα μέλη ομάδας.

3.5 Δημοσιεύοντας Φακέλους και Εκτυπωτές

Το Active Directory απλοποιεί αρκετά την εργασία με τους κοινούς πόρους δικτύων σε σύγκριση με την παραδοσιακή μέθοδο ξεφυλλίσματος των domains. Εάν ένας πόρος έχει δημοσιευθεί στο Active Directory, οι χρήστες μπορούν εύκολα να το εντοπίσουν (δείτε, παραδείγματος χάριν, η εντολή **Search | For Printers** στο **Start** μενού) και να συνδεθούν σε αυτούς (δείτε την εικόνα 3.2). Επιπλέον, για να απλοποιήσετε τη διαδικασία εντόπισης πόρων, μπορεί να θελήσετε να τους δημοσιεύσετε όλους σε ένα OU.



Εικόνα 3.2: Αναζήτηση όλων των εκτυπωτών στην επιχείρηση (δάσος)

Εκδίδοντας ένα φάκελο ή έναν εκτυπωτή στο Active Directory σημαίνει, με άλλα λόγια, τη δημιουργία ενός νέου αντικειμένου καταλόγου - κοινόχρηστου φακέλου ή εκτυπωτή, αντίστοιχα.

Οι κοινόχρηστοι φάκελοι στο Active Directory έχουν ένα χαρακτηριστικό γνώρισμα που βοηθά τους χρήστες για να ψάξουν για τις πληροφορίες σύμφωνα με τα χαρακτηριστικά του. Επιλέξτε έναν δημοσιευμένο φάκελο στη διατομή δέντρων του **Active Directory Users and Computers** snap-in, ανοίξτε το παράθυρο ιδιοτήτων του, και πατήστε στο **Keywords**. Μπορείτε να προσθέσετε τις λέξεις που συσχετίζονται λογικά με το περιεχόμενο του φακέλου στον κατάλογο. Κατόπιν, εάν ένας χρήστης αρχίζει μια αναζήτηση για κοινόχρηστους φακέλους στο παράθυρο **Find**, μπορεί να διευκρινίσει τις λέξεις κλειδιά και να βρει τους πόρους βασισμένους στο περιεχόμενό τους παρά στα ονόματά τους.

Οι εκτυπωτές (ακριβέστερα - συσκευές εκτυπωτών) συνδεδεμένοι με υπολογιστές που τρέχουν Windows 2000/XP/.NET μπορούν να δημοσιευθούν μόνο από το παράθυρο ιδιοτήτων ενός εκτυπωτή (η σημαία **List in the Directory** στην ετικέτα **Sharing**). Σε άλλες περιπτώσεις, μπορείτε να χρησιμοποιήσετε το script Pubprn.vbs.

Εξ ορισμού, ο τοπικός εκτυπωτής σε έναν υπολογιστή πελάτη του domain δεν δημοσιεύεται κατά τη διάρκεια της εγκατάστασής του εάν δεν τον μοιράζεστε αμέσως. Εάν ένας εκτυπωτής εγκαθίσταται σαν κοινόχρηστος, δημοσιεύεται αμέσως στο Active Directory στο computer's container. Μπορείτε να καθαρίσετε την σημαία **List in the Directory** σε κάθε στιγμή, και το αντικείμενο εκτυπωτών θα διαγραφεί από το Active Directory.

Κατά τον έκδοση ενός φακέλου, πρέπει να είστε προσεκτικοί, επειδή το σύστημα δεν θα ελέγξει το εισαγόμενο όνομα φακέλων, και, κατά συνέπεια, μπορεί να αντιμετωπίσετε ένα λάθος στο μέλλον, αλλά μόνο όταν ανοίγετε το φάκελο

Εάν τα ονόματα RDN και NetBIOS ενός Windows 2000 domain είναι διαφορετικά, θα πάρετε το λάθος - " The system cannot find the file specified " - κατά την έκδοση ενός εκτυπωτή. Για να επιλύσετε το πρόβλημα, πρέπει να εγκαταστήσετε το πιο πρόσφατο Windows 2000 Service Pack (τουλάχιστον, SP 1).

Μπορείτε να διαμορφώσετε τη διαδικασία έκδοσης και περικοπής των εκτυπωτών στο domain με τη χρησιμοποίηση των πολιτικών ομάδας (δείτε το **Computer Configuration | Administrative Templates | Printers** στο **Group Policy Object Editor** snap-in).

Στα Windows 2000 όπως και στα Windows.NET domains, είναι δυνατό να ενεργοποιηθεί το *Location Tracking*, ένα χαρακτηριστικό γνώρισμα που επιτρέπει στους χρήστες να βρουν εκτυπωτές αναλόγως στις φυσικές θέσεις τους.

3.5.1 Το Script Pubprn.vbs

Μπορείτε να εκτελέσετε το script συστήματος Pubprn.vbs χωρίς παραμέτρους και να πάρετε τις πληροφορίες βοήθειας. Η ακόλουθη εντολή, παραδείγματος χάριν, δημοσιεύει τον εκτυπωτή HP6MP που συνδέεται με τον υπολογιστή WKS10 στο OU προσωπικού στο domain *net.dom*

pubprn \\wks10\hp6mp "LDAP://OU=Staff,DC=net,DC=dom"
Το σύστημα ελέγχει το όνομα εκτυπωτών και την ύπαρξη του αντικειμένου που διευκρινίζεται από το όνομα του LDAP. Εάν ο εκτυπωτής έχει δημοσιευθεί επιτυχώς, θα δείτε ένα μήνυμα το όνομα του LDAP του εκτυπωτή στο Active Directory.

3.5.2 Σύνδεση Με Κοινόχρηστες Πηγές

Οι διαδικασίες αναζήτησης είναι ο προτιμημένος τρόπος για τους κοινούς πόρους δικτύων σε AD-based domains. Ένας χρήστης μπορεί να βρει τον απαιτούμενο εκτυπωτή ή τον κοινό φάκελο εύκολα και να εκτελέσει οποιαδήποτε λειτουργία διαθέσιμη κοιτάζοντας το δέντρο του domain.

Η εμβέλεια της εύρεσης μπορεί να ποικίλει από ένα συγκεκριμένο container (OU) στο domain μέχρι ένα ολόκληρο δάσος. (Η επιλογή **Entire Directory** είναι ισοδύναμη με την έρευνα του Global Catalog.) Επιπλέον, οι χρήστες μπορούν να διευκρινίσουν τα διάφορα κριτήρια αναζήτησης όπως η ταχύτητα εκτυπωτών, ανάλυση, και τα λοιπά. Η εικόνα 3.2 περιέχει ένα παράδειγμα για το πώς να βρείτε όλους τους εκτυπωτές στο δάσος. Όπως μπορείτε να δείτε στη στήλη **Server Name**, οι εκτυπωτές προέρχονται από διάφορα domains. Ένας χρήστης μπορεί να διαλέξει έναν εφαρμόσιμο εκτυπωτή και να επιλέξει την απαραίτητη λειτουργία από τις επιλογές πλαισίου.

Οι χρήστες μπορούν να εκτελέσουν τις ακόλουθες ενέργειες στον κοινόχρηστο φάκελο: άνοιγμα, εύρεση στον φάκελο, αντιστοίχιση ενός δίσκου δικτύου, και άλλα.

3.6 Διαχειρίζοντας Ρόλους FSMO Στο Δάσος

Επειδή η θέση των κύριων ρόλων του *Flexible Single Master Operation* (FSMO) είναι πολύ σημαντική για την κατάλληλη λειτουργία ενός multi-domain δάσους, ένας διαχειριστής πρέπει να ξέρει ποιοι domain controllers κατέχουν έναν συγκεκριμένο ρόλο(ους) σε κάθε στιγμή για όλη την ζωή του δικτύου. Επομένως, πρέπει να έχει τις

εγκαταστάσεις για να βρει τους role masters εύκολα και για να μεταφέρει έναν ρόλο από ένα DC σε άλλο. Επιπλέον, είναι απαραίτητο να υπάρχει ένας τρόπος να μεταφερθεί εξαναγκαστικά ένας ρόλος από έναν ‘’πεθαμένο’’ DC. Αυτή η διαδικασία αναφέρεται ως "κατάσχεση του ρόλου".

3.6.1 Εύρεση των Ιδιοκτητών των ΡόλωνFSMO

Για να βρεθούν οι ιδιοκτήτες των ρόλων FSMO (operation masters), ένας διαχειριστής μπορεί να χρησιμοποιήσει τα "τυποποιημένα" διαχειριστικά εργαλεία:

- Το **Active Directory Users and Computers** snap-in εμφανίζει το RID, PDC, και Infrastructure masters.
- Το The **Active Directory Domains and Trusts** snap-in εμφανίζει το Domain Naming master.
- Το The **Active Directory Schema** snap-in εμφανίζει το Schema master

Αυτή η προσέγγιση είναι, εντούτοις, χρονοβόρα, και έχει νόημα προκειμένου να χρησιμοποιηθούν μερικά εργαλεία γραμμής-εντολών ή scripts. Μερικά τέτοια εργαλεία περιγράφονται κατωτέρω.

3.6.2 Η Εφαρμογή των Windows.NET — DsQuery

Μια ολοκαίνουργια εφαρμογή γραμμής-εντολών, η DsQuery.exe, θα σας βοηθήσει για να βρείτε έναν συγκεκριμένο role master, παραδείγματος χάριν:

```
C:\>dsquery server -hasfsmo rid
"CN=NETDC1,CN=Servers,CN=NET-Site,CN=Sites,CN=Configuration,
  DC=net, DC=dom"
```

Μπορείτε επίσης να προσδιορίσετε άλλους ρόλους: `pdc`, `infr`, `name`, `schema`.

3.6.3 Windows Domain Manager (NetDom.exe)

Το NetDom.exe μπορεί να εμφανίσει όλους τους operation masters που είναι γνωστοί σε ένα διευκρινισμένο DC. Χρησιμοποιήστε την ακόλουθη σύνταξη εντολής:

```
C:\>netdom QUERY /Domain:net.dom FSMO
```

3.6.4 DumpFSMOs.cmd

Αυτό το αρχείο εντολής είναι, στην πραγματικότητα, μια αλυσίδα οδηγιών στο εργαλείο NTDSutil. (Αυτές οι οδηγίες μπορούν επίσης να εισαχθούν με το χέρι.) Η κύρια εντολή σε εκείνο το αρχείο είναι η ακόλουθη:

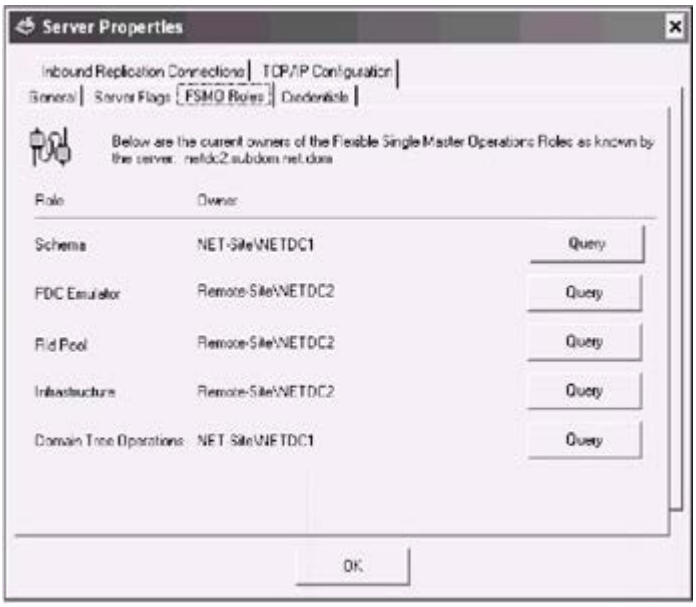
```
ntdsutil roles Connections "Connect to server %1" Quit
     "select Operation Target" "List roles for connected server"
     Quit Quit Quit
```

Η μόνη υποχρεωτική παράμετρος είναι το όνομα του DC από τον οποίο οι πληροφορίες ανακτώνται. Ένα δείγμα οθόνης παραγωγής παρουσιάζεται κατωτέρω (η υπαγόρευση της εφαρμογής είναι με έντονους μαύρους χαρακτήρες):

```
C:\>dumpfsmos.cmd netdc1
   ntdsutil: roles
   fsmo maintenance: Connections
   server connections: Connect to server netdc1
   Binding to netdcl ...
   Connected to netdc1 using credentials of locally logged on user.
   server connections: Quit
   fsmo maintenance: select Operation Target
   select operation target: List roles for connected server
   Server "netdc1" knows about 5 roles
   Schema - CN=NTDS Settings, CN=NETDC1, CN=Servers,
     CN=NET-Site,CN=Sites,CN=Configuration,DC=net,DC=dom
   Domain - CN=NTDS Settings,CN=NETDC1,CN=Servers,
     CN=NET-Site,CN=Sites,CN=Configuration,DC=net,DC=dom
   PDC - CN=NTDS Settings,CN=NETDC1,CN=Servers,
     CN=NET-Site,CN=Sites,CN=Configuration,DC=net,DC=dom
   RID - CN=NTDS Settings,CN=NETDC1,CN=Servers,
     CN=NET-Site,CN=Sites,CN=Configuration,DC=net,DC=dom
   Infrastructure - CN=NTDS Settings,CN=NETDC3,CN=Servers,
     CN=NET-Site,CN=Sites,CN=Configuration,DC=net,DC=dom
   select operation target: Quit
   fsmo maintenance: Quit
   ntdsutil: Quit
   Disconnecting from netdc1...
```

3.6.5 Active Directory Replication Monitor (ReplMon.exe)

Όλοι οι operation masters μπορούν να εμφανιστούν με το ReplMon.exe. Αρχίστε το εργαλείο και προσθέστε κεντρικούς υπολογιστές στην λίστα του **Monitored Servers** (δέντρο). (Σε αυτήν την περίπτωση, είναι αρκετό να προσθέσει ένας κεντρικός υπολογιστής μόνο.) Επιλέξτε ένα DC από την διατομή δέντρων, ανοίξτε το παράθυρο ιδιοτήτων, και κάντε κλικ την ετικέτα **FSMO Roles**. Η εικόνα 3.3 παρουσιάζει ένα δείγμα αυτής της άποψης αυτής της ετικέτας.



Εικόνα 3.3: Εξέταση όλων των operation masters (οι ιδιοκτήτες των ρόλων FSMO) για ένα domain

Από αυτό το παράθυρο, μπορείτε να εξετάσετε οποιοδήποτε operation master με το πάτημα του **Query**. Το ReplMon απαντά με το ακόλουθο μήνυμα: "Active Directory Replication Monitor was able/unable to resolve, connect, and bind to the server hosting this FSMO role."

Επιπλέον, Το ReplMon μπορεί να εμφανίσει όλους Global Catalog servers στην επιχείρηση (επιλέξτε την εντολή **Show Global Catalog Servers in Enterprise** στις επιλογές πλαισίου ενός ελεγχόμενου κεντρικού υπολογιστή).

3.6.6 Μεταφορά Ενός Ρόλου FSMO

Συνήθως, για να μεταφερθεί ένας ρόλος FSMO από ένα DC σε άλλο, τα διαχειριστικά snap-ins πρέπει να χρησιμοποιηθούν. Για να καταληφθεί ένας ρόλος, πρέπει να χρησιμοποιήσετε το NTDSutil.exe.

3.6.7 RID, PDC, και Infrastructure Operation Masters

Μπορεί να θελήσετε, για κάποιους λόγους (π.χ., πριν να κλείσετε έναν DC για συντήρηση), να μεταφέρετε έναν ρόλο FSMO από το role's master σε ένα άλλο DC στο domain. Στο παράθυρο του **Active Directory Users and Computers** snap-in, πρέπει πρώτα να συνδέσετε με το DC που είναι ο πιθανός (νέος) operation master, πηγαίνοντας στον κόμβο ρίζας στη διατομή δέντρων, και επιλέξτε την εντολή **Operation Masters** είτε στις επιλογές πλαισίου είτε στο μενού **Action**. πατήστε στην κατάλληλη ετικέτα: **RID, PDC**, ή **Infrastructure**. Θα δείτε τον τρέχοντα ιδιοκτήτη ενός ρόλου FSMO και του πιθανού κύριου ονόματος. Πατήστε το κουμπί **Change**, και θα πάρετε έναν νέο operation master.

Να είστε προσεκτικοί κατά τη μεταφορά του ρόλου υποδομής (Infrastructure role). Εάν υπάρχουν δύο ή περισσότεροι DCs στο domain, σιγουρευτείτε ότι ένα μήνυμα παρόμοιο με τον ακόλουθο δεν έχει εμφανιστεί στο Directory Service log στο operation master:

```
Event Type: Error

   Event Source: NTDS General

   Event Category: Directory Access

   Event ID: 1419

   Date: 5/31/2002

   Time: 6:07:14 PM

   User: NT AUTHORITY\ANONYMOUS LOGON

   Computer: NETDC1

   Description:
```

Ο τοπικός domain controller είναι και ένας global catalog και infrastructure operations master. Αυτοί οι δύο ρόλοι δεν είναι συμβατοί.

Εάν ένας άλλος domain controller υπάρχει στο domain, πρέπει να infrastructure operations master. Ο ακόλουθος domain controller είναι ένας καλός υποψήφιος για αυτόν τον ρόλο.

```
   Domain controller:

   CN=NTDS Settings, CN=NETDC3, CN=Servers, CN=NET-
   Site, CN=Sites, CN=Configuration, DC=net, DC=dom
```

Εάν όλοι οι domain controllers σε αυτήν το domain είναι global catalogs, κατόπιν εκεί δεν υπάρχουν ενημέρωσης της υποδομής για να ολοκληρωθούν, και αυτό το μήνυμα αγνοείται.

3.6.8 Domain Naming Operation Master

Το **Active Directory Domains and Trusts** snap-in σας επιτρέπει να μεταφέρετε τον FSMO ρόλο του *Domain naming master* σε οποιοδήποτε DC στο δέντρο του domain. Αυτή η διαδικασία είναι απλή: συνδεθείτε με τον DC που θα είναι ο ιδιοκτήτης του νέου ρόλου, πηγαίνετε στον κόμβο ρίζας στη διατομή δέντρων, και επιλέξτε την εντολή **Operations Master** από τις επιλογές πλαισίου. Σιγουρευτείτε ότι τα ονόματα του τρέχοντος master και μελλοντικού master είναι σωστά, πατήστε στο **Change**, και επιβεβαιώστε τη λειτουργία. Θυμηθείτε ότι μόνο ένας κεντρικός υπολογιστής στο δάσος (επιχείρηση) μπορεί να εκτελέσει τον ρόλο του Domain naming master, και επιπλέον, εκείνος ο κεντρικός υπολογιστής πρέπει να είναι ένας Global Catalog server.

3.6.9 Schema Operation Master

Το **Active Directory Schema** snap-in επιτρέπει τη μεταφορά του FSMO ρόλου του *Schema Master* σε οποιοδήποτε DC στο δάσος. Πρέπει πρώτα να συνδεθείτε με τον πιθανό master του ρόλου, πηγαίνετε στον κόμβο ρίζας στην διατομή δέντρων, και επιλέξτε την εντολή **Operations Master** από τις επιλογές πλαισίου. Αφού επιλέξετε το όνομα του DC, πατήστε στο **Change**. Θυμηθείτε ότι μόνο ένας κεντρικός υπολογιστής στο δάσος μπορεί να εκτελέσει τον ρόλο του Schema Master.

Για να τροποποιήσετε το schema στα Windows 2000, πρέπει πρώτα να ενεργοποιήσετε αυτήν την λειτουργία. Όταν έχετε μεταφέρει τον ρόλο του Schema Master σε ένα DC, η σημαία **The Schema may be modified on this Domain Controller** παραμένει καθορισμένη στον schema master. Αυτό εντούτοις μπορεί να μην είναι σύμφωνα με τις προθέσεις σας.

3.6.10 Χρησιμοποιώντας το NTDSutil

Το NTDSutil μπορεί να χρησιμοποιηθεί για τη μεταφορά οποιουδήποτε ρόλου FSMO. Αυτό είναι το μόνο εργαλείο που επιτρέπει σε έναν διαχειριστή να ορίσει εξαναγκαστικά έναν ρόλο σε ένα DC. (Υποτίθεται ότι ο παλαιός ιδιοκτήτης αυτού του ρόλου έχει καταστραφεί και δεν μπορεί να επισκευαστεί.)

3.7 Ανανεώνοντας την Πολιτική Ομάδας

Όταν ένας διαχειριστής αλλάξει ένα GPO, μπορεί να θελήσει να ανανεώσει την εφαρμογή πολιτικής της ομάδας για να ελέγξει το αποτέλεσμα των νέων ρυθμίσεων. (Βεβαίως, είναι δυνατό να επανεκκινήσει τον υπολογιστή ή να καταχωρίσει ξανά τον χρήστη στο domain . Εντούτοις, αυτό δεν είναι πάντα κατάλληλο). Σε υπολογιστές που τρέχουν Windows 2000 για να εκτελεστεί αυτή η λειτουργία, μπορείτε να χρησιμοποιήσετε την εφαρμογή γραμμής εντολών SecEdit.exe. Τα συστήματα Windows XP/.NET προσφέρουν μια νέα δυνατότητα (που πρέπει να χρησιμοποιήσετε) – το GPupdate.exe - για εκείνο τον σκοπό.

Η σύνταξη εντολής είναι πολύ απλή. Για να ανανεωθούν οι πολιτικές χρηστών, εισάγετε οποιαδήποτε από τις ακόλουθες εντολές (εφαρμόσιμες στο σύστημά σας):

```
C:\>secedit /refreshPolicy user_policy — on Windows 2000
C:\>gpupdate /Target:User — on Windows .NET
```

Η ακόλουθη εντολή ανανεώνει τις πολιτικές του υπολογιστή:

```
C:\>secedit /refreshPolicy machine_policy
C:\>gpupdate /Target:Computer
```

Η εντολή GPupdate χωρίς παραμέτρους ανανεώνει τις πολιτικές και του χρήστη και του υπολογιστη.

Εάν θέλετε να επανεφαρμόσετε τις πολιτικές (GPOs), ακόμα κι αν δεν έχουν αλλάξει από την τελευταία φορά που εφαρμόστηκαν, προσθέστε την παράμετρο /enforce στην εντολή SecEdit ή την παράμετρο /Force στην εντολή GPupdate. (Κανονικά, Τα GPOs εφαρμόζονται μόνο μιά φορά τα αμετάβλητα GPOs παραβλέπονται.)

3.8 Προκαλώντας το Replication

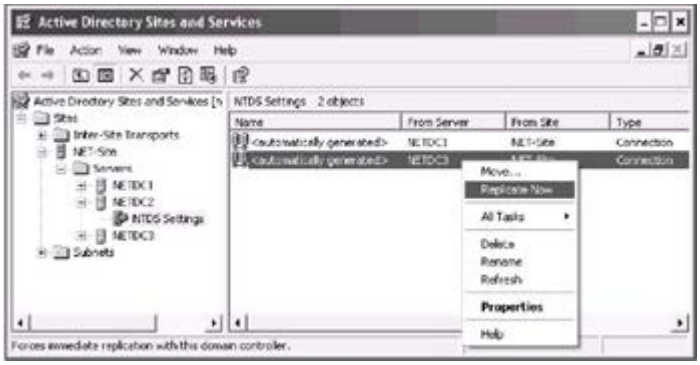
Ένας διαχειριστής έχει τρία εργαλεία που μπορούν να χρησιμοποιηθούν για να προκαλέσουν το replication του Active Directory είτε όλων των χωρισμάτων καταλόγου (πλαίσια) είτε ακριβώς ενός διευκρινισμένου χωρίσματος μεταξύ ενός domain controller και ενός είτε όλων άμεσων συνεργατών του replication του:

- Το Active Directory Sites and Services snap-in
- Η εφαρμογή γραμμής εντολών RepAdmin
- Η εφαρμογή GUI ReplMon

Όπως είναι χαρακτηριστικό για σχεδόν οποιοδήποτε διαχειριστικό καθήκον, μπορείτε επίσης να χρησιμοποιήσετε τα scripts.

3.8.1 Το *Active Directory Sites and Services* Snap-in

Αυτό το snap-in επιτρέπει σε έναν διαχειριστή να αρχίσει το replication όλων των διαμορφωμένων χωρισμάτων καταλόγου από κάθε συνεργάτη του replication χωριστά. Επιλέξτε έναν DC από το **Servers** container της εφαρμόσιμης περιοχής και του πηγαίνετε προς το αντικείμενο του **NTDS Settings**. Μπορείτε να προκαλέσετε το replication από οποιοδήποτε κεντρικό υπολογιστή που αντιπροσωπεύεται από ένα αντικείμενο *σύνδεσης* στη σωστή διατομή (δείτε το παράδειγμα στην εικόνα 3.4). Επιλέξτε μια σύνδεση και πατήστε το **Replicate Now** στις επιλογές πλαισίου. Πρέπει να περιμένετε έως ότου ολοκληρωθεί το replication (με το μήνυμα "Active Directory has replicated the connections" εάν είναι επιτυχής).



Εικόνα 3.4: Προκαλώντας το replication από έναν άμεσο συνεργάτη

Όλα τα χωρίσματα καταλόγου που διαμορφώνονται για εκείνο τον συνεργάτη γίνονται replicate. (Μπορείτε να δείτε όλα τα ονόματά τους - συμπεριλαμβανομένων των χωρισμάτων καταλόγου εφαρμογής – στο παράθυρο ιδιοτήτων μιας σύνδεσης.) Δεν έχετε καμία επιλογή να κάνετε replicate ένα χώρισμα μόνο.

3.8.2 Εργαλείο Διάγνωσης του Replication (RepAdmin.exe) (ST)

Με το RepAdmin.exe, μπορείτε να κάνετε replicate κάθε χώρισμα καταλόγου χωριστά από μια ή όλες τις πηγές. (Αυτό το εργαλείο γραμμής εντολών έχει τις ίδιες λειτουργικές ικανότητες με το ReplMon, ένα εργαλείο GUI.) Παραδείγματος χάριν, για να προκαλέσει το replication για έναν κεντρικό υπολογιστή προορισμού, μπορείτε να χρησιμοποιήσετε την ακόλουθη εντολή:

```
C:\>repadmin /syncall netdc2.net.dom DC=net,DC=dom,
```

όπου `netdc2.net.dom` είναι το dns όνομα του κεντρικού υπολογιστή, και το DC=net, DC=dom είναι ένα όνομα χωρίσματος (το domain naming partition σε αυτήν την περίπτωση).

Η διαφορά μεταξύ αυτής της εντολής και της λειτουργίας που παρουσιάζεται στην εικόνα 3.4 είναι η ακόλουθη:

- Η εντολή κάνει replicate μόνο ένα χώρισμα, αλλά από όλους τους συνεργάτες.
- Στο snap-in παράθυρο γίνονται replicate όλα τα χωρίσματα, αλλά από έναν συνεργάτη μόνο.

Για να αναγκάσετε το replication σε ολόκληρη την περιοχή (δάσος), μπορείτε να γράψετε παρόμοιες εντολές για κάθε DC και όλα τα χωρίσματα καταλόγου σε ένα αρχείο εντολής, το οποίο θα χρησιμεύσει για να εκπληρώσει το συνολικό replication στο Domain.

Η έκδοση Windows.NET του RepAdmin παρέχει μια νέα σημαία /A για τις /syncall διαδικασίες. Η ακόλουθη εντολή συγχρονίζει όλα τα χωρίσματα που αποθηκεύονται στο *NETDC1* DC με όλους τους συνεργάτες του replication:

```
C:\>repadmin /syncall netdc1.net.dom /A
```

Η ακόλουθη εντολή κάνει replicate ένα χώρισμα από έναν συνεργάτη (καθορισμένο από το GUID του)

```
C:\>repadmin /sync DC=net,DC=dom netdc1.net.dom
  a10bc624-6d04-44e7-adf9-5ef4282efbb1
```

Κανονικά, Το RepAdmin περιμένει το replication να ολοκληρωθεί. Μπορείτε να προσθέσετε την παράμετρο / async στην εντολή για να αρχίσει μια λειτουργία και να μην περιμένει την ολοκλήρωσή του

3.8.3 Active Directory Replication Monitor (ReplMon.exe)

Ένα εργαλείο GUI, το ReplMon.exe, παρέχει σε έναν διαχειριστή τους ακόλουθους τρόπους για replication:

- Συγχρονίζει κάθε χώρισμα καταλόγου με όλους τους συνεργάτες του replication (υπάρχουν τρεις πρόσθετες επιλογές διαθέσιμες με αυτόν τον τρόπο)
- Συγχρονίζει αυτό το χώρισμα καταλόγου με όλους τους συνεργάτες του replication
- Συγχρονίζει αυτό το χώρισμα καταλόγου με αυτόν τον συνεργάτη του replication

Δεν χρειάζεστε ποτέ να περιμένετε να ολοκληρωθεί μια λειτουργία replication, όλα τα αποτελέσματα λειτουργίας γράφονται στα αρχεία ημερολογίου (log files).

Επιπρόσθετα Εργαλεία Replication	Προκειμένου να αναγκάσουμε τον συγχρονισμό των ομάδων αντιγράφων που διαχειρίζονται από το **File Replication Service** (FRS), για παράδειγμα τα περιεχόμενα του χώρου SYSVOL χρησιμοποιείστε την εντολή `ntfrsutl`

Για να συγχρονιστεί ένας κεντρικός υπολογιστής βασισμένος στα Windows 2000 ή στα Windows .NET που είναι κύριος του ρόλου PDC Emulator FSMO με τους **Backup Domain Controllers** (BDCs) σε ένα ανάμικτο domain, χρησιμοποιήστε το εργαλείο NLtest.exe. Δείτε /REPL, /SYNC, /BDC_QUERY, και άλλες παραμέτρους αυτού του εργαλείου. Το αρχείο εντολής LBridge.cmd από το *Windows 2000 Server Resource Kit* πρέπει να χρησιμοποιηθεί για την αντιγραφή των αρχείων από το κοινόχρηστο System Volume (SYSVOL) στον κατάλογο εξαγωγής σε ένα BDC βασισμένο στα Windows 4.0

3.9 Μεταβιβάζοντας τον Διαχειριστικό Έλεγχο

Ένα από τα πιο αξιοπρόσεκτα χαρακτηριστικά γνωρίσματα που έχει το Active Directory είναι η δυνατότητα του να αποστέλλει το σύνολο ή μέρος της διαχειριστικής δύναμης πάνω από ένα OU ή ένα εμπορευματοκιβώτιο καταλόγου σε μια ομάδα ή έναν χρήστη (και στα Windows 2000 και στα Windows .NET domains). Η αποστολή του ελέγχου είναι ουσιαστικά το ίδιο πράγμα με το " wizard-aided " χορήγηση των αδειών στα αντικείμενα του Active Directory σε έναν χρήστη ή μια ομάδα. Μπορείτε με το χέρι να ορίσετε τις άδειες απαραίτητες για την εκτέλεση αυτού του διαχειριστικού στόχου σε έναν χρήστη ή σε μια ομάδα, αλλά αυτή η διαδικασία απλοποιείται αρκετά χάρη στο *Delegation of Control Wizard*. Ο έλεγχος εξουσιοδότησης είναι αρκετά μια απλή λειτουργία, και τα προβλήματα είναι δυνατά μόνο όταν ανακαλούνται οι ανατεθειμένοι στόχοι από το χρήστη ή την ομάδα.

Ένας διαχειριστής μπορεί να εξουσιοδοτήσει τον έλεγχο (π.χ., χρησιμοποιήστε το the Delegation of Control Wizard παρά να οριστούν οι άδειες με το χέρι) για τα ακόλουθα αντικείμενα του Active Directory (οι κοινοί διαχειριστικοί στόχοι αναφέρονται σε παρενθέσεις):

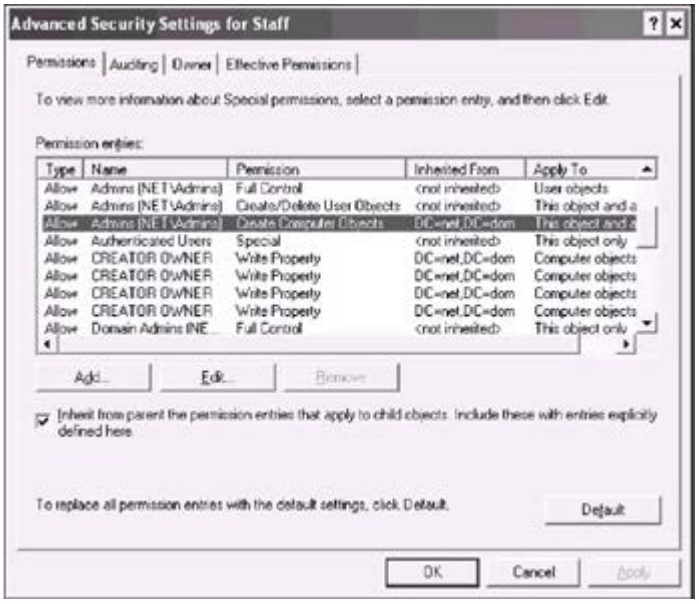
- Στο **Active Directory Sites and Services** snap-in (οι χαρακτηριστικές άδειες είναι πλήρους ελέγχου, Read/Write, Create/Delete All Child Objects, Read/Write όλες τις ιδιότητες):
    - *Sites* container
    - *Inter-Site Transport* container
    - *Subnets* container
    - A site(s) (only *Manage Group Policy links* task)
    - *Server* container in site(s)
- Στο **Active Directory Users and Computers** snap-in (ο κατάλογος διαθέσιμων αδειών εξαρτάται από τον τύπο του κοντεϊνερ του Active Directory):
    - Ολόκληρο το domain (ένωση ενός υπολογιστή στο domain, συνδέσεις του Manage Group Policy)
    - Οργανωτική μονάδα (δημιουργία, διαγραφή, και διαχείριση των λογαριασμών χρηστών, ανατοποθέτηση των κωδικών στους λογαριασμούς χρηστών, ανάγνωση όλων των πληροφοριών χρηστών δημιουργία, διαγραφή, και διαχείριση ομάδων, Τροποποίηση την ιδιότητα μέλους μιας ομάδας και συνδέσεις για διαχείριση των πολιτικών ομάδας. Στα Windows.NET, υπάρχουν μερικοί πρόσθετοι στόχοι.)
    - *Computers* container
    - *ForeignSecurityPrincipals* container
    - *System* container
    - *Users* container

Για να αρχίσει η διαδικασία μεταβίβασης ελέγχου, τρέξτε το κατάλληλο snap-in, πηγαίνετε σε ένα Active Directory container, OU, ή στο ίδιο το domain στη διατομή δέντρων, και επιλέξτε την εντολή **Delegate control** στις επιλογές πλαισίου ή στο **Action** menu. Ανάλογα με τον τύπο του κοντεϊνερ, μπορείτε να επιλέξετε έναν κοινό στόχο(ους) ή να δημιουργήσετε έναν διαφορετικό στόχο. Στην πρώτη περίπτωση, χρησιμοποιείτε ένα προκαθορισμένο σύνολο αδειών, ενώ στη δεύτερη περίπτωση, επιλέγετε τα αντικείμενα και τις άδειες οι ίδιοι, που σας επιτρέπει να είστε πιο συγκεκριμένοι στην εξουσιοδότηση των διαχειριστικών δικαιωμάτων.

Αν και είναι πολύ απλό να εξουσιοδοτήσετε τον έλεγχο, η ανάκληση των διαχειριστικών δικαιωμάτων από έναν χρήστη ή μια ομάδα απαιτεί λίγο περισσότερη προσπάθεια και σαφέστερη κατανόηση της διαδικασίας. Πρέπει να ενεργοποιήσετε την λειτουργία *Advanced Features*, να επιλέξτε το εμπορευματοκιβώτιο του οποίου ο έλεγχος έχει εξουσιοδοτηθεί, και να ανοίξτε την ετικέτα ασφάλειας στο παράθυρο ιδιοτήτων του εμπορευματοκιβωτίου. Κατόπιν, βρείτε τις άδειες και τις ρυθμίσεις ελέγχου πρόσβασης για το χρήστη ή την ομάδα, και διαγράψτε τους. Με αυτόν τον τρόπο, επεμβαίνετε στις καταχωρήσεις ACL για ένα αντικείμενο καταλόγου. Η

αντιπροσωπεία του ελέγχου γίνεται χρησιμοποιώντας την ίδια διαδικασία, αλλά απλοποιείται χάρη στον μάγο. Η κατανόηση αυτής της πτυχής θα σας βοηθήσει να χειριστείτε τα αντικείμενα καταλόγου εύκολα και ελαστικά και, κατά συνέπεια, να συντονίσετε το Active Directory αναλόγως τους στόχους σας

Εξετάστε την εικόνα 3.5. Η αντιπροσωπεία του μάγου ελέγχου έχει εκτελεσθεί δύο φορές. Κατ' αρχάς, η άδεια να ενωθούν οι υπολογιστές στο domain έχει μεταβιβαστεί στην ομάδα Admins. (Μπορείτε να δείτε ότι η άδεια όπως κληρονομείται από το πλαίσιο του domain DC=net,DC=dom.) Δεύτερον, η ομάδα Admins έχει λάβει την άδεια να δημιουργήσει, διαγράψει, και να διαχειριστεί τους λογαριασμούς χρηστών στο OU του προσωπικού. Εκείνο το δικαίωμα καθορίζεται στο επίπεδο OU και δεν κληρονομείται. Κατά συνέπεια, οι άδειες για πλήρη έλεγχο, δημιουργία/διαγραφή αντικειμένων χρηστών, και δημιουργία αντικειμένων υπολογιστών έχει προστεθεί στους καταλόγους ελέγχου πρόσβασης (ACL) του εμπορευματοκιβωτίου περιοχών και του OU προσωπικού. (Στην εικόνα 3.5, μπορείτε να δείτε αυτές τις άδειες στη διατομή **Permission entries**.) Θα μπορούσατε να προσθέσετε αυτά τα δικαιώματα με το χέρι, αλλά ο μάγος σας βοηθά να το κάνετε αυτό χωρίς λάθος και σας ελευθερώνει από να πρέπει να ξέρετε για όλες τις λεπτομέρειες κληρονομιάς και δικαιωμάτων του Active Directory



Εικόνα 3.5: Το αποτέλεσμα της χρήσης του Delegation of Control Wizard: Το επιλεγμένο δικαίωμα δίνει την δυνατότητα στην ομάδα των Admins και να προσθέσουν υπολογιστές στο domain και να διαχειριστούν χρήστες μέσα στο Staff OU.

Εάν θέλετε να ανακαλέσετε όλα τα διαχειριστικά δικαιώματα από την ομάδα Admins, πρέπει να εκτελέσετε τα ακόλουθα βήματα:

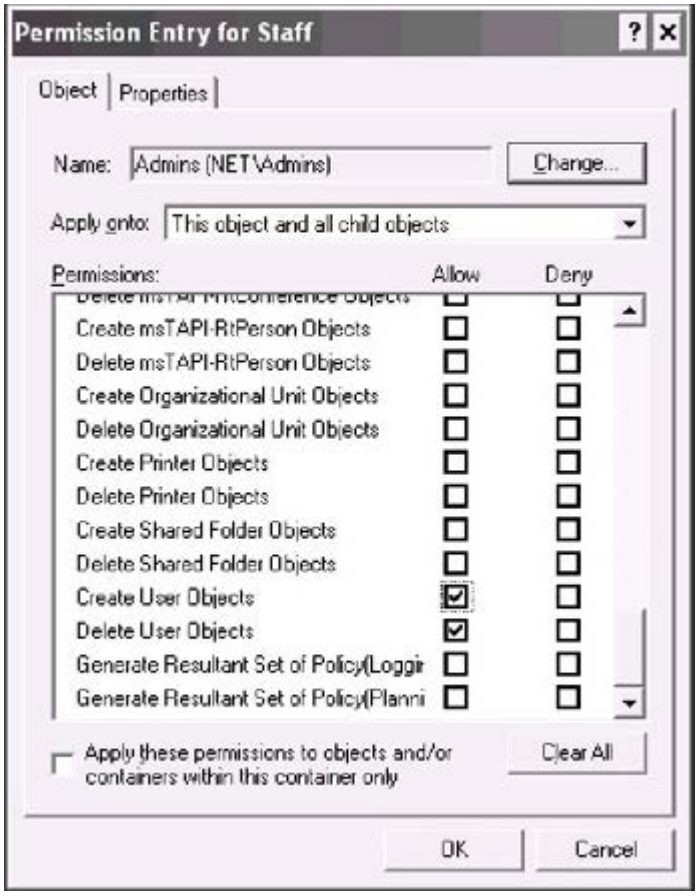
1. Για να ανακαλέσετε τη δύναμη ελέγχου άνω του Staff OU, διαγράψτε τις πρώτες δύο γραμμές στη διατομή **Permission entries**.

   Στα Windows.NET, μπορείτε να πατήσετε το κουμπί προεπιλογή, και όλες οι άδειες που προστίθενται για το επιλεγμένο αντικείμενο καταλόγου θα

διαγραφούν. Να είστε προσεκτικοί, εφόσον: 1) άλλοι χρήστες ή ομάδες μπορεί να έχουν διαχειριστικά δικαιώματα πέρα από το αντικείμενο, και έτσι θα διαγράψετε όλες τις πρόσθετες άδειες και, 2) οι κληρονομημένες άδειες θα αποκατασταθούν.

2. Για να διαγράψετε τις κληρονομημένες άδειες - η άδεια Create Computer Objects στην περίπτωσή μας - ανοίγει την ετικέτα **Security** εκείνου του αντικειμένου όπου οι άδειες έχουν καθοριστεί, και διαγράφει την αντίστοιχη γραμμή(ες) στη διατομή **Permission entries**.

Αφ' ετέρου, μπορεί να θελήσετε να επιτρέψετε στην ομάδα Admins να εκτελέσει μερικούς πρόσθετους στόχους (αφότου έχει εκτελεσθεί μία φορά το Delegation of Control Wizard). Πατήστε **Edit** στην ετικέτα **Permissions** (δείτε την εικόνα 3.5). Το παράθυρο **Permission Entry** θα σας επιτρέψει να καθορίσετε τις άδειες (ή τον εκπροσώπηση/ανακάλεση του διαχειριστικού ελέγχου, όπου είναι το ίδιο πράγμα) στο επιλεγμένο αντικείμενο έπειτα που ο μάγος επιτρέπει. Δεδομένου ότι μπορείτε να δείτε στην εικόνα 3.6, υπάρχουν διάφορες διαδικασίες των οποίων η εκτέλεση από τον επιλεγμένο χρήστη ή ομάδα είναι πιθανό να επιτραπεί/απαγορεύθει



Εικόνα 3.6: "Τέλειο Ρύθμισμα" των δικαιωμάτων στο επιλεγμένο αντικείμενο καταλόγου.

3.10 Ελέγχοντας την Πρόσβαση σε Αντικείμενα του Active Directory

Γενικά, η διαδικασία της ενεργοποίησης του έλεγχου αποτελείται από δύο βήματα. Για να ελέγξετε την πρόσβαση στο Active Directory, πρέπει να:

1. Ενεργοποιήσετε την κατάλληλη πολιτική ελέγχου.
2. Διευκρινίστε τα γεγονότα στον έλεγχο.

Η πρόσβαση ελέγχου στα αντικείμενα του Active Directory αφορά τις διαδικασίες που εκτελούνται στον domain controller. Επομένως, η πιο κατάλληλη θέση για να επιτρέψετε τον έλεγχο είναι η *Default Domain Controllers Policy* (ή ένα άλλο GPO που συνδέεται με το *Domain Controllers* OU). Μπορείτε να χρησιμοποιήσετε είτε το **Group Policy Object Editor** snap-in συνδεμένο με εκείνο το GPO είτε το **Domain Controller Security Policy** snap-in. Επιλέξτε το **Computer Contiguration | Windows Settings | Security Setting | Local Policies | Audit Policy** και πατήστε δύο φορές στο *Audit directory service access* policy (εικόνα 3.7). (Προεπιλογή ρύθμισης για όλες τις πολιτικές ελέγχου - κανένας έλεγχος.) Έπειτα θέστε την σημαία **Define these policy settings** και επιλέξτε το κουτάκι **Success** και/ή **Failure**.

Εικόνα 3.7: Επιτρέποντας τα γεγονότα ελέγχου σχετικά με την πρόσβαση στα ενεργά αντικείμενα καταλόγου

Αφότου έχει τεθεί η πολιτική, μπορείτε αμέσως να το εφαρμόσετε είτε με την εντολή `secedit/refreshpolicy machine_policy` ή `gpupdate /Target:Computer`

Για τις διαδικασίες διαβάσματος, συνιστάται να ελέγχετε τα γεγονότα αποτυχίας, επειδή ένας μεγάλος αριθμός επιτυχών καταχωρημένων γεγονότων μπορεί γρήγορα να ξεχειλίσει το ημερολόγιο ασφαλείας.

Η απόδοση των domain controllers μπορεί επίσης να υποφέρει. Για τις λειτουργίες εγγραφή, δημιουργία/διαγραφή, και άλλες παρόμοιες διαδικασίες (που είναι πολύ λιγότερο συχνές από τις διαδικασίες ανάγνωσης), είναι δυνατό να ελεγχθούν και τα γεγονότα επιτυχίας και αποτυχίας.

Εξ ορισμού, η ειδική πρόσβαση (επιτυχή και αποτυχημένα γεγονότα) σε όλα τα

αντικείμενα σε ένα domain ελέγχεται για την ομάδα *Everyone*. Όλα τα αντικείμενα του domain κληρονομούν αυτήν την ρύθμιση από το domain container ρίζας (εικόνα 3.8). Μερικά εμπορευματοκιβώτια έχουν πρόσθετες ρυθμίσεις ελέγχου. Όλες οι ρυθμίσεις περιλαμβάνουν τον έλεγχο για τις "κρίσιμες" διαδικασίες, όπως εγγραφή, Διαγραφή, Τροποποίηση, και άλλα.

Εικόνα 3.8: Οι προεπιλογής ρυθμίσεις ελέγχου για το κοντεϊνερ χρηστών

Μπορείτε να δείτε όλες τις καταχωρήσεις ελέγχου στο παράθυρο ιδιοτήτων ενός αντικειμένου: ανοίξτε την ετικέτα **Security**, πατήστε στο **Advanced**, και ανοίξτε την ετικέτα **Auditing**. Κατόπιν πατήστε στο **Edit** για να δείτε ή να αλλάξετε τις παραμέτρους ελέγχου. Εάν ανοίγετε την ετικέτα **Auditing** για ένα αντικείμενο καταλόγου εκτός της ρίζας, θα παρατηρήσετε ότι όλα τα ελεγμένα κουτιά δεν είναι ενεργά. Αυτό σημαίνει ότι όλες οι παράμετροι κληρονομούνται από το αντικείμενο γονέων. Δεν μπορούν να τροποποιηθούν άμεσα, έτσι μπορεί να χρειαστεί να εξετάσετε το αντικείμενο γονέων ή ρίζας. Εάν επιλέξετε ένα ελεύθερο κουτί, το σύστημα θα δημιουργήσει μια νέα είσοδο ελέγχου και θα την προσθέσει στον κατάλογο για το επιλεγμένο αντικείμενο μόνο.

Μπορείτε να δείτε όλες τις πληροφορίες για τα γεγονότα ελέγχου ημερολόγιο ασφαλείας του Event Viewer. Η πηγή για αυτά τα γεγονότα είναι " Security ", και η κατηγορία είναι " Directory Service Access ".

3.11 Επανακτώντας το Active Directory

3.11.1 Γενικές Πληροφορίες

Η τυποποιημένη εφεδρική εφαρμογή (NTBackup.exe) σας επιτρέπει να κρατήσετε αντίγραφα ασφαλείας αλλά και να αποκαταστήσετε κρίσιμα δεδομένα και το Active Directory. Οι διαδικασίες με το Active Directory μπορούν μόνο να γίνουν τοπικά για κάθε domain controller. Μια εφεδρική λειτουργία εκτελείται ενώ ένα DC είναι online. Για να αποκαταστήσετε το Active Directory σε ένα DC, πρέπει να ξεκινήσετε αυτό το DC σε *Directory Service Restore Mode* (πατώντας < F8 > στο ξεκίνημα του υπολογιστή).

3.11.2 Κατάσταση Συστήματος

Η δημιουργία αντιγράφων ασφαλείας του Active Directory είναι ένα μέρος της διαδικασίας του σωσίματος των δεδομένων του *System State* ενός DC. Δεν μπορείτε να κρατήσετε αντίγραφα ασφαλείας (ή να αποκαταστήσετε) μεμονωμένα στοιχεία της κατάστασης του συστήματος. Σε έναν κεντρικό υπολογιστή μέλος ή έναν τερματικό σταθμό, η κατάσταση συστήματος περιλαμβάνει τα εξής:

- Boot Files
- COM+ Class Registration Database
- Registry

Σε έναν domain controller, δύο άλλα στοιχεία προστίθενται (εικόνα 3.9):

εικόνα 3.9: Στοιχεία της κατάστασης συστήματος domain controller

- Active Directory (τα αρχεία ntds.dit, edb.chk, edb *.log, και resl.log και res2.log)

- SYSVOL (System Volume) (εξ ορισμού, ο *%SystemRoot%*\SYSVOL\sysvol φάκελος)

Εάν οι υπηρεσίες πιστοποιητικών είναι εγκατεστημένες σε έναν κεντρικό υπολογιστή ή ένα DC, υπάρχει ένα επιπλέον στοιχείο:

- Certificate Server

Σύμφωνα με τα προηγούμενα είναι δυνατό να βγάλουμε δύο πολύ σημαντικά συμπεράσματα:

- Δεν μπορείτε να κρατήσετε αντίγραφα ασφαλείας του System State σε ένα DC και να το αποκαταστήσετε σε έναν άλλο DC, από την στιγμή που το System State περιλαμβάνει τέτοιες σημαντικές πληροφορίες όπως το COM+ Class Registration Database, TCP/IP configuration, κ.λπ.... Εάν αποκαθιστάτε εφεδρικά μέσα σε έναν άλλο υπολογιστή, θα πάρετε τις ίδιες παραμέτρους συστημάτων όπως έχει το αρχικό DC, που οδηγεί σε μοιραία σύγκρουση.
- Δεν υπάρχει λόγος για να σώσετε/αποκαταστήστε την διαμόρφωση του Active Directory "ο ίδιος", π.χ., ανεξάρτητα από τη διαμόρφωση των domain controllers. Κατά τη διάρκεια κάθε αποκατάστασης της κατάστασης του συστήματος θα αναδημιουργήσετε ένα συγκεκριμένο DC. Γί'αυτό η εξαγωγή/ εισαγωγή εργαλείων, όπως το LDIFDE και το CSVDE, θα μπορούσε να είναι πολύ χρήσιμη, δεδομένου ότι σας επιτρέπουν να σώσετε/αποκαταστήσετε μόνο τις διάφορες πληροφορίες του Active Directory.

3.11.3 Schema

Οι τροποποιήσεις του σχήματος είναι αμετάκλητες, έτσι δεν μπορείτε να αποκαταστήσετε μια παλαιότερη έκδοση του σχήματος. Τα δημιουργημένα χαρακτηριστικά και κατηγορίες δεν μπορούν να διαγραφούν, και είναι μόνο δυνατό να απενεργοποιηθούν. Κατά την αποκατάσταση του Active Directory, δεν μπορείτε να επιλέξετε το χώρισμα σχημάτων σαν απαρέγκλιτο

3.11.4 Tombstones

Ένα σχέδιο αποκατάστασης πρέπει να λάβει υπόψη τη διάρκεια ζωής των Active Directory *tombstones* (60 ημέρες, εξ ορισμού η ελάχιστη τιμή είναι 2 ημέρες). Αυτή η παράμετρος αποθηκεύεται (εάν καθορίζεται) στις ιδιότητες tombstoneLifetime ενός αντικειμένου καταλόγου που ονομάζεται *N=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=<ForestRoot>*. Η ταφόπετρα είναι ένα διαγραμμένο αντικείμενο που διατηρείται στο Active Directory κατά τη διάρκεια της διάρκειας ζωής του, πριν το σύστημα τελικά το καταστρέψει. Η ηλικία της εφεδρικής ταινίας δεν πρέπει να υπερβεί αυτήν την

χρονική περίοδο, διαφορετικά τα ξεπερασμένα στοιχεία θα απορριφθούν.

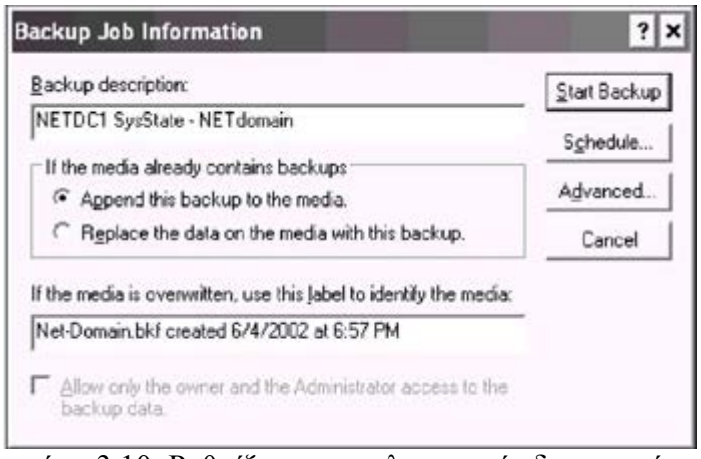
3.11.5 Χρησιμοποιώντας Αντίγραφα Ασφαλείας για την Εγκατάσταση Πρόσθετων Domain Controllers

Για να μειωθεί το ποσό των replicated δεδομένων ενώ προάγοντας έναν Windows.NET-based server στον πρόσθετο domain controller, μπορείτε να χρησιμοποιήσετε ένα εφεδρικό αρχείο που περιέχει την κατάσταση συστήματος ενός υπάρχοντος DC. Επομένως, πρέπει αρχικά να σώσετε τις τρέχουσες πληροφορίες του Active Directory..

3.11.6 Backing up Active Directory

Κρατώντας αντίγραφα ασφαλείας της κατάστασης συστήματος:

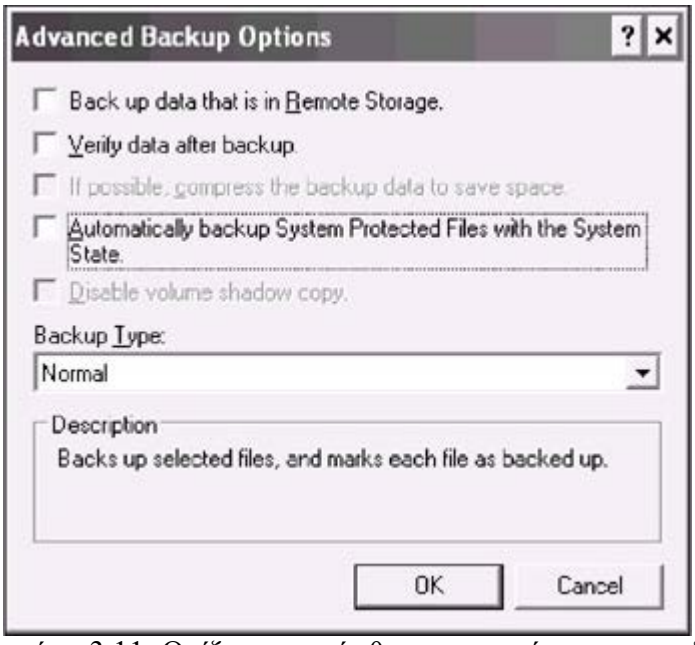
1. Τρέξτε την εφαρμογή δημιουργίας αντιγράφων ασφαλείας: πατήστε το **Start | All Programs | Accessories | System Tools | Backup** ή εισάγετε ntbackup στο παράθυρο **Run**.
2. Πατήστε στην ετικέτα **Backup** και ελέγξτε το κουτί **System State** στη διατομή του δέντρου. (Μπορείτε επίσης να περιλάβετε μερικά αρχεία στο αντίγραφο ασφαλείας.)
3. Εισάγετε το όνομα του εφεδρικού αρχείου στα εφεδρικό μέσα ή στο πεδίο ονόματος αρχείων (κρατήστε την επέκταση αρχείων BKF) και πατήστε το **Start Backup**.
4. Στο παράθυρο **Backup Job Information** (εικόνα 3.10), εισάγετε τα απαραίτητα στοιχεία και πατήστε **Advanced**.



εικόνα 3.10: Ρυθμίζοντας μια λειτουργία δημιουργίας αντιγράφων ασφαλείας

5. Το επόμενο παράθυρο (εικόνα 3.11) θα σας επιτρέψει να θέσετε τις επιλογές εφεδρείας. Το The System State πρέπει πάντα να αποθηκεύεται ως κανονικό αντίγραφο ασφαλείας. Να θελήσετε να καθαρίσετε το πεδίο **Automatically**

backup System Protected Files with the System State καθορισμένο εξ ορισμού εάν χρειάζεστε ένα συμπαγές εφεδρικό αρχείο χωρίς όλα αρχεία συστήματος. Συνήθως, είναι αρκετό να έχετε ένα τέτοιο συμπαγές αρχείο (40-50 MB για μικρά domains) για πολλές διαδικασίες σχετικές με την αποθήκευση/αποκατάσταση του Active Directory. Ένα πλήρες αντίγραφο ασφαλείας της κατάστασης του συστήματος θα είναι περίπου 300 MB στο μέγεθος.



εικόνα 3.11: Ορίζοντας πρόσθετες παραμέτρους στην δημιουργία αντιγράφων ασφαλείας

6. Κλείστε το παράθυρο **Advanced Backup Options** και πατήστε το **Start Backup** και η διαδικασία **Backup** θα αρχίσει

3.11.7 Αποκαθιστώντας το Active Directory

Η αποκατάσταση είναι μια πιο περίπλοκη διαδικασία από το backup . Γενικά, έχετε δύο επιλογές:

- Επαναεγκαταστήστε το σύστημα στο χαλασμένο υπολογιστή, προάγετε το σε έναν domain controller, και αντιγράψτε τις πληροφορίες του Active Directory από άλλα DCs μέσω του replication. Θα πάρετε ένα εξ ολοκλήρου νέο DC, και, επομένως, πρέπει να διαγραφούν οποιεσδήποτε αναφορές στο παλαιό DC από το Active Directory.
- Αποκαταστήστε το Active Directory από τα εφεδρικά μέσα, διατηρώντας την ταυτότητας του DC (sid, GUID, κ.λπ....).

Υπάρχουν τρεις διαφορετικές μέθοδοι αποκατάστασης της κατάστασης του συστήματος από εφεδρικά μέσα:

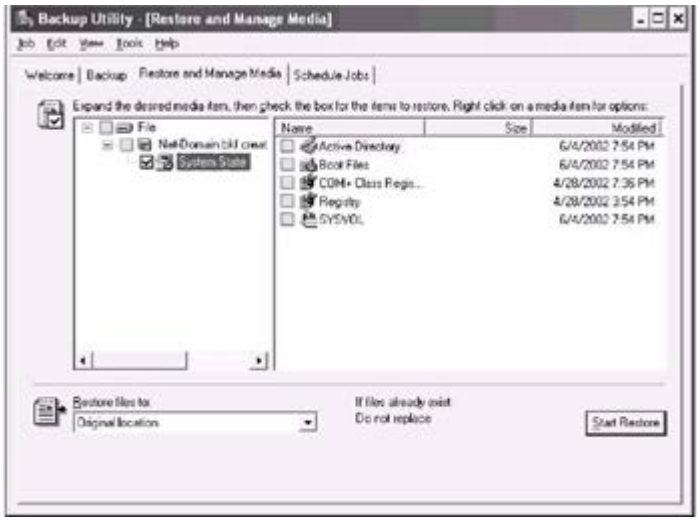
- Εκτελέστε ένα **primary restore** όταν έχετε το μοναδικό DC στο domain και θέλετε να ξαναδημιουργήσετε αυτήν την περιοχή. Μια αρχική αποκατάσταση δημιουργεί μια νέα βάση δεδομένων FRS. Επομένως, τα αποκατεστημένα στοιχεία θα γίνουν replicated σε άλλους controllers στο domain.
- Εάν υπάρχει τουλάχιστον ένα λειτουργικό DC στο domain, εκτελέστε ένα **non-authoritative (normal) restore**. Το επισκευασμένο DC θα λάβει τα τρέχοντα στοιχεία από άλλα DCs μέσω του κανονικού replication. Τα αποκατεστημένα στοιχεία δεν θα γίνουν ποτέ replicated σε άλλα DCs. Αυτός είναι ο πιο χρησιμοποιημένος τύπος αποκατάστασης.
- Εάν θέλετε να αποκαταστήσετε ακούσια τα διαγραμμένα δεδομένα του Active Directory και να τα κάνετε replicate στα άλλα DCs, εκτελέστε ένα **authoritative restore**. Δεν μπορείτε να εκτελέσετε ένα "αληθινό" πισωγύρισμα, εφόσον η απαρέγκλιτη αποκατάσταση δεν έχει επιπτώσεις στις αλλαγές που γίνονται στον κατάλογο αφότου δημιουργήθηκε το αντίγραφο ασφαλείας. Αυτά τα νέα στοιχεία θα γίνουν replicate στο αποκατεστημένο DC.

Θυμηθείτε ότι σε κάθε περίπτωση το Active Directory μπορεί να αποκατασταθεί μόνο όταν ένας DC έχει ξεκινήσει στο Directory Service Restore Mode.

3.11.8 Βασική Αποκατάσταση

Για να αποκαταστήσετε έναν αυτόνομο domain controller:

1. Τρέξτε την εφαρμογή εφεδρείας και ανοίξτε το **Restore and Manage Media** (εικόνα 3.12).



εικόνα 3.12: Αποκαθιστώντας την κατάσταση του συστήματος από ένα αντίγραφο ασφαλείας.

2. Επιλέξτε τα απαραίτητα μέσα και ελέγξτε το κουτί **System State**. Τα αρχεία πρέπει να αποκατασταθούν στην αρχική θέση.
3. Πατήστε το **Start Restore** και επιβεβαιώστε υπερκαλύπτοντας την επικρατούσα κατάσταση του συστήματος στο εμφανιζόμενο παράθυρο προειδοποίησης.
4. Πατήστε **Advanced** στο παράθυρο **Confirm Restore**.
5. Θέστε το τετραγωνίδιο που παρουσιάζεται στην εικόνα 3.13. Κλείστε το παράθυρο, και αρχίστε την αποκατάσταση.

Εικόνα 3.13: Αυτό το τετραγωνίδιο ορίζεται μόνο για βασική αποκατάσταση.

6. Όταν η εφαρμογή εφεδρείας θα τελειώσει, θα σας προτείνει να επανεκκινήσετε τον υπολογιστή, απάντηση θετικά - επανεκκινήστε τον υπολογιστή σε normal mode.

3.11.9 Μη-Επιτακτική Αποκατάσταση

Μια μη-επιτακτική αποκατάσταση εκτελείται όπως μια αρχική αποκατάσταση. Η διαφορά είναι ότι πρέπει να κρατήσετε τις προεπιλεγμένες ρυθμίσεις όλων των επιλογών, π.χ., το τετραγωνίδιο που παρουσιάζεται στην εικόνα 3.13 πρέπει να αποεπιλεχθεί. Το αποκατεστημένο DC θα λάβει όλες τις αλλαγές από τους συνεργάτες του replication.

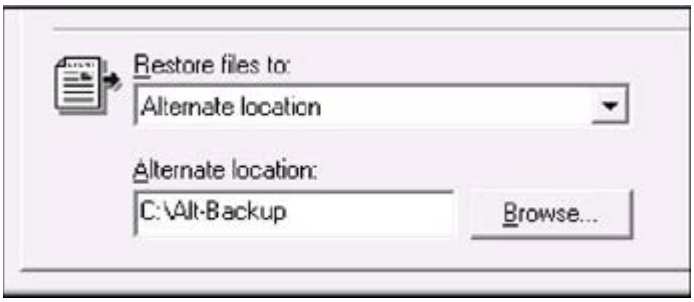
3.11.10 Επιτακτική Αποκατάσταση

Για να εκτελέσετε μια επιτακτική αποκατάσταση του Active Directory συμπεριλαμβανομένου του όγκου SYSVOL, διενεργήστε τις ακόλουθες διαδικασίες:

1. Τρέξτε την εφαρμογή εφεδρείας και εκτελέστε μια μη-επιτακτική αποκατάσταση Όταν η εφαρμογή εφεδρείας ολοκληρώνει την εργασία της, προτείνει ότι ξαναξεκινάτε τον υπολογιστή (εικόνα 3.14). Πρέπει να πατήσετε Οχι.

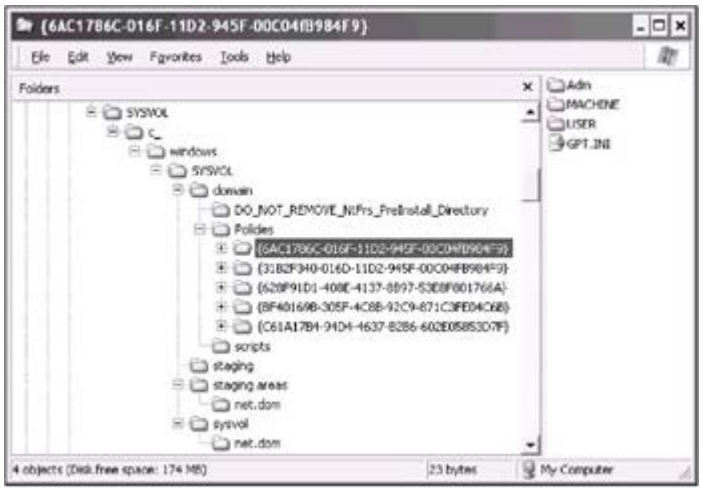
Εικόνα 3.14: Πατήστε Όχι εάν εκτελείτε μια μη-επιτακτική αποκατάσταση

2. Αποκαταστήστε την κατάσταση του συστήματος σε μια εναλλακτική θέση. Δείτε ένα παράδειγμα στην εικόνα 3.15



Εικόνα 3.15: Επιλογή μιας εναλλακτικής θέσης μια λειτουργία αποκατάστασης.

3. Στους Windows .NET-based servers οι ακόλουθοι φάκελοι θα εμφανιστούν στον συγκεκριμένο φάκελο ή στον δίσκο (Εικόνα 3.16):



Εικόνα 3.16: Δομή του φακέλου SYSVOL σε μια εναλλακτική θέση

   - Active Directory (ntds.dit, edb *.log αυτά τα αρχεία μπορούν να χρησιμοποιηθούν αργότερα για να προαγάγουν έναν κεντρικό υπολογιστή σε πρόσθετο DC)
   - Αρχεία εκκίνησης
   - COM+ βάση δεδομένων εγγραφής κατηγορίας (ComReg.DB.bak)
   - μητρώο (προεπιλογή, SAM, SECURITY, λογισμικό, σύστημα)
   - SYSVOL (αυτός ο φάκελος απεικονίζει τη δομή του όγκου SYSVOL)
4. Όταν αποκαθιστάτε τα στοιχεία σε μια εναλλακτική θέση, το πρόγραμμα δεν προτρέπει να επανεκκινήσετε τον υπολογιστή. Κλείστε το πρόγραμμα εφεδρείας.

5. Τρέξτε το NTDSutil.exe από την γραμμή εντολών. Ένας δειγματικός διάλογος για την εντολή *authoritative restore* τοποθετείται κατωτέρω (ένα υποδέντρο αποκαθίσταται σε αυτό το παράδειγμα):

```
C:\>ntdsutil
ntdsutil: Authoritative restore
authoritative restore: Restore subtree OU=Staff,DC=net,DC=dom
[Confirm the restore operation — click Yes in the pop-up window.}
```


```
Opening DIT database... Done.

The current time is 06-04-02 20:41.05.
Most recent database update occured at 06-03-02 17:52.23.
Increasing attribute version numbers by 200000.

Counting records that need updating...
Records found: 0000000038
Done.

Found 38 records to update.
Updating records...
Records remaining: 0000000000
Done.

Successfully updated 38 records.

Authoritative Restore completed successfully.
authoritative restore: Quit
ntdsutil: Quit
```

10. Επανεκκινήστε τον υπολογιστή σε normal mode και περιμένετε μέχρι ο όγκος SYSVOL να δημοσιευθεί (ψάξτε τον αριθμό γεγονότος 13516 στο File Replication Service log και χρησιμοποιήστε την εντολή κοινής χρήσης δικτύου για έλεγχο όταν θα ολοκληρωθεί η διαδικασία).
11. Αντιγράψτε τα περιεχόμενα του όγκου SYSVOL από την εναλλακτική θέση σε μια υπάρχουσα. Αυτές οι αλλαγές του όγκου SYSVOL θα είναι οι πιο πρόσφατες και, επομένως, θα γίνει replicated σε άλλα DCs ως επιτακτικά στοιχεία.

Στο παράδειγμα που παρουσιάζεται, ένα αντικείμενο OU έχει αποκατασταθεί. Μπορείτε να επιλέξετε ένα μεμονωμένο αντικείμενο (σε περιβάλλον Windows.NET), υποδέντρο, ή ολόκληρο χώρισμα καταλόγου όπως επιτακτικό. Αυτό, εντούτοις, δεν επεκτείνεται στο χώρισμα σχημάτων

Παρατηρήστε τη γραμμή με έντονα γράμματα που δείχνει μια αύξηση των αριθμών έκδοσης ιδιοτήτων, και δύο προηγούμενες γραμμές. Οι αριθμοί έκδοσης αυξάνονται κατά 100.000 για κάθε ημέρα αφότου έχει εκτελεσθεί το αρχικό backup. Μπορείτε να δείτε τις αλλαγές των μεταδεδομένων με τη χρησιμοποίηση του ReplMon.exe. Στην περίπτωσή μας, παραδείγματος χάριν, η ακόλουθη εντολή θα χρησιμοποιηθεί:

```
repadmin /showmeta OU=Staff, DC=net, DC=dom netdc4.net.dom
```

Με τη χρησιμοποίηση αυτής της εντολής σε διαφορετικά DCs, μπορείτε να ελέγξετε εάν η επιτακτική αποκατάσταση ήταν επιτυχής, και εντοπίστε τη διάδοση του replication. Εάν αντικείμενα στην εγκατάσταση του Active Directory σας έχουν πολύ χαμηλή αστάθεια, μπορεί να θελήσετε να αγνοήσετε την προκαθορισμένη αξία της αύξησης έκδοσης. Χρησιμοποιήστε μια εντολή παρόμοια με την εξής:

```
restore subtree OU=Staff, DC=net,DC=dom verinc 1000
```

4. Εργαλεία ασφάλειας

4.1 Επισκόπηση

Αυτό το κεφάλαιο περιγράφει τα εργαλεία σχετικά με την ασφάλεια του Active Directory και πρώτιστα, τις άδειες στα αντικείμενα καταλόγου. Αυτά τα εργαλεία επιτρέπουν σε έναν διαχειριστή να εκτελέσει τους ακόλουθους στόχους:

- άποψη / ή τροποποίηση των άδειων των αντικείμενων καταλόγου (ACLDiag, DsACLs) και έλεγχος της μεταβίβασης των διαχειριστικών στόχων
- έλεγχος της κληρονομιάς ACLs σε διαφορετικά επίπεδα της ιεραρχίας και του replication του ACLs μεταξύ των domain controllers (SDCheck)
- έλεγχος της επικύρωσης του Kerberos (KerbTray, KList)

4.2 Διαγνωστικά ACL (ACLDiag.exe) (ST)

Συχνότερα, ένας διαχειριστής βλέπει και τροποποιεί τις ρυθμίσεις ασφάλειας (μιας *Access Control List*, ACL) σε ένα αντικείμενο Active Directory με τη χρησιμοποίηση της καρτέλας ασφάλειας του παραθύρου ιδιοτήτων του αντικειμένου. Αυτό το παράθυρο μπορεί να ανοίξει από ένα κατάλληλο ένα διαχειριστικό snap-in.

Μερικές φορές, είναι καταλληλότερο να αναλυθούν οι κατάλογοι ACL σε μια "plain text" μορφή. Το εργαλείο ACLDiag θα επιτρέψει σε έναν διαχειριστή να δει όλες τις πληροφορίες για την ασφάλεια ενός καταλόγου αντικειμένου. Οποιοσδήποτε χρήστης μπορεί να τρέξει το ACLDiag, αλλά η έξοδος του εργαλείου θα εξαρτηθεί από τα δικαιώματα του χρήστη, για να δει το αντικείμενο (ή μερικά άλλα αντικείμενα).

Οι επιλογές ACLDiag's θα συζητηθούν στα παραδείγματα του εξής τμήματος. (Να προτιμήσετε να χρησιμοποιήσετε το εργαλείο DsACLs αν και δεν έχει μερικά από τα χαρακτηριστικά γνωρίσματα του ACLDiag, αλλά επιτρέπει τις τροποποιήσεις ACL και φαίνεται να είναι πιο αξιόπιστο.)

Είναι απαραίτητο να σημειώσουμε ότι αυτό το εργαλείο απαιτεί αρκετό χρόνο για να τρέξει, ειδικά όταν η παράμετρος /geteffective είναι ενεργοποιημένη και αυτό που παράγει πρέπει συνήθως να επαναπροσανατολιστεί σε ένα αρχείο.

4.3 Προβολή όλων των αδειών

Το ACLDiag μπορεί να επιδείξει όλες τις άδειες που καθορίζονται άμεσα ή που κληρονομούνται σε ένα αντικείμενο Active Directory, όπως και τις ρυθμίσεις λογιστικού ελέγχου. Η έξοδος του εργαλείου είναι δομημένη για να βοηθήσει έναν διαχειριστή να αναλύσει τις πληροφορίες. Ουσιαστικά, το εργαλείο έχει δύο υπορουτινες: Διάγνωση ασφάλειας (μπορείτε να το παρακάμψετε με τη χρήση της παραμέτρου /skip) και Διάγνωση αποτελεσματικών δικαιωμάτων. Δείτε, παραδείγματος χάριν, σε ποια μορφή το ACLDiag εμφανίζει τις άδειες για ένα OU. (Για καλύτερη κατανόηση οι τίτλοι του τμήματος εξόδου είναι με μαύρους χαρακτήρες.)

```
C:\>acldiag "OU=Staff, DC=net, DC=dom"

Security Diagnosis for OU=Staff, DC=net, DC=dom
Description

        Owner: NET\Domain Admins

        Permissions effective on the object:
                Allow NT AUTHORITY\Authenticated Users Read all
properties
                Allow NT AUTHORITY\Authenticated Users List
contents
                Allow NT AUTHORITY\Authenticated Users List
object
                Allow NET\Domain Admins Create all subobjects
                Allow NET\Domain Admins Delete all subobjects
...
Permissions inherited by subobjects:
      Inherit to All Subobjects:
                Allow BUILTIN\Administrators Create all
subobjects
                 (Inherited permission from DC=net, DC=dom)
                Allow BUILTIN\Administrators Read all properties
                (Inherited permission from DC=net, DC=dom)
...
      Inherit to Group objects only:
...
```

```
        Inherit to User objects only:
...
        Inherit to InetOrgPerson objects only:
...
Auditing effective on this object:
                Audit Successful and Failed Create all subobjects
attempts by \Everyone
                Audit Successful and Failed Delete all subobjects
attempts by \Everyone
...
Auditing inherited to subobjects:
        Inherit to All Subobjects:
                Audit Successful and Failed Create all subobjects
attempts by \Everyone
                Audit Successful and Failed Delete all subobjects
attempts by \Everyone
...
```

Όπως είδαμε παραπάνω υπάρχει μια νέα αρχή ασφάλειας στα Windows.NET - ένας τύπος αντικειμένου που ονομάζεται inetOrgPerson. Φυσικά, μπορείτε να δημιουργήσετε αντικείμενα αυτού του τύπου και να ορίσετε άδειες σε αυτά

4.4 Βλέποντας τα αποτελεσματικά δικαιώματα

Για να δείτε τα αποτελεσματικά δικαιώματα όλων ή μερικών χρηστών ή ομάδων, χρησιμοποιήστε την παράμετρος /geteffective . Παραδείγματος χάριν, η ακόλουθη εντολή εμφανίζει τα δικαιώματα σε ένα OU για όλους τους χρήστες και τις ομάδες. Εάν τα δικαιώματα δεν καθορίζονται άμεσα για έναν χρήστη ή μια ομάδα, το αντίστοιχο τμήμα εξόδου θα είναι κενό. Όπως μπορείτε να δείτε, οι αναλυτικές πληροφορίες για τις άδειες κάθε αντικειμένου δίνονται.

```
C:\>acldiag "OU=Staff, DC=net, DC=dom" /geteffective: * /skip
Security Diagnosis for OU=Staff, DC=net, DC=dom

Effective Rights Diagnosis

NET\Domain Admins:
                    Can Modify Membership (via NET\Domain Admins
membership)
                    All control accesses for class Organizational
Unit (via
   NET\Domain Admins membership)
                    Can List object (via NET\Domain Admins
membership)
                    Can List contents (via NET\Domain Admins
membership)
                    Write all properties for class Organizational
Unit (via
   NET\Domain Admins membership)
                    Read all properties for class Organizational Unit
(via
   NET\Domain Admins membership)
```

```
                        Delete all subobjects of class Organizational
Unit (via
   NET\Domain Admins membership)
                        Create all subobjects of class Organizational
Unit (via
   NET\Domain Admins membership)

   JSmith@net.dom:
                        Can List contents
                        Read all properties for class Organizational Unit
   NET\Staff-Admins:
                        Delete all subobjects of class Organizational
Unit (via
   NET\Staff-Admins membership)
                        Create all subobjects of class Organizational
Unit (via
   NET\Staff-Admins membership)

   NET\Enterprise Admins:
                        Can Modify Membership
                        All control accesses for class Organizational
Unit
                        Can List object
                        Can List contents
                        Write all properties for class Organizational
Unit
                        Read all properties for class Organizational Unit
                        Delete all subobjects of class Organizational
Unit (via
                        NET\Enterprise Admins membership)
                        Create all subobjects of class Organizational
Unit
```

4.5 Επαλήθευση της δικαιοδοσίας του ελέγχου

Το ACLDiag επιτρέπει σε έναν διαχειριστή να ελέγχει εάν η δικαιοδοσία του *βοηθού ελέγχου* έχει τρέξει για ένα αντικείμενο, και εάν αυτός ο μάγος έχει τρέξει επιτυχώς ή όχι . Εξετάστε ένα παράδειγμα. Στο ακόλουθο σενάριο, ο χρήστης `jsmith@net.dom` και η ομάδα `Staff-Admins@net.dom` έχουν λάβει τα συγκεκριμένα διαχειριστικά δικαιώματα πάνω από το *Staff* OU. (Θυμηθείτε ότι στα Windows .NET, υπάρχουν 11 κοινοί διαχειριστικοί στόχοι για τα αντικείμενα OU στα in Windows 2000 - μόνο έξι διεργασίες.) Με τη χρησιμοποίηση μιας εντολής παρόμοιας με την ακόλουθη, μπορείτε εύκολα να καθορίσετε ποιος έχει τα εξουσιοδοτημένα δικαιώματα και ποια είναι αυτά :

```
   C:\>acldiag "OU=Staff, DC=net, DC=dom" /chkdeleg _skip
   Security Diagnosis for OU=Staff, DC=net, DC=dom

   Delegation Template Diagnosis:

          Create, delete, and manage user accounts allowed to
NET\Staff-Admins
                  Status: OK
```

```
                Applies on this object: YES
                Inherited from parent: NO

        Reset user passwords and force password change at next logon
        allowed to JSmith@net.dom
                Status: OK
                Applies on this object: YES
                Inherited from parent: NO

        Read all user information allowed to JSmith@net.dom
                Status: OK
                Applies on this object: YES
                Inherited from parent: NO

        Create, delete and manage groups allowed to NET\Staff-Admins

                Status: MISCONFIGURED
                Applies on this object: YES
                Inherited from parent: NO

        Modify the membership of a group
                Status: NOT PRESENT

        Manage Group Policy links allowed to NET\Staff-Admins
                Status: OK
                Applies on this object: YES
                Inherited from parent: NO

        Generate Resultant Set of Policy (Planning)
                Status: NOT PRESENT

        Generate Resultant Set of Policy (Logging)
                Status: NOT PRESENT

        Create, delete, and manage inetOrgPerson accounts
                Status: NOT PRESENT

        Reset inetOrgPerson passwords and force password change at
next
        logon allowed to JSmith@net.dom
                Status: OK
                Applies on this object: YES
                Inherited from parent: NO

        Read all inetOrgPerson information
                Status: NOT PRESENT
```

Παρατηρείστε ότι εάν μια κοινή διεργασία δεν έχει ανατεθεί, το εργαλείο αναφέρει τη κατάσταση ως NOT PRESENT. Όπως μπορείτε να δείτε, η κατάσταση διεργασίας είναι MISCONFIGURED. (Σε αυτήν την περίπτωση, ένα από τα ACEs που συνθέτει τη διαχειριστική διεργασία έχει διαγραφεί.) Εάν η παράμετρος /fixdeleg δεν μπορεί να διορθώσει το πρόβλημα, πρέπει να τρέξετε την δικαιοδοσία του βοηθού ελέγχου πάλι. Μπορείτε επίσης να τρέξετε την εφαρμογή DsACLs.exe χρησιμοποιώντας την παράμετρος /s, η οποία αναστοιχειοθετεί όλες τις άδειες του αντικειμένου στο προεπιλεγμένο schema. (Χρησιμοποιήστε αυτήν την επιλογή με προσοχή! Δείτε το

τμήμα "Αποκατάσταση Ρυθμίσεων Ασφάλειας" παρακάτω σε αυτό το κεφάλαιο.)

Για να φτιαχτούν οι εξουσιοδοτημένες ρυθμίσεις ελέγχου, χρησιμοποιήστε την ακόλουθη εντολή:

```
C:\>acldiag "OU=Staff, DC=net, DC=dom" /chkdeleg /fixdeleg /skip
```

Η εντολή επιβεβαιώνει όλες τις άδειες και εάν λείπει κάποια, το πρόγραμμα ρωτάει εάν θέλουμε να διορθώσουμε το πρόβλημα. Παραδείγματος χάριν:

```
Create, delete and manage groups allowed to NET\Staff-Admins
        Status: MISCONFIGURED
        Applies on this object: YES
        Inherited from parent: NO

        Do you want to fix this delegation? (y/n)y
```

4.6 Σύγκριση με το Schema προκαθορισμένων αδειών

Για να ελεγχθεί εάν ένα αντικείμενο Active Directory διατηρεί όλες τις άδειες που τέθηκαν τη στιγμή της δημιουργίας του, χρησιμοποιήστε μια εντολή παρόμοια με την εξής:

```
C:\>acldiag "OU=Staff, DC=net, DC=dom" /schema /skip

Security Diagnosis for OU=Staff, DC=net, DC=dom

Schema Defaults Diagnosis
        Schema defaults: Present
        Obtained            : At CREATION
```

Στην περίπτωση που παρουσιάζεται, το εργαλείο αναφέρει ότι το αντικείμενο κράτησε όλες τις άδειες ορισμένες από την δημιουργία του. Εάν κάποια άδεια έχει αφαιρεθεί, το εργαλείο επιδεικνύει το μήνυμα

```
Schema defaults: Partial
```

Για να δούμε τις προεπιλεγμένες (schema) άδειες σε έναν κατάλογο, πρέπει να αναφερθούμε στο χώρισμα του schema. Για ένα αντικείμενο OU, χρησιμοποιήστε μια εντολή παρόμοια με την εξής:

```
C:\>acldiag "CN=Organizational-Unit, CN=Schema, CN=Configuration,

   DC=net, DC=dom"
```

4.7 DsACLs (DsACLs.exe) (ST)

Σε αντίθεση με ACLDiag, το εργαλείο γραμμής εντολών DsACLs επιτρέπει σε έναν διαχειριστή να δει και να τροποποιήσει τους καταλόγους ACL καταλόγους αντικειμένων π.χ. για να φέρει εις πέρας όλες τις διαθέσιμες διαδικασίες στην καρτέλα ασφαλείας στο παράθυρο ιδιοτήτων του αντικειμένου. (Για τα αντικείμενα καταλόγου, το DsACLs κάνει μια εργασία παρόμοια με αυτή του CACLs.exe για τα αντικείμενα συστημάτων αρχείων.) Η τροποποίηση των περιγραφέων ασφάλειας μπορεί να απαιτήσει μια καλή κατανόηση του προτύπου ασφάλειας του αντικειμένου Active Directory και ειδικά την κληρονομικότητα των αδειών.

4.8 Βλέποντας τις ρυθμίσεις ασφάλειας

Μπορείτε να αναλύσετε την ακόλουθη έξοδο της οθόνης και να αποφασίσετε ποιο εργαλείο - DsACLs ή ACLDiag - είναι καταλληλότερο για σας να χρησιμοποιήσετε όταν παρακολουθείτε η εξέταση των περιγραφέων ασφάλειας του καταλόγου. (Η προηγούμενη εντολή λειτουργεί γρηγορότερα, αλλά δεν είναι τόσο περιεκτική όσο η τελευταία. Παραδείγματος χάριν, οι γραμμές αφορούσαν την ομάδα Admins του *Domain* στην εξαγωγή και των δύο εντολών. Ίσως, οι ίδιοι θέλετε να επιλέξετε ένα αντικείμενο και να συγκρίνετε τα πλήρη αποτελέσματα.) Όταν η παράμετρος /A διευκρινίζεται, οι πληροφορίες ιδιοκτητών και ελέγχου εμφανίζονται. Στον λογιστικού κατάλογο ελέγχου, "Όλα" σημαίνει ότι ένας λογιστικός έλεγχος εκτελείται και για τα επιτυχή και τα αποτυχημένα γεγονότα.

```
C:\>dsacls OU=Staff, DC=net, DC=dom /A
Owner: NET\Domain Admins
Group: NET\Domain Users

Audit list:
Effective Permissions on this object are:
All     Everyone  SPECIAL ACCESS   <Inherited from parent>
                  DELETE
                  WRITE PERMISSIONS
...
Permissions inherited to subobjects are:
Inherited to all subobjects
All    Everyone   SPECIAL ACCESS   <Inherited from parent>
                  DELETE
                  WRITE PERMISSIONS
...
Access list:
Effective Permissions on this object are:
Allow NT AUTHORITY\Authenticated Users             SPECIAL ACCESS
                                                   READ PERMISSONS
...
Allow NET\Domain Admins                            FULL CONTROL
Allow NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS   SPECIAL ACCESS
                                                   READ PERMISSIONS
...
Allow NT AUTHORITY\SYSTEM                          FULL CONTROL
Allow BUILTIN\Administrators                       SPECIAL ACCESS
```

```
<Inherited from parent>
                                                    DELETE
                                                    READ PERMISSIONS
...
Permissions inherited to subobjects are:
Inherited to all subobjects
Allow BUILTIN\Administrators                        SPECIAL ACCESS
<Inherited from parent>
                                                    DELETE
                                                    READ PERMISSIONS
...
Inherited to computer
...
Inherited to group
...
Inherited to user
...
Inherited to inetOrgPerson
...
The command completed successfully
```

4.9 Χορήγηση και αφαίρεση των αδειών

Τώρα ας εξετάσουμε μερικά παραδείγματα για το πώς να τροποποιήσουμε τους περιγραφείς ασφάλειας. Η πρώτη εντολή χορηγεί στο χρήστη jsmith@net.dom το δικαίωμα ανάγνωσης (List Contents, Read All Properties, and Read Permissions) για όλα τα αντικείμενα (και συμπεριλαμβανομένου) του `Staff` OU:

```
C:\>dsacls OU=Staff, DC=net, DC=dom /G jsmith@net.dom:GR /I:T
```

Μπορείτε να ελέγξετε το αποτέλεσμα της λειτουργίας με όλα τα πιθανά (και αναφερθέντα ήδη) μέσα.

Η δεύτερη εντολή αποτρέπει το χρήστη από την ανάγνωση δύο ιδιοτήτων του αντικειμένου OU:

```
C:\>dsacls OU=Staff, DC=net, DC=dom /D jsmith@net.dom:RP;PLink
      jsmith@net.dom: RP; gPOptions
```

Προσοχή: Τα ονόματα ιδιοτήτων στην τελευταία εντολή είναι διακρινων ευαίσθητα. Μπορείτε να διευκρινίσετε οποιοδήποτε εφαρμόσιμο αριθμό ιδιοτήτων στην ίδια εντολή.

4.10 Επαναφορά Ρυθμίσεων Ασφαλείας

Για διάφορους λόγους, μπορείτε να θελήσετε να επιστρέψετε τις ρυθμίσεις ασφάλειας ενός αντικειμένου στις αρχικές (προεπιλογής τους). Οι προεπιλεγμένες ρυθμίσεις για μια κατηγορία αντικειμένου καθορίζονται στο Active Directory schema.

(Επιπλέον, οι ρυθμίσεις που κληρονομούνται από τα αρχικά εφαρμόζονται στο αντικείμενο επίσης .) Παραδείγματος χάριν, η ακόλουθη εντολή αποκαθιστά τις προεπιλογές για ένα αντικείμενο OU: `C:\>dsacls OU=Staff, DC=net, DC=dom /S`

(Μπορείτε ακόμη να χρησιμοποιήσετε την παράμετρο /T και να επαναφέρετε τις προεπιλογές σε ολόκληρο το δέντρο των αντικειμένων.)

Εάν η λειτουργία είναι επιτυχής, η εντολή acldiag <όνομα αντικειμένου> /schema /skip θα αναφέρει τα εξής:

```
Schema Defaults Diagnosis
        Schema defaults: Present
        Obtained            : At CREATION
```

Να είστε προσεκτικοί γιατί η εντολή dsacls /s διαγράφει τις τοποθετήσεις λογιστικού ελέγχου από το αντικείμενο. Η εντολή

```
C:\>dsacls OU=Staff, DC=net, DC=dom /A
```

θα εμφανίσει το εξής μήνυμα:

```
Audit list:
{This object is protected from inheriting permissions from the
parent}
THERE ARE NO ACCESS CONTROL ENTRIES
...
```

Για να αποκαταστηθούν οι προεπιλεγμένες ρυθμίσεις λογιστικού ελέγχου, ανοίξτε το παράθυρο ιδιοτήτων του αντικειμένου (στο **Active Directory Users and Computers** ή στο **ADSI Edit** snap-in), κάντε κλικ στην ετικέτα ασφάλειας, και έπειτα στην προηγμένος . Στην ετικέτα ελέγχου στο παράθυρο **Access Control Settings** , επιλέξτε Allow για τις κληρονομικές καταχωρήσεις ελέγχου από το γονέα για να διαδώσετε σε αυτό το κιβώτιο αντικειμένου, και πατήστε εφαρμογή. Κάντε κλικ στο OK στο υπερεμφανιζόμενο παράθυρο προειδοποίησης και κλείστε όλα τα ανοιγμένα παράθυρα.

Προσοχή: Εάν δεν αποκαταστήσετε τις ρυθμίσεις λογιστικού ελέγχου μετά από την εντολή dsacls /s,η εντολή ACLDiag της έκδοσης των Windows 2000 με παραμέτρους /chkdeleg ή /schema θα αποτύχει. Στην έκδοση Windows .NET λειτουργεί κανονικά.

4.11 Kerberos

Ευτυχώς, πολλοί διαχειριστές δεν χρειάζεται ποτέ να διαμορφώσουν το Kerberos. Λειτουργεί όπως περιγράφεται στη θεωρεία, το όποιο βεβαίως είναι μια ανακούφιση αυτές τις μέρες των σύνθετων λειτουργικών συστημάτων (OSs). Μερικοί διαχειριστές όμως μπορεί να χρειαστούν να διαμορφώσουν την προεπιλογή του Kerberos λίγο. Η διαμόρφωση του Kerberos είναι αρκετά εύκολη, αλλά προτού να σας παρουσιάσω το πώς, πρώτα επιτρέψτε μου να παρουσιάσω πώς λειτουργεί το Kerberos. Οι ρυθμίσεις διαμόρφωσης του Kerberos εξαρτώνται πολύ από η μια από την άλλη και μια μοναδική λανθασμένη ρύθμιση μπορεί να γονατίσει το δίκτυό σας.

4.12 Πώς λειτουργεί το Kerberos

Το Kerberos λειτουργεί σε ένα σύστημα κρυπτογραφίας τύπου μοιραζόμενου κλειδιού. Υπάρχουν τρεις ρόλοι μέσα στον κόσμο του Kerberos:

- Key Distribution Center (KDC)—Ο ρόλος αυτός διαδραματίζεται από όλους τους ελεγκτές domains των Windows 2000 (Win2K).
- Ένας πελάτης που πρέπει να αποκτήσει πρόσβαση στους πόρους δικτύων.
- Ένας κεντρικός υπολογιστής που παρέχει τους πόρους δικτύων σε έναν πελάτη.

Το Kerberos καθορίζει δύο συγκεκριμένες διαδικασίες. Η πρώτη διαδικασία επιτρέπει στους πελάτες να εισέλθουν στο δίκτυο και το γαντζωθούν στο KDC. Η δεύτερη διαδικασία επιτρέπει στους πελάτες να έχουν πρόσβαση στους πόρους των κεντρικών υπολογιστών.

4.13 Kerberos Tray (KerbTray.exe) (RK)

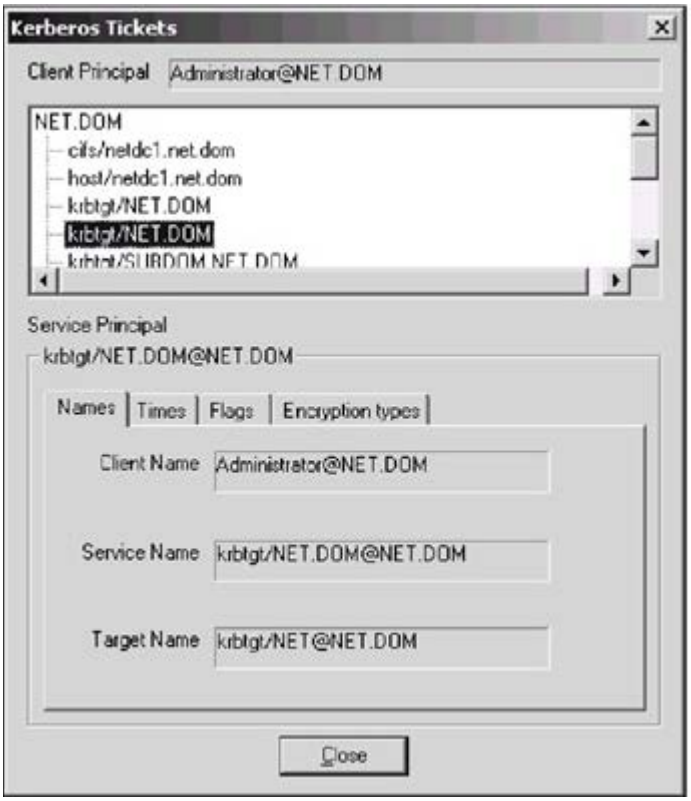
Το *Kerberos Tray* Kerberos απαριθμεί όλα τα εναποθηκευμένα εισιτήρια Kerberos και επιτρέπει σε σας για να δείτε τις ιδιότητες των εισιτηρίων καθώς επίσης και για να εκκαθαρίσει τα εισιτήρια. Αυτές οι πληροφορίες μπορούν να βοηθήσουν στην επίλυση των προβλημάτων με την επικύρωση και την πρόσβαση στους πόρους του δικτύου. (Εάν ένας υπολογιστής βασισμένος στο AD δεν έχει λάβει το αρχικό ticket-granting-ticket (TGT) από το *Kerberos Distribution Center* (KCC), κατά τη διάρκεια της πρώτης σύνδεσης στην domain, ή εάν τα εναποθηκευμένα εισιτήρια έχουν λήξει και δεν έχουν ανανεωθεί, ο υπολογιστής δεν θα επικυρωθεί για να έχει πρόσβαση στους πόρους.) Για την επικύρωση του Kerberos που εκτελείται επιτυχώς, πρέπει να εξασφαλίσετε ότι όλοι οι υπολογιστές συγχρονίζουν τις χρονικές τοποθετήσεις με μια κοινή χρονική υπηρεσία (μέσα σε πέντε λεπτά από το δέλτα).

Το εργαλείο αρχίζει σε ελαχιστοποιημένη κατάσταση και μπορείτε να βρείτε το εικονίδιο του στο δεξί κάτω μέρος της οθόνης.(Taskbar). Εάν κινήσετε το δρομέα του ποντικού πάνω από το εικονίδιο, ο χρόνος που απομένει στο αρχικό TGT θα εμφανιστεί. (Εικόνα 4.1 αριστερά).

Εικόνα 4.1: Το εργαλείο δίσκων του Kerberos επιδεικνύει το χρόνο που αφήνεται στο αρχικό TGT προτού να λήξει (αριστερά).Οι επιλογές πλαισίου του εργαλείου (δεξιά) επιτρέπουν σε σας να επιλέξετε μια λειτουργία

Εάν κάνετε διπλό κλικ στο εικονίδιο ή επιλέξετε την εντολή **List Tickets** από τις επιλογές του πλαισίου (Εικόνα 4.1,δεξια), το παράθυρο του κύριου εργαλείου θα εμφανιστεί (Εικόνα 4.2). Εμφανίζει όλα τα εναποθηκευμένα εισιτήρια στο Kerberos που

χρειάστηκαν κατά την σύνδεση του πρώτου χρήστη.



Εικόνα 4.2: Σε αυτό το παράθυρο, μπορείτε να δείτε τις πληροφορίες για όλα τα εναποθηκευμένα εισιτήρια και τις ιδιότητές τους

Η εντολή **Purge Tickets** καθαρίζει ολόκληρη την εναποθήκευση εισιτηρίων (έτσι, το KerbTray διαφέρει από το εργαλείο καταλόγων Kerberos, το όποιο είναι σε θέση να διαγράψει τα εισιτήρια επιλεκτικά). Καμία προειδοποίηση δεν εκδίδεται πριν καθαρίσει την εναποθήκευση, έτσι να είστε προσεκτικοί! Ενώ η εναποθήκευση είναι κενή, μπορείτε να αποτραπείτε από την επικύρωση σας στους πόρους, και μια έξοδος και είσοδος στο σύστημα θα απαιτηθεί.

Σημείωση: Το παράθυρο των εφαρμογών δεν είναι ενημεροσιμο. Επομένως, εάν θεωρείτε ότι νέα εισιτήρια εμφανίστηκαν (όταν συνδέεστε με έναν νέο πόρο ή μια νέα υπηρεσία), κλείστε το παράθυρο και το ανοίξτε το πάλι.

Ας συζητήσουμε τις ιδιότητες του κύριου εισιτηρίου, οι όποιες εμφανίζονται από το εργαλείο.

- Το πεδίο **Client Principal** περιέχει το όνομα του τρέχοντος λογαριασμού σύνδεσης. Εάν η εναποθήκευση εισιτηρίων είναι κενή, αυτός ο τομέας επιδεικνύει το μήνυμα "No network credentials".
- όλα τα εισιτήρια αποκομίζονται μέχρι η σύνδεση να παρατεθεί στο παράθυρο κύλισης. Οι ιδιότητες του επιλεγμένου εισιτηρίου επιδεικνύονται στις περαιτέρω ετικέτες.
- Οι συμβολοσειρές κάτω από τη λίστα κύλισης περιλαμβάνουν το όνομα μιας αρχής ασφάλειας για το επιλεγμένο εισιτήριο. Εάν ο χρόνος εισιτηρίων τελειώσει,

η συμβολοσειρά "Expired" εμφανίζεται και καμία ιδιότητα δεν παρουσιάζεται στις ετικέτες.

- Η ετικέτα ονομάτων περιέχει:
  - Όνομα πελάτη - αιτών του εισιτηρίου. Στις περισσότερες περιπτώσεις (έχοντας πρόσβαση στους πόρους στην τρέχουσα domain) αυτό είναι το ίδιο όνομα που εμφανίζεται στο πεδίο **Client Principal**.
  - Όνομα υπηρεσιών - το κύριο όνομα ασφάλειας (λογαριασμός) για την υπηρεσία. Η ιδιότητα samAccountName του αντικειμένου καταλόγου του απολογισμού αποθηκεύει αυτό το όνομα.
  - Όνομα στόχων - ένα από τα ονόματα υπηρεσιών που περιλαμβάνονται στις multi-valued servicePrincipalName ιδιότητες του αντικειμένου καταλόγου του υπολογιστή. Αυτό είναι το όνομα υπηρεσιών που το εισιτήριο έχει λάβει

Ο χρόνος όταν λήφθηκε το εισιτήριο (χρόνος έναρξης) και ο χρόνος λήξης του (χρόνος τέλους) παρουσιάζονται στη χρονική ετικέτα. Η ερμηνεία της ετικέτας σημαιών απαιτεί μια βαθύτερη κατανόηση του πρωτοκόλλου Kerberos. Η αρχική σημαία τίθεται μόνο για το εισιτήριο που λήφθηκε χωρίς το TGT.

4.14 Kerberos List (KList.exe) (RK)

Αυτή η γραμμή εντολών πρακτικά έχει τις ίδιες πιθανότητες και δυνατότητες όπως περιγράψαμε στο εργαλείο *Kerberos* προηγουμένως. Αυτό το εργαλείο έχει τις εξής εντολές:

- `klist tgt` εμφανίζει το αρχικό TGT.
- `klist tickets` λίστα όλων των εναποθηκευμένων εισιτηρίων.
- `klist purge` επιτρέπει την διαγραφή ενός εισιτηρίου σε ένα κείμενο διάλογου.

Ακολουθεί ένα παράδειγμα αυτού του διάλογου:

```
C:\>klist purge
Cached Tickets: (10)

   Server: krbtgt/SUBDOM.NET.DOM@NET.DOM
      KerbTicket Encryption Type: RSADSI RC4-HMAC (NT)
      End Time: 6/12/2004 1:33:40
      Renew Time: 12/12/2004 15:33:40

Purge? (y/n) : y
        Deleting ticket:
           ServerName = krbtgt/SUBDOM.NET.DOM (cb=42)
           RealmName = NET.DOM (cb=14)
Submit Buffer size = 84
        Ticket purged!
```

Πρέπει να απαντήσεις "yes" ή "no" για κάθε εισιτήριο.

Εάν ο χρηστής δεν έχει εναποθηκευμένο κανένα εισιτήριο το εργαλείο θα

επιστρέψει το μήνυμα "Cached Tickets: (0)".

4.15 Εφαρμογή ελέγχου περιγραφέα ασφαλείας (SDCheck.exe) (Security Descriptor Check Utility)

Το εργαλείο της γραμμής εντολών SDCheck προορίζεται πρώτιστα να βοηθήσει τους διαχειριστές να ελέγξουν και να παρακολουθήσουν τα ακόλουθα ζητήματα σχετικά με τους περιγραφείς ασφάλειας των αντικειμένων καταλόγου:

- διάδοση κληρονομημένου ACLs για ένα διευκρινισμένο αντικείμενο καταλόγου
- αντίγραφο ACLs μεταξύ των διαφορετικών ελεγκτών domains

Ας εξετάσουμε πώς να εκπληρώσουμε αυτούς τους στόχους χρησιμοποιώντας την ακόλουθη έξοδο δειγμάτων. Σε αυτό το σενάριο, θα εξετάσουμε το ACLs ενός αντικειμένου χρηστών (Vasilis@net.dom) που αυτός ανήκει σε ένα τοποθετημένο OU. (Ο ελεγκτής domains A πρέπει επίσης να διευκρινιστεί στην εντολή.) Μερικές γραμμές, όπως και τα σχόλια που τοποθετούνται στο κείμενο κάτω από αυτές τις γραμμές, παρουσιάζονται στο κείμενο με μαύρους χαρακτήρες.

```
C:\>sdcheck netdc1.net.dom Vasilis@net.dom
Security Descriptor Check Utility - build(3621)

Input: Vasilis@net.dom
Object: CN=Vasilis, OU=Marketing, OU=Staff, DC=net, DC=dom
Domain: net.dom
Domain: DC=net, DC=dom
Server: netdc1.net.dom

*** Warning: No values returned for dSCorePropagationData on
DC=net, DC=dom

Object: CN=Vasilis, OU=Marketing, U=Staff, DC=net, DC=dom
Classes: top person organizational Person user
SD: 2060 bytes
Metadata: 06/13/2002 20:26:22 @ netdc4.net.dom ver: 3
History:  06/13/2002 20:28:43 flags(0x1) SD propagation
          06/13/2002 20:36:08 flags(0x1) SD propagation
          06/13/2002 20:49:29 flags (0x1) SD propagation
          06/13/2002 20:51:06 flags (0x1) SD propagation
    [Με την εξέταση των μεταδεδομένων σε διαφορετικό DCs, ένας
διαχειριστής μπορεί να παρακολουθήσει την αντιγραφή του αλλαγμένου
περιγραφέα ασφάλειας. Παραδείγματος χάριν, μπορείτε να σημειώσετε ότι ο
αριθμός έκδοσης σε ένα άλλο DC διαφέρει από την έκδοση παρουσίας, και
ότι ένα άλλο DC έχει δημιουργήσει τις αλλαγές. Για να δείτε τα
μεταδεδομένα αντιγραφής, μπορείτε επίσης να χρησιμοποιήσετε την εντολή
repadmin /showmeta.]

Object: OU=Marketing, OU=Staff, DC=net, DC=dom
Classes: top organizationalUnit
SD: 1332 bytes
Metadata: 06/13/2002 20:20:41 @ netdc1.net.dom ver: 3
History:  06/13/2002 20:28:43 flags (0x1) SD propagation
          06/13/2002 20:36:08 flags (0x1) SD propagation
          06/13/2002 20:49:29 flags (0x1) SD propagation
```

```
                06/13/2002 20:51:06 flags (0x1) SD propagation

      Object:  OU=Staff, DC=net, DC=dom
      Classes: top organizationalUnit
      SD:      1332 bytes
      Metadata:  06/13/2002 20:51:06 @ netdc1.net.dom ver: 6
      History:   06/13/2002 20:22:10 flags (0x1) SD propagation
                 06/13/2002 20:49:29 flags (0x1) SD propagation
```

[Σημειώστε τις γραμμές μέσα απο το ιστορίκο του αντικειμένου. Αυτές οι πληροφορίες βοηθούν έναν διαχειριστή για να επισημάνει τις αλλαγές και να καθορίσει τη δημιουργία του κοντεινερ. Παραδείγματος χάριν, οι αλλαγές που έγιναν στο επίπεδο Staff OU στις 30:51:06 έχει διαδοθεί επιτυχώς σε όλα τα αντικείμενα παιδιά συμπεριλαμβανομένου του αντικειμένου χρηστή Vasilis. Στις 20:49:29, ο περιγραφέας ασφάλειας των domains έχει αλλάξει, και οι αλλαγές έχουν επεκταθεί κατευθείαν σε ολόκληρο το domain. Εάν οι χρονικές τιμές είναι διαφορετικές σε μερικά επίπεδα, η κληρονομικότητα μπορεί να εμποδιστεί και αυτό το γεγονός πρέπει να εξεταστεί.]

```
      Object: DC=net, DC=dom
      Classes: top domain domainDNS
      SD: 1400 bytes
      Metadata: 06/13/2002 20:49:29 @ netdc1.net.dom ver: 4

  Checking ACL inheritance ... [Αυτή η δόκιμη θα εμφανίσει τα ACL
κληρονομικά λάθη σε κάθε επίπεδο εάν κάποιο λάθος υπάρξει.]
           Parent: 3 - DC=net, DC=dom
           Child: 2 - OU=Staff, DC=net, DC=dom
    *** OK

  Checking ACL inheritance ...
           Parent: 2 - OU=Staff, DC=net, DC=dom
           Child: 1 - OU=Marketing, OU=Staff, DC=net, DC=dom
    *** OK

    Checking ACL inheritance ...
            Parent: 1 - OU=Marketing, OU=Staff, DC=net, DC=dom
            Child: 0 - CN=Vasilis, OU=Marketing, OU=Staff, DC=net,
DC=dom
    *** OK
```

Το αποτέλεσμα που παρουσιάζεται είναι ένα παράδειγμα μιας επιτυχούς δοκιμής.

Για να ελέγξουμε τη "συνοχή" του κληρονομημένου ACLs, χρησιμοποιήστε την παράμετρο -debug. Υποθέστε, στο παράδειγμά μας, ότι η μετάδοση ACLs εμποδίζεται στο Marketing OU επίπεδο. Αυτό σημαίνει ότι η κληρονομιά από το γονέα και οι καταχωρήσεις άδειας που ισχύουν για τα αντικειμένων παιδιών στην ετικέτα **Permissions** στο παράθυρο **Advanced Security Settings** έχει καθαριστεί. Για να δείτε αυτό το παράθυρο, ανοίξτε το παράθυρο Marketing's **Properties** και κάντε κλικ στο **Advanced** στην ετικέτα **Security**. (Στα Windows 2003, οι επιτρεπόμενες κληρονομικές άδειες από το γονέα που διαδίδονται στο αντικείμενο και βρίσκονται στην ετικέτα **Security** χρησιμοποιούνται για αυτόν τον σκοπό.)

Στην περίπτωσή μας, μπορείτε γρήγορα να εντοπίσετε εάν μια κληρονομιά

εμποδίζεται ή όχι με τη χρήση της εντολής:

```
C:\>sdcheck netdc1.net.dom Vasilis@net.dom -debug
```

Σε μια συγκεκριμένη στιγμή, τα αποτελέσματα εργαλείων εμφανίζουν μια προειδοποίηση:

```
   ...
   Checking ACL inheritance ...
           Parent: 2 - OU=Staff, DC=net, DC=dom
           Child: 1 - OU=Marketing, OU=Staff, DC=net, DC=dom
   *** Warning: Child has SE_DACL_PROTECTED set, therefore doesn't
inherit
   - skipping test
   *** OK
   ...
```

Εάν η κληρονομικότητα ACL δεν εμποδιστεί, η δοκιμή θα τρέξει χωρίς καμία προειδοποίηση.

5. ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

Σε αυτό το σημείο θα μελετήσουμε τη χρήση του Active Directory της Microsoft ως υπηρεσία επικύρωσης για τα συστήματα Linux. Αν και το Linux έχει ένα πολύ καλό σύστημα επικύρωσης βασισμένο σε υπηρεσίες καταλόγου (OpenLDAP), μπορεί να είναι επιθυμητό σε μερικές ιστοσελίδες να επικυρωθούν οι χρήστες του Linux ενάντια σε έναν κεντρικό υπολογιστή με Windows 2003 της Microsoft.

Αν και εδώ χρησιμοποιείται το Linux η χρήση του μηχανισμού επικύρωσης λειτουργεί καλά και σε άλλα συστήματα Unix που έχουν ένα μηχανισμό PAM/NSS.

Πριν προσπαθήσετε οποιαδήποτε από αυτά, πρέπει να εξοικειωθείτε με τις έννοιες του PAM και του NSS, και εξοικειωθείτε με το πώς να εγκαταστήσετε το PAM και το NSS στη διανομή Linux ή στο λειτουργικό σύστημά σας.

Επίσης, προτού να αρχίσω, πρέπει να σας δηλώσω ότι πραγματικά δεν πιστεύω ότι το Active Directory είναι ο καλύτερος τρόπος να επικυρωθούν οι πελάτες του Linux, ούτε είναι αυτό ο καλύτερος τρόπος να επικυρωθούν οι χρήστες σε ένα περιβάλλον με πολλές πλατφόρμες. Μπορεί να είναι η περίπτωση που στο δίκτυό σας, για πολιτικούς και οικονομικούς λόγους, περιορίζεστε στη χρησιμοποίηση του Active Directory ως προϊόν καταλόγου, εντούτοις, και έτσι το παρόν κείμενο μπορεί να ωφελήσει κάποιον σας εσάς εάν είστε ανεπαρκής να ξανασκεφτείτε, την IT στρατηγική σε αυτήν σας την περιοχή.

Η Microsoft δεν υποστηρίζει την επικύρωση στο Active Directory για οποιοδήποτε πελάτη μη-Microsoft, και δεν υποστηρίζει τις οδηγίες που περιλαμβάνονται

σε αυτό το άρθρο από καμιά άποψη. Εάν επιθυμείτε να ακολουθήσετε τις οδηγίες σε αυτό το κείμενο θα το κάνετε με δική σας ευθύνη.

5.1 Συστήματα Πιστοποίησης

Ο παραδοσιακός τρόπος επικύρωσης χρηστών σε ένα σύστημα με Linux είναι να υποθηκεύσουν τους λογαριασμούς και τους κωδικούς πρόσβασης στο /etc/passwd αρχείο ή, συχνότερα, τους συνδυασμούς των /etc/passwd και /etc/shadow.

Αυτό είναι συνετό όταν υπάρχει μόνο ένα σύστημα Linux σε ένα δίκτυο, επειδή το /etc/passwd αρχείο αποθηκεύεται στο τοπικό σύστημα. Αν και είναι δυνατό να μοιραστεί ένα ενιαίο /etc/passwd αρχείο μεταξύ των πολλαπλών συστημάτων Linux, χρησιμοποιώντας εργαλεία όπως το rsync, έχει περισσότερο νόημα για να έχει μια συγκεντρωμένη βάση δεδομένων επικύρωσης που περιέχει όλους τους λογαριασμούς και κωδικούς πρόσβασης των χρηστών.

Υπάρχουν πολλά τέτοια συγκεντρωμένα συστήματα επικύρωσης διαθέσιμα, συμπεριλαμβανομένου του Kerberos, NIS, και άλλων. Το LDAP είναι ένα πρωτόκολλο που μπορεί να χρησιμοποιηθεί για να επιτρέψει σε έναν αρκετά ισχυρό μηχανισμό να υποθηκεύσει την συγκεντρωτική βάση δεδομένων επικύρωσης καθώς επίσης και τις πληροφορίες των χρηστών.

5.2 Διαπλατφορμική Πιστοποίηση

Ο στόχος της επικύρωσης των διαπλατφορμικών εφαρμογών είναι να υπάρξει μια ενιαία, συγκεντρωμένη βάση δεδομένων κωδικού πρόσβασης που μπορεί να χρησιμοποιηθεί για να επικυρώσει τους χρήστες και στο δύο Unix, Windows, και ίσως ακόμη και άλλα συστήματα όπως Macintosh ή NetWare.

Επειδή η LDAP-based πιστοποίηση υποστηρίζεται στα πιο πρόσφατα συστήματα της Microsoft, συμπεριλαμβανομένων των Windows 2000, 2003 και XP και υποστηρίζεται επίσης σε Linux και άλλα συστήματα Unix (όπως Solaris). Επίσης κάνει μια άριστη επιλογή για ένα διαπλατφορμικό σύστημα επικύρωσης. Σημειώστε ότι υπάρχουν περιορισμοί σε αυτό. Αρχικά, οι πελάτες της Microsoft για τα Windows 2000, 2003 και XP είναι συγκεκριμένοι για την επικύρωση ενάντια σε έναν Active Directory server. Αν και το OpenLDAP χρησιμοποιεί το ίδιο πρωτόκολλο LDAP, υπάρχουν άλλα χαρακτηριστικά γνωρίσματα του Active Directory (συμπεριλαμβανομένης μιας τροποποιημένης έκδοσης Kerberos με ένας συγκεκριμένος μηχανισμός της Microsoft που καλείται "PAC") που σημαίνει ότι οι πελάτες του Active Directory δεν θα είναι απαραιτήτως σε θέση να πιστοποιηθούν στον OpenLDAP.

Ο δεύτερος περιορισμός ότι πελάτες του Active Directory (στην κατάσταση LDAP) είναι μόνο διαθέσιμοι στα Windows 2000, 2003 και XP. Αν και το Active Directory θα λειτουργήσει σε μία «παλαιότερη» κατάσταση για να υποστηρίξει τους παλαιότερους πελάτες της Microsoft, χρήστες συστημάτων όπως τα Windows NT και τα Windows ME/98/95 που επιθυμούν να έχουν πλήρες LDAP/Kerberos βασισμένη υποστήριξη επικύρωσης, αναγκάζονται να αναβαθμιστούν.

Φυσικά, ένας άλλος περιορισμός του Active Directory είναι ότι τρέχει μόνο στα Windows 2000,2003 server. Δεν υπάρχει καμία έκδοση του Active Directory για άλλες πλατφόρμες. Αντίθετα, πολλές από τις άλλες διαθέσιμες υπηρεσίες καταλόγου (όπως εκείνες του iPlanet και Novell) υποστηρίζονται ως κεντρικοί υπολογιστές σε πολλές πλατφόρμες.

5.3 Εναλλακτικές Λύσεις LDAP

Άλλες εναλλακτικές λύσεις του Active Directory υπάρχουν όπου επιθυμείται ένα LDAP-based σύστημα επικύρωσης. Αυτές περιλαμβάνουν:

- OpenLDAP. Όπως αναφέρεται νωρίτερα, αυτό είναι ένα άριστο σύστημα επικύρωσης για τους πελάτες του Linux.. Εντούτοις, οι πελάτες της Microsoft δεν θα είναι σε θέση να επικυρώσουν σε αυτό.
- Υπηρεσία καταλόγου iPlanet. Η υπηρεσία καταλόγου iPlanet τρέχει σε πλατφόρμες Windows, όπως και στα συστήματα Linux και Solaris. Αν και ο κεντρικός υπολογιστής καταλόγου iPlanet περιέχει τα Windows NT στο σύστημα συγχρονισμού κωδικών πρόσβασης LDAP, η άμεση επικύρωση στον κεντρικό υπολογιστή καταλόγου iPlanet δεν είναι δυνατή από τα συστήματα Windows.
- NDS. Η υπηρεσία καταλόγου του Novell είναι πιθανώς η πιο αξιόπιστη υλοποίηση μιας διαπλατφορμικής υπηρεσίας καταλόγου. Οι κεντρικοί υπολογιστές τρέχουν Solaris, Linux, Windows και NetWare. Οι πελάτες είναι διαθέσιμοι για πολλές πλατφόρμες συμπεριλαμβανομένων σχεδόν όλων των πλατφόρμων Windows της Microsoft (συμπεριλαμβανομένων των Windows 98 και των Windows NT), και επίσης Linux και Solaris. Το NDS είναι πρότυπο-συγκαταβατικό και έχει βρεθεί να αποδίδει καλά σε πολλές εφαρμογές. Εάν μια αληθινή διαπλατφορμική υπηρεσία καταλόγου απαιτείται, τότε το NDS είναι πιθανώς η καλύτερη επιλογή. Ο μόνος περιορισμός του NDS είναι το κόστος, το οποίο μπορεί να είναι αρκετά υψηλό σε ένα περιβάλλον με μια μεγάλη βάση χρηστών.

5.4 MKS AD4Unix

5.4.1 Τι Είναι το AD4Unix?

Το MKS AD4Unix είναι ένα plug-in επέκτασης για τον Active Directory Server της Microsoft, το οποίο επιτρέπει στην πιστοποίηση σχετικά με το Unix και τις πληροφορίες χρηστών να αποθηκευτούν στον Active Directory. Το AD4Unix περιλαμβάνει μια αναπροσαρμογή του schema, και μια επέκταση στο User & Group manager (μέρος του διαχειριστικού περιβάλλοντος του Active Directory , το οποίο είναι στη συνέχεια μέρος της διαχειριστικής κονσόλας MMC).

Ο αρχικός στόχος του AD4Unix είναι να δημιουργήσει μια ενοποιημένη βάση δεδομένων λογαριασμών για τα Windows και τους κεντρικούς υπολογιστές Unix μέσω του Active Directory. Αυτό είναι που συγκεκριμένα επιτρέπει την διαπλατφορμική επικύρωση χρησιμοποιώντας το Active Directory.

5.4.2 Λήψη του MKS AD4Unix

Το MKS AD4Unix μπορεί να ληφθεί μέσω της ιστοσελίδας του AD4Unix.

Το AD4Unix παραδίδεται ως ένα ενιαίο αρχείο .MSI (Microsoft Installer) που μπορεί να εγκατασταθεί άμεσα επάνω σε έναν κεντρικό υπολογιστή με Windows 2000, 2003.

5.4.3 Εγκατάσταση του MKS AD4Unix

Οι αρχικές εντολές εγκατάστασης για το AD4Unix, και οι οδηγίες για τη χρήση του γράφτηκαν από τον JJ Streicher-Bremer για το AD4Unix 1.1.1. Τα πράγματα έχουν αλλάξει κάπως από τότε, υπάρχει τώρα ένα πακέτο εγκατάστασης (MSI format), εντούτοις υπάρχουν ακόμα μερικά δυσλειτουργικά μέρη επειδή το πακέτο εγκατάστασης δεν είναι τέλειο.

Ο σκοπός μου ήταν η εγκατάσταση ενός AD4Unix. Έτσι πήρα έναν υπολογιστή με κενό σκληρό δίσκο και εγκατέστησα τα Windows 2003 και έπειτα το AD4Unix από την αρχή. Αυτό πήρε λίγη ώρα.

Αυτές οι οδηγίες είναι βασισμένες σε έναν Windows 2003 server, και το AD4Unix στην έκδοση 1.5. Εδώ ακολουθεί ένα ημερολόγιο καταγραφής γεγονότων αυτών που έκανα για να βάλω το προϊόν σε λειτουργία:

- Εγκατέστησα τα Windows 2003, από το CD εγκατάστασης. Δεδομένου ότι είχα έναν ενιαίο κενό σκληρό δίσκο, είπα ακριβώς στα Windows 2003 να εγκατασταθούν στο σκληρό δίσκο και να χρησιμοποιήσουν όλο το διαθέσιμο χώρο του. Εάν υπάρχουν περισσότεροι από έναν σκληρό δίσκο (να χρησιμοποιηθούν οι οδηγίες της Microsoft για να καταχωρούνται σε ξεχωριστούς δίσκους τα αρχεία ημερολογίου και οι κατάλογοι) θα πρέπει έπειτα να ασχοληθείτε λίγο με την εγκατάσταση. Ακολούθησα ακριβώς τις οδηγίες εγκατάστασης και επέλεξα τις προεπιλογές.
- Επέλεξα να εγκαταστήσω μόνο την υποστήριξη αμερικανικής αγγλικής γλώσσας (που ήταν η προεπιλογή κατά τη διάρκεια της εγκατάστασης των Windows 2003). Είχα κάποιο πρόβλημα εγκαθιστώντας το AD4Unix όταν επέλεξα μια εναλλακτική γλώσσα προεπιλογής επειδή το AD4Unix δεν υποστηρίζει όλες τις γλώσσες των Windows. Μπορώ να καταλάβω αυτόν τον περιορισμό, και εν πάση περιπτώσει είχε επιπτώσεις μόνο στον κεντρικό υπολογιστή στον οποίο εγκαθιστούσα τα Windows 2003 και όχι άλλους τερματικούς σταθμούς. Ελπίζουμε ότι στο μέλλον θα υπάρξει καλύτερη γλωσσική υποστήριξη για το AD4Unix.
- Εγκατέστησα το πακέτο κρυπτογράφησης Windows 2003 High Encryption Pack. Ίσως αυτό είναι μια άλλη περίπτωση της κόλασης των DLL με την οποία όλοι οι

διαχειριστές των Microsoft Windows βρίσκονται αντιμέτωποι κάθε φορά Η εγκατάσταση αυτού του πακέτου απαίτησε μια εκ νέου επανεκκίνηση.

- Εγκατέστησα το Windows 2003 Service Pack 1. Σημειώστε ότι όλα τα Service Packs των Windows είναι διαθέσιμα από την ιστοσελίδα της Microsoft. Αυτό απαίτησε μια εκ νέου επανεκκίνηση.
- Με την χρησιμοποίηση του οδηγού " Configure Your Server ", εγκατέστησα το Active Directory. Σε αυτήν την περίπτωση, δεδομένου ότι ήταν μια νέα εγκατάσταση σε ένα απομονωμένο περιβάλλον, δημιούργησα ένα νέο domain, νέο δέντρο, νέο δάσος των δέντρων, και δημιούργησα μια νέα dns ζώνη. Μπορείτε να επιθυμήσετε να διαμορφώσετε τον κεντρικό υπολογιστή σας διαφορετικά, ή να τον ενώσετε σε ένα υπάρχον δέντρο ή ένα δάσος. Προσέξτε ότι είμαστε έτοιμοι να εγκαταστήσουμε τις ενημερώσεις σχημάτων, οι οποίες θα μπορούσαν να δημιουργήσουν πρόβλημα σε οποιοδήποτε υπάρχον δέντρο ή δάσος καταλόγου που έχετε, εκτός αν τις εγκαταστήσετε σωστά.
- Επιτρεπτές αναπροσαρμογές σχημάτων στον domain controller. Για να κάνει αυτό, ακολουθήστε αυτές τις οδηγίες:
- Ανοίξτε ένα παράθυρο γραμμής εντολών (έναρξη->Puv- >cmd)
- Πληκτρολογήστε την εντολή: **regsvr32 γ:\winnt\system32\schmmgmt.dll** Αυτό καταχωρεί το schmmgmt.dll ως MMC (Microsoft Management Console). Μπορείτε τώρα να κλείσετε το παράθυρο γραμμής εντολών με τη πληκτρολόγηση του exit.
- Δημιουργήστε ένα Schema Management MSC, ως εξής:
- Start -> Run -> MMC
- Από τις επιλογές κονσόλων, επιλέξτε το " add/remove snap-in " και έπειτα πατήστε το κουμπί " Add".
- Επιλέξτε το Active Directory Schema και πατήστε " Add "
- πατήστε " Close "
- πατήστε "OK"
- Επιλέξτε τον domain controller που θέλετε να ενημερώσετε το σχήμα του:
- Δεξί κλικ στο "Active Directory Schema" και επιλέξτε "Change Domain Controller"
- Επιλέξτε το "Specify name " και τον τύπο στο dns όνομα ή τη διεύθυνση του Domain controller σας.
- Επιτρέψτε τις ενημερώσεις στον domain controller
- Δεξί κλικ στο "Active Directory Schema" και επιλέξτε το "Operations Master"
- Πατήστε στο επονομαζόμενο τετραγωνίδιο "The Schema may be modified on this Domain Controller "
- Πατήστε OK
- Τώρα είναι δυνατό να εγκατασταθεί το ADS4Unix plugin. Για να το κάνετε αυτό, βρείτε τη θέση όπου το αρχείο .MSI αποθηκεύτηκε, και κάντε διπλό κλικ σε αυτό στο διαχειριστή αρχείων.
- Πείτε ναι στις ερωτήσεις για τις ενημερώσεις σχημάτων.
- Στις επιλογές έναρξης στο πλαίσιο " Programs " πρέπει τώρα να υπάρξουν πρόσθετες επιλογές με τον τίτλο "AD4Unix". Αυτό περιέχει το πρόγραμμα διαμόρφωσης AD4Unix (MKSADPluginSettings). Τρέξτε αυτό το πρόγραμμα διαμόρφωσης, και καθορίστε ένα όνομα NIS. Δεν έχει μεγάλη σημασία τι θα

εισάγετε εδώ μέσα, δεδομένου ότι δεν θα χρησιμοποιείτε τα NIS, αλλά κάτι πρέπει να εισαχθεί.

5.5 Προσθήκη των λημμάτων χρηστών

Τώρα που τα AD4Unix plugins έχουν εγκατασταθεί, είναι δυνατό να χρησιμοποιηθεί το Active Directory Users and Computers για να εισαχθούν νέοι χρήστες του Unix στο σύστημα του Active Directory. Θα μπορούσατε επίσης να τροποποιήσετε τις ιδιότητες χρηστών και ομάδας στο Unix των υπαρχόντων χρηστών του Active Directory σας για να καταστήσετε εκείνους τους χρήστες ορατούς σε ένα σύστημα Unix.

Για να προσθέσετε έναν νέο χρήστη, τρέξτε το πρόγραμμα " Active Directory Users and Computers " από το μενού " Administrative Tools ". Σημειώστε ότι πρέπει να τρέξετε αυτό το πρόγραμμα από τον ίδιο υπολογιστή στον οποίο εγκαταστάθηκαν τα ADS4Unix plugins - εάν διαχειριστείτε κανονικά τη βάση χρηστών σας από έναν άλλο τερματικό σταθμό έπειτα που θα πρέπει να εγκαταστήσετε τα plugins εκεί επίσης, ίσως αυτή τη φορά χωρίς τις ενημερώσεις σχημάτων.

Αφού δημιουργήσετε έναν νέο χρήστη, το παράθυρο επέμβασης χρηστών (που λαμβάνεται πατώντας δύο φορές έναν χρήστη στον κατάλογο χρηστών) περιέχει μια πρόσθετη ετικέτα, με τον τίτλο " Unix settings ". Αυτό περιέχει τους ακόλουθους πρόσθετους τομείς:

- NIS: Θέστε αυτό στο NIS domain που δημιουργήσατε στο πρόγραμμα διαμόρφωσης.
- UID: Η αριθμητική ταυτότητα χρηστών Unix αυτού του χρήστη.
- GID: Η αριθμητική ταυτότητα ομάδας Unix αυτού του χρήστη.
- Description: Αυτό αντικαθιστά τον τομέα "comment" στο αρχείο /etc/passwd.
- Home folder: Αυτός είναι ο αρχικός κατάλογος του χρήστη στο Unix.
- Shel: Αυτό πρέπει να τεθεί σε κάτι χρήσιμο, π.χ.: /bin/bash για έναν χρήστη όπου απαιτούνται διαλογικά logins, ή ίσως /bin/false για έναν χρήστη που δεν έχει την άδεια για μια διαλογική σύνοδο σύνδεσης.

Σημειώστε ότι αυτοί οι τομείς κάνουν replicate τις πληροφορίες στο αρχείο /etc/passwd που βρίσκεται κανονικά σε ένα σύστημα Unix.

5.6 Καταχωρήσεις ομάδας

Για τις ομάδες του Active Directory, τώρα επίσης θα υπάρξει μια ετικέτα " Unix settings " στο εργαλείο Active Directory Users and Groups. Αυτή η ετικέτα περιέχει δύο τομείς:

- Group: Το συμβολικό όνομα ομάδας Unix για αυτήν την ομάδα.
- GID: Η αριθμητική ταυτότητα ομάδας Unix για αυτήν την ομάδα.

Η προσθήκη ενός χρήστη σε μια ομάδα Unix γίνεται πάλι μέσω του εργαλείου Active Directory Users and Groups, απλά με την ίδια μέθοδο που θα χρησιμοποιούσατε

για να προσθέσετε έναν λογαριασμό χρήστη του Active Directory σε μια ομάδα του Active Directory. Η ιδιότητα μέλους ομάδας στο Linux ή στο Unix αντανακλά την ιδιότητα μέλους στο Active Directory.

5.7 Άλλα συστατικά

Τώρα που διαμορφώνεται το Active Directory, πρέπει να διαμορφώσουμε ένα υπολογιστή Linux για να ενεργήσει ως πελάτης του Active Directory. Αυτό περιλαμβάνει την οργάνωση μερικών κομματιών του λογισμικού, που είναι τα παρακάτω:

- OpenLDAP (συγκεκριμένα η πλευρά πελατών του OpenLDAP).
- NSS_LDAP και PAM_LDAP.

5.8 OpenLDAP πελάτης

Ο πελάτης OpenLDAP μπορεί να ληφθεί με διάφορους τρόπους. Αυτό περιλαμβάνει:

- Λήψη του κώδικα πηγής από το OpenLDAP.
- Εγκατάσταση των .RPM ή .DEB αρχεία για τον OpenLDAP για τη διανομή σας.

Τα τμήματα πελατών που μας ενδιαφέρουν συμπεριλαμβάνοντας τις κοινές βιβλιοθήκες και το πρόγραμμα ldapsearch, τις οποίες θα χρησιμοποιήσουμε για δοκιμή. Εάν πρόκειται να μεταγλωττίσετε τα NSS_LDAP και PAM_LDAP από την πηγή επίσης, θα χρειαστείτε τα αρχεία επιγραφών του OpenLDAP. Όλα αυτά τα αρχεία πρέπει να εγκατασταθούν όταν τρέχετε το "make install" από τον κατάλογο πηγής OpenLDAP.

Εάν έχετε ένα σύστημα Red Hat έπειτα μπορείτε να θελήσετε να εγκαταστήσετε τα OpenLDAP RPMs. Στο Red Hat αυτά είναι τα openldap και openldap-client RPM αρχεία. Πρέπει να χρησιμοποιήσετε μια πρόσφατη έκδοση OpenLDAP. Σημειώστε ότι δεν χρειάζεστε τα RPM του openldap-server.

Εάν εγκαθιστάτε ένα σύστημα Red Hat Linux, θα βρείτε το αρχείο διαμόρφωσης πελατών OpenLDAP εγκατεστημένο στο σύστημά σας όπως το /etc/openldap/ldap.conf. Πρέπει να ανοίξετε αυτό το αρχείο με έναν συντάκτη κειμένων (όπως VI ή ο Emacs) και να περιλάβετε τις ακόλουθες δύο γραμμές:

```
HOST <serveraddress>
BASE <searchbase>
```

Όπου "<serveraddress>" είναι η dns διεύθυνση ονόματος ή η IP του Active Directory server σας (προτιμώ να χρησιμοποιήσω τη διεύθυνση IP, σε περίπτωση αποτυχίας του dns, τουλάχιστον έπειτα θα είστε σε θέση να βρείτε τον κεντρικό υπολογιστή LDAP σας), και το "<searchbase>" είναι η βάση αναζήτησης του LDAP σας που οργανώνεται από το Active Directory. Αυτό θα είχε εισαχθεί από σας όταν οργανώνετε το Active Directory χρησιμοποιώντας το μάγο, και είναι πιθανώς μια σειρά όπως αυτή "dc=yourcompany, dc=com" ή παρόμοια.

Μόλις διαμορφώσετε το ldap.conf αρχείο σας, πρέπει να είστε σε θέση να πραγματοποιήσετε μια απλή ερώτηση LDAP χρησιμοποιώντας το πρόγραμμα ldapsearch. Παραδείγματος χάριν:

```
ldapsearch - X ""
```

Σημειώστε την κενή σειρά στα εισαγωγικά στο τέλος της γραμμής εντολής. Τρέχοντας αυτή την εντολή αναζήτησης πρέπει να δείτε κάποιες ενδιαφέρουσες εάν όχι ιδιαίτερα πληροφοριακές λεπτομέρειες.

Μια από τις ενδιαφέρουσες ιδιορρυθμίες του Active Directory είναι ότι δεν επιτρέπει τις αναζητήσεις κάτω από το κορυφαίο επίπεδο του καταλόγου ενώ δεσμεύεται ανώνυμα (μην επικυρωμένα) στον κατάλογο. Έτσι, παραδείγματος χάριν, η ακόλουθη αναζήτηση θα αποτύχει:

```
ldapsearch - X "sAMAccountName=del"
```

Εκτιμώντας ότι, αφού συνδεθεί (παραδείγματος χάριν, ως διαχειριστής), η εντολή θα πετύχει:

```
ldapsearch - X - δ "cn=Administrator, cn=Users,
dc=somecompany, dc=com" - W/
  "sAMAccountName=del"
```

(η ανωτέρω εντολή θα σας προτρέψει για έναν κωδικό πρόσβασης - πρέπει να παρέχετε τον κωδικό πρόσβασης του διαχειριστή για το Active Directory σας).

Σημειώστε ότι εάν το βασικό DN σας για το Active Directory είναι "dc=somecompany, dc=com" έπειτα το προεπιλεγμένο διαχειριστικό DN σας θα είναι "cn=Administrator, cn=Users, dc=somecompany, dc=com". Αυτό μπορούσε να είχε αλλάξει εάν έχετε τροποποιήσει την εγκατάσταση του Active Directory σας, έτσι ελέγξτε αυτό πριν το χρησιμοποιείτε στην ανωτέρω ερώτηση LDAP.

Πρέπει να κάνετε τον πελάτη OpenLDAP να δουλεύει πριν να προχωρήσετε περαιτέρω. Εάν δεν μπορείτε να εκτελέσετε τουλάχιστον τις απλές κορυφαίες αναζητήσεις επιπέδων στο Active Directory σας, θα πρέπει να εντοπίσετε και να λύσετε οποιαδήποτε προβλήματα πριν να προχωρήσετε στο επόμενο βήμα.

5.9 NSS_LDAP

Το παρόν έγγραφο προορίζεται να σας βοηθήσει στην ενσωμάτωση της επικύρωσης μεταξύ LINUX και Microsoft Active Directory. Χρησιμοποιώντας τις pam_ldap και nss_ldap υπομοναδες από το padl.com το Active Directory μπορεί να χρησιμοποιηθεί ως μια κεντρική πηγή επικύρωσης και για τα δυο συστήματα Windows και LINUX .

Στην πλευρά του Linux, τα σημαντικότερα συστατικά είναι τα nss_ldap και pam_ldap. Οι υπομονάδες έρχονται επίσης με τις πιο σύγχρονες διανομές Linux συμπεριλαμβανομένου του Red Hat.

Εάν επαναπεταγλωττίσετε από την πηγή, πάρετε την τελευταία έκδοση του nss_ldap, σιγουρευτείτε ότι χρησιμοποιείτε τις ακόλουθες δύο επιλογές στη γραμμή ./configure κατά την μεταγλώττιση:

```
/configure --enable-schema-mapping --enable-rfc2307bi
```

Η σημαία --enable-rfc2307bis απαιτείται για οποιαδήποτε έκδοση του nss_ldap). Εάν προτιμάτε να εγκαταστήσετε από .DEB ή .PM αρχεία, θα πρέπει να σιγουρευτείτε ότι το nss_ldap και pam_ldap υπομονάδες εγκαθίστανται στο σύστημά σας.

Εντούτοις, θα πρέπει να ανακατασκευάσετε το nss_ldap RPM, ως εξής.

5.10 Επαναμετταγλωτίζοντας το αρχείο NSS_LDAP RPM

Τα αρχείο nss_ldap που παρέχεται από την Red Hat δεν περιλαμβάνει μια ιδιαίτερη σημαία που απαιτείται για να επιτρέψει στο nss_ldap να εργαστεί ενάντια στο Active Directory schema (το οποίο είναι διαφορετικό από το OpenLDAP schema που χρησιμοποιείται κανονικά σε συστήματα Red Hat Linux). Ο καλύτερος τρόπος να επιτραπεί αυτή η σημαία είναι να επαναμετταγλωτίσετε το αρχείο nss_ldap RPM.

Εγκαταστήστε το πηγαίο RPM αρχείο χρησιμοποιώντας:

```
rpm -ihv nss_ldap-xxx.i386.src.rpm
```

Θα πρέπει έπειτα να ανοίξετε το αρχείο/το /usr/src/redhat/SPECS/nss_ldap.spec. Γύρω στη γραμμή 67 του αρχείου, θα βρείτε την εντολή διαμόρφωσης, η οποία έχει ως εξής:

```
%configure --with-ldap=openldap --libdir=/lib
```

Θα πρέπει να την αλλάξετε σύμφωνα με τα παρακάτω:

```
%configure --with-ldap=openldap --libdir=/lib --enable-schema-mapping
```

Επίσης, κοντά στην κορυφή του αρχείου θα βρείτε τη γραμμή:

```
Release: 2
```

Αλλάξτε το αυτό σε:

```
Release: 3
```

Μπορείτε έπειτα να ανακατασκευάσετε το RPM χρησιμοποιώντας:

```
cd /usr/src/redhat/SPECS
rpm -ba --clean nss_ldap.spec
```

Αφότου τελειώνει η διαδικασία κατασκευής, θα έχετε ένα αρχείο στο /usr/src/redhat/RPMS/i386 που θα ονομάζεται nss_ldap-xxx-3.i386.rpm. Πρέπει να εγκαταστήσετε αυτό το αρχείο χρησιμοποιώντας την ακόλουθη εντολή:

```
rpm -Uhv  usr/src/redhat/RPMS/i386/nss_ldap-172-3.i386.rpm
```

Σημειώστε ότι η σημαία --enable-rfc2307bis flag στη γραμμή %configure είναι επίσης απαραίτητη για οποιαδήποτε έκδοση του nss_ldap. Η έκδοση του NSS_LDAP που έρχεται με το Red Hat έτσι αυτή η σημαία δεν χρειάζεται, αλλά εάν λάβετε ένα πιο πρόσφατο RPM έπειτα που θα χρειαστείτε την ακόλουθη γραμμή διαμόρφωσης αντί αυτής που παρουσιάζεται ανωτέρω:

configure --with-ldap=openldap --libdir=/lib
 --enable-schema-mapping   --enable-rfc2307bis

5.11 NSS_LDAP διαμόρφωση

Το αρχείο διαμόρφωσης για το nss_ldap είναι το αρχείο /etc/ldap.conf. Αυτό κανονικά θα έχει δημιουργηθεί στο σύστημά σας όταν εγκαταστήσατε την υπομονάδα nss_ldap.

Μόλις εγκαταστήσετε το nss_ldap και το pam_ldap, θα πρέπει να ανοίξετε την γραμμή /etc/ldap.conf ως εξής.

5.12 Authconfig

Το Red Hat Linux έρχεται με ένα πρόγραμμα διαμόρφωσης πιστοποίησης αποκαλούμενο authconfig, το οποίο μπορείτε να χρησιμοποιήσετε για να εκτελέσετε τη βασική διαμόρφωση για να επιτρέψετε στο σύστημά σας να χρησιμοποιήσει την επικύρωση LDAP. Για να τρέξει αυτό, συνδεθείτε ως root και εκτελέστε την ακόλουθη εντολή:

```
Authconfig
```

Στην πρώτη οθόνη, επιλέξτε "Use LDAP". Εισάγετε τη διεύθυνση IP του κεντρικού υπολογιστή LDAP (που είναι ο Windows 2003 Active Directory) και του βασικού DN που εισαγάγατε όταν οργανώσατε το Active Directory (π.χ.: dc=yourcompany, dc=com). Επίσης σιγουρευτείτε ότι το " Use LDAP Authentication " είναι τσεκαρισμένο.

Το Authconfig προορίζεται στο να οργανώσει ένα σύστημα που επικυρώνει σε έναν κεντρικό υπολογιστή OpenLDAP, και επομένως δεν εκτελεί όλες τις λειτουργίες που απαιτούνται για να οργανώσουν το σύστημά σας που επικυρώνει ενάντια στο Active Directory. Για να ολοκληρώσετε τη διαμόρφωση, θα πρέπει να ανοίξετε το αρχείο /etc/ldap.conf, το οποίο είναι το αρχικό αρχείο διαμόρφωσης για το OpenLDAP.

Πρέπει επίσης φύγουν από σχόλια οι ακόλουθες γραμμές, οι οποίες πρέπει να είναι στο βασικό LDAP.conf αρχείο σας:

```
nss_base_passwd cn=Users,<your_base_dn>?sub
nss_base_shadow cn=Users,<your_base_dn>?sub
```

```
nss_map_objectclass posixAccount User
nss_map_objectclass shadowAccount User
nss_map_attribute uid sAMAccountName
# nss_map_attribute userPassword msSFUPassword
nss_map_attribute homeDirectory msSFUHomeDirectory
nss_map_objectclass posixGroup Group
nss_map_attribute uniqueMember member
nss_map_attribute cn sAMAccountName
pam_login_attribute sAMAccountName
pam_filter objectclass=user
pam_password ad
```

Σημειώστε ότι οι ανωτέρω εισαγωγές διαμόρφωσης αρχείων, <your_base_dn> πρέπει να αντικατασταθούν από το Base DN που δημιουργήθηκε όταν εγκαταστήσατε το Active Directory. Θα έχετε χρησιμοποιήσει αυτό αρκετές φορές από πριν ήδη, παραδείγματος χάριν στο αρχείο /etc/openldap/ldap.conf.

5.13 Επιτρέποντας τις ανώνυμες αναζητήσεις στο Active Directory

Σε αυτή τη φάση, όλα πρέπει σχεδόν να δουλεύουν. Πρέπει να είστε σε θέση να συνδεθείτε ως χρήστης στο Active Directory του domain σας, χρησιμοποιώντας τον κωδικό πρόσβασης του Active Directory, και κυρίως και συνδέεστε. Θα δείτε μερικά μηνύματα λάθους, που συμπεριλαμβάνουν:

```
id: cannot find name for user ID 1001
id: cannot find name for group ID 1000
```

Αυτό είναι επειδή το Active Directory σας δεν μπορεί να αναζητηθεί ανώνυμα. Υπάρχουν δύο λύσεις για αυτό το πρόβλημα:

1. Επιτρέψτε τις ανώνυμες αναζητήσεις στον Active Directory.
2. Εισάγετε ένα DN διαχειριστή και κωδικό πρόσβασης στο /etc/ldap.conf

Για να επιτρέψετε τις ανώνυμες αναζητήσεις στο Active Directory, ακολουθήστε αυτά τα βήματα:

- Στον Windows 2003 Active Directory server, τρέξτε το διαχειριστικό εργαλείο Active Directory Users and Groups.
- Επιλέξτε το κορυφαίο επίπεδο του καταλόγου από την άποψη δέντρων στο αριστερό πλαίσιο, και πατήστε δεξί κλικ. Θα εμφανιστούν μερικές επιλογές. Επιλέξτε το πρώτο στοιχείο, το οποίο πρέπει να είναι " Delegate Control"
- Πατήστε "Next"
- Στο επόμενο παράθυρο, με τον τίτλο " Users or Groups ", πατήστε "Add"
- Στον επόμενο κατάλογο, επιλέξτε " ANONYMOUS LOGON " και πατήστε "Add". Μπορεί επίσης να χρειαστεί να επιλέξετε το "Everyone" και την ομάδα "Guests", ανάλογα με το πώς διαμορφώνετε το Active Directory. Πατήστε OK όταν γίνει αυτό.
- Πατήστε "Next"

- Επιλέξτε το "Create a custom task to delegate"
- Πατήστε "Next"
- Στον επόμενο κατάλογο, επιλέξτε το "Read". συγχρόνως θα επιλεχθεί το "Read All Properties". Πατήστε "Next" όταν γίνει αυτό.
- Πατήστε "Finish"

5.14 Εισάγοντας ένα Διαχειριστικό DN στο /etc/ldap.conf

Μια εναλλακτική λύση για να επιτραπούν οι ανώνυμες αναζητήσεις στο Active Directory είναι να επιτραπούν οι ρουτίνες nss_ldap για να δεσμεύσει ως έναν διαχειριστή DN στον κατάλογό σας και να εκτελέσει τις αναζητήσεις με προνομιούχο τρόπο. Για να κάνετε αυτό, εισάγετε τις ακόλουθες γραμμές στο αρχείο /etc/ldap.conf

binddn cn=Administrator, cn=Users, <your_base_dn>
bindpw <your_administrator_password>

Το ανωτέρω παράδειγμα δείχνει ότι το όνομα χρήστη του διαχειριστή όπως και ο κωδικός πρόσβασης έχουν κωδικοποιηθεί στο καθαρό κείμενο στο αρχείο /etc/ldap.conf! Δυστυχώς, αυτό το αρχείο πρέπει πάντα να παραμείνει αναγνώσιμο προς τα έξω, επειδή ειδάλλως οι χρήστες που συνδέονται στο σύστημα δεν θα είναι σε θέση να διαβάσουν τα στοιχεία από τον κατάλογο. Δεν πρέπει να το κάνετε αυτό σε ένα σύστημα όπου οποιοσδήποτε χρήστης έχει shell access στο σύστημά σας, ή μπορεί με οποιοδήποτε άλλο τρόπο να διαβάσει αυτό το αρχείο.

Φυσικά, υπάρχει μια τρίτη εναλλακτική λύση, η οποία είναι να δημιουργηθεί ένας νέος χρήστης μέσα στο Active Directory και να οριστεί σε αυτόν τον χρήστη κανένα δικαίωμα εκτός από την πρόσβαση ανάγνωσης στον κατάλογο. Θα μπορούσατε έπειτα να κλειδώσετε τη σύνδεση και τον κωδικό πρόσβασης αυτού του χρήστη στο αρχείο /etc/ldap.conf, παρά το διαχειριστικό DN και τον κωδικό πρόσβασης. Δεν θεωρώ αυτήν την μέθοδο καθόλου ασφαλέστερη από την χορήγηση ανώνυμων δεσμεύσεων. Εντούτοις, οποιοσδήποτε χρήστης που θα μπορούσε (ανώνυμα ίσως) να διαβάσει αυτό το αρχείο θα μπορούσε να διαβάσει το όνομα σύνδεσης και τον κωδικό πρόσβασης του ειδικού DN που έχετε δημιουργήσει.

5.15 PAM_LDAP

Σε ένα σύστημα Red Hat, το PAM_LDAP είναι μέρος του NSS_LDAP RPM. Το PAM_LDAP εξ ορισμού χρησιμοποιεί το ίδιο αρχείο διαμόρφωσης (/etc/ldap.conf), έτσι όλες οι αλλαγές του nss_ldap λειτουργούν επίσης για το pam_ldap

Σημειώστε ότι το PAM_LDAP χρησιμοποιείται μόνο για την επικύρωση, ενώ το NSS_LDAP χρησιμοποιείται για όλες τις πληροφορίες χρηστών. Ένας χρήστης μπορεί ακόμα να συνδεθεί σε ένα σύστημα Linux χωρίς να δουλεύει το NSS_LDAP, αν και θα λάβουν συχνά μηνύματα λέγοντας " I have no name!". Εάν αυτό συμβαίνει σε σας, είναι πιθανό να δουλεύει σωστά το PAM_LDAP αλλά να έχει πέσει το NSS_LDAP.

Σημειώστε ότι για να είστε σε θέση να αλλάξετε τους κωδικούς πρόσβασης σε έναν Active Directory server από Linux, πρέπει να έχετε ενεργοποιημένα τα SSL και TLS, και τα δύο στο client end και στο server end.

5.16 Πόροι Ιστού

Υπάρχουν πολλοί πόροι στο διαδίκτυο που μπορούν να σας βοηθήσουν να βάλετε σε τάξη το δίκτυό σας κάνοντας το λειτουργικό.

Η τεκμηρίωση του Active Directory, που παρέχεται από τη Microsoft. Η σελίδα κοινοπραξίας για το OpenLDAP. Η σελίδα της Innosoft για το LDAP Η σελίδα για το MKS AD4Unix. Η PADL που δημιούργησε τις υπομονάδες nss_ldap και pam_ldap που είναι διαθέσιμα δωρεάν. Το Quartet, είναι ένα νέο πρόγραμμα, το οποίο προσπαθεί να εφαρμόσει ένα μεγάλο μέρος της λειτουργίας του Active Directory στο Linux.

Ο καθένας που εργάζεται σε ένα διαπλατφορμικό περιβάλλον Unix και Windows πρέπει να εξοικειωθεί με το πρόγραμμα SAMBA. Η έκδοση 3.0 της SAMBA μπορεί να ενώσει ένα Active Directory domain. Η εργασία προχωρεί στο να πάρει τις πληροφορίες χρηστών για την SAMBA που είναι αποθηκευμένες στον LDAP.

5.17 Συνδεση ενός Linux server στο Active Directory με την χρήση της Samba 3,0

Δεδομένου ότι το Linux γίνεται πιο διαδεδομένο στις επιχειρήσεις, η διαλειτουργικότητα μεταξύ του και των επιβεβλημένων λειτουργικών συστημάτων γίνεται σημαντικότερη. Τελικά, κανένας δεν θέλει να προσθέσει ένα νέο σύστημα εάν αυτό απαιτεί εξ ολόκληρου ένα νέο σύνολο εργαλείων διαχείρισης και πρόσθετους λογαριασμούς χρηστών.

Ένα εργαλείο που έχει γίνει πανταχού παρόν στις διαμορφώσεις του Linux είναι η Samba, η οποία είναι ανοιχτού κώδικα πρόγραμμα υπηρεσίας αρχείων και πιστοποίησης. Η έκδοση των Windows 2003 και η χρήση του Active Directory περιέπλεξαν την ενσωμάτωση ενός Linux server στο περιβάλλον της Microsoft, η όποια είχε κάνει θραύση με τα WINDOWS NT και την Samba έκδοση 2.2.X. Αν και η Samba μπορεί ακόμα να χρησιμοποιηθεί ως ελεγκτής περιοχών, αυτό απαιτεί έναν ανάμικτο Windows 2003 domain, στο οποίο μερικοί domain controllers των WINDOWS NT 4.0 είναι ακόμα παρόντες. (Η Samba θεωρείται domain controller των WINDOWS NT 4.0.)

Επιπλέον, Τα Windows 2003 (και XP) χρησιμοποιούν τον domain controller με πρωτόκολλο επικύρωσης Kerberos, το οποίο παρουσιάζει νέες προκλήσεις για τη διαλειτουργικότητα. Μερικοί διαχειριστές θέλουν να μεταβούν προς έναν ενεργό Active Directory domain αλλά ακόμα παρέχουν μια κεντρική υπηρεσία επικύρωσης και γιαυτό πρέπει να επινοηθεί ένας νέος τρόπος αντιμετώπισης της επικύρωσης.

Η ομάδα της Samba παρέχει τα μέσα να χειριστείς την ίδια διεργασία στη νεώτερη έκδοση, η οποία είναι ακόμα υπό ανάπτυξη. Σας παρουσιάζεται πώς να χρησιμοποιήσετε την πιο πρόσφατη έκδοση της Samba για να επιτρέψει στον Linux server σας να επικυρώνει ενάντια στον Windows 2003 domain controller.

Αυτό το άρθρο υιοθετεί την πιο πρόσφατη έκδοση Samba 3,0. Αν και δεν είναι έτοιμη για δίκτυα παραγωγής, ο κώδικας λειτουργεί και σύμφωνα με το χρονοπρόγραμμα, δεν θα αλλάξει δραστικά όταν θα είναι πλήρης. Μετά από μια μεγάλη συνέντευξη από την ομάδα ανάπτυξης της Samba, καθησυχάστηκα ότι οι ερχόμενες αλλαγές της Samba 3,0 θα είναι πρώτιστα η προσθήκη των χαρακτηριστικών γνωρισμάτων και η σταθεροποίηση του κώδικα. Η εγκατάσταση και οι διαμορφώσεις που παρουσιάζονται σε αυτό το άρθρο πιθανά δεν θα αλλάξουν.

5.18 Τι χρειαζόμαστε

Για να εγκατασταθεί και λειτουργήσει η Samba 3,0 πρέπει να έχουμε:
· Windows 2003 Server που ενεργεί ως domain controller.
· Τις βιβλιοθήκες ανάπτυξης του OpenLDAP για Linux.
· Τις βιβλιοθήκες ανάπτυξης του MIT Kerberos για Linux.
· Την πιο πρόσφατη έκδοση της Samba.

Εάν δεν είσαι βέβαιος εάν είναι εγκατεστημένες αυτές οι βιβλιοθήκες, μπορείτε να χρησιμοποιήσετε την εντολή RPM.
rpm -qa |grep openldap που βλέπει εάν έχετε τις βιβλιοθήκες openldap-devel
rpm qa | grep krb για να ελέγξετε για τις βιβλιοθήκες Kerberos.
Εάν έχουν χαθεί οποιεσδήποτε από αυτές τις βιβλιοθήκες, μπορούμε να τις εγκαταστήσουμε με την εντολή *rpm i <όνομα βιβλιοθήκης>*.

Οι διευθύνσεις IP των μηχανών που χρησιμοποιούνται σε αυτό το έγγραφο θα είναι:
Windows.NET - 192.168.0.12
Linux - 192.168.0.13

5.19 Εγκατάσταση της Samba 3,0

Η εγκατάσταση Samba 3,0 είναι αρκετά απλή. Ακολουθήστε αυτά τα βήματα:

1. Αποσυμπιέστε την Samba 3,0 με την εντολή *gunzip -cd samba-3.0-alpha17.tar.gz | tar xvf -.*
2. Αλλαγή στον κατάλογο του πρόσφατα δημιουργημένου καταλόγου με το *cd samba-3.0-alpha17/source*.
3. Τρέξτε το script διαμόρφωσης, με χρησιμοποίηση της εντολής */configure -prefix=/usr/local/samba* για να καθοδηγήσει το script να εγκαταστήσει την Samba στο */usr/local/samba*.
4. Σιγουρευτείτε ότι οι γραμμές *#define HAVE KRB5 1* and *#define HAVE LDAP 1* είναι παρών στο αρχείο *include/config.h* .
5. Μεταγλωτήστε την εφαρμογή με την εντολή *make* .
6. Εγκαταστήστε την εφαρμογή με την εντολή *make install* .

5.20 Εγκατάσταση Win2K3

1) Εγκατάσταση του πακέτου υψηλής-κρυπτογράφησης. Διάλεξα αυτό το πακέτο υψηλής κρυπτογράφησης για να ενεργοποίηση το SSL πάνω από τον ldap.
2) Επιτρέψτε την ενημέρωση του schema στον Domain Controller. Θα πρέπει να χρησιμοποιήσετε το schema διαχείρισης MMC για να το κάνετε αυτό. Το snapin DLL αντιγράφεται στο σύστημα όταν εγκαθίσταται το πακέτο διαχείρισης σε έναν τερματικό σταθμό. Πιστεύω ότι τα αρχεία εγκαθίστανται επίσης όταν αναβαθμίζετε έναν κεντρικό υπολογιστή μέλος σε ένα Domain Controller.

Εάν αυτή είναι η πρώτη φορά που τρέχετε αυτό το εργαλείο, θα πρέπει να καταχωρήσετε τη διαχείριση DLL με τα Windows. Υποθέτω ότι οι υπάλληλοι της Microsoft δεν θέλουν μια "τυχαία" τροποποίηση στο schema από εμάς. Για να καταχωρήσετε το dll τρέξτε την εντολή "regsvr32 c:\winnt\system32\schmmgmt.dll"

5.21 Δημιουργία ενός διαχειριστικού Msc schema

start...run...mmc
console...add/remove snapin...add
Επιλέξτε το Active Directory Schema και κάντε κλικ στο add
κλικ στο close
κλικ στο OK
Διαλέξτε τον domain controller που θέλετε να αναβαθμίσετε το schema
Δεξι κλικ στο “Active Directory Schema" και επιλέξτε "Change Domain Controller"
Επιλέξτε "Specify name" και πληκτρολογήστε στον DNS το όνομα η την διεύθυνση του Domain controller σας
Επιτρέψτε τις ενημερώσεις του domain controller
Δεξι κλικ στο "Active Directory Schema" και επιλέξτε "Operations Master"
Κλικ στο εικονίδιο "The Schema may be modified on this Domain Controller"
Κλικ στο OK

5.22 Ενημέρωση του σχήματος

1) Τροποποιήστε το αρχείο schema για να απεικονίσετε το domain σας
2) Κάνετε μια σφαιρική αναζήτηση και αντικαταστήστε στο αρχείο το "{targetdomain}" με ",dc=το domain σου,dc=[com,net,org....]""
3) Εισάγετε το schema - "ldifde -i -k -f your_modified_schema_file.ldif". Αυτό είναι ένα από τα εργαλεία που εγκαθίστανται με το πηγαίο πακέτο.
4) Εγκατάσταση του SSL - εγκαταστήστε τις υπηρεσίες cert και ορίστε ένα cert στον κεντρικό υπολογιστή
5) Προσθέστε τους χρήστες σας

Χρησιμοποιείστε το ldp.exe για να προσθέσουν τις ιδιότητες για τα gecos, uidNumber, gidNumber, loginShell, msSFUHomeDirectory, msSFUName

5.23 Εγκαταστηστε στο LINUX

Κατεβαστε την πιό πρόσφατη έκδοση του nss_ldap από το ftp.padl.com.Θα πρέπει να αναμεταγλωρησετε το nss_ldap με το --enable-schema-mapping and the --enable-rfc2307bis.
Επομενως η πληκτρολογηση ειναι:
./configure --enable-rfc2307bis --enable-schema-mapping && make && make install
Αυτό θα διαμορφώσει και θα εγκαταστήσει τη νέα βιβλιοθήκη.

Κατόπιν επεμβείτε στο ldap.conf σας

Έκανα μερικές αλλαγές στο schema MSSFU. Χρησιμοποίησα

nss_map_attribute uid sAMAccountName

αντι του

#nss_map_attribute uid msSFUName

και

nss_map_attribute uniqueMember Member

αντι του

#nss_map_attribute uniqueMember posixMember

Αυτές οι αλλαγές έκαναν το nss_ldap να χρησιμοποιεί τον απλό AD για τις ιδιότητες των userid and group membership.

Ακόμη έχω δυο διευθύνσεις IP στην γραμμή του host.

5.24 Αυτό είναι το /etc/ldap.conf αρχείο μου

@(#)$Id: ldap.conf,v 1.8 2002/02/26 08:50:37 root Exp $

host 192.168.0.20 192.168.0.19

base dc=ratisle,dc=net

ldap_version 3

binddn anonymous@test.net

scope sub

ssl yes

pam_filter objectclass=user
pam_login_attribute sAMAccountName
pam_password ad
nss_base_passwd ou=users,ou=sb consulting,dc=ratisle,dc=net?one
nss_base_shadow ou=users,ou=sb consulting,dc=ratisle,dc=net?one
nss_base_group ou=group,ou=sb consulting,dc=ratisle,dc=net?one
nss_map_objectclass posixAccount User
nss_map_attribute uid sAMAccountName
nss_map_attribute uniqueMember Member
nss_map_attribute userPassword msSFUPassword
nss_map_attribute homeDirectory msSFUHomeDirectory
nss_map_objectclass posixGroup Group
nss_map_attribute cn sAMAccountName

5.25 Παραμετροποιώντας το Kerberos

Πρέπει να διαμορφώσετε μερικές παραμέτρους για να ενημερώσετε τη διαδικασία Kerberos πώς να χειριστείτε τον Active Directory server. Παρουσιάζετε ολόκληρο το περιεχόμενο του */etc/krb5.conf* αρχείου μου. Κάνετε τις κατάλληλες τροποποιήσεις, λάβετε υπόψη ότι σε Kerberos το SLOWE.COM και slowe.com δεν ταιριάζουν.

Έχετε ένα πράγμα ακόμα να ελέγξετε. Δεν μπορώ να τονίσω αρκετά τη σημασία του συγχρονισμού ρολογιών μεταξύ του Windows 2003 Server και του Linux server. Εάν ο χρόνος απόκρισης είναι περισσότερο από πέντε λεπτά, οι δύο κεντρικοί υπολογιστές θα είναι σε θέση να επικοινωνήσουν, αλλά καμία πληροφορία τύπου ticket δεν θα λειτουργήσει. Αυτό είναι εύκολο να αντιμετωπιστεί με τη χρήση του kinit: Αρκετά μεγάλη ασυμετρική κίνηση ρολογιών ενώ αποκτώνται τα πιστοποιητικά όταν δοκιμάζεται το Kerberos.

Για να σιγουρευτείτε ότι η σύνδεσή σας λειτουργεί, τρέξτε την εντολή */usr/kerberos/bin/kinit nuser@SLOWE.COM*. Η εντολή kinit του Kerberos θα εξετάσει την επικοινωνία μεταξύ των κεντρικών υπολογιστών σας. Η σύνταξη είναι *kinit user@REALM*, όπου REALM είναι το Active Directory domain name σας και πρέπει να είναι κεφαλαία. Εάν δεν χρησιμοποιείτε όλα τα γράμματα κεφαλαία, θα λάβετε αυτό το λάθος:
kinit(v5): Cannot find KDC for requested realm while getting initial credentials.

Εάν η επικοινωνία λειτουργεί, θα προτρέπεστε για τον κωδικό πρόσβασης του χρήστη. Όταν εισαχθεί σωστά, πολύ απλά θα επιστρέψετε σε κονσόλα bash. Εάν εισάχθούν λάθος θα λάβετε το μύνημα λάθους:
kinit(v5): Preauthentication failed while getting initial credentials.

6. Διαχείριση του Active Directory Χρησιμοποιώντας το Windows Script

Στην ανάπτυξη των προγραμμάτων για το Active Directory, θα εργαστείτε συχνά με τα κοινά αντικείμενα καταλόγου όπως οι χρήστες, ομάδες, υπολογιστές, και εκτυπωτές. Το ADSI (Active Directory Service Interfaces) καθιστά την εργασία σας ευκολότερη με την παροχή των διεπαφών που σχεδιάζονται συγκεκριμένα για τον τύπο αντικειμένου με το οποίο θέλετε να εργαστείτε. Το περιβάλλον του Windows scripting καθιστά τη ζωή ενός διαχειριστή δικτύων ευκολότερη με την παροχή της πρόσβασης στο Active Directory μέσω του ADSI χρησιμοποιώντας τις σχετικά απλές γλώσσες προγραμματισμού. Αυτό το κεφάλαιο περιέχει πολύ κώδικα πηγής δειγμάτων, συνήθως στις μικρές λειτουργίες, που επεξηγεί πώς να εκτελεστούν συγκεκριμένοι στόχοι.

6.1 Windows Scripting

Για πολλά έτη, οι διαχειριστές δικτύων και οι "power users" χρησιμοποιούσαν αρχεία δέσμης του MS-DOS (batch files .bat) για να αυτοματοποιήσουν ορισμένους στόχους. Όταν τα Windows έκαναν αισθητή την παρουσία τους, η ανάγκη να αυτοματοποιηθούν μερικοί στόχοι υπήρχε ακόμα, αλλά η Microsoft δεν συμπεριέλαβε οποιαδήποτε ικανότητα scripting στα Windows.

Όχι πριν από την ανάπτυξη της αυτοματοποίησης, που επέτρεψε στις γλώσσες για scripting να έχουν πρόσβαση στα αντικείμενα COM, ήταν πραγματικά πιθανό σε περιβάλλον Windows. Η αυτοματοποίηση επιτρέπει στις γλώσσες με δυνατότητα scripting να δημιουργήσουν τις περιπτώσεις αντικειμένων COM και να έχει πρόσβαση στις ιδιότητες και τις μεθόδους εκείνων των αντικειμένων στο χρόνο εκτέλεσης.

Βασικά, οι πρώτοι οικοδεσπότες των scripts ήταν οι εφαρμογές της Microsoft, Word και Excel, μεταξύ των άλλων. Αυτές οι εφαρμογές περιέλαβαν επίσης Microsoft Visual Basic για εφαρμογές (VBA), μια ελαφρώς υποβαθμισμένη έκδοση της δημοφιλούς γλώσσας που έρχεται ως τμήμα του προγραμματιστικού περιβάλλοντος της Visual Basic.

Δεδομένου ότι το Διαδίκτυο έγινε δημοφιλέστερο, η Microsoft συμπεριέλαβε υποστήριξη για τα VBScript, μια ακόμη πιο υποβαθμισμένη έκδοση του Visual Basic από το VBA, και το JScript, την εφαρμογή της Microsoft για JavaScript, στον Microsoft Internet Explorer και Microsoft Internet Information Server (IIS).

Μια εξάπλωση των γλωσσών, συμπεριλαμβανομένων των VBA, VBScript, JScript, μεγάλες εφαρμογές όπως το Word, client Web browsers, και Web servers, όλοι μπορούν να κάνουν χρήση των αντικείμενων COM που υποστηρίζουν την αυτοματοποίηση.

6.2 Windows Script Host

Το ελλείπον κομμάτι είναι ένα ανεξάρτητου περιβάλλοντος εκτέλεσης μιας εφαρμογής, όπου εκεί έρχεται το Windows Script Host. Το 1998, η Microsoft ένανε διαθέσιμο για κατέβασμα το Windows Script Host 1.0 και το περιέλαβε στο Windows NT 4.0 Option Pack και στα Windows 98. Το Windows Script Host δεν εκτελεί πραγματικά τα χειρόγραφα καθαυτού, αλλά παρέχει μια μηχανή *scripting* να εκτελεστεί ένα μεμονωμένο *script*.

Η μηχανή script είναι συγκεκριμένη για μια γλώσσα προγραμματισμού. Τα συστατικά του Windows Script περιλαμβάνουν τις μηχανές για VBScript και JScript. Αλλες γλώσσες, όπως Perl και Python, επίσης έχουν διαθέσιμες μηχανές. Η δυνατότητα να κωδικοποιήσετε στη γλώσσα της επιλογής σας και το πρόγραμμά σας να εκτελέσει δια μέσου της πλατφόρμας των Windows είναι εξαιρετικά ισχυρή. Κάθε μηχανή για script παρέχει τα εγγενή χαρακτηριστικά γνωρίσματα στις γλώσσες, όπως το *For Each* statement της VBScript ή σχόλια (/* */ and //) της Jscript και C/C++. Πολλά Perl scripts που γράφονται ως CGI Web server scripts μπορούν τώρα να είναι εύκολα και να τρέχουν ανεξάρτητα από έναν Web server.

6.3 Αρχεία Windows Script

Η έκδοση 1.0 του Windows Script Host φορτώνει μια ιδιαίτερη μηχανή script βασισμένη στην επέκταση ονομάτων αρχείου του αρχείου που περιέχει τον κώδικα του script. Παραδείγματος χάριν, ένα αρχείο που ονομάζεται Simple.vbs θα καθοδηγούσε το Windows Script Host για να φορτώσει τη μηχανή VBScript, αν και το Simple.js θα έδειχνε ότι μια μηχανή JScript απαιτείται. Αρχίζοντας από τον Windows Script Host 2.0, που είναι διαθέσιμο στα Windows 2000, ο Windows Script Host προσθέτει την υποστήριξη για έναν νέο τύπο αρχείου, ένα Windows Script file (.wsf), που χρησιμοποιεί τις ετικέτες XML για να καθορίσει τα διάφορα τμήματα. Ένα σημαντικό όφελος ενός .wsf είναι ότι μπορεί να περιέχει πολλαπλά scripts, σε οποιαδήποτε υποστηριγμένη γλώσσα. Ένα πρακτικό παράδειγμα αυτής της ικανότητας θα ήταν η σειρά εργαλείων ενός διαχειριστή συστημάτων. Αυτά τα εργαλεία είναι πιθανό να γραφτούν σε διάφορες γλώσσες. Με ένα .wsf, αυτά τα εργαλεία μπορούν να συλλεχθούν και να συσσωρευθούν σε έναν ενιαίο .wsf αρχείο. Τα scripts που περιλαμβάνονται σε ένα .wsf αρχείο μπορεί επίσης να επικαλεστούν τις διαδικασίες που περιλαμβάνονται στο ίδιο ή σε άλλο .wsf αρχείο.

Ένα wsf είναι δομημένο διαφορετικά από ένα αρχείο .vbs ή js. Ένα .wsf είναι ουσιαστικά ένα αρχείο XML. Αυτή η μορφή επιτρέπει αρκετή ευελιξία στη δημιουργία των scripts, όπως η συμπερίληψη πολλών χειρογράφων σε ένα ενιαίο αρχείο και ο χειρισμός των γεγονότων. Τα στοιχεία XML που θα χρησιμοποιήσω είναι *job*, *script*, και *reference*. Το στοιχείο *job* λέει στον Windows Script Host να μεταχειριστεί το περιεχόμενό του ως μια διεργασία. Πολλαπλάσιες εργασίες μπορούν να περιληφθούν σε ένα ενιαίο αρχείο και να παραπεμφθούν χρησιμοποιώντας ένα επιχείρημα γραμμής εντολών. Το στοιχείο *script* διευκρινίζει σε ποια γλώσσα γράφεται το script. Αυτό χρησιμοποιείται από τον Windows Script Host για να φορτώσει τη σωστή μηχανή

scripting. Το στοιχείο *reference* διευκρινίζει μια βιβλιοθήκη τύπων, ποιος θα αναφερθεί αργότερα σε αυτό το κεφάλαιο

6.4 Windows Script Object Model

Το Windows Script παρέχει ένα πρότυπο αντικειμένων που μπορεί να χρησιμοποιηθεί από οποιαδήποτε μηχανή script. Το αντικείμενο WScript παρέχει την πρόσβαση στις πληροφορίες για το περιβάλλον εκτέλεσης, όπου το αντικείμενο WshArguments περιέχει τις πληροφορίες και τις μεθόδους για να ανακτήσει διαφωνίες γραμμής εντολών (command-line arguments) – μια προϋπόθεση του scripting. Αλλα αντικείμενα στο πρότυπο περιλαμβάνουν το WshShell, μια διεπαφή στην shell διεπαφή του χρήστη των Windows, και το WshNetwork, όποιος επιτρέπει στα scripts να χρησιμοποιήσουν τις πηγές αρχείων και εκτυπωτών σε ένα δίκτυο. Το πρότυπο περιλαμβάνει επίσης τα αντικείμενα που αντιπροσωπεύουν τα drives, φάκελους, και αρχεία. Οποιοδήποτε script που τρέχει κάτω από τον Window Script Host μπορεί να χρησιμοποιήσει αυτά τα αντικείμενα. Ο πίνακας 6-1 απαριθμεί μερικά από τα αντικείμενα του Windows Script Host μαζί με τα αντικείμενα που παρέχονται από τη μηχανή χρόνου εκτέλεσης των Windows Script.

Αντικείμενο	Περιγραφή	Παρεχόμενο απο
WScript	Στοιχεία και μέθοδοι που αντιπροσωπεύουν το τρέχον περιβάλλον εκτέλεσης	Windows Script Host
WshArguments	Συλλογή των επιχειρημάτων γραμμής εντολών	Windows Script Host
WshEnviroment	Collection of named system environment variables	Windows Script Host
WshNetwork	Συλλογή των ονομασμένων μεταβλητών περιβάλλοντος συστήματος	Windows Script Host
WshShell	Μέθοδοι για να ελέγξει τις διαδικασίες και το μητρώο και για να δημιουργήσει νέους συντομότερους δρόμους	Windows Script Host
WshShortcut	Αντιπροσωπεύει ένα αρχείο συντόμευσης	Windows Script Host

Πίνακας 6-1 *Μερικά από τα αντικείμενα του Windows Script.*

6.5 Βιβλιοθήκες Τύπων (Type Libraries)

Μια βιβλιοθήκη τύπων είναι ένας ορισμός ενός ή περισσότερων αντικειμένων COM που περιλαμβάνει τις πληροφορίες για τις διεπαφές των αντικειμένων όπως οι ιδιότητες, μέθοδοι, παράμετροι, και τύποι δεδομένων. Μια βιβλιοθήκη τύπων επιτρέπει

στους μεταγλωττιστές όπως το Microsoft Visual C++ και Visual Basic για να εκτελέσουν τον έλεγχο τύπου, παραδείγματος χάριν, η επαλήθευση ότι τα στοιχεία που διαβιβάζονται σε μια μέθοδο είναι σωστά. Βελτιώνει επίσης την απόδοση επειδή ο μεταγλωττιστής μπορεί να δημιουργήσει τον κώδικα που άμεσα επικαλείται μια μέθοδο, παρά να εκτελεστεί μια σειρά βημάτων στο χρόνο εκτέλεσης. Αυτό καλείται πρόωρη σύνδεση (*early binding*)

Οι βιβλιοθήκες τύπων περιέχουν επίσης τους ορισμούς για τις σταθερές, απαριθμήσεις, και δομές.

6.6 Δημιουργώντας και Αλλάζοντας τα Scripts

Αν και το να δημιουργήσετε απλά scripts είναι εύκολο, έχει όμως και τα μειονεκτήματά του. Αυτήν την περίοδο τα περιβάλλοντα ανάπτυξης διαθέσιμα από τη Microsoft για τη δημιουργία των scripts είναι περιορισμένα. Οι προγραμματιστές εξοικειωμένοι με τη συνεργασία με πλούσιους κειμενογράφους και εκσφαλματωτές (debuggers) σε Visual C++ 6.0 και Visual Basic 6.0 έχουν κολλήσει χρησιμοποιώντας το σημειωματάριο για να δημιουργήσουν πολλά scripts. Ακόμη και ο script editor στο Microsoft Visual InterDev 6.0 αναγνωρίζει μόνο τα scripts που σχεδιάζονται για το συγκεκριμένο περιβάλλον. Ενώ Visual InterDev 6.0 μπορεί να ρυθμιστεί για να παρέχει το χρωματισμό σύνταξης και την ολοκλήρωση δήλωσης IntelliSense, δεν μπορείτε να χρησιμοποιήσετε τον ενσωματωμένο διορθωτή εύκολα. Πολλοί προγραμματιστές script, χρησιμοποιούν το σημειωματάριο και το Microsoft Script Debugger για να δημιουργήσουν τις μικρές εφαρμογές scripting.

Η παρούσα έκδοση του περιβάλλοντος ανάπτυξης της Microsoft, το Visual Studio.NET, φέρνει την ευπρόσδεκτη ανακούφιση στους προγραμματιστές για την ανάπτυξη scripts. Μπορείτε να δημιουργήσετε ένα .wsf χρησιμοποιώντας το νέο περιβάλλον επεξεργασίας XML και να εκμεταλλευθείτε το χαρακτηριστικό γνώρισμα IntelliSense του Visual Studio για να σας παρέχεται η ολοκλήρωση της δήλωσης και να χρησιμοποιήσετε τους εξελισσόμενους καταλόγους ιδιοτήτων και μεθόδων. Στρέψτε την προσοχή σας τώρα στη χρησιμοποίηση του Windows Script για να διαχειριστείτε πραγματικά τους πόρους δικτύου στο Active Directory.

6.7 Διαχείριση Χρηστών

Η πιό ορατή και κοινή διαχειριστική διεργασία στο Active Directory διαχειρίζεται τους λογαριασμούς χρηστών. Πριν από το Active Directory, οι λογαριασμοί χρηστών υπήρξαν πρώτιστα για λόγους έγκρισης και ασφάλειας. Με το Active Directory, η εστίαση έχει μετατοπιστεί στην αντιπροσώπευση των πραγματικών ανθρώπων. Οι πληροφορίες για τους ανθρώπους στον ενεργό κατάλογο αντιπροσωπεύονται με δύο μορφές: χρήστες και επαφές. Ένα αντικείμενο της κατηγορίας χρηστών αντιπροσωπεύει ένα μεμονωμένο πρόσωπο και περιέχει την ονομασία, επαφή, και πληροφορίες ασφάλειας. Ένα αντικείμενο της κατηγορίας επαφών είναι παρόμοιο, αλλά παραλείπει τις

πληροφορίες ασφάλειας. Οι επαφές χρησιμοποιούνται για να παρακολουθήσουν των ανθρώπων σε έναν οργανισμό που δεν είναι χρήστες δικτύων. Οι επαφές μπορούν επίσης να αντιπροσωπεύσουν ανθρώπους εξωτερικούς στην οργάνωση, όπως οι πελάτες.

6.8 Η Διεπαφή IADsUser

Όταν το ADSI δεσμεύεται σε οποιοδήποτε αντικείμενο, κάνει έναν γρήγορο έλεγχο της κατηγορίας σχημάτων του αντικειμένου. Το ADSI έπειτα καθορίζει εάν η κατηγορία περιλαμβάνει μια κατάλληλη διεπαφή. Στην περίπτωση των αντικειμένων των κατηγοριών *user* ή *contact*, το ADSI παρέχει τη διεπαφή IADsUser, που συμπυκνώνει τις πληροφορίες κοινές και για τους χρήστες και τις επαφές. Οι πίνακες 6-2 και 6-3 παρουσιάζουν τις ιδιότητες και μεθόδους του IADsUser

Ιδιότητες του ADsUser	**Τύπος Δεδομένων**	**Αντίστοιχο Χαρακτηριστικό στο Active Directory**	**Περιγραφή**
AccountDisabled	Boolean	*userAccountControl* (*UF_ACCOUNTDISA BLE* flag)	Εάν True, ο λογαριασμός απενεργοποιείται .
AccountExpira tionDate	Date	*accountExpires*	Ημερομηνία και ώρα όταν ένας λογαριασμός λήγει
BadLoginAddress	String	Not supported under Active Directory	Η διεύθυνση του υπολογιστή που προκάλεσε το κλείδωμα του λογαριασμού
BadLoginCount	Long	*badPwdCount*	Ο αριθμός των αποτυχημένων προσπαθειών σύνδεσης
Department	String	*department*	Το όνομα του τμήματος με το οποίο σχετίζεται ο χρήστης.
Description	String	*description*	Μια περιγραφή του χρήστη.

Πίνακας 6.2: *ιδιότητες της διεπαφής IADsUser*.

Μεθόδοι του IADsUser	Περιγραφή
ChangePassword	Αλλάζει τον κωδικό πρόσβασης χρηστών. Οι νέοι και τρέχοντες κωδικοί πρόσβασης πρέπει να παρασχεθούν
Groups	Επιστρέφει μια συλλογή των ομάδων που ο χρήστης ανήκει.
SetPassword	Θέτει τον κωδικό πρόσβασης για τον λογαριασμό του χρήστη

Πίνακας 6.3: *Μέθοδοι της διεπαφής IADsUser.*

Η διεπαφή IADsUser δημιουργήθηκε ενώ το Active Directory σχεδιαζόταν ακόμα, έτσι οι ιδιότητες της διεπαφής IADsUser δεν ταιριάζουν πάντα με τις ιδιότητες διαθέσιμες σε ένα αντικείμενο χρηστών πολύ καλά.

6.9 Δημιουργώντας Χρήστες

Διάφορα σημαντικά στοιχεία πρέπει να εξεταστούν κατά δημιουργία των χρηστών. Κατ' αρχάς, πρέπει να καταλάβετε ποιες ιδιότητες απαιτούνται όταν δημιουργείται το αντικείμενο. Δεύτερον, πρέπει να ξέρετε ποιες πληροφορίες να βάζετε σε ποιο αντικείμενο. Δυστυχώς, το Active Directory θέτει διάφορα "gotchas" που συντίθενται από τις διαφορές μεταξύ των ιδιοτήτων του IADsUser και των ιδιοτήτων του Active Directory που χαρτογραφούνται

Ένα τέτοιο "gotcha" είναι οι ιδιότητες διευθύνσεων για έναν χρήστη. Ενώ η διεπαφή IADsUser παρέχει την ιδιοκτησία PostalAddress, η χρησιμοποίηση αυτής της ιδιοκτησίας για να έχει πρόσβαση στην ταχυδρομική διεύθυνση ενός χρήστη δεν θα λειτουργήσει κάτω από το Active Directory. Δεν πρέπει να χρησιμοποιήσετε την ιδιοκτησία PostalAddress επειδή το Active Directory χρησιμοποιεί χωριστές ιδιότητες για την οδό (streetAddress), πόλη (*l*), περιοχή (*st*), και ταχυδρομικός κώδικας (postalCode). Με το Active Directory, πρέπει να χρησιμοποιήσετε τη μέθοδο Get της διεπαφής IADs για να έχετε πρόσβαση σε αυτές τις ιδιότητες.

6.10 Χαρακτηριστικά Ονομάτων (Naming Attributes)

Το Active Directory απαιτεί δύο ιδιότητες για να τεθεί κατά τη δημιουργία ενός νέου αντικειμένου *user*. Η πρώτη είναι η ιδιότητα *cn* (*Common-Name*). Αυτό είναι απλά το όνομα του αντικειμένου και μπορεί ή όχι να αφορά το όνομα του χρήστη. Όπως με όλα τα αντικείμενα στο Active Directory, το όνομα του αντικειμένου πρέπει να είναι μοναδικό μέσα στο κοντεϊνερ του. Εάν ένας χρήστης προστίθεται σε ένα κοντεϊνερ που έχει ήδη ένα αντικείμενο με το ίδιο όνομα, η λειτουργία δημιουργίας αποτυγχάνει.

Η δεύτερη απαιτούμενη ιδιότητα, και μια πιθανή πηγή σύγκρουσης, είναι η ιδιότητα sAMAccountName. Αυτό είναι το όνομα σύνδεσης που χρησιμοποιείται από τις εκδόσεις των Windows πριν από τα Windows 2000. Με το Active Directory, η συμβολοσειρά που ο χρήστης πληκτρολογεί κατά την σύνδεση μπορεί να είναι η τιμή

sAMAccountName ή ένα κύριο όνομα χρηστών (user principal name UPN). Το UPN είναι πιό εύκαμπτο από την ιδιότητα sAMAccountName δεδομένου ότι αποτελείται από δύο μέρη – το πρώτο είναι ένα όνομα χρήστη που ακολουθείται από το σύμβολο at (@), και ο δεύτερος ένα Domain Name System (dns) γνωστό ως επίθημα UPN. Γενικά, το UPN ενός χρήστη θα είναι η διεύθυνση ηλεκτρονικού ταχυδρομείου του, vpsarras@teleinfom.teiep.gr ή vasilios.psarras@teleinfom.teiep.gr, παραδείγματος χάριν. Το UPN είναι χρήσιμο επειδή δίνει στους χρήστες κοινό και ευκολομνημόνευτο προσδιοριστικό – την διεύθυνση του ηλεκτρονικού ταχυδρομείο τους – για να συνδεθούν στο δίκτυο.

Ανεξάρτητα από το UPN, η ιδιότητα sAMAccountName πρέπει ακόμα να είναι μοναδική στο domain. Υπάρχουν δύο τρόποι να αποφευχθεί μια σύγκρουση με τις διπλές τιμές για την ιδιότητα sAMAccountName. Μια απλή μέθοδος είναι να προσπαθήσετε να προσθέσετε το χρήστη και να ανιχνεύσετε εάν έχει εμφανιστεί ένα λάθος. Ένας άλλος τρόπος είναι να ρωτηθεί ο global catalog (GC) server με την προτεινόμενη αξία για το sAMAccountName, δεδομένου ότι η ιδιότητα sAMAccountName είναι μεταξύ εκείνων που περιλαμβάνονται στο υποσύνολο του global catalog. Η σειρά ερώτησης του LDAP θα ήταν (sAMAccountName=proposedvalue). Αφού η ιδιότητα sAMAccountName είναι επίσης μια συνταγμένη ιδιότητα, ο global catalog server μπορεί να εκτελέσει μια αποδοτική αναζήτηση. Εάν ένα αντικείμενο επιστρέφεται από την αναζήτηση, το προτεινόμενο όνομα χρησιμοποιείται ήδη. Με καθεμία μέθοδο, εάν μια σύγκρουση ονόματος ανιχνεύεται, το script μπορεί έπειτα να προτρέψει για ένα άλλο όνομα λογαριασμού ή να προσπαθήσει να παραγάγει ένα μοναδικό. Τα ονόματα λογαριασμού πρέπει να είναι 20 χαρακτήρες ή λιγότεροι, και γενικά μην περιέχετε τα διαστήματα.

6.11 Το Script Δημιουργίας Χρηστών

Η απαρίθμηση 6-1 παρουσιάζει ένα script, που προσθέτει έναν χρήστη στο Active Directory. Μπορείτε εύκολα να τροποποιήσετε αυτό το δείγμα που διαβάζει τις πληροφορίες από ένα αρχείο κειμένων ή μια βάση δεδομένων για να δημιουργήσετε τους πολλούς χρήστες συγχρόνως. Το script επιδεικνύει πώς να δημιουργήσετε ένα αντικείμενο χρηστών στο κοντεϊνερ *Users* και να θέσετε διάφορες ιδιότητες χρησιμοποιώντας τις διεπαφές IADs και IADsUser. Παρατηρήστε ότι η μέθοδος Create της διεπαφής IADsContainer, χρησιμοποιείται για να δημιουργήσει το αντικείμενο χρηστών. Όλα τα νέα αντικείμενα στο Active Directory δημιουργούνται με τη μέθοδο Create του IADsContainer.

```
<job id="CreateUser">
<reference guid="{97D25DB0-0363-11CF-ABC4-02608C9E7553}"/>
<script language="VBScript">
`
` CreateUser - δημιουργεί το χρήστη παραδείγματος
`
` Συμβολοσειρές που χρησιμοποιούνται για να προσδιορίσουν και να
' περιγράψουν το νέο χρήστη
` Όνομα σύνδεσης
```

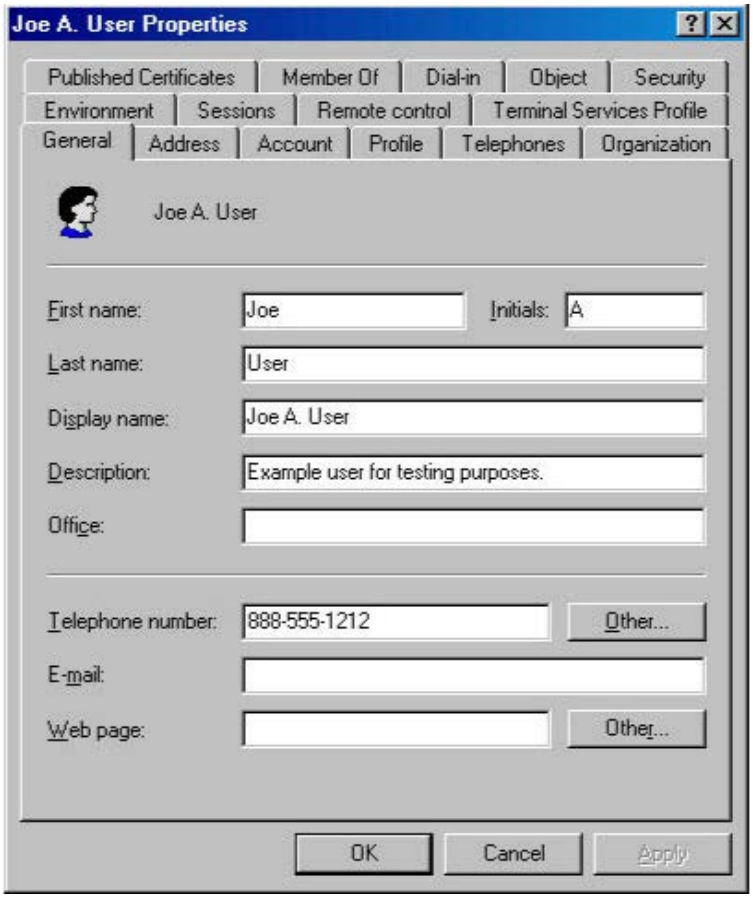
```
 strUserAcct = "JAUser"
strFullName = "Joe A. User"
strFirstName = "Joe"
strLastName = "User"
strPassword = "mypassword"
` Πολύ σύγχυση σε αυτά.  Ο βοηθός χρησιμοποιεί τα αρχικά ως "μέση αρχή"
strMiddleName = "Average"
strInitials = "A"
` Περιγραφικές πληροφορίες
strUserDesc = "Example user for testing purposes."
strTelephone = "888-555-1212"
strStreet = "One Microsoft Way"
strCity = "Redmond"
strState = "WA"
strZIPCode = "98052"

 ` Πληροφορίες εμφάνισης
WScript.Echo "Creating new user `" & strFullName & "`..."


` Δεσμευτείτε στο rootDSE και πάρτε το προεπιλεγμένο χώρισμα των domain
προεπιλογήςSet adsRootDSE = GetObject("LDAP://rootDSE")
strDomainDN = adsRootDSE.Get("defaultNamingContext")


` Δεσμευτείτε στο κοντεΐνερ Users ενός Domain
strADsPath = "LDAP://CN=Users," & strDomainDN
Set adsContainer = GetObject(strADsPath)


` Πηγαίνετε στην επόμενη γραμμή ένα ένα λάθος εμφανιστεί


` Δημιουργήστε το αντικείμενο στο κοντεϊνερ χρησιμοποιώντας ολόκληρο το
όνομα
Set adsUser = adsContainer.Create("user", "cn=" + strFullName)


` Ορίστε το όνομα λογαριασμού του χρήστη
adsUser.Put "sAMAccountName", strUserAcct


` Ορίστε το UPN του χρήστη
adsUser.Put "userPrincipalName", strUserAcct


` Ενημερώστε τον server με τις απαιτούμενες ιδιότητες
adsUser.SetInfo


` Έλεγχος για λάθη
If Err.Number <> 0 Then
    ` Εξετάστε την περίπτωση λάθους, ο χρήστης να υπάρχει ήδη
    If Err.Number = &H80071392 Then
        ` Εμφάνιση των μηνυμάτων λάθων και έξοδος
       WScript.Echo "The user name `" & strFullName & "` already exist
s."
```

```
        WScript.Quit 1
    Else
        WScript.Echo "Unexpected error creating user." & vbNewLine & _
            Err.Description & " (" & Hex(Err.Number) & ")"
        WScript.Quit 1
    End If
End If


` Ο χειρισμός λαθών εκτός λειτουργίας
On Error GoTo 0


` Χρήση των ιδιοτήτων του για να ορίσουμε άλλα μέρη δεδομένων
` Ενημέρωση της τοπικής εναποθηκευμένης ιδιοκτησίας με τις
πληροφορίες ενός νέου χρήστη
adsUser.GetInfo


` Ορίστε τον κωδικό του χρήστη. Το  SetInfo πρέπει να καλείται εκ των
προτέρων.
adsUser.SetPassword strPassword


` Απαιτείται ο χρήστης για να αλλάξει τον κωδικό στο login
adsUser.Put "pwdLastSet", 0


` Ενεργοποίηση του λογαριασμού
adsUser.AccountDisabled = False


` Ορισμός του εμφανιζόμενου ονόματος του χρήστη.
adsUser.FullName = strFullName


` Ορισμός πληροφοριών ονόματος του χρήστη.
adsUser.FirstName = strFirstName
adsUser.LastName = strLastName
adsUser.OtherName = strMiddleName
adsUser.Put "initials", strInitials


` Ορισμός της περιγραφής χρησιμοποιώντας την ιδιότητα Description
adsUser.Description = strUserDesc


` Ορισμός του τηλεφωνικού αριθμού.
adsUser.TelephoneNumber = strTelephone


` Ορισμός πληροφοριών διεύθυνσης.
` Πρέπει να χρησιμοποιήσουμε τις ιδιότητες του Active Directory, όχι
την ιδιοκτησία PostalAddress .
adsUser.Put "streetAddress", strStreet
adsUser.Put "l", strCity
adsUser.Put "st", strState
```

```
adsUser.Put "postalCode", strZIPCode


` Εφαρμογή των ιδιοτήτων στον κατάλογο.
adsUser.SetInfo


` Απελευθέρωση αντικειμένων
Set adsUser = Nothing
Set adsContainer = Nothing


` Τέλος
WScript.Echo "User created successfully."
</script>
</job>
```

Απαρίθμηση 6-1: το *CreateUser.wsf δείχνει πώς να δημιουργήσουμε έναν χρήστη.*

Όταν τρέχετε το script CreateUser, ένας χρήστης που ονομάζεται "Vasilios P. User" δημιουργείται στο κοντεϊνερ χρηστών. Το σχήμα 6.1 παρουσιάζει πλαίσιο διαλόγου ιδιοτήτων για το νέο χρήστη στο Active Directory Users and Computers.



Σχήμα 6.1: *Το πλαίσιο διαλόγου ιδιοτήτων για τον νέο χρήστη που δημιουργήθηκε με το CreateUser script.*

6.12 Προκαθορισμένες Τιμές Χρήστη

Εάν δεν θέτετε ρητά τις ιδιότητες και τα χαρακτηριστικά απαριθμημένα στους πίνακες 6-4 και 6-5 κατά τη δημιουργία ενός νέου χρήστη, το Active Directory θα χρησιμοποιήσει τις προκαθορισμένες τιμές.

Ιδιότητες IADsUser	**Προκαθορισμένη τιμή**
AccountDisabled	True
AccountExpirationDate	1/1/1970. Αυτό υποδεικνύει ότι ο λογαριασμός δεν λήγει ποτέ.
PasswordLastChanged	Το προκαθορισμένο είναι, που σημαίνει ότι ο χρήστης πρέπει να αλλάξει τον κωδικό στο επόμενο logon.
PasswordRequired	False

Πίνακας 6.4: *Προκαθορισμένες τιμές ιδιοτήτων για ένα αντικείμενο χρήστη.*

Ιδιότητες User	**Προκαθορισμένη τιμή**
memberOf	Εάν δεν διευκρινίζεται, αυτή η ιδιότητα παραμένει κενή εντούτοις η ομάδα Domain Users τίθεται ως αρχική ομάδα για τον χρήστη.
nTSecurityDescriptor	Ένας περιγραφέας ασφάλειας δημιουργείται από το συνδυασμό του τμήματος *user* και από τον κύριο περιγραφέα ασφάλειας αντικειμένων.
objectCategory	Θέστε στο Person. Αυτή η ιδιότητα τίθεται αυτόματα από το Active Directory και δεν μπορεί να τροποποιηθεί.

Πίνικας 6.5: *Προκαθορισμένες τιμές χαρακτηριστικών για ένα αντικείμενο χρήστη.*

6.13 Κωδικοί Πρόσβασης

Ο κωδικός πρόσβασης για έναν λογαριασμό χρήστη περιλαμβάνεται στις ιδιότητες του unicodePwd του αντικειμένου χρηστών. Ο πραγματικός κωδικός πρόσβασης αποθηκεύεται στον κατάλογο χρησιμοποιώντας μια τεχνική κρυπτογράφησης γνωστή ως *one-way format* (OWF). Δεν μπορείτε άμεσα να διαβάσετε ή να γράψετε στις ιδιότητες unicodePwd ακόμα κι αν έχετε τα κατάλληλα προνόμια ασφάλειας. Αυτός ο περιορισμός αποτρέπει τον κωδικό πρόσβασης από τη διαβίβαση του σε καθαρό κείμενο πέρα από το δίκτυο.

Προκειμένου να τεθεί ή να αλλαχτεί ο κωδικός πρόσβασης ενός χρήστη, πρέπει να χρησιμοποιήσετε τις μεθόδους SetPassword ή ChangePassword της διεπαφής IADsUser. Η χρήση της συγκεκριμένης μεθόδου εξαρτάται από το πλαίσιο ασφάλειας της εφαρμογής.

Η μέθοδος SetPassword δέχεται μια παράμετρο σειράς και την χρησιμοποιεί για να αντικαταστήσει τον τρέχοντα κωδικό πρόσβασης. Αυτή η μέθοδος μπορεί να χρησιμοποιηθεί από τους διαχειριστές για να επαναρυθμίσει τον κωδικό πρόσβασης ενός χρήστη. Όταν το SetPassword χρησιμοποιείται σε ένα πρόγραμμα που δημιουργεί ένα αντικείμενο χρηστών, η ιδιότητα pwdLastSet πρέπει να τεθεί σε 0, που δείχνει ότι ο χρήστης πρέπει να αλλάξει τον κωδικό πρόσβασής του την επόμενη φορά που συνδέεται. Στο Active Directory Users and Computers, αυτή η επιλογή είναι διαθέσιμη στην ετικέτα λογαριασμού του πλαισίου διαλόγου ιδιοτήτων του χρήστη, σε ένα πλαίσιο που ονομάζεται User Must Change Password At Next Logon. Είναι ορθή πρακτική ασφάλειας να απαιτήσουμε από τους χρήστες να αλλάξουν τον κωδικό πρόσβασής τους σε κάτι της επιλογής τους, παρά να χρησιμοποιηθεί ένας κωδικός πρόσβασης προεπιλογής, ο όποιος μπορεί να μείνει απροστάτευτος. Το script CreateUser που παρουσιάζεται στη απαρίθμιση 6-1 θέτει τις ιδιότητες pwdLastSet σε 0.

Η μέθοδος ChangePassword δέχεται δύο παραμέτρους: ο παλαιός κωδικός πρόσβασης και ο νέος κωδικός πρόσβασης. Επειδή απαιτεί γνώση του υπάρχοντος κωδικού πρόσβασης, αυτή η μέθοδος μπορεί να χρησιμοποιηθεί από τους τελικούς χρήστες.

Η απαρίθμηση 6-2 παρουσιάζει ένα script που μπορεί να χρησιμοποιηθεί για να αλλάξει έναν κωδικό πρόσβασης. Δέχεται τρεις παραμέτρους της γραμμής εντολών. Η πρώτη είναι το όνομα του χρήστη, παραδείγματος χάριν, "Vasilios P. User". Οποιοσδήποτε τύπος που αναγνωρίζεται από τα Windows μπορεί να χρησιμοποιηθεί, όπως domainname\username ή username@domainname.com. Οι δεύτερες και τρίτες παράμετροι είναι οι τρέχοντες και νέοι κωδικοί πρόσβασης, αντίστοιχα. Σημειώστε ότι τα εισαγωγικά απαιτούνται για οποιεσδήποτε παραμέτρους που έχουν διαστήματα. Εδώ είναι ένα παράδειγμα.

```
changepassword "Vasilis P. User" mypassword mynewpassword
```

```
<job id="ChangePassword">
<reference guid="{97D25DB0-0363-11CF-ABC4-02608C9E7553}"/>
<script language="VBScript">
`
` ChangePassword
  Δέχεται ένα όνομα καιπαραπέμπει για παλιό και νεό κωδικό πρόσβασης.
`
` Δέχεται ένα όνομα χρήστη και επαναπροσδιορίζει τον κωδικό πρόσβασης.
` Το όνομα πρέπει να είναι πλήρης ("Vasilios Psarras") ή να είναι σε
μορφή domainname\username ("coppersoftware\charles")
` Έλεγχος για το αν υπάρχει ένα όρισμα γραμμής εντολών
Set wshArguments = WScript.Arguments


If (wshArguments.Count = 3) Then


    ` Θεωρήστε το όρισμα γραμμής εντολών σαν το όνομα που θα
χρησιμοποιήσετε
    strUser = wshArguments(0)
    strOldPassword = wshArguments(1)
    strNewPassword = wshArguments(2)
```

```
Else
    WScript.Echo "Incorrect number of arguments." & vbNewLine & _
        "Usage:  ChangePassword.wsf username " & _
        "oldpassword newpassword"
    WScript.Quit 1
End If


` Χρήση του NameTranslate για να δείτε τον υπολογιστή στον κατάλογο
Set adsNameTranslate = CreateObject("NameTranslate")
adsNameTranslate.Init ADS_NAME_INITTYPE_GC, vbNullString


` Ορίστε το όνομα χρήστη στο nametranslate
` Καθορίστε άγνωστους τύπους, έτσι ώστε το σύστημα να μαντέψει.
adsNameTranslate.Set ADS_NAME_TYPE_UNKNOWN, strUser


` Λήψη του DN ενός αντικειμένου
strDN = adsNameTranslate.Get(ADS_NAME_TYPE_1779)


` Κάντε το DN ένα ADsPath προθέτοντας τον παροχέα ADSI
strADsPath = "LDAP://" & strDN


` Δέσμευση ενός αντικειμένου χρήστη
Set adsUser = GetObject(strADsPath)

 ` Επιβεβαίωση αλλαγής
strPrompt = "Change password for " & adsUser.FullName & " from `" & _
    strOldPassword & "` to `" & strNewPassword & "`?"
nConfirmed = MsgBox(strPrompt, vbYesNo, "Change Password")


If nConfirmed = vbYes Then
    ` Πήγαινε στην επόμενη γραμμή εάν γίνει ένα λάθος
    On Error Resume Next


    ` Αλλαγή του κωδικού πρόσβασης
    adsUser.ChangePassword strOldPassword, strNewPassword


    ` Έλεγχος για λάθη
    If Err.Number <> 0 Then
        ` Display error message
        Select Case (Err.Number)
            Case &H80070056
                WScript.Echo "The specified password for " & _
                    adsUser.FullName & " is not correct."
            Case &H800708C5
                WScript.Echo "The specified password does not " & _
                    "meet policy requirements."
            Case Else
                WScript.Echo "Unexpected error changing password." & _
                    vbNewLine & Err.Description & " (" & _
```

```
                    Hex(Err.Number) & ")"
        End Select
    Else
        WScript.Echo "Password successfully changed for " & _
            adsUser.FullName
    End If
End If


</script>
</job>
```

Απαρίθμιση 6-2 *To ChangePassword.wsf δείχνει πώς να αλλάξετε τον κωδικό πρόσβασης σε έναν υπάρχον χρήστη.*

6.14 Δουλεύοντας με τον Exchange Server 2003

Ο Microsoft Exchange 2003 Server είναι η πιό πρόσφατη έκδοση της Microsoft του επιχειρηματικού e-mail server της. Ο Exchange 2003 χρησιμοποιεί το Active Directory για να αποθηκεύσει τα στοιχεία διαμόρφωσης για τον εαυτό του και επεκτείνει πολλές κατηγορίες με τις νέες ιδιότητες και τους προσδιοριστές επίδειξης. Όταν ένας χρήστης ή μια επαφή είναι *mailbox-enabled*, ο Exchange 2003 έχει μια ταχυδρομική θυρίδα για το χρήστη ή την επαφή και έχει ενημερώσει τις πληροφορίες του προσώπου στο Active Directory για να δείξει τη διεύθυνση του ηλεκτρονικού ταχυδρομείου τους και τη θέση της ταχυδρομικής θυρίδας τους.

Ένας κοινός στόχος κατά το δημιουργία των χρηστών είναι να δημιουργηθεί μια ταχυδρομική θυρίδα στον Exchange 2003 συγχρόνως. Ο Exchange 2003 καθιστά αυτό εύκολο με την παροχή των διαχειριστικών διεπαφών που αθροίζουν μερικές υπάρχουσες διεπαφές ADSI. Αυτό γίνεται με τη χρησιμοποίηση του χαρακτηριστικού γνωρίσματος επέκτασης ADSI. οι ιδιότητες και οι μέθοδοι του Exchange 2003, οι διεπαφές *IMailboxStore* και *ImailRecipient,* είναι διαθέσιμες όταν δεσμεύονται σε ένα αντικείμενο κατηγορίας χρηστών ή επαφών.

Οι διεπαφές IMailboxStore και IMailRecipient είναι μέρος των Collaboration Data Objects για το Exchange Management (CDOEXM). Το CDOEXM επεκτείνει τα ADSI και τα αντικείμενα στοιχείων και συνεργασίας (CDO) για να περιλάβει τις ιδιότητες και τις μεθόδους για να διαχειριστεί τον Exchange 2003.

6.15 Διαχειρίζοντας Ομάδες

Ψηλά στον κατάλογο κοινών διαχειριστικών στόχων είναι η διαχείριση ομάδων. Μια ομάδα είναι απλά ένας κατάλογος σχετικών αντικειμένων. Γενικά, μια ομάδα περιέχει έναν κατάλογο χρηστών, υπολογιστές, ή άλλες ομάδες. Ένα παράδειγμα μιας ομάδας είναι όλοι οι διευθυντές σε έναν οργανισμό. Η προσθήκη του αντικειμένου χρηστών κάθε διευθυντή στην ομάδα παρέχει συγκεντρωμένη διαχείριση και ευκολότερη επικοινωνία με όλους τους διευθυντές. Ο πρόεδρος μιας επιχείρησης μπορεί έπειτα να στείλει το ηλεκτρονικό ταχυδρομείο σε μια μόνο διεύθυνση, όπως η

managers@coppersoftware.com, για να φθάσουν σε όλους τους διευθυντές αμέσως. Οι διαχειριστές δικτύων μπορούν να ορίσουν συγκεκριμένα προνόμια ασφάλειας σε μια ομάδα που επιτρέπει στα μέλη της ομάδας να εκτελέσουν συγκεκριμένους στόχους. Παραδείγματος χάριν, στην ομάδα του διευθυντή μπορεί να δοθεί η πρόσβαση σε περιορισμένους κοινούς φακέλους ή αρχεία.

6.16 Τύποι Ομάδων

Το Active Directory αντιπροσωπεύει μια ομάδα ως ενιαίο αντικείμενο της κατηγορίας *group*. Αυτό το αντικείμενο περιέχει τα χαρακτηριστικά που περιγράφουν τις ιδιότητες της ομάδας και τα μέλη ομάδας. Υπάρχουν δύο τύποι ομάδων: *distribution* και *security*.

Μια ομάδα διανομής χρησιμοποιείται για την διανομή καταλόγων ηλεκτρονικού ταχυδρομείου ή άλλους, όχι σχετικούς με την ασφάλεια σκοπούς. Παραδείγματος χάριν, ο κατάλογος ανθρώπων που θα λάβει το ενημερωτικό δελτίο της επιχείρησης θα μπορούσε να περιληφθεί σε μια ομάδα διανομής που ονομάζεται Newsletter Readers. Μια ομάδα διανομής στο Active Directory είναι η ίδια στην έννοια και χρησιμοποιείται από τον Microsoft Exchange 2003 Server για τον ίδιο σκοπό.

Μια ομάδα ασφάλειας χρησιμοποιείται για να εφαρμόσει ένα κοινό σύνολο αδειών πρόσβασης στα μέλη της ομάδας. Οι ομάδες ασφάλειας έχουν τα ίδια οφέλη με τις ομάδες διανομής αλλά επίσης παρέχουν τις πληροφορίες ασφάλειας. Οι άδειες που ορίζονται στην ομάδα εφαρμόζονται στα μέλη της ομάδας όταν συνδέονται στο δίκτυο.

Οι ομάδες διανομής και ασφάλειας στονActive Directory έχουν ένα πεδίο που καθορίζει πώς τίθενται οι άδειες ασφάλειας. Μια ομάδα έχει το ένα από τρία πεδία: *universal*, *global,* ή *domain local*. Μια καθολική ομάδα καλύπτει όλες τα domains μέσα σε μια ομάδα. Οι χρήστες μπορούν να προστεθούν από οποιοδήποτε domain, και οι άδειες της ομάδας ισχύουν σε όλες τα domains στο δάσος. Μια σφαιρική ομάδα απευθύνεται στο domain στο οποίο η ομάδα δημιουργήθηκε. Μόνο οι χρήστες στο ίδιο domain μπορούν να προστεθούν, αλλά οι άδειες ισχύουν για όλες τα domains στο δάσος. Το τοπικό πεδίο του domain είναι το αντίθετο του σφαιρικού πεδίου. Μια τοπική ομάδα ενός domain μπορεί να έχει μέλη από οπουδήποτε στο δάσος, αλλά οι άδειες εφαρμόζονται μόνο στο domain που η ομάδα δημιουργήθηκε.

Στις περισσότερες περιπτώσεις, οι σφαιρικές ομάδες είναι ικανοποιητικές. Η αλλαγή των μελών σε μια καθολική ομάδα προκαλεί την αντιγραφή μεταξύ των domains και των κεντρικών υπολογιστών σφαιρικών καταλόγων (global catalog servers). Εάν μια καθολική ομάδα απαιτείται, σκεφτείτε την δημιουργία σφαιρικών ομάδων σε κάθε domain και την προσθήκη μελών για εκείνο το domain. Κατόπιν προσθέστε κάθε σφαιρική ομάδα στην καθολική ομάδα. Αυτό θα αποτρέψει την περιττή αντιγραφή κάθε φορά που αλλάζει η σφαιρική ομάδα ιδιότητα μέλους. Οι τοπικές ομάδες του domain είναι καλύτερες για την ανάθεση των ειδικών αδειών σε μια βάση ανά- per-domain και για τον έλεγχο της πρόσβασης στα εκτός καταλόγου αντικείμενα όπως τα αρχεία και οι κοινοί φάκελοι.

6.17 Διεπαφές Ομάδας ADSI

Το ADSI περιλαμβάνει μια διεπαφή για τη συνεργασία με ομάδες, κατάλληλα ονομασμένο IADsGroup. Αυτή η διεπαφή περιέχει τις μεθόδους *Add* και *Remove* για να διαχειρίζεται τον κατάλογο μελών ομάδας. Οι ιδιότητες και οι μέθοδοι του IADsGroup παρατίθενται στους πίνακες 6-6 και 6-7.

Ιδιότητα του *IADsGroup*	**Τύπος Δεδομένων**	**Περιγραφή**
Description	String	Μια περιγραφή της ομάδας.

Πίνακας 6.6: *Ιδιότητες της διεπαφής IADsGroup.*

Μεθόδοι του IADsGroup	**Περιγραφή**
Add	Προσθέτει χρήστες ή άλλες αρχές ασφαλείας στην ομάδα.
IsMember	Ελέγχει να δει εάν το συγκεκριμένο αντικείμενο είναι μέλος της ομάδας.
Members	Επιστρέφει μια συλλογή των αντικειμένων των μελών μιας ομάδας χρησιμοποιώντας την διεπαφή *IADsMember*.
Remove	Απομακρύνει ένα μέλος από την ομάδα.

Πίνακας 6.7: *Μεθόδοι της διεπαφής IADsGroup.*

6.18 Δημιουργώντας μια Ομάδα

Για να δημιουργήσετε μια ομάδα, ξεκινήστε με την κλήση της μεθόδου Create της διεπαφής IADsContainer. Η μέθοδος Create της διεπαφής IADsContainer χρησιμοποιήθηκε νωρίτερα στο script CreateUser για να δημιουργήσει ένα αντικείμενο χρηστών, και η χρησιμοποίηση του για να δημιουργήσει μια ομάδα δεν είναι διαφορετική. Κατόπιν συμπληρώστε τις απαραίτητες πληροφορίες για την ομάδα.

Για μια ομάδα, το Active Directory απαιτεί τις ιδιότητες *cn*, *groupType*, και *sAMAccountName* να γεμιστούν προτού ένα πρόγραμμα ή ένα script να καλέσει το SetInfo. Η ιδιότητα *cn* είναι απλά το όνομα της ομάδας. Η ιδιότητα *groupType* είναι ο συνδυασμός σταθερών από την απαρίθμηση ADS_GROUP_TYPE_ENUM. Το sAMAccountName είναι το όνομα που χρησιμοποιείται από παλαιότερους πελάτες όπως τα Windows 95, Windows 98, και Windows NT 4.0 για να έχουν πρόσβαση στην ομάδα που χρησιμοποιεί τις λειτουργίες SAM API όπως η NetGroupGetInfo. Το sAMAccountName για τις ομάδες μπορεί να είναι μέχρι 256 χαρακτήρες μακρύ. Όπως αναφέρεται νωρίτερα, το όριο για τους χρήστες είναι 20 χαρακτήρες.

Αφού όλες οι απαραίτητες ιδιότητες συμπληρωθούν με τις τιμές, η μέθοδος SetInfo του IADs καλείται για να ενημερώσει τον κεντρικό υπολογιστή καταλόγου. Ένα

νέο αντικείμενο ομάδας δεν σώζεται πραγματικά στον κατάλογο έως ότου καλείται η μέθοδος SetInfo.

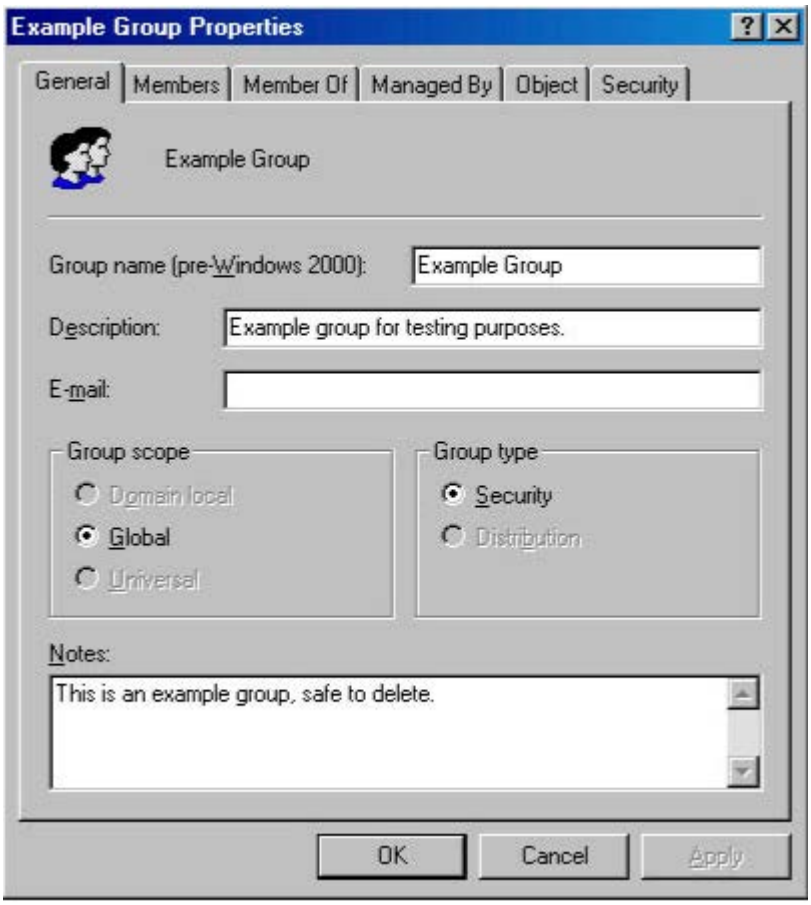
Η απαρίθμηση 6-3 παρουσιάζει ένα script, που δημιουργεί μια εξουσιοδοτημένη ομάδα ασφάλειας με το σφαιρικό πεδίο. Μόλις δημιουργηθεί η ομάδα και διευκρινιστούν οι απαραίτητες ιδιότητες, καλείται η μέθοδος SetInfo. Το script ελέγχει για οποιαδήποτε λάθη που έχουν εμφανιστεί. Εάν οποιοιδήποτε εμφανίζονται, το script επιδεικνύει τις πληροφορίες λάθους και τερματίζει. Εάν κανένα λάθος δεν εμφανίζεται, το script συνεχίζει να θέτει τις περιγραφικές ιδιότητες της ομάδας και ενημερώνει έπειτα τον κεντρικό υπολογιστή με μια τελική κλήση στο SetInfo

```
<job id="CreateGroup">
<reference guid="{97D25DB0-0363-11CF-ABC4-02608C9E7553}"/>
<script language="VBScript">
` CreateGroup.wsf - Δημιουργεί μια παραδειγματική ομάδα στο κοντεϊνερ
των Users
`
` Η συμβολοσειρά που χρησιμοποιείται για να αναγνωρίσει και να
περιγράψει την νέα ομάδα
strGroupName = "Example Group"
strGroupDesc = "Example group for testing purposes."
strGroupInfo = "This is an example group, safe to delete."


` Πληροφορίες εμφάνισης
WScript.Echo "Creating group `" & strGroupName & "`..."


` Δέσμευση στο RootDSE και λήψη του προκαθορισμένου χωρίσματος του
domain
Set adsRootDSE = GetObject("LDAP://RootDSE")
strDomainDN = adsRootDSE.Get("defaultNamingContext")


` Δέσμευση στο κοντεϊνερ Users του domain
strADsPath = "LDAP://CN=Users," & strDomainDN
Set adsContainer = GetObject(strADsPath)


` Πήγαινε στην επόμενη γραμμή εάν προκύψει ένα λάθος.
On Error Resume Next


` Δημιουργία του αντικειμένου ομάδας στον κοντεϊνερ.
Set adsGroup = adsContainer.Create("group", "CN=" + strGroupName)


` Ορισμός τύπου όπως ασφάλεια και πεδίο στο σφαιρικό
lGroupType = ADS_GROUP_TYPE_SECURITY_ENABLED Or _
    ADS_GROUP_TYPE_GLOBAL_GROUP
adsGroup.Put "groupType", lGroupType


` Ορισμός του ονόματος του λογαριασμού για την ομάδα.
` Μπορεί να είναι όπως ένα πλήρης όνομα μιας ομάδας (<256 χαρακτήρες)
```

```
adsGroup.Put "sAMAccountName", strGroupName


` Ενημέρωση του server με απαραίτητες ιδιότητες
adsGroup.SetInfo


` Έλεγχος για λάθη
If Err.Number <> 0 Then
    ` Έλεγχος λάθους για το αν η ομάδα υπάρχει ήδη
    If Err.Number = &H80071392 Then
        ` Εμφάνιση μηνύματος λάθους και έξοδος
          WScript.Echo "The group `" & strGroupName & _
              "` already exists."
          WScript.Quit 1

    Else
        WScript.Echo "Unexpected error creating group." & vbNewLine & _
            Err.Description & " (" & Hex(Err.Number) & ")"
        WScript.Quit 1
    End If
End If


` Εκτός λειτουργίας ο έλεγχος λαθών.
On Error Goto 0


` Ορισμός της περιγραφής χρησιμοποιώντας την ιδιότητα Description
adsGroup.Description = strGroupDesc


` Ορισμός του πεδίου σημειωμάτων χρησιμοποιώντας  την ιδιότητα info
adsGroup.Put "info", strGroupInfo


` Εφαρμογή των ιδιοτήτων στην εισαγωγή της ομάδας.
adsGroup.SetInfo


` απελευθέρωση αντικειμένων
Set adsGroup = Nothing
Set adsContainer = Nothing


` Τέλος
WScript.Echo "Group created successfully."
</script>
</job>
```

Απαρίθμηση 6-3: *To CreateGroup.wsf μας δείχνει πώς να δημιουργήσουμε μια ομάδα security-enabled με σφαιρικό πεδίο.*

Όταν τρέχετε το script CreateGroup, μια ομάδα που ονομάζεται τη "ομάδα παραδείγματος" δημιουργείται στο κοντεϊνερ χρηστών. Το σχήμα 6-2 παρουσιάζει το πλαίσιο διαλόγου ιδιοτήτων για τη νέα ομάδα στο Active Directory Users and Computers



Σχήμα 6.2 *Κείμενο διαλόγου ιδιοτήτων για την καινούργια ομάδα που δημιουργήθηκε με το CreateGroup script.*

6.19 Απαριθμώντας Ομάδες

Χρησιμοποιώντας την διεπαφή IADsGroup, μπορείτε να λάβετε τον κατάλογο μελών μιας ομάδας. Όταν καλείτε τη μέθοδο *Members* του IADsGroup, λαμβάνετε μια διεπαφή *IADs-Members*, η οποία εκθέτει τη συλλογή των μελών. Το IADsMembers είναι παρόμοιο και στη λειτουργία και στο σκοπό με το IADsContainer. Και οι δύο επιτρέπουν την απαρίθμηση χρησιμοποιώντας την δήλωση *For Each* σε Visual Basic και VBScript. Ο πίνακας 6-8 παρουσιάζει τις ιδιότητες του IADsMembers.

Ιδιότητες του *IADsMembers*	Τύπος Δεδομένων	Περιγραφή
Count	Long	Αριθμός μελών στη συλλογή.
Filter	Variant array of strings	Η σειρά ονομάτων κατηγορίας που χρησιμοποιείτε για να φιλτράρει την απαρίθμηση των μελών. Όπως τη μέθοδο *Filter* της διεπαφής IADsContainer.
get__NewEnum(Not exposed in Visual Basic)	Object	Δημιουργεί ένα νέο αντικείμενο απαριθμητή που υποστηρίζει τη διεπαφή IEnumVARIANT. Καλείται έμμεσα από την Visual Basic με τη χρησιμοποίηση της δήλωσης *For Each*. Επιστρέφει έναν δείκτη διεπαφής IUnknown. Σημειώστε ότι υπάρχουν δύο χαρακτήρες υπογράμμισης (_) στο όνομα.

Πίνακας 6.8: *Ιδιότητες της διεπαφής IADsMembers.*

Ο ακόλουθος κώδικας επεξηγεί πώς να απαριθμήσουμε τα μέλη μιας ομάδας.

```
` Λήψη της συλλογής των μελών
Set adsMembers = adsGroup.Members


` Απαρίθμηση κάθε μέλους
For Each adsMember In adsMembers


    ` Εμφάνιση του πλήρους ονόματος του μέλους
    WScript.Echo adsMember.Get("name")
Next
```

6.20 Τροποποιώντας την Ιδιότητα Μέλους της Ομάδας

Οι μεθόδοι *Add* και *Remove* του IADsGroup χρησιμοποιούνται για να τροποποιήσουν την ιδιότητα μέλους μιας ομάδας. Η απαρίθμηση 6-4 παρουσιάζει το script ModifyGroup, που δείχνει πώς να προσθέσετε, αφαιρέσετε, ελέγξτε, και να κατηγοριοποιήσετε τα μέλη σε μια ομάδα. Τα script ModifyGroup τρέχει σε command prompt και δέχεται ένα όνομα ομάδας, μια δράση (*add*, *del*, *test*, or *list*), και ένα όνομα χρήστη. Βασισμένο στην εισαγωγή, το script θα προσθέσει το χρήστη στην ομάδα, θα απομακρύνει τον χρήστη από την ομάδα, θα χρησιμοποιήσει τη μέθοδο IsMember για να επιβεβαιώσει την ιδιότητα μέλους, ή θα απαριθμήσει τα μέλη ομάδας. Εδώ είναι μερικά παραδείγματα της χρήσης του:

```
cscript modifygroup.wsf "coppersoftware\Example Group" /add "Joe A. Use
r"
cscript modifygroup.wsf "coppersoftware\Example Group" /test "Joe A. Us
er"
```

```
cscript modifygroup.wsf "coppersoftware\Example Group" /list
cscript modifygroup.wsf "coppersoftware\Example Group" /del "Joe A. Use
r"
```

Για να απαριθμήσετε τα μέλη της ομάδας, η μέθοδος *Members* καλείται να επιστρέψει μια συλλογή των μελών, που είναι απαριθμημένη χρησιμοποιώντας την δήλωση *For Each*.

```
<job id="ModifyGroup">
<reference guid="{97D25DB0-0363-11CF-ABC4-02608C9E7553}"/>
<script language="VBScript">
`
` Το ModifyGroup μπορεί να προσθέσει, αφαιρέσει, ελέγξει, και να
κατηγοριοποιήσει τα μέλη σε μια ομάδα

`
` Έλεγχος για το αν υπάρχει κάποιο όρισμα στην γραμμή εντολών.
Set wshArguments = WScript.Arguments


` Λήψη παραμέτρων βάσει του αριθμού των ορισμάτων
Select Case wshArguments.Count



Case 1
        strGroup = wshArguments(0)

    Case 2
        strGroup = wshArguments(0)
        strAction = wshArguments(1)

    Case 3
        strGroup = wshArguments(0)
        strAction = wshArguments(1)
        strUser = wshArguments(2)
End Select


` Έλεγχος για ομάδα χωρίς όνομα ή αιτήσεις βοηθείας.
If strGroup = "" Or InStr(1, strGroup, "?", vbTextCompare) > 0 Then


    ` Εμφάνιση χρήσης και έξοδος.
    strUsage = "Usage: modifygroup `groupname'"
    strUsage = strUsage & vbCrLf & "             [ /add  username ]"
    strUsage = strUsage & vbCrLf & "             [ /del  username ]"
    strUsage = strUsage & vbCrLf & "             [ /test username ]"
    strUsage = strUsage & vbCrLf & "             [ /list ]"
    `
    strUsage = strUsage & vbCrLf & _
        "Where username is either UPN (charles@coppersoftware.com) "
    strUsage = strUsage & vbCrLf & "or Domain (domainname\username)"
    WScript.Echo strUsage
    WScript.Quit (1)
```

```
End If


` Καθορισμός της ενέργειας που απαιτείται
` Λήψη των δύο πιο αριστερών χαρακτήρων της παραμέτρου και έλεγχος
για το αν ταιριάζουν στην λίστα ορισμών.
nAction = InStr(1, "/t/l/a/d", Left(strAction, 2), vbTextCompare)


` Χρήση του NameTranslate για την αναζήτηση της ομάδας στον κατάλογο.
Set adsNameTranslate = CreateObject("NameTranslate")


` Ορισμός του GC για γρήγορες αναζητήσεις
adsNameTranslate.Init ADS_NAME_INITTYPE_GC, vbNull


` Ορισμός του ονόματος της ομάδας στο NameTranslate
` Ορισμός άγνωστων τύπων για να έχουμε διευκρίνιση του αντικειμένου.
adsNameTranslate.Set ADS_NAME_TYPE_UNKNOWN, strGroup


` Λήψη του DN της ομάδας.
strGroupDN = adsNameTranslate.Get(ADS_NAME_TYPE_1779)

` Δέσμευση στο αντικείμενο ομάδας.
Set adsGroup = GetObject("LDAP://" & strGroupDN)


` Εάν ένας χρήστης έχει καθοριστεί λήψη των πληροφοριών του.
If strUser <> "" Then


    ` Ορισμός του ονόματος χρήστη στο NameTranslate
    adsNameTranslate.Set ADS_NAME_TYPE_UNKNOWN, strUser


    ` Λήψη του DN του χρήστη
    strUserDN = adsNameTranslate.Get(ADS_NAME_TYPE_1779)

    ` Δέσμευση στο αντικείμενο χρήστη.
    Set adsUser = GetObject("LDAP://" & strUserDN)
Else

    ` Εάν δεν έχει οριστεί κάποιος χρήστης, κάνε μόνο λίστα.
    nAction = 3
End If

` Εκτέλεσε μια ενέργεια
Select Case nAction

    Case 1
        ` Έλεγχος για μέλη.
        If adsGroup.IsMember(adsUser.ADsPath) Then

            ` Εμφάνιση εάν υπάρχουν μέλη
            WScript.Echo adsUser.FullName & " is a member of the " & _
```

```
                adsGroup.Get("name") & " group."
        Else

            ` Εμφάνιση εάν δεν υπάρχουν μέλη
            WScript.Echo adsUser.FullName & " is not a member of the "
& _
                adsGroup.Get("name") & " group."
        End If

    Case 5
        ` Πρόσθεσε ενέργεια
        WScript.Echo "Adding " & adsUser.FullName & " to group " & _
            adsGroup.Get("name")

        ` Πρόσθεσε τον χρήστη στην ομάδα
        adsGroup.Add adsUser.ADsPath

    Case 7
        ` Αφαίρεση ενέργειας, λήψη επιβεβαίωσης.
        strPrompt = strAction & adsUser.FullName & strVerb & _
            adsGroup.Get("name") & "?"


        If MsgBox(strPrompt, vbYesNo, "Modify Group") = vbYes Then

            WScript.Echo "Removing " & adsUser.FullName & _
                " from group " & adsGroup.Get("name")

            ` Απομάκρυνση του χρήστη από την ομάδα
            adsGroup.Remove adsUser.ADsPath
        End If

    Case Else
        ` Κάποια άλλη ενέργεια, λίστα μελών
        WScript.Echo "Listing all members in group " & adsGroup.Name

        ` Παράληψη στην επόμενη γραμμή στα λάθη
        On Error Resume Next

        ` Λήψη της περιγραφής
        strDescription = adsGroup.Description

        ` Εάν κάτι επιστρέψει, εμφάνισέ το
        If strDescription <> "" Then

            ` Δημιουργία συμβολοσειράς περιγραφής
            strDescription = "Description: " & strDescription
            WScript.Echo strDescription

        End If

        ` Εμφάνιση διαχωριστικών
        WScript.Echo String(Len(strDescription), "-")

        ` Λήψη της συλλογής των μελών.
        Set adsMembers = adsGroup.Members
```

```
        ` Απαρίθμηση κάθε μέλους.
        For Each adsMember In adsMembers

            ` Εμφάνιση του ονόματος του μέλους.
            WScript.Echo adsMember.Get("name")
        Next

        ` Ενεργοποίηση του ελέγχου λαθών.
        On Error GoTo 0
End Select


WScript.Echo "Finished."


</script>
</job>
```

Απαρίθμηση 6-4: *Το ModifyGroup.wsf εμφανίζει πώς να προσθέσουμε, αφαιρέσουμε, ελέγξουμε και πώς να κάνουμε μια λίστα των μελών της ομάδας.*

Εάν προσπαθείσετε να χρησιμοποιήσετε το script ModifyGroup ή οποιαδήποτε διεπαφή στο Active Directory για να απαριθμήσετε τα μέλη του Domain Users group, θα διαπιστώσετε ότι κανένας δεν παρατίθεται. Κάθε χρήστης που δημιουργείται στην domain είναι αυτόματα μέλος της ομάδας Domain Users, Η Microsoft συνειδητοποίησε ότι χιλιάδες τιμές θα μπορούσαν να γραφτούν στις ιδιότητες μελών της ομάδας. Αυτό θα προκαλούσε προβλήματα με την αντιγραφή και την απόδοση, οπότε Domain Users απλά δεν ασχολείται προσπαθώντας να κρατηθεί η ομάδα Domain Users ενημερωμένη. Εντούτοις, Domain Users διατηρεί μια ένωση μεταξύ της ομάδας χρηστών περιοχών και των μελών του μέσω των ιδιοτήτων primaryGroupID του αντικειμένου χρηστών. Όταν ένας νέος χρήστης δημιουργείται, σε αυτήν την ιδιότητα δίνεται το προσδιοριστικό ασφάλειας της ομάδας Domain Users.

6.21 Διαχειρίζοντας Υπολογιστές

Όπως τους χρήστες, οι υπολογιστές έχουν επίσης τους λογαριασμούς στο Active Directory. Στην πραγματικότητα, η κατηγορία *computer* κληρονομεί από την κατηγορία *user*. Οι λογαριασμοί υπολογιστών αντιμετωπίζονται όπως τους λογαριασμούς χρηστών για λόγους των αδειών ασφάλειας και πρόσβασης στο δίκτυο και στο domain. Ένας λογαριασμός υπολογιστή χρησιμοποιείται για να επικυρώσει έναν υπολογιστή στο δίκτυο χωριστά από έναν χρήστη προκειμένου να προσεγγιστούν οι κοινοί πόροι.

Ένα όνομα υπολογιστών μπορεί να είναι 15 χαρακτήρες ή λιγότεροι και ακολουθείται επίσης με ένα σήμα δολαρίου ($). Αυτό είναι μια παλαιά σύμβαση του LAN Manager για να χωρίσει τους λογαριασμούς μηχανών από τους λογαριασμούς χρηστών. Οι λογαριασμοί υπολογιστών μπορούν να τεθούν με κωδικούς πρόσβασης, αλλά οι κωδικοί πρόσβασης χρησιμοποιούνται μόνο έως ότου επικυρώνεται ο υπολογιστής από το domain και δημιουργηθεί ένα ασφαλές κανάλι. Αυτό είναι γνωστό

σαν ένωση ενός υπολογιστή σε ένα domain. Ένας νέος κωδικός πρόσβασης καθιερώνεται όταν ενωθεί ο υπολογιστής στο domain. Οι υπολογιστές τοποθετούνται γενικά στο κοντεϊνερ υπολογιστών, αν και οι διαχειριστές δικτύων μπορούν να τους τοποθετήσουν σε μια οργανωτική μονάδα.

Η απαρίθμηση 6-5 παρουσιάζει ένα script, που δημιουργεί έναν λογαριασμό υπολογιστών στο κοντεϊνερ υπολογιστών. Χρησιμοποίησα το γνωστό GUID για το κοντεϊνερ υπολογιστών. Αφού η πραγματική αξία του GUID για το κοντεϊνερ *Computers* δεν είναι στον τύπο βιβλιοθήκης ActiveDS.tlb, χρησιμοποίησα μια δήλωση Const για να κρατήσω την αξία του. Το ίδιο πράγμα ισχύει για τις σημαίες χρηστών (UF _ *) που πρέπει επίσης να καθοριστούν.

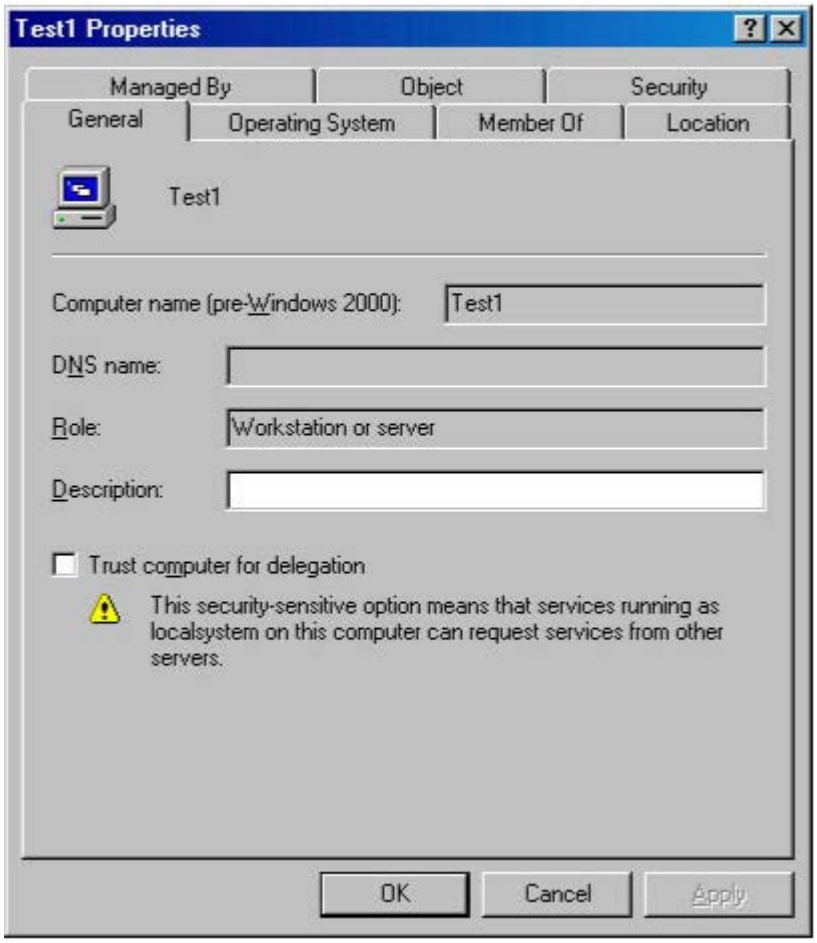
```
<job id="CreateComputer">
<reference guid="{97D25DB0-0363-11CF-ABC4-02608C9E7553}"/>
<script language="VBScript">
`
` CreateComputer – Δημιουργεί έναν λογαριασμό υπολογιστή
`
` Σταθερές από το Active Directory δεν συμπεριλαμβάνονται στον τύπο
βιβλιοθήκης
Const ADS_GUID_COMPUTRS_CONTAINER = "aa312825768811d1aded00c04fd8d5cd"
Const UF_WORKSTATION_TRUST_ACCOUNT = &H1000
Const UF_ACCOUNTDISABLE = &H2
Const UF_PASSWD_NOTREQD = &H20


` Όνομα υπολογιστή
strCompName = "Test1"


` Εμφάνιση πληροφοριών
WScript.Echo "Creating new computer account `" & strCompName & "`..."


` Δέσμευση στο RootDSE και λήψη των προκαθορισμένων χωρισμάτων του
domain
Set adsRootDSE = GetObject("LDAP://RootDSE")
strDomainDN = adsRootDSE.Get("defaultNamingContext")


` Χρήση του WKGUID για δέσμευση στο κοντεϊνερ των υπολογιστών
strGUIDPath = "LDAP://"
strGUIDPath = strGUIDPath & "<WKGUID="
strGUIDPath = strGUIDPath & ADS_GUID_COMPUTRS_CONTAINER
strGUIDPath = strGUIDPath & ","
strGUIDPath = strGUIDPath & strDomainDN
strGUIDPath = strGUIDPath & ">"


` δέσμευση στο κοντεϊνερ των υπολογιστών
Set adsContainer = GetObject(strGUIDPath)
```

```
` Η δέσμευση του UID είναι πολύ περιορισμένη, οπότε ξαναδέσμευσε χωρίς
την χρήση του GUID
strADsPath = "LDAP://" & adsContainer.Get("distinguishedName")
Set adsContainer = GetObject(strADsPath)


` Πήγαινε στην επόμενη γραμμή εάν γίνει ένα λάθος.
On Error Resume Next


` Δημιουργία ενός αντικειμένου στο κοντεϊνερ.
Set adsComputer = adsContainer.Create("computer", "cn=" + strCompName)



` Όρισε το ποσό των ονομάτων για τον υπολογιστή.
` Πρέπει να είναι 15 χαρακτήρες ή λιγότερο και να ακολουθείται από ένα
σήμα δολαρίου
adsComputer.Put "sAMAccountName", strCompName & "$"


` Πρέπει να οριστεί το userAccountControl πριν εφαρμοστούν οι αλλαγές
` εφόσον είναι read-only μετά την δημιουργία


` Ορισμός της σημαίας του λογαριασμού για να τον δηλώσει σαν λογαριασμό
υπολογιστή.
adsComputer.Put "userAccountControl", UF_WORKSTATION_TRUST_ACCOUNT Or _
    UF_ACCOUNTDISABLE Or UF_PASSWD_NOTREQD


` Ενημέρωση του server με τις απαιτούμενες ιδιότητες.
adsComputer.SetInfo


` Έλεγχος για λάθη
If Err.Number <> 0 Then
    ` Έλεγχος λάθους, το αν ήδη υπάρχει ο υπολογιστής
    If Err.Number = &H80071392 Then
        ` Εμφάνιση μηνυμάτων λαθών και έξοδος
        WScript.Echo "The computer `" & strCompName & "` already exists
."
        WScript.Quit 1
    Else
        WScript.Echo "Unexpected error creating computer." & _
            vbNewLine & Err.Description & " (" & Hex(Err.Number) & ")"
        WScript.Quit 1
    End If
End If


` Απενεργοποίηση του χειρισμού λαθών
On Error GoTo 0


` Ορισμός άλλων χαρακτηριστικών για τα αντικείμενα του υπολογιστή
` Ανανέωση της τοπικής εναποθήκευσης
```

```
adsComputer.GetInfo


` Ορισμός ενός προκαθορισμένου κωδικού πρόσβασης. Μόνο ο
χρησιμοποιούμενος υπολογιστής μπορεί να συνδεθεί στο domain.
` Πρέπει να είναι με μικρά γράμματα
strPassword = strCompName & "$"
strPassword = LCase(strPassword)
adsComputer.SetPassword strPassword


` Ενεργοποίηση του λογαριασμού
` Οι ιδιότητες IADsUser λειτουργούν σε λογαριασμούς υπολογιστών
adsComputer.AccountDisabled = False


` Εφαρμογή των ιδιοτήτων στον κατάλογο.
adsComputer.SetInfo



 ` Απελευθέρωση αντικειμένων
Set adsComputer = Nothing
Set adsContainer = Nothing


` Τέλος
WScript.Echo "Computer created successfully."


</script>
</job>
```

Απαρίθμηση 6-5 *Το CreateComputer.wsf δείχνει πώς να δημιουργήσετε έναν λογαριασμό για υπολογιστή.*

Όταν τρέχετε το script CreateComputer, ένας λογαριασμός υπολογιστών που ονομάζεται "Test1" δημιουργείται στο κοντεϊνερ υπολογιστών. Το σχήμα 6-3 παρουσιάζει ένα πλαίσιο διαλόγου ιδιοτήτων για το νέο λογαριασμό υπολογιστών στο Active Directory Users and Computers.



Σχήμα 6-3 *Ιδιότητες του πλαισίου διαλόγου για το νέο λογαριασμό υπολογιστή που δημιουργήθηκε με το CreateComputer script.*

6.22 Διαχειρίζοντας τις Υπηρεσίες

Το Active Directory χρησιμοποιεί την έννοια ενός σημείου σύνδεσης για να επιτρέψει στις υπηρεσίες να διαφημιστούν σε όλο το δίκτυο. Ένα σημείο σύνδεσης είναι ένα απλό αντικείμενο που αντιπροσωπεύει μια περίπτωση μιας ιδιαίτερης υπηρεσίας. Πολλά χαρακτηριστικά γνωρίσματα των Windows 2003 εκμεταλλεύονται τα σημεία σύνδεσης, συμπεριλαμβανομένης της ουράς εκτύπωσης, κοινόχρηστων φακέλων, Windows Sockets, και του Remote Procedure Call (RPC). Εδώ είναι λίγο περισσότερες οι λεπτομέρειες για τη διαχείριση των πιο κοινών υπηρεσιών, κοινή χρήση εκτυπωτών και αρχείων.

6.23 Διαχείριση της ουράς εκτύπωσης

Η απαρίθμηση 6-6 παρουσιάζει το script PrintOps, το όποιο είναι ένα πλήρες εργαλείο ελέγχου εκτυπωτών. Ο κώδικας είναι αυτεξήγητος, αλλά με αυτό μπορείτε να απαριθμήσετε όλες τις ουρές εκτύπωσης και τις εργασίες εκτυπωτή σε έναν Υπολογιστή, να σταματάτε προαιρετικά και να επαναλαμβάνετε την εκτύπωση. Μπορείτε επίσης να εξαλείψετε όλες τις εργασίες εκτύπωσης. Εδώ είναι μερικά παραδείγματα της χρήσης του.

```
cscript printops.wsf coppersoftware\copper1 /list
cscript printops.wsf coppersoftware\copper1 /pause
cscript printops.wsf coppersoftware\copper1 /resume
cscript printops.wsf coppersoftware\copper1 /flush
<job id="PrintOps">
<reference guid="{97D25DB0-0363-11CF-ABC4-02608C9E7553}"/>
<script language="VBScript">
`
` PrintOps
` List, pause, resume, and purge print queues
`
Set wshArguments = WScript.Arguments

` Λήψη παραμέτρων βασισμένο σε έναν αριθμό ορισμών

Select Case wshArguments.Count

    Case 1
        strComputer = wshArguments(0)

    Case 2
        strComputer = wshArguments(0)
        strAction = wshArguments(1)

End Select

` Έλεγχος για ομάδα χωρίς όνομα ή αιτήσεις βοηθείας

If strComputer = "" Or InStr(1, strGroup, "?", vbTextCompare) > 0 Then

    ` Εμφανιση χρήσης και τερματισμός

    strUsage = "Usage: PrintOps `domain\computername'"
    strUsage = strUsage & vbCrLf & "            [ /list   ]"
    strUsage = strUsage & vbCrLf & "            [ /flush  ]"
    strUsage = strUsage & vbCrLf & "            [ /pause  ]"
    strUsage = strUsage & vbCrLf & "            [ /resume ]"
    WScript.Echo strUsage
    WScript.Quit (1)
End If

If strAction = "" Then
    strAction = "/list"
```

```
End If


` Υπολογίστε τη δράση
` Λήψη των 2 τελευταίων αριστερών χαρακτήρων της παραμέτρου και
έλεγχος για το αν ταιριάζουν στην λίστα ορισμών

nAction = InStr(1, "/f/p/r/l", Left(strAction, 2), vbTextCompare)


` Χρησιμοποίηση του NameTranslate για αναζήτηση υπολογιστή στον
κατάλογο

Set adsNameTranslate = CreateObject("NameTranslate")


` Προσδιορισμος του GC για γρήγορες αναζητήσεις
adsNameTranslate.Init ADS_NAME_INITTYPE_GC, vbNull


` Ορισμός του ονόματος του υπολογιστή στο NameTranslate
` Ορισμός άγνωστων τύπων για να έχουμε διευκρίνιση αντικειμένων
` Προσθήκη ενός σήματος δολαρίου για να υποδεικνύει έναν λογαριασμό
υπολογιστή
adsNameTranslate.Set ADS_NAME_TYPE_UNKNOWN, strComputer & "$"


` Λήψη του DN του υπολογιστή
strComputerDN = adsNameTranslate.Get(ADS_NAME_TYPE_1779)


` Δέσμευση σε αντικείμενο υπολογιστή
Set adsComputer = GetObject("LDAP://" & strComputerDN)


` Απαρηθμιση των εκτυπώσεων ουράς σε αυτόν τον υπολογιστή
adsComputer.Filter = Array("PrintQueue")


WScript.Echo "Print queues on " & adsComputer.Get("name") & "..."


For Each varPrintQueue In adsComputer

    Set adsPrintQueue = GetObject(varPrintQueue.ADsPath)

    strQueue = adsPrintQueue.Get("Name")
    strQueue = strQueue & vbCrLf & "Model: " & vbTab & _
        adsPrintQueue.Model
    strQueue = strQueue & vbCrLf & "Description: " & vbTab & _
        adsPrintQueue.Description
    strQueue = strQueue & vbCrLf & "Location: " & vbTab & _
        adsPrintQueue.Location
    strQueue = strQueue & vbCrLf & "Path: " & vbTab & _
        adsPrintQueue.PrinterPath
    WScript.Echo strQueue
```

```
` Λήψη μιας διεπαφής στην σειρά αναμονής λειτουργιών
Set adsPrintQueueOps = adsPrintQueue

` Διεκπαιρέωση μιας εργασίας
Select Case nAction

    Case 1
        ` Flush printer queues
        WScript.Echo "Removing all print jobs from queue..."

        adsPrintQueueOps.Purge

    Case 3
        ` Pause the print queue
        WScript.Echo "Pausing print jobs..."

        adsPrintQueueOps.Pause

    Case 5
        ` Resume the print queue
        WScript.Echo "Resuming print jobs..."

        adsPrintQueueOps.Resume

    Case Else
        ` Some other action, list jobs in queue
        strAction = "Listing all jobs in queues " & adsComputer.Nam
e
        WScript.Echo strAction

        ` Display separator
        WScript.Echo String(Len(strAction), "-")

        ` Skip to the next line on errors
        On Error Resume Next


        For Each adsPrintJob In adsPrintQueueOps.PrintJobs

            strJob = "Job: " & adsPrintJob.Description
            strJob = strJob & vbCrLf & "User: " & adsPrintJob.User
            strJob = strJob & vbCrLf &  "Priority: " & _
                adsPrintJob.Priority
            strJob = strJob & vbCrLf &  "Pages: " & _
                adsPrintJob.TotalPages
            strJob = strJob & vbCrLf &  "Size: " & adsPrintJob.Size
            WScript.Echo strJob


        Next

        ` Turn error handling back on
        On Error GoTo 0
End Select

` Display Queue Status
```

```
    Select Case adsPrintQueueOps.status
        Case 0
            strStatus = "Normal"
        Case 1
            strStatus = "Paused "
        Case 2
            strStatus = "Error "
        Case 3
            strStatus = "Pending Deletion "
        Case 4
            strStatus = "Paper Jam "
        Case 5
            strStatus = "Paper Out "
        Case 6
            strStatus = "Manual Feed "
        Case 7
            strStatus = "Paper Problem "
        Case 8
            strStatus = "Offline "
        Case &H100
            strStatus = "I/O Active "
        Case &H200
            strStatus = "Busy "
        Case &H400
            strStatus = "Printing "
        Case &H800
            strStatus = "Output Bin Full "
        Case &H1000
            strStatus = "Not Available "
        Case &H2000
            strStatus = "Waiting "
        Case &H4000
            strStatus = "Processing "
        Case &H8000
            strStatus = "Initializing "
        Case &H1000
            strStatus = "Warming Up "
        Case &H2000
            strStatus = "Toner Low "

        Case &H4000
            strStatus = "No Toner "
        Case &H8000
            strStatus = "Page Punt"
        Case &H100000
            strStatus = "User Intervention Required"
        Case &H200000
            strStatus = "Out Of Memory "
        Case &H400000
            strStatus = "Door Open "
        Case &H800000
            strStatus = "Server Unknown "
        Case &H1000000
            strStatus = "Power Save "
        Case Else
            strStatus = "Unknown status (" & adsPrintQueueOps.status &
")"
```

```
    End Select

WScript.Echo "Status: " & strStatus


Next

WScript.Echo "Finished."


</script>
</job>
```

Απαρίθμηση 6-6 *Το PrintOps.wsf επιδεικνύει πώς να απαριθμήσετε, διακοψετε, επαναλάβετε, και απαλάξετε εργασίες απο τις σειρές αναμονής εκτύπωσης.*

6.24 Όγκοι (Volumes)

Ένα χαρακτηριστικό γνώρισμα του Active Directory που δεν τραβάει την προσοχή που του αξίζει είναι τα αντικείμενα όγκου. Αυτά τα αντικείμενα αντιπροσωπεύουν τους κοινούς φακέλλους. Παραδείγματος χάριν, μπορείτε να πείτε σε κάποιον να έχετε πρόσβαση σε έναν κοινό φάκελλο σε έναν συγκεκριμένο υπολογιστή χρησιμοποιώντας ένα όνομα UNC όπως \\server1\applications. Αυτή η διαδρομή λειτουργεί υπέροχα μέχρι ο \\server1 να τεθεί εκτός λειτουργίας και να αντικατασταθεί με τον \\server2. Οι χρήστες θα μπορούν να περιηγηθούν και να ψάξουν το δίκτυο για κοινούς φακέλλους, αλλά αυτό θα μπορούσε να γίνει απίστευτα κουραστικό σε έναν μεγάλο οργανισμό με δεδάδες, ή ακόμα και εκατοντάδες υπολογιστές.

Ακριβώς όπως με τους εκτυπωτές, το Active Directory επιτρέπει την έκδοση των κοινών φακέλλων. Αντίθετα από τους εκτυπωτές, εντούτοις, ένας κοινός φάκελλος δεν περιλαμβάνεται σε μια ιεραρχία αντικειμένου υπολογιστών. Οι κοινοί φάκελλοι αντιπροσωπεύονται στο Active Directory με τα αντικείμενα της κατηγορίας όγκου. Τα αντικείμενα της κατηγορίας όγκου είναι πολύ απλά, περιέχοντας ακριβώς έξι ιδιότητες πέρα από εκείνες που διευκρινίζονται από την κορυφαία κατηγορία. Τρεις από τις ιδιότητες κληρονομούνται από την κατηγορία connectionPoint, και τρία διευκρινίζονται από την κατηγορία *volume*. Ο πίνακας 6-9 απαριθμεί αυτές τις ιδιότητες.

Χαρακτηριστικά του *Volume*	**Source Class**	**Περιγραφή**
cn	*connectionPoint*	Υποχρεωτικό κοινό όνομα single-valued
keywords	*connectionPoint*	Πολυτιμικές συμβολοσειρές που δείχνουν τις λέξεις κλειδιά που συνδέονται με αυτόν τον όγκο.
managedBy	*connectionPoint*	Μια συμβολοσειρά DN που δείχνει το χρήστη που διαχειρίζεται αυτόν τον όγκο.

contentIndexing-Allowed	*volume*	Τιμή Boolean που υποδυκνύει εαν το περιεχόμενο συντάσεται σε αυτόν τον όγκο.
lastContentIndexed	*volume*	Χρονοσφραγίδα για όταν το περιεχόμενο του όγκου τελευταία συντάχθηκε
uNCName	*volume*	Υποχρεωρική συμβολοσειρά που συμπεριλαμβάνει την διαδρομή UNC του όγκου, για παραδειγμά: \\servername\foldername

Πίνακας 6.9: *Χαρακτηριστικά του όγκου class.*

6.25 Δημοσιεύοντας και Χρησιμοποιώντας Κοινόχρηστους Φακέλους

Αντίθετα από τους εκτυπωτές, δεν υπάρχει καμία παροχή να δημοσιευθεί αυτόματα ένας κοινός φάκελλος στο Active Directory. Τα αντικείμενα *volume* αντιπροσωπεύοντας κοινούς φακέλους μπορούν να δημιουργηθούν μόνο στη ρίζα περιοχών ή μέσα σε μια οργανωτική μονάδα. Αυτό έχει νόημα επειδή οι διαχειριστές μπορούν να ομαδοποιήσουν όλους τους απαραίτητους πόρους για ένα τμήμα σε μια ενιαία οργανωτική μονάδα. Η χρησιμοποίηση της επιλογής ευρημάτων στο φάκελλο καταλόγου του My Network Places, οι χρήστες μπορούν να ρωτήσουν για διαθέσιμους κοινούς φακέλλους. Οι χρήστες μπορούν επίσης να περιήγηθούν στο Directory namespace ψάχνοντας για κοινούς φακέλλους, που είναι πολύ γρηγορότερο από την ανίχνευση καταλόγων κεντρικών υπολογιστών. Μόλις βρεθεί ένας κοινός φάκελλος μπορείτε να ανοίξετε ένα παράθυρο ή να αντιστοιχίσετε ένα γράμμα οδηγού στον φάκελλο. Μπορείτε να αντιστοιχίσετε ένα γράμμα οδηγού σε έναν κοινό φάκελλο προγραμματιστικά με τη χρησιμοποίηση του αντικειμένου WshNetwork που παρέχεται από το Windows Script.

6.26 Windows Management Instrumentation (WMI)

Αν και το ADSI σχεδιάστηκε για τη διαχείριση καταλόγου, περιλαμβάνει επίσης διάφορα διαχειριστικά χαρακτηριστικά γνωρίσματα δικτύων. Η διαχείριση δικτύων ενδιαφέρει συνήθως την απαρίθμηση των συσκευών που συνδέονται με το δίκτυο και τη διαχείρηση εκείνων των συσκευών. Για να βοηθήσει τη διαχείριση δικτύων, Η Microsoft εστιάζει σε μια τεχνολογία, παρόμοια στην αρχιτεκτονική ADSI, αποκαλούμενη *Windows Management Instrumentation* (WMI).

Το WMI είναι μια εφαρμογή της Microsoft της Web-Based Enterprise Management (WBEM) πρωτοβουλία του Distributed Management Task Force (DMTF), ένας συνασπισμός βιομηχανίας που διαμορφώθηκε για να παρέχει τα πρότυπα και τις συστάσεις βιομηχανίας για να μειώσει τις επιχειρήματικές δαπάνες διαχείρησης. Αυτός σημαίνει για τους προγραμματιστές ότι είναι ένα πρότυπο αντικειμένου που επιτρέπει

την ευκολότερη διαχείριση των πόρων δικτύων. Ενώ στοχεύει πρώτιστα στους διαχειριστές δικτύων, το WMI είναι χρήσιμο σε όλους τους προγραμματιστές των καταλογών-ενήμερων προϊόντων.

Με το WMI, μπορείτε να έχετε πρόσβαση και να χειριστείτε όχι μόνο τις πληροφορίες συσκευών δικτύων για τους κεντρικούς υπολογιστές αλλά και τους μεμονωμένους τερματικούς σταθμούς. Με το μοντέλο αντικειμένου, μπορείτε να έχετε πρόσβαση στις πληροφορίες για τους σκληρούς δίσκους ενός υπολογιστή, να πάρετε τις πληροφορίες για τους τύπους αρχείων, ελεύθερο χώρο, και πληροφορίες για την ασφάλεια, παραδείγματος χάριν. Ρυθμίζοντας την ασφάλεια στα αντικείμενα υπολογιστών και δικτύων προγραμματιστικά γίνεται πολύ ευκολότερη. Για παράδειγμα, οι διαχειριστές δικτύων μπορούν να χρησιμοποιήσουν το WMI για να απαριθμήσουν όλους τους υπολογιστές στην επιχείρηση που έχει έναν ιδιαίτερο οδηγό video που χρειάζεται ενημέρωση.

6.27 Αντιστοίχηση Γραμμάτων Οδηγων σε Κοινόχρηστούς Φακέλους

Η απαρίθμηση 6-7 παρουσιάζει ένα script, που απαριθμεί τους κοινόχρηστους φακέλους που δημοσιεύονται στο Active Directory και τους αντιστοιχεί σε γράμματα οδηγών Το δείγμα δεν είναι ιδιότροπο αντιστοιχεί όλους τους κοινόχρηστους φακέλους που μπορεί να βρει στη ρίζα του καταλόγου. Το script χρησιμοποιεί τις ιδιότητες του uNCName από *volume αντικείμενο* για να ανακαλύψει το όνομα της διαδρομής UNC του κοινόχρηστου φακέλου. Το αντικείμενο WshNetwork χρησιμοποιεί αυτό το όνομα διαδρομής για να εκτελέσει τη λειτουργία αντιστοίχησης μεταξύ ενός γράμματος οδηγού και του φακέλου.

```
<job id="MapSharedFolders">
<reference guid="{97D25DB0-0363-11CF-ABC4-02608C9E7553}"/>
<script language="VBScript">

' MapSharedFolders – Απαριθμεί όλα τα αντικείμενα όγκου στην ρίζα του '
καταλόγου και διασύνδεση αυτών σε γράμματα οδηγών


' Δημιουργία του αντικειμένου WSH Network που θα εκτελέσει την
αντιστοίχηση
Set objWshNetwork = WScript.CreateObject("WScript.Network")


` Σύνδεση στη ρίζα του αντικειμένου LDAP
Set objADsRootDSE = GetObject("LDAP://RootDSE")


 ` Διαμόρφωση μιας συμβολοσειράς ADsPath στο προεπιλεγμένο όνομα του
domain
strPath = "LDAP://" + objADsRootDSE.Get("defaultNamingContext")


` Σύνδεση στον κατάλογο που προσδιορίζεται στην διαδρομή
Set objADsContainer = GetObject(strPath)
```

```
` Μόνο απαριθμιμένοι κοινόχρηστοι κατάλογοι
objADsContainer.Filter = Array("volume")


` Για λογους απόδοσης, λήψη μόνο των uNCName ιδιοτήτων
objADsContainer.Hints = Array("uNCName")


` Εμφάνιση του χρησιμοποιούμενου ADsPath
WScript.Echo "Enumerating all shared folders in " & objADsContainer.Nam
e


` Αρίθμηση δια μέσου όλων των υπάρχοντων οδηγών για εύρεση του
` τελευταίου γράμματος οδηγού
Set objFileSystem = CreateObject("Scripting.FileSystemObject")


For Each objDrive in objFileSystem.Drives
    strLastDriveLetter = objDrive.DriveLetter
Next


` Βρόχος μέσω κάθε αντικειμένου στο κοντέινερ
For Each objADs In objADsContainer
    ` Λήψη της UNC διαδρομής και καταχώρηση της
    strSharePath = objADs.Get("uNCName")


    ` Εμφάνιση του ονόματος του αντικειμένου και της διαδρομής
    WScript.Echo objADs.Name & vbTab & strSharePath


    ` Προσαύξηση του γράμματος του οδηγού
    ` BUGBUG:  Θα αποτύχει μετά το Z!
    strLastDriveLetter = chr( 1 + Asc(strLastDriveLetter) )


    ` Επισύναψη ενώς συμβόλου (:) στο ονομα του οδηγού
    strDriveLetter = strLastDriveLetter & ":"


    ` Αντιστοίχηση του κοινόχρηστου σε ένα γράμμα οδηγού
    objWshNetwork.MapNetworkDrive strDriveLetter, strSharePath
Next


` Εμφάνιση όλων των τωρινών αντιστοιχισμένων δικτυακών οδηγών
WScript.Echo "Current network drive mappings:"


` Αρίθμηση οδηγών (0 είναι γράμμα, 0+1 είναι UNC διαδρομή)
Set objWshNetworkDrives = objWshNetwork.EnumNetworkDrives


For numDrive = 0 to objWshNetworkDrives.Count - 1 Step 2
```

```
` Εμφάνιση του γράμματος οδηγού και της διαδρομής
    WScript.Echo objWshNetworkDrives.Item(numDrive) & vbTab & _
        objWshNetworkDrives.Item(numDrive + 1)
Next


` Τέλος
WScript.Echo "Finished."
</script>
</job>
```

Απαρίθμηση 6-7 *Το MapSharedFolder.wsf επιδεικνύει πώς να απαριθμήσετε τους κοινούς φακέλους και να τους συνδέσετε με το γράμμα του οδηγού*

Η εντολή Net Use επιτρέπει σε σας να συνδέσετε έναν κοινό φάκελο στο επόμενο διαθέσιμο γράμμα οδηγού χρησιμοποιώντας τον αστερίσκο (*). Στο script MapSharedFolder, εντούτοις, πρέπει να παρέχετε ένα γράμμα οδηγού και ενα χαρακτήρα σύμβολο άνω και κάτω τελειών (Π.χ., Z:) κατά τον κλήση της μεθόδου MapNetworkDrive.

Βιβλιογραφία

1. Microsoft Windows 2000 Active Directpry Programming, Charles Opperman
2. Active Directory Cookbook for Windows 2003 & Windows 2000, O'Reilly
3. Active Directory for Microsoft Windows 2003, Technical Reference, Mike Mulcare, Stan Reimer, Microsoft
4. Windows 2000 Active Directory Survival Guide Planning and Implementation, Richard Schwartz, Wiley Computer Publishing
5. Tips and Tricks Guide to Windows 2000 and Active Directory Administration, Don Jones, Sean Daily, Aelita Software
6. Inside Windows Server 2003, William Boswell, Addison Wesley
7. The Ultimate Windows Server 2003 System Administrator's Guide, Robert Williams, Mark Walla, Addison Wesley
8. Windows .NET Server 2003 Domains & Active Directory, Aleksey Tchekmarev, A-LIST Publishing
9. Active Directory Bible Curt Simmons
10. MCSE Training Kit—Microsoft Windows 2000 Active Directory Services
11. Active Directory, 2nd Edition, Robbie Allen, Alistair G. Lowe-Norris, O'Reilly
12. Windows .NET Server 2003 Domains & Active Directory, Aleksey Tchekmarev, A-LIST Publishing
13. Windows 2000 Active Directory Second Edition, Melissa C. Craft, Thomas Llewellyn, Syngress