ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΤΜΗΜΑ: ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Χαρακτηριστικά και συγκριτική παρουσίαση των λειτουργικών συστημάτων για διακομιστές

Μπίνας Γεώργιος Α.Μ.: 711130001

Ηρακλής Τσαμαντιώτης Α.Μ.: 711130004

Επιβλέπων Καθηγητής: Κωνσταντίνος Ευσταθίου

ΑΘΗΝΑ 2021

Εξεταστική Επιτροπή:

Ευσταθίου Κωνσταντίνος: Καθηγητής Πανεπιστημίου Δυτικής Αττικής

Ioannis Voyiatzis Digitally signed by Ioannis Voyiatzis
Date: 2021.03.30 10:27:09 +03'00'

Βογιατζής Ιωάννης: Καθηγητής Πανεπιστημίου Δυτικής Αττικής

Αμοργινός Ιωάννης: Λέκτορας Εφαρμογών Πανεπιστημίου Δυτικής Αττικής

Δήλωση Συγγραφέων Διπλωματικής Εργασίας

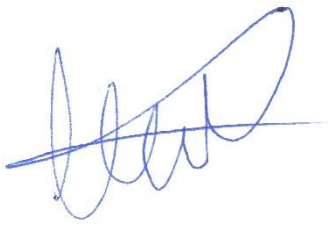
Ο κάτωθι υπογεγραμμένος Μπίνας Γεώργιος του Ιωάννη, με αριθμό μητρώου 711130001, φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών,

ο κάτωθι υπογεγραμμένος Τσαμαντιώτης Ηρακλής του Ευαγγέλου, με αριθμό μητρώου 711130004, φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών,

δηλώνουμε υπεύθυνα ότι:

«Είμαστε συγγραφείς αυτής της πτυχιακής/διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχαμε για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες κάναμε χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνουμε ότι αυτή η εργασία έχει συγγραφεί από εμάς αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μας, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μας ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση των πτυχίων μας».



Μπίνας Γεώργιος **Τσαμαντιώτης Ηρακλής**

Περιεχόμενα

Λέξεις κλειδιά

Παρακάτω παρατίθενται οι λέξεις κλειδιά της διπλωματικής μας εργασίας με στόχο την ηλεκτρονική βιβλιογραφική αρχειοθέτησή της.

- Κατηγορίες Server
- Workstation
- Servers
- Mainframes
- Super Computers
- CISC
- RISC
- NISC
- Αρχιτεκτονικές Κύριας Μνήμης
- UMA – NUMA – QPI – SUMA
- Pipeline
- Scalar
- Superscalar
- Xeon CPU
- ARM Αρχιτεκτονική
- Κατηγορίες Λειτουργικών Συστημάτων
- Λειτουργικά Συστήματα Windows Server
- Windows Server 2008
- Windows Server 2008 Domain Name System
- Windows Server 2008 Active Directory Components
- Windows Server 2008 Security
- Windows Server 2008 IIS Web Server
- Windows Server 2008 DHCP
- Windows Server 2008 Fault Tolerance Technologies
- Windows Server 2008 Hyper-V
- Windows Server 2008 File Server
- Windows Server 2008 e-mail and Microsoft Exchange
- Windows Server 2008 Print Server

Ευχαριστίες

Με την περάτωση της παρούσης διπλωματικής εργασίας θα θέλαμε να ευχαριστήσουμε θερμά τον κ. Ευσταθίου Κωνσταντίνο, Καθηγητή του Πανεπιστημίου Δυτικής Αττικής του Τμήματος Μηχανικών Πληροφορικής, για την αμέριστη βοήθεια και καθοδήγησή του στην εκπόνηση αυτής της διπλωματικής εργασίας καθώς επίσης και όλα τα μέλη του Πανεπιστημίου Δυτικής Αττικής για τις γνώσεις και την βοήθεια που μας προσφέρανε κατά την διάρκεια των προπτυχιακών μας σπουδών.
Τέλος, δεν μπορούμε να παραλείψουμε να ευχαριστήσουμε την οικογένειά μας για την ηθική συμπαράσταση και στήριξή τους.

Εισαγωγή

Η βιομηχανία διακομιστών υπολογιστών βρίσκεται στο στάδιο μιας μεγάλης αλλαγής που διεγείρεται από αυξανόμενη ζήτηση για αποθήκευση και επεξεργασία δεδομένων ως αποτέλεσμα της εξέλιξης της τεχνολογίας και της ανάγκης που υπάρχει την σημερινή εποχή, καθώς όλος ο κύκλος της οικονομίας, της διαχείρισης οργανισμών, της λειτουργίας αμέτρητων ηλεκτρονικών συσκευών που επικοινωνούν μεταξύ τους και παρέχουν υπηρεσίες και δυνατότητες στους χρήστες τους, έχουν ανάγκη τόσο από εξωτερικούς αποθηκευτικούς χώρους όσο και από κόμβους οι οποίοι τους επιτρέπουν να επικοινωνούν με άλλα συστήματα.

Αν και πολλοί οργανισμοί σήμερα στρέφονται σε λύσεις cloud για την κάλυψη των αναγκών τους, εντούτοις υπάρχουν αρκετές περιπτώσεις στις οποίες αυτό δεν είναι είτε εφικτό, λόγω του μεγάλου κόστους, είτε δεν προτιμάτε λόγω του ότι ο οργανισμός πιθανών να διατηρεί πολύ εμπιστευτικά δεδομένα για τα οποία θέλει να έχει τον πλήρη έλεγχο και να μην βρίσκονται αυτά στους διακομιστές κάποιου τρίτου παρόχου. Ως αποτέλεσμα των παραπάνω περιορισμών οι οργανισμοί αυτοί θα πρέπει να δημιουργήσουν ένα ιδιωτικό δίκτυο το οποίο θα είναι σε θέση να καλύψει τις ανάγκες τους τόσο μεσοπρόθεσμα όσο και μακροπρόθεσμα, και το οποίο θα έχει την δυνατότητα για ενδεχόμενη μελλοντική αναβάθμιση ανάλογα τις εξελισσόμενες ανάγκες του οργανισμού στην πάροδο του χρόνου.

Ως εκ τούτου η παρούσα διπλωματική εργασία έχει ως στόχο να κάνει μια αναλυτική παρουσίαση στις τεχνολογίες υλικού των διακομιστών και στα λειτουργικά συστήματα για διακομιστές με σκοπό να ενημερώσει, να βοηθήσει και να δώσει κατευθυντήριες γραμμές στους αναγνώστες ώστε να βρίσκονται σε θέση να επιλέξουν τα βέλτιστα προϊόντα για την κατασκευή και παραμετροποίηση ενός εταιρικού δικτύου, ανάλογα με τις ανάγκες του οργανισμού τους, τόσο σε επίπεδο υλικού όσο και λογισμικού.

Καθώς η παρούσα διπλωματική εργασία παρέχει μία αρκετά εκτενή ανάλυση τόσο στην ιστορική εξέλιξη, του υλικού και των λειτουργικών συστημάτων για διακομιστές, όσο και στις αρχιτεκτονικές και στις τεχνολογίες υλικού, μπορεί να χρησιμοποιηθεί και σε ακαδημαϊκό κοινό δίνοντας πληροφορίες και γνώσεις για τις βασικές αρχές της επιστήμης των υπολογιστών, την λειτουργία, τις ανάγκες και την διαχείριση των διακομιστών καθώς τις τάσεις, τις εξελίξεις και τις δυνατότητες της τεχνολογίας σήμερα.

Περίληψη

Στο χώρο των διακομιστών υπολογιστών λόγω της ραγδαίας εξέλιξης του Διαδικτύου, της έλευσης των Big Data, των Cloud Υπηρεσιών, του Internet of Things και πολλών άλλων νέων υπηρεσιών, είναι σε εξέλιξη ο εκσυγχρονισμός και η ανανέωση του συνόλου του υλικολογισμικού εξοπλισμού όλων των οργανισμών, μικρών και μεγάλων. Η αλλαγή αυτή οφείλεται στην αυξανόμενη ζήτηση για αποθήκευση και επεξεργασία δεδομένων καθώς και παροχής ακόμα πιο αξιόπιστων υπηρεσιών.

Λαμβάνοντας υπόψη τα παραπάνω, η παρούσα διπλωματική εργασία αποτελεί μια έρευνα γύρω από τις τεχνολογίες που υλοποιούνται στο χώρο μεγάλων οργανισμών και επιχειρήσεων, τόσο σε επίπεδο αρχιτεκτονικών υλικού των διακομιστών όσο και στο επίπεδο λειτουργικών συστημάτων που χρησιμοποιούνται ευρέως. Ειδικότερα, στα πλαίσια της παρούσας διπλωματικής εργασίας μελετώνται και αναλύονται οι κατηγορίες των σημερινών server με βάση τον σκοπό χρήσης τους καθώς και οι διαφορές τους ως προς το μέγεθος του όγκου των δεδομένων που μπορούν να υποστηρίξουν. Στην συνέχεια πραγματοποιείται μια εκτενής ανάλυση στις αρχιτεκτονικές υλικού των Server, όπως αρχιτεκτονικές CPU, αρχιτεκτονικές Motherboard, αρχιτεκτονικές NUMA και άλλα γύρω από τις αρχιτεκτονικές υλικού. Γίνεται μια αναφορά στην πολλά υποσχόμενη τεχνολογία των ARM CPU καθώς και Server που έχουν υλοποιηθεί σε ARM αρχιτεκτονική. Πραγματοποιείται μια ιστορική εξέλιξη των λειτουργικών συστημάτων για Server, εκδόσεις ανοιχτού λογισμικού, Linux, καθώς και εκδόσεις της Microsoft. Πραγματοποιείται μια σύγκριση μεταξύ τους και αναλύονται τα υπέρ και τα κατά. Τέλος, πραγματοποιείται μια εκτενής ανάλυση στο Λειτουργικό Σύστημα Windows Server 2008 με τις σημαντικότερες υπηρεσίες του, όπως Domain Name System (DNS), Active Directory (AD), Ασφάλεια, IIS Web Servers, Υπηρεσία DHCP, Τεχνολογίες ανοχής σφαλμάτων, HYPER-V, File Server, η υπηρεσία e-mail - Microsoft Exchange και η υπηρεσία Print Server. Για όλες τις παραπάνω υπηρεσίες πραγματοποιήθηκε λεπτομερής περιγραφή από την αρχική εγκατάσταση των Windows Server 2008 σε πραγματικό μηχάνημα μέχρι και όλες τις υπηρεσίες που περιγράφονται αναλυτικότερα με φωτογραφικό υλικό όλων των βημάτων κατά την διάρκεια εγκατάστασής τους ώστε να βοηθούν τον αναγνώστη στην καλύτερη κατανόηση των όσων παρουσιάζονται λεκτικά.

Η μεθοδολογία που χρησιμοποιήθηκε για τη συγγραφή της παρούσας διπλωματικής εργασίας περιελάμβανε εκτενή έρευνα τόσο σε ξενόγλωσσα βιβλία και άρθρα τα οποία παραθέτουν τα Windows Server 2008 όσο και σε πηγές του διαδικτύου.

Summary

In the field of computer servers, due to the rapid development of the Internet, the advent of Big Data, Cloud Services, Internet of Things and many other new services, the modernization and renewal of all the firmware of all organizations is in progress, both small and large. This change is due to the growing demand for data storage and processing as well as the provision of even more reliable services. In view of the above, this dissertation is a research on the technologies implemented in large organizations and companies, both at the level of server hardware architecture and at the level of widely used operating systems. In particular, in the context of this dissertation, the categories of current servers are studied and analyzed based on the purpose of their use and their differences in the size of the volume of data they can support. An extensive analysis is then performed on Server hardware architectures, such as CPU architectures, Motherboard architectures, NUMA architectures, and more around hardware architectures. A reference is made to the promising technology of ARM CPUs and Servers that have been implemented in ARM architecture. There is a historical evolution of operating systems for Server, Linux and Unix versions of open source software as well as versions of Microsoft. A comparison is made between them and the pros and cons are analyzed. Finally, an extensive analysis is performed on the Windows Server 2008 Operating System with its most important services, such as Domain Name System (DNS), Active Directory (AD), Security, IIS Web Servers, DHCP Service, Troubleshooting Technologies, HYPER-V, File Server, the e-mail service- Microsoft Exchange and Print Server. A detailed description of all the above services was provided from the initial installation of Windows Server 2008 on a real machine to all the services described in more detail with photographs of all the steps during their installation to help the reader better understand what is presented verbally.

The methodology used to write this dissertation included extensive research into both foreign language books and articles cited by Windows Server 2008 as well as Internet resources.

1. Εισαγωγή και Ιστορική Αναδρομή

Η ανάγκη για υπολογιστές ή υπολογιστικές συσκευές, οι οποίες αρχικά προορίζονταν μόνο για καταμέτρηση, υπήρχε από την αρχαιότητα για την ανθρωπότητα.

Μία από τις παλαιότερες μηχανές που χρησιμοποιούνταν για υπολογισμούς ήταν ο άβακας, που εφευρέθηκε στον αρχαίο πολιτισμό της Μεσοποταμίας πριν από περίπου 5000 χρόνια. Αργότερα διαδόθηκε σε άλλους πολιτισμούς, όπως τους Αιγύπτιους, τους Πέρσες, τους Κινέζους κτλ. Ορισμένες παραλλαγές του άβακα εξακολουθούν να χρησιμοποιούνται σε διάφορες απομακρυσμένες τοποθεσίες σε όλο τον κόσμο. Η συσκευή προοριζόταν για να αντιπροσωπεύει αριθμούς (ποσότητες) και να βοηθήσει σε απλές αριθμητικές πράξεις όπως προσθέσεις και αφαιρέσεις. Ωστόσο, είναι πολύ δύσκολο να χρησιμοποιηθεί για πιο περίπλοκους υπολογισμούς.

Στην πορεία των αιώνων δημιουργήθηκαν και άλλες υπολογιστικές συσκευές. Μία από αυτές είναι το Napier Bones, μια μικρή και εξελιγμένη συσκευή που προορίζεται για περίπλοκους υπολογισμούς όπως πολλαπλασιασμούς και διαιρέσεις. Εφευρέθηκε στις αρχές του 17ου αιώνα από τον John Napier, έναν σκωτσέζικο μαθηματικό.

Ο αγώνας για την εύρεση μιας συσκευής που θα απλοποιούσε τους μαθηματικούς υπολογισμούς συνεχίστηκε και έτσι ένας Γάλλος μαθηματικός, ο Blaise Pascal, δημιούργησε ένας μηχανικό υπολογιστή που χρησιμοποιούσε ένα σύνολο διασυνδεδεμένων τροχών, μια έννοια παρόμοια με τους μηχανισμούς των μηχανικών ρολογιών.

Ωστόσο, πολλοί θεωρούν τον Charles Babbage ως τον πραγματικό «πατέρα του υπολογιστή». Ο Babbage ήταν ένας Άγγλος μαθηματικός που εφηύρε μια συσκευή που θεωρείται ο πρώτος μηχανικός υπολογιστής. Αν και δεν υλοποιήθηκε, άνοιξε το δρόμο για άλλες νεότερες ιδέες. Δεδομένου ότι οι προσθέσεις και οι αφαιρέσεις μπορούν να υλοποιηθούν σχετικά εύκολα χρησιμοποιώντας μηχανικό τροχό, ο Babbage, όπως και οι προκάτοχοί του, έψαχνε τρόπους αντικατάστασης των σύνθετων μαθηματικών υπολογισμών, όπως πολυωνυμικές συναρτήσεις από ένα σύνολο με απλές λειτουργίες χρησιμοποιώντας μόνο προσθέσεις και αφαιρέσεις. Η συσκευή ονομάστηκε μηχανή διαφοράς, αφού ξεπέρασε την ανάγκη για πολλαπλασιασμούς και διαιρέσεις με μια μέθοδο πεπερασμένων διαφορών.

Αν και ο Babbage σχεδίασε την μηχανή διαφοράς, δεν την υλοποίησε ποτέ. Ο γιος του Χένρι συνέχισε το έργο του και δημιούργησε μια συσκευή χρησιμοποιώντας εξαρτήματα που βρέθηκαν στο εργαστήριο του πατέρα του. Ωστόσο, χρειάστηκαν επιπλέον 150 χρόνια για να ολοκληρωθεί πλήρως η συσκευή χρησιμοποιώντας καλύτερες τεχνολογίες παραγωγής και καλύτερα υλικά.

Κατασκευάστηκαν πολλές συσκευές, όλες βασισμένες στα πρωτότυπα σχέδια του Babbage. Ο ίδιος ο Babbage συνειδητοποίησε ότι η «πραγματική» λύση για μια υπολογιστική συσκευή δεν μπορεί να εφαρμοστεί χρησιμοποιώντας την μηχανή διαφορών, οπότε εγκατέλειψε αυτήν την ιδέα και άρχισε να εργάζεται σε μία αναλυτική μηχανή.

Αν και η ιδέα της αναλυτικής μηχανής δεν προχώρησε πέρα από τον πίνακα σχεδίασης, οι αρχές που εκφράζονται (μονάδα επεξεργασίας, μονάδα ελέγχου, μνήμη, συσκευές εισόδου και εξόδου) είναι οι ακρογωνιαίοι λίθοι των σύγχρονων υπολογιστών.

Ο Herman Hollerith, ο οποίος στα τέλη του δέκατου ένατου αιώνα εφηύρε μια μηχανή διαλογής με βάση διάτρητες κάρτες, θεωρείται από πολλούς ως «πατέρας» των

σύγχρονων υπολογιστών. Όπως συμβαίνει συχνά στην ιστορία οι τεχνολογικές εξελίξεις προκύπτουν από την ανάγκη της επίλυσης ενός προβλήματος.

Κατά το δεύτερο μισό του δέκατου ένατου αιώνα, μεγάλα κύματα μεταναστών κινήθηκαν προς τις Ηνωμένες Πολιτείες ελπίζοντας για μία καλύτερη ζωή. Για τον πληθυσμό αυτό και λαμβάνοντας υπόψη ότι το σύνταγμα των ΗΠΑ απαιτεί απογραφή κάθε δέκα χρόνια, η διαθέσιμη τεχνολογία για την εποχή εκείνη δεν επαρκούσε και η απογραφή θα χρειαζόταν πολύ μεγάλο χρονικό διάστημα λαμβάνοντας υπόψιν όλα τα στοιχεία που έπρεπε να καταγραφούν. Χαρακτηριστικά η απογραφή του 1880 χρειάστηκε 10 χρόνια για να ολοκληρωθεί.

Έτσι το γραφείο απογραφής εξέδωσε Αίτηση Υποβολής Προτάσεων για να λυθεί αυτό το πρόβλημα. Η νικηφόρα πρόταση από τον Herman Hollerith βασίστηκε σε ένα μηχάνημα που μπορούσε να διαβάσει δεδομένα αποθηκευμένα σε διάτρητες κάρτες. Η τεχνολογία αυτή χρησιμοποιήθηκε από υπολογιστές για αρκετές δεκαετίες.

Κατά το πρώτο μισό του εικοστού αιώνα, διάτρητα χαρτιά χρησιμοποιήθηκαν ευρέως για αποθήκευση και εισαγωγή δεδομένων σε υπολογιστές, και χρησίμευαν ως ένα από τα πρώτα μέσα εισόδου / εξόδου. Μόνο κατά τη διάρκεια της δεκαετίας του 1980, διάτρητες οι κάρτες αντικαταστάθηκαν από άλλες πιο σύγχρονες συσκευές.

Η τεχνολογία των διάτρητων καρτών ήταν η πρώτη εμφάνιση μιας μηχανής που αντικατέστησε τους ανθρώπους στη διαχείριση μεγάλου όγκου δεδομένων και έτσι ο Hollerith καταγράφηκε ως ένας από τους ιδρυτές της σύγχρονης πληροφορικής. Η τεχνολογία χρησιμοποιήθηκε και άλλες χώρες, και ως εκ τούτου, ο Hollerith ίδρυσε την Tabulating Machines Company, η οποία κέρδισε το 1900 RFP για την απογραφή. Το 1911, συγχωνεύοντας δύο άλλες εταιρείες, μεγάλωσε και έγινε CTR (Computing Tabulating Recording Company), η οποία το 1924 άλλαξε το όνομά της σε IBM.

Η σύγχρονη εποχή των υπολογιστών ξεκίνησε με το Mark I, έναν ηλεκτρομηχανικό υπολογιστή που αναπτύχθηκε από τον Howard H. Aiken. Χρηματοδοτήθηκε και κατασκευάστηκε από την IBM και στάλθηκε στο Πανεπιστήμιο του Χάρβαρντ το
1944. Ο υπολογιστής ήταν φυσικά πολύ μεγάλος (μήκους άνω των 50 ποδιών) και αφού χρησιμοποιούσε μηχανικά ρελέ, ήταν πολύ θορυβώδες. Η ιδέα πίσω από την αρχιτεκτονική βασίστηκε στον αναλυτικό κινητήρα που σχεδιάστηκε από τον Babbage αλλά υλοποιήθηκε χρησιμοποιώντας έναν ηλεκτροκινητήρα. Ενώ οι σύγχρονοι υπολογιστές χρησιμοποιούν δυαδικό σύστημα, ο Mark I χρησιμοποιούσε δεκαδικά ψηφία και οι χρόνοι εκτέλεσης ήταν αργοί ακόμη και σε σύγκριση με τον ανθρώπινο εγκέφαλο:

- Τρεις προσθέσεις / αφαιρέσεις ανά δευτερόλεπτο
- Τέσσερα έως έξι δευτερόλεπτα για πολλαπλασιασμούς
- Δεκαπέντε δευτερόλεπτα για διαιρέσεις

Οι οδηγίες εκτέλεσης διαβάστηκαν από τη διάτρητη ταινία χαρτιού, και τα δεδομένα εισάγονταν χρησιμοποιώντας χειροκίνητους διακόπτες που αντιπροσωπεύουν αριθμούς.

Ένα άλλο σημαντικό ορόσημο στην ιστορία του υπολογιστή ήταν ο Ηλεκτρονικός Αριθμητικός Ολοκληρωτής και Υπολογιστής (ENIAC).Το ENIAC ήταν ο πρώτος ηλεκτρονικός υπολογιστής χωρίς μηχανικά εξαρτήματα. Λόγω της ικανότητάς του να τρέχει διάφορα προγράμματα, θεωρείται ο πρώτος υπολογιστής γενικής χρήσης. Ο κύριος σκοπός πίσω από τον σχεδιασμό του ήταν να διευκολύνει την κουραστική εργασία που εμπλέκεται στον υπολογισμό και την προετοιμασία πινάκων του πυροβολικού.

Ο σχεδιασμός και η κατασκευή του μηχανήματος πραγματοποιήθηκε στο Πανεπιστήμιο της Πενσυλβανίας με επικεφαλής τον John Mauchly και τον Presper Eckert. Το έργο

ξεκίνησε το 1943 και ο υπολογιστής λειτουργούσε το 1946. Ήταν πολύ αργά για να συνεισφέρει στις πολεμικές προσπάθειες, αλλά από τότε που λειτούργησε μέχρι το 1955, χρησιμοποιήθηκε για πολλά άλλα βαριά υπολογιστικά έργα, όπως η βόμβα υδρογόνου. Το ENIAC, όπως όλοι οι άλλοι υπολογιστές εκείνη την εποχή, ήταν πολύ μεγάλος και καταλάμβανε πάνω από 1800 τετραγωνικά πόδια. Χρησιμοποιούσε πάνω από 17.000 σωλήνες κενού, οι οποίοι τότε δεν ήταν πολύ αξιόπιστοι. Ως αποτέλεσμα ο υπολογιστής δεν λειτουργούσε για μεγάλο χρονικό διάστημα, σχεδόν το ήμισυ του χρόνου. Ωστόσο, όταν δούλευε, ήταν ο γρηγορότερος διαθέσιμος υπολογιστής, ικανός να εκτελέσει 5000 προσθέσεις / αφαιρέσεις, 357 πολλαπλασιασμούς και 38 διαιρέσεις ανά δευτερόλεπτο.

Το πιο σημαντικό χαρακτηριστικό, και αυτό που υλοποιεί η προηγμένη τεχνολογία υπολογιστών, είναι ότι ένας υπολογιστής πρέπει να είναι μια μηχανή γενικής χρήσης όπου μπορεί να εκτελέσει πολλά διαφορετικά προγράμματα. Αυτή η αρχή είναι σήμερα ένας από τους κύριους ακρογωνιαίους λίθους στις αρχιτεκτονικές υπολογιστών. Αυτό οδήγησε στην ανάπτυξη πολλών γλωσσών προγραμματισμού και συνέβαλε άμεσα την ευρεία χρήση των υπολογιστών ως αυτόνομων συστημάτων καθώς και ενσωματωμένων σε πολλά μηχανήματα και συσκευές.

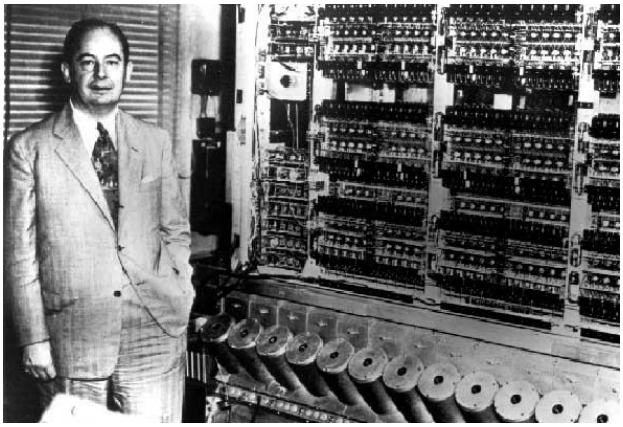
Ένα σημαντικό βήμα στην εξέλιξη των ηλεκτρονικών υπολογιστών επιτεύχθηκε με την εφεύρεση του τρανζίστορ το 1947. Τα τρανζίστορ αντικατέστησαν τους σωλήνες κενού και τους ηλεκτρομηχανικούς διακόπτες, που ήταν σημαντικά μεγαλύτεροι, κατανάλωναν μεγάλες ποσότητες ηλεκτρικής ενέργειας και ήταν ανεπαρκώς αξιόπιστοι. Η εφεύρεση τρανζίστορ, που άλλαξε για πάντα την αγορά ηλεκτρονικών ειδών, παρείχε ένα σημαντικό βήμα στην πρόοδο της σύγχρονης τεχνολογίας.

Αρχιτεκτονική Von Neumann

Ο John von Neumann, ο οποίος εργάστηκε στο έργο της βόμβας υδρογόνου, συμμετείχε εν μέρει στην δημιουργία του ENIAC, κυρίως λόγω της δυνατότητας του στην επίλυση σύνθετων υπολογισμών που απαιτούνται για την βόμβα. Μέσω αυτής της εμπλοκής του, ο von Neumann σχεδίασε μια αρχιτεκτονική υπολογιστών που χρησιμοποιείται ακόμη και σήμερα στο σχεδιασμό σύγχρονων υπολογιστών (σχήμα 1.1).

Η αρχιτεκτονική von Neumann αποτελείται από μια κοινόχρηστη μνήμη που χρησιμοποιείται για την αποθήκευση τόσο εντολών όσο και δεδομένων. Το μοντέλο ορίζει πολλά διαφορετικά αλλά διασυνδεδεμένα στοιχεία που συνθέτουν την υπολογιστική αρχιτεκτονική.

Το μοντέλο αναφέρεται ως μοντέλο αποθηκευμένου προγράμματος, καθώς μπορούν διαφορετικά προγράμματα να φορτωθούν στη μνήμη του υπολογιστή, σε αντίθεση με τα πρώτα μοντέλα υπολογιστών όπου υποστήριζαν ένα μόνο πρόγραμμα. Αυτό ήταν μία σημαντική εξέλιξη που προήλθε από την von Neumann αρχιτεκτονική και ανέπτυξε τη χρήση υπολογιστών.

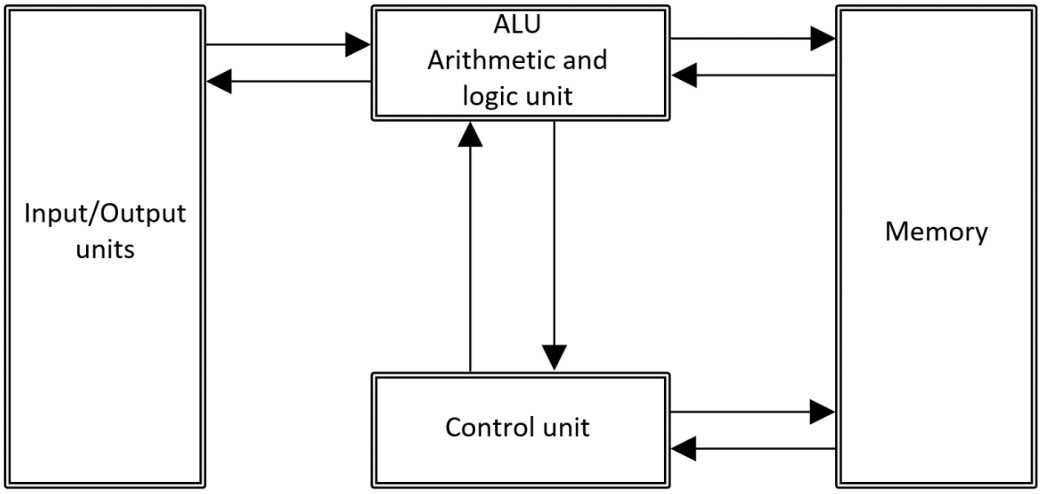


Εικόνα 1.1

Το μοντέλο ορίζει πολλές λειτουργικές μονάδες με ξεχωριστό διαχωρισμό μεταξύ τους. Για παράδειγμα,

- Διαχωρισμός της μονάδας επεξεργασίας από τη μνήμη. Η μονάδα επεξεργασίας (ή ο επεξεργαστής) είναι υπεύθυνος για την εκτέλεση των εντολών και δεν σχετίζεται με κανέναν τρόπο με την τοποθεσία των εντολών ή τα δεδομένα. Ένα ειδικό συστατικό στοιχείο της μονάδας ελέγχου στο εσωτερικό του επεξεργαστή είναι υπεύθυνο για ανάκτηση των εντολών και των τελεστών που απαιτούνται για την εκτέλεση του. Ένα παρόμοιο στοιχείο είναι υπεύθυνο για τη συλλογή του αποτελέσματος της εκτελεσμένης εντολής και την αποθήκευσή του στην καθορισμένη τοποθεσία.
- Διαχωρισμός της μονάδας εκτέλεσης από τη μονάδα ελέγχου. Αρχικά, οι δύο μονάδες συνδυάστηκαν στη μονάδα εκτέλεσης, η οποία είναι υπεύθυνη για την εκτέλεση των εντολών των προγραμμάτων. Μετά το διαχωρισμό, η μονάδα ελέγχου είναι υπεύθυνη για τον προγραμματισμό της εκτέλεσης καθώς και για την παροχή όλων των απαραίτητων στοιχείων για εκτέλεση (εντολές, τελεστές), ενώ η μονάδα εκτέλεσης εκτελεί μόνο τις εντολές.
- Διαχωρισμός των μονάδων εισόδου και εξόδου από άλλα στοιχεία του συστήματος χωρίζοντας κάθε μονάδα από τις άλλες μονάδες. Το αποτέλεσμα, για παράδειγμα, είναι ο υψηλός βαθμός αρθωτότητας που όλοι απολαμβάνουμε με τον προσωπικό υπολογιστή. Λόγω αυτού του διαχωρισμού, μπορεί κάποιος για παράδειγμα να αγοράσει έναν υπολογιστή από κάποιον κατασκευαστή, ενώ το ποντίκι και το πληκτρολόγιο μπορούν να ληφθούν ξεχωριστά.

Η πρώτη εφαρμογή της αρχιτεκτονικής von Neumann πραγματοποιήθηκε στο Institute of Advanced Technology (IAS) (στο Πανεπιστήμιο του Princeton). Ο υπολογιστής IAS είχε τη δυνατότητα να φορτώνει προγράμματα, σε αντίθεση με τις προηγούμενες χειροκίνητες ρυθμίσεις διακοπτών. Ο υπολογιστής σχεδιάστηκε ειδικά για πολύπλοκους μαθηματικούς υπολογισμούς, χρησιμοποιήθηκε δυαδικό σύστημα και είχε αρκετούς καταχωρητές.



Σχήμα 1.1

Η ταχεία τεχνολογική ανάπτυξη και πρόοδος που σημειώθηκε τις τελευταίες δεκαετίες είναι μεγαλύτερη από τις προσδοκίες των ειδικών. Ο αριθμός των τρανζίστορ ανά τσιπ

συνεχίζει να αυξάνεται. Ωστόσο, λόγω παγκόσμιων αλλαγών, όπως η ενεργειακή κρίση, καθώς και η τεράστια ζήτηση για φορητούς και ενεργειακά αποδοτικούς επεξεργαστές, αντί να αυξάνεται η ταχύτητα του επεξεργαστή, καταβάλλεται μεγάλη προσπάθεια για μείωση της απαιτούμενης κατανάλωσης ισχύος και διασποράς θερμότητας. Η κατανάλωση ενέργειας έχει γίνει ένας εξέχων παράγοντας στις αποφάσεις αγοράς και πρέπει να εξετάζεται επίσης στις διαδικασίες σχεδιασμού υλικού.

Ο νόμος του Moore

Σε μια δημοσίευση που δημοσιεύθηκε στην Electronics στις 19 Απριλίου 1965, ο τότε διευθυντής έρευνας και ανάπτυξης της Fairchild Semiconductor's και αργότερα συνιδρυτής της Intel, Gordon Moore, έγραψε μια ενδιαφέρουσα πρόβλεψη σχετικά με τον αριθμό των τρανζίστορ σε ένα ολοκληρωμένο κύκλωμα. Προέβλεπε ότι ο αριθμός αυτός θα διπλασιάζετε κάθε χρόνο για τουλάχιστον μία δεκαετία. Την επόμενη δεκαετία μελετώντας ξανά τα υπάρχοντα δεδομένα αναθεώρησε την άποψή του και είπε ότι ο αριθμός των τρανζίστορ θα διπλασιάζετε κάθε δύο χρόνια. Η πρόβλεψη αυτή επαληθεύτηκε στο πέρασμα των χρόνων καθώς από τότε ο αριθμός αυτός όντος διπλασιάζετε κάθε 18 μήνες περίπου. Έτσι η πρόβλεψη αυτή ονομάστηκε Νόμος του Moore. Σύμφωνα με αυτόν τον νόμο μπορούμε να θεωρήσουμε ότι πρόβλημα τα οποία σήμερα θεωρούνται άλυτα λόγω της έλλειψης επεξεργαστικής ισχύος σε λίγα χρόνια θα λυθούν καθώς αυτή η ισχύς θα μεγαλώνει.

Αν και υπάρχουν πολλοί τρόποι για την ταξινόμηση των υπολογιστών, ωστόσο, με την πάροδο των ετών, η κυρίαρχη ταξινόμηση έχει γίνει σύμφωνα με τη χρήση των συστημάτων. Σε γενικές γραμμές, υπάρχουν τρεις κύριες ομάδες υπολογιστών.

- *Microcomputers*, οι οποίοι συνήθως είναι μικροί, χαμηλού κόστους και προορίζονται για έναν χρήστη ή μία συσκευή. Σχεδόν κάθε γραφείο και σπίτι διαθέτει ένα προσωπικό υπολογιστή.
- *Minicomputers*, οι οποίοι χρησιμοποιούνται γενικά σε περιβάλλον πολλαπλών χρηστών. Ιστορικά, οι υπολογιστές αυτοί αναπτύχθηκαν για να παρέχουν μια λύση για ένα συγκεκριμένο τμήμα και όχι για ολόκληρο τον οργανισμό. Όμως με τις ραγδαίες εξελίξεις στην απόδοση των υπολογιστών, όπως προβλέπει και ο νόμος του Moore, τα τελευταία χρόνια οι Minicomputers έχουν μετατραπεί σε μικρούς διακομιστές.
- *Mainframes*, οι οποίοι είναι μεγάλα υπολογιστικά συστήματα. Αυτά τα συστήματα παρέχουν εφαρμογές για την υποστήριξη όλων των επιχειρηματικών διαδικασιών. Τα Mainframes είναι συνήθως πολύ ισχυρά. Αρχικά, τα mainframes ήταν ιδιόκτητα συστήματα με ένα ιδιόκτητο λειτουργικό σύστημα. Στις αρχές του 21ου αιώνα, πολλά από τα Mainframes αντικαταστάθηκαν από μεγάλους διακομιστές, οι οποίοι παρέχουν την ίδια λειτουργικότητα. Οι διακομιστές αυτοί είναι κατασκευασμένοι χρησιμοποιώντας πολλούς μικροεπεξεργαστές που λειτουργούν παράλληλα.

2. Κατηγορίες σημερινών server με βάση τον σκοπό χρήσης τους

2.1. Προσωπικοί υπολογιστές

Ο προσωπικός υπολογιστής (PC) είναι ένας υπολογιστής πολλαπλών χρήσεων του οποίου το μέγεθος, οι δυνατότητες και η τιμή το καθιστούν εφικτό για ατομική χρήση. Οι προσωπικοί υπολογιστές προορίζονται να λειτουργούν απευθείας από έναν τελικό χρήστη και όχι από έναν ειδικό σε υπολογιστές ή τεχνικό. Σε αντίθεση με τα μεγάλα υπολογιστικά συστήματα η κοινή χρήση χρόνου από πολλά άτομα ταυτόχρονα δεν χρησιμοποιείται στους προσωπικούς υπολογιστές.

Την δεκαετία του 1960 οι εταιρίες που χρησιμοποιούσαν υπολογιστές έπρεπε να γράψουν τα δικά τους προγράμματα για να κάνουν οποιαδήποτε χρήσιμη εργασία με τα μηχανήματα. Οι χρήστες προσωπικών υπολογιστών είτε ανέπτυσσαν τις δικές τους εφαρμογές είτε ποιο συνηθισμένα εκτελούσαν σε αυτά τα μηχανήματα εμπορικό λογισμικό, το οποίο ήταν συνήθως ιδιόκτητο, ή και δωρεάν λογισμικό, λογισμικό ανοιχτού κώδικα, το οποίο παρέχονταν έτοιμο προς εκτέλεση. Το λογισμικό για προσωπικούς υπολογιστές συνήθως αναπτύσσεται και διανέμεται ανεξάρτητα από τους κατασκευαστές υλικού ή λειτουργικού συστήματος. Οι χρήστες προσωπικών υπολογιστών δεν χρειάζεται πλέον να γράφουν τα δικά τους προγράμματα για να κάνουν χρήση προσωπικού υπολογιστή.

Εικόνα 2.1

Τα προγράμματα εφαρμογών για τους προσωπικούς υπολογιστές περιλαμβάνουν επεξεργαστές κειμένου, λογιστικά φύλα, βάσεις δεδομένων, Web Browsers, e-mail clients, προγράμματα αναπαραγωγής πολυμέσων, παιχνίδια, κλπ. Οι προσωπικοί υπολογιστές σήμερα συνδέονται στο Internet και σε τοπικά δίκτυα είτε με καλωδιακή, είτε με ασύρματη σύνδεση. Ανάλογα διακρίνονται σε desktop, laptop, netbook, tablet.

Από τις αρχές της δεκαετίας του 1990, τα λειτουργικά συστήματα της Microsoft και το υλικό της Intel κυριάρχησαν σε μεγάλο μέρος της αγοράς προσωπικών υπολογιστών, πρώτα με το MS-DOS και στη συνέχεια με τα Microsoft Windows. Οι εναλλακτικές λύσεις στα λειτουργικά συστήματα Windows της Microsoft καταλαμβάνουν ένα μερίδιο μειοψηφίας του κλάδου. Σε αυτά περιλαμβάνονται το macOS της Apple και τα δωρεάν και ανοιχτού κώδικα λειτουργικά συστήματα τύπου Unix, όπως το Linux.

2.2. Workstation

Ένας σταθμός εργασίας είναι ένας ειδικός υπολογιστής σχεδιασμένος για τεχνικές ή επιστημονικές εφαρμογές. Προορίζονται κυρίως για χρήση από ένα άτομο κάθε φορά, συνδέονται συνήθως με ένα τοπικό δίκτυο και εκτελούν λειτουργικά συστήματα

πολλαπλών χρηστών. Ο όρος σταθμός εργασίας έχει επίσης χρησιμοποιηθεί για να αναφέρεται σε όλα, από ένα τερματικό υπολογιστή mainframe σε έναν υπολογιστή συνδεδεμένο σε ένα δίκτυο. Η πιο συνηθισμένη μορφή αναφέρεται στην κατηγορία του υλικού που προσφέρεται από αρκετές εταιρείες, όπως η Sun Microsystems, η Silicon Graphics , Apollo Computer, DEC, HP, NeXT και IBM που άνοιξαν την πόρτα για την επανάσταση 3D animation γραφικών στα τέλη της δεκαετίας του 1990.
Οι σταθμοί εργασίας προσφέρουν υψηλότερη απόδοση από τους κύριους προσωπικούς υπολογιστές, ειδικά σε σχέση με CPU και γραφικά, χωρητικότητα μνήμης και δυνατότητα πολλαπλών εργασιών. Οι σταθμοί εργασίας είναι βελτιστοποιημένοι για την οπτικοποίηση και τον χειρισμό διαφορετικών τύπων πολύπλοκων δεδομένων, όπως τρισδιάστατος μηχανικός σχεδιασμός, μηχανική προσομοίωση (π.χ. υπολογιστική ρευστή δυναμική), κινούμενη εικόνα και απόδοση εικόνων και μαθηματικές γραφικές παραστάσεις. Συνήθως, η μορφή του είναι παρόμοια με αυτή ενός επιτραπέζιου υπολογιστή, που αποτελείται από μια οθόνη υψηλής ανάλυσης, ένα πληκτρολόγιο και ένα ποντίκι τουλάχιστον, αλλά προσφέρουν επίσης πολλές οθόνες, tablet γραφικών, τρισδιάστατα ποντίκια (συσκευές χειρισμού αντικειμένων 3D και πλοήγησης εικόνων), Οι σταθμοί εργασίας ήταν το πρώτο τμήμα της αγοράς υπολογιστών που παρουσίασε προηγμένα αξεσουάρ και εργαλεία συνεργασίας.
Στην παρακάτω εικόνα φαίνεται ο Precision 7920 Tower Workstation της εταιρίας DELL.

Εικόνα 2.2

Οι αυξανόμενες δυνατότητες των mainstream υπολογιστών στα τέλη της δεκαετίας του 1990 έχουν θολώσει τις γραμμές μεταξύ υπολογιστών και τεχνικών / επιστημονικών

σταθμών εργασίας. Τυπικοί σταθμοί εργασίας χρησιμοποιούσαν προηγουμένως ιδιόκτητο υλικό που τους έκανε διαφορετικούς από τους υπολογιστές. Για παράδειγμα, η IBM χρησιμοποίησε επεξεργαστές βασισμένους σε RISC για τους σταθμούς εργασίας της και επεξεργαστές Intel x86 για προσωπικούς υπολογιστές κατά τη διάρκεια της δεκαετίας του 1990 και του 2000. Ωστόσο, στις αρχές της δεκαετίας του 2000, αυτή η διαφορά εξαφανίστηκε σε μεγάλο βαθμό, καθώς οι σταθμοί εργασίας χρησιμοποιούν πλέον πολύ εμπορευματοποιημένο υλικό που κυριαρχείται από μεγάλους προμηθευτές υπολογιστών, όπως η Dell, η Hewlett-Packard και η Fujitsu, που πωλούν Microsoft Windows ή Linux συστήματα που εκτελούνται σε επεξεργαστές x86-64.
Στα δίκτυα, ο όρος workstation αναφέρεται σε κάθε τερματικό υπολογιστή συνδεδεμένο σε αυτά.

2.3. Servers

Ο διακομιστής (server) είναι ένας υπολογιστής ή σύστημα που παρέχει πόρους, δεδομένα, υπηρεσίες ή προγράμματα σε άλλους υπολογιστές, γνωστούς ως πελάτες, μέσω ενός δικτύου. Θεωρητικά, κάθε φορά που οι υπολογιστές μοιράζονται πόρους με άλλους υπολογιστές-πελάτες (clients) , θεωρούνται servers. Υπάρχουν πολλοί τύποι server, συμπεριλαμβανομένων web servers , και virtual servers.

Ένα μεμονωμένο σύστημα μπορεί να παρέχει πόρους και να τους χρησιμοποιεί ταυτόχρονα. Αυτό σημαίνει ότι μια συσκευή θα μπορούσε να είναι ταυτόχρονα server και client.

Μερικοί από τους πρώτους servers ήταν υπολογιστές mainframe ή minicomputer. Οι minicomputers ήταν πολύ μικρότεροι από τους mainframe, εξ ου και το όνομα. Ωστόσο, καθώς εξελίχθηκε η τεχνολογία, κατέληξαν να γίνουν πολύ μεγαλύτεροι από τους επιτραπέζιους υπολογιστές, οι οποίοι καθιστούσαν τον όρο μικροϋπολογιστής κάπως κωμικός.

Αρχικά, τέτοιοι servers συνδέονταν με clients γνωστούς ως τερματικά που δεν έκαναν πραγματικούς υπολογισμούς. Αυτά τα τερματικά υπήρχαν απλά για την αποδοχή εισόδου μέσω πληκτρολογίου ή συσκευής ανάγνωσης καρτών και για την επιστροφή των αποτελεσμάτων οποιωνδήποτε υπολογισμών σε οθόνη προβολής ή εκτυπωτή. Ο πραγματικός υπολογισμός γινόταν στον διακομιστή.

Αργότερα, οι διακομιστές ήταν συχνά μεμονωμένοι, ισχυροί υπολογιστές συνδεδεμένοι μέσω δικτύου σε ένα σύνολο λιγότερο ισχυρών clients. Αυτή η αρχιτεκτονική δικτύου αναφέρεται συχνά ως μοντέλο client-server, στο οποίο τόσο ο client όσο και ο server διαθέτουν υπολογιστική ισχύ, αλλά ορισμένες εργασίες ανατίθενται στους servers. Σε προηγούμενα υπολογιστικά μοντέλα, όπως το μοντέλο mainframe-terminal, το mainframe λειτουργούσε ως server, παρόλο που δεν αναφέρεται από αυτό το όνομα.

Καθώς η τεχνολογία έχει εξελιχθεί, ο ορισμός ενός server έχει εξελιχθεί μαζί του. Αυτές τις μέρες, ένας server μπορεί να είναι απλά λογισμικό που εκτελείται σε μία ή περισσότερες φυσικές υπολογιστικές συσκευές. Τέτοιοι servers αναφέρονται συχνά ως virtual servers. Αρχικά, virtual servers χρησιμοποιήθηκαν για να αυξήσουν τον αριθμό των λειτουργιών που θα μπορούσε να κάνει ένας φυσικός server. Σήμερα, οι virtual servers εκτελούνται συχνά από τρίτους και είναι διαθέσιμοι μέσω του διαδικτύου, αυτό είναι ένα μέρος του cloud computing.

Ένας server μικρών επιχειρήσεων είναι συνήθως ένας διακομιστής χαμηλού επιπέδου σχεδιασμένος να είναι προσιτός και διαχειρίσιμος σε ένα περιβάλλον μικρών

επιχειρήσεων. Οι διακομιστές Small Business είναι κατάλληλοι για έναν έως δεκάδες υπαλλήλους και ενδέχεται να έχουν προεγκατεστημένο το λογισμικό που απαιτείται για την εκτέλεση του διακομιστή.

Σε μια μικρή επιχείρηση ένας διακομιστής χρησιμοποιείται συχνά για τη διαχείριση πολλαπλών υπηρεσιών δικτύου, όπως email, διαχείριση απειλών, σύνδεση στο Internet, κοινή χρήση αρχείων και εκτυπωτών, απομακρυσμένη πρόσβαση και δημιουργία αντιγράφων ασφαλείας δεδομένων.

Οι διακομιστές μικρών επιχειρήσεων διαφέρουν από τους διακομιστές που χρησιμοποιούνται σε μεγάλες εταιρείες και κέντρα δεδομένων, οι οποίοι είναι συχνά αφιερωμένοι στην εκτέλεση μιας κύριας εργασίας. Πολλοί αποκλειστικοί διακομιστές (όπως διακομιστές εκτύπωσης, διακομιστές Web ή διακομιστές βάσης δεδομένων) δεν εκτελούν καμία άλλη λειτουργία εκτός από την καθορισμένη εργασία τους. Επίσης, αν και έχουν αρκετά κοινά χαρακτηριστικά, διαφέρουν και από τους προσωπικούς υπολογιστές καθώς έχουν διαφορετικό σκοπό και το υλικό τους είναι σχεδιασμένο να εξυπηρετεί αυτό τον σκοπό.

2.4. Mainframes

Πρώτον, ας αντιμετωπίσουμε την ορολογία. Σήμερα, οι κατασκευαστές υπολογιστών δεν χρησιμοποιούν πάντα τον όρο mainframe για να αναφέρονται σε υπολογιστές mainframe. Αντ' αυτού, οι περισσότεροι ονόμασαν οποιονδήποτε υπολογιστή εμπορικής χρήσης - μεγάλο ή μικρό – ως διακομιστή, με το mainframe να είναι ο μεγαλύτερος τύπος διακομιστή που χρησιμοποιείται σήμερα. Ο όρος mainframe χρησιμοποιείτε γενικά για να περιγράψει υπολογιστές που μπορούν να υποστηρίξουν πολλές εφαρμογές και συσκευές εισόδου / εξόδου για ταυτόχρονη εξυπηρέτηση χιλιάδων χρηστών.

Οι διακομιστές πολλαπλασιάζονται. Μια επιχείρηση μπορεί να έχει μια μεγάλη συλλογή διακομιστών που περιλαμβάνει διακομιστές συναλλαγών, διακομιστές βάσεων δεδομένων, διακομιστές ηλεκτρονικού ταχυδρομείου και διακομιστές Web.

Πολύ μεγάλες συλλογές διακομιστών ονομάζονται μερικές φορές server farms (στην πραγματικότητα, ορισμένα κέντρα δεδομένων καλύπτουν εκτάσεις σε στρέμματα). Το υλικό που απαιτείται για την εκτέλεση μιας λειτουργίας διακομιστή μπορεί να κυμαίνεται από ένα σύμπλεγμα προσωπικών υπολογιστών που είναι τοποθετημένοι σε rack έως τα πιο ισχυρά mainframe που κατασκευάζονται σήμερα.

Ένα mainframe είναι το κεντρικό αποθετήριο δεδομένων ή ο κόμβος, στο κέντρο επεξεργασίας δεδομένων μιας εταιρείας, που συνδέεται με χρήστες μέσω λιγότερο ισχυρών συσκευών, όπως σταθμοί εργασίας ή τερματικά. Η παρουσία ενός mainframe συνεπάγεται συχνά μια συγκεντρωτική μορφή υπολογισμού, σε αντίθεση με μια κατανεμημένη μορφή υπολογιστών.

Η συγκέντρωση των δεδομένων σε ένα αποθετήριο mainframe γλιτώνει τους πελάτες από την ανάγκη να διαχειριστούν ενημερώσεις σε περισσότερα από ένα αντίγραφα των επιχειρηματικών τους δεδομένων, γεγονός που αυξάνει την πιθανότητα τα δεδομένα αυτά να είναι ενημερωμένα.

Ωστόσο, η διάκριση μεταξύ κεντρικών και κατανεμημένων υπολογιστών θολώνει ταχέως καθώς τα μικρότερα μηχανήματα συνεχίζουν να κερδίζουν σε ισχύ επεξεργασίας και τα mainframe γίνονται όλο και πιο ευέλικτα και πολλαπλών χρήσεων. Οι πιέσεις της αγοράς απαιτούν από τις σημερινές επιχειρήσεις να επαναξιολογούν συνεχώς τις στρατηγικές τους για να βρουν καλύτερους τρόπους υποστήριξης μιας μεταβαλλόμενης

αγοράς. Ως αποτέλεσμα, τα mainframe χρησιμοποιούνται πλέον συχνά σε συνδυασμό με δίκτυα μικρότερων διακομιστών σε πολλές διαμορφώσεις. Η δυνατότητα δυναμικής αναδιάρθρωσης ενός mainframe πόροι υλικού και λογισμικού (όπως επεξεργαστές, μνήμη και συνδέσεις συσκευών), ενώ οι εφαρμογές συνεχίζουν να εκτελούνται, υπογραμμίζει περαιτέρω την ευέλικτη, εξελισσόμενη φύση του σύγχρονου mainframe.

Καθώς το hardware των mainframe έχει γίνει πιο πολύπλοκο, έτσι και τα λειτουργικά συστήματα που λειτουργούν σε mainframe ακολουθούν αυτή την τάση. Πριν από χρόνια, στην πραγματικότητα, οι όροι ορίζονταν ο ένας στον άλλο: ένα mainframe ήταν οποιοδήποτε σύστημα υλικού που διέθετε ένα μεγάλο λειτουργικό σύστημα . Αυτό το νόημα έχει θολώσει τα τελευταία χρόνια, επειδή αυτά τα λειτουργικά συστήματα μπορούν να λειτουργούν σε πολύ μικρά συστήματα.

Οι κατασκευαστές υπολογιστών και οι επαγγελματίες πληροφορικής χρησιμοποιούν συχνά τον όρο πλατφόρμα για να αναφέρονται στο υλικό και το λογισμικό που σχετίζονται με μια συγκεκριμένη αρχιτεκτονική υπολογιστών. Για παράδειγμα, ένας κεντρικός υπολογιστής και το λειτουργικό του σύστημα θεωρούνται πλατφόρμα. Ακόμη και οι προσωπικοί υπολογιστές μπορούν να θεωρηθούν πολλές διαφορετικές πλατφόρμες, ανάλογα με το λειτουργικό σύστημα που χρησιμοποιείται.

Λοιπόν, ας επιστρέψουμε στην ερώτησή μας τώρα: "Τι είναι το mainframe;" Σήμερα, ο όρος mainframe μπορεί καλύτερα να χρησιμοποιηθεί για να περιγράψει ένα στυλ λειτουργίας, εφαρμογών και εγκαταστάσεων λειτουργικού συστήματος. Για να ξεκινήσετε με έναν ορισμό που λειτουργεί, «ένα mainframe είναι αυτό που χρησιμοποιούν οι επιχειρήσεις για να φιλοξενήσουν τις εμπορικές βάσεις δεδομένων, τους διακομιστές συναλλαγών και τις εφαρμογές που απαιτούν μεγαλύτερο βαθμό ασφάλειας και διαθεσιμότητας από ό, τι συνήθως υπάρχει σε μηχανήματα μικρότερης κλίμακας».

Τα πρώτα συστήματα mainframe στεγάζονταν σε τεράστια μεταλλικά κουτιά ή πλαίσια μεγέθους δωματίου, από εκεί πιθανότατα προήλθε από και ο όρος mainframe. Το πρώιμο mainframe απαιτούσε μεγάλες ποσότητες ηλεκτρικής ενέργειας και κλιματισμού και το δωμάτιο ήταν γεμάτο κυρίως με συσκευές I / O. Επίσης, ένας τυπικός ιστότοπος πελάτη είχε εγκατεστημένα πολλά mainframe, με τις περισσότερες από τις συσκευές I / O συνδεδεμένες σε όλα τα mainframe. Κατά τη μεγαλύτερη περίοδο, από άποψη φυσικού μεγέθους, ένα τυπικό mainframe καταλάμβανε 600 έως 3000 τετραγωνικά μέτρα. Ορισμένες εγκαταστάσεις ήταν ακόμη μεγαλύτερες από αυτό.

Από το 1990 περίπου, οι επεξεργαστές mainframe και οι περισσότερες από τις συσκευές I / O τους έγιναν φυσικά μικρότεροι, ενώ η λειτουργικότητα και η χωρητικότητά τους συνέχισαν να αυξάνονται. Τα συστήματα mainframe σήμερα είναι πολύ μικρότερα από τα προηγούμενα συστήματα, περίπου στο μέγεθος ενός μεγάλου ψυγείου.
Σε ορισμένες περιπτώσεις, είναι πλέον δυνατή η εκτέλεση ενός λειτουργικού συστήματος mainframe σε έναν υπολογιστή που προσομοιώνει ένα mainframe.

Τέτοιοι εξομοιωτές είναι χρήσιμοι για την ανάπτυξη και τον έλεγχο επιχειρηματικών εφαρμογών πριν από τη μεταφορά τους σε ένα κεντρικό σύστημα παραγωγής.

Είναι σαφές ότι ο όρος mainframe έχει επεκταθεί πέρα από την απλή περιγραφή των φυσικών χαρακτηριστικών ενός συστήματος. Αντ' αυτού, η λέξη ισχύει συνήθως για κάποιο συνδυασμό των ακόλουθων χαρακτηριστικών:

- Συμβατότητα με λειτουργικά συστήματα mainframe, εφαρμογές και δεδομένα.
- Κεντρικός έλεγχος των πόρων.

- Υλικό και λειτουργικά συστήματα που μπορούν να μοιράζονται την πρόσβαση σε μονάδες δίσκου με άλλα συστήματα, με αυτόματο κλείδωμα και προστασία έναντι καταστροφικής ταυτόχρονης χρήσης δεδομένων δίσκου.
- Ένα στυλ λειτουργίας, που συχνά περιλαμβάνει προσωπικό επιχειρήσεων που χρησιμοποιεί λεπτομερή βιβλία διαδικασιών λειτουργίας και εξαιρετικά οργανωμένες διαδικασίες για δημιουργία αντιγράφων ασφαλείας, ανάκτηση, εκπαίδευση και αποκατάσταση καταστροφών σε μια εναλλακτική τοποθεσία.
- Υλικό και λειτουργικά συστήματα που λειτουργούν συνήθως με εκατοντάδες ή χιλιάδες ταυτόχρονες λειτουργίες εισόδου / εξόδου.
- Τεχνολογίες ομαδοποίησης που επιτρέπουν στον πελάτη να χειρίζεται πολλαπλά αντίγραφα του λειτουργικού συστήματος ως ενιαίο σύστημα. Αυτή η διαμόρφωση, γνωστή ως Parallel Sysplex, είναι ανάλογη της ιδέας με ένα σύμπλεγμα UNIX, αλλά επιτρέπει την προσθήκη ή αφαίρεση συστημάτων όταν απαιτείται καθώς οι εφαρμογές συνεχίζουν να εκτελούνται. Αυτή η ευελιξία επιτρέπει στους πελάτες του mainframe να εισάγουν νέες εφαρμογές ή να διακόψουν τη χρήση των υπαρχουσών εφαρμογών, ακολουθώντας τις αλλαγές στην επιχειρηματική δραστηριότητα.
- Πρόσθετες δυνατότητες κοινής χρήσης δεδομένων και πόρων. Σε ένα Parallel Sysplex, για παράδειγμα, είναι δυνατό για χρήστες σε πολλά συστήματα να έχουν ταυτόχρονη πρόσβαση στις ίδιες βάσεις δεδομένων, με την πρόσβαση στη βάση δεδομένων να ελέγχεται σε επίπεδο εγγραφής.

Καθώς η απόδοση και το κόστος τέτοιων πόρων υλικού, όπως η κεντρική μονάδα επεξεργασίας (CPU) και τα μέσα αποθήκευσης εξωτερικού χώρου, και ο αριθμός και οι τύποι συσκευών που μπορούν να συνδεθούν με την CPU αυξάνονται, το λογισμικό του λειτουργικού συστήματος μπορεί να εκμεταλλευτεί πλήρως το βελτιωμένο υλικό. Επίσης, οι συνεχείς βελτιώσεις στη λειτουργικότητα του λογισμικού συμβάλλουν στην ανάπτυξη κάθε νέας γενιάς συστημάτων υλικού.

Οι mainframes είναι σε θέση να χειρίζονται και να επεξεργάζονται πολύ μεγάλες ποσότητες δεδομένων γρήγορα. Οι υπολογιστές mainframe χρησιμοποιούνται σε μεγάλα ιδρύματα όπως η κυβέρνηση, οι τράπεζες και οι μεγάλες εταιρείες. Μετρώνται σε MIPS (million instructions per second) και μπορούν να ανταποκρίνονται σε εκατοντάδες εκατομμύρια χρήστες κάθε φορά.

2.5. Super Computers

Οι Super Computers είναι μια κατηγορία εξαιρετικά ισχυρών υπολογιστών. Ο όρος αναφέρετε συνήθως στα γρηγορότερα συστήματα υψηλής απόδοσης που διατίθενται ανά πάσα στιγμή. Τέτοιοι υπολογιστές έχουν χρησιμοποιηθεί κυρίως για επιστημονικές και μηχανολογικές εργασίες που απαιτούν υπολογισμούς υψηλής ταχύτητας. Οι κοινές εφαρμογές για υπερυπολογιστές περιλαμβάνουν δοκιμή μαθηματικών μοντέλων για σύνθετα φυσικά φαινόμενα ή σχέδια, όπως κλίμα και καιρός, εξέλιξη του κόσμου, πυρηνικά όπλα και αντιδραστήρες, νέες χημικές ενώσεις (ειδικά για φαρμακευτικούς σκοπούς) και κρυπτογραφία. Καθώς το κόστος των υπερυπολογιστών μειώθηκε τη δεκαετία του 1990, περισσότερες επιχειρήσεις άρχισαν να χρησιμοποιούν υπερυπολογιστές για έρευνα αγοράς και άλλα μοντέλα που σχετίζονται με τις επιχειρήσεις.

Οι υπερυπολογιστές έχουν συγκεκριμένα χαρακτηριστικά. Σε αντίθεση με τους συμβατικούς υπολογιστές, έχουν συνήθως περισσότερες από μία CPU (κεντρική μονάδα επεξεργασίας), η οποία περιέχει κυκλώματα για την ερμηνεία των οδηγιών του προγράμματος και την εκτέλεση αριθμητικών και λογικών λειτουργιών με τη σωστή σειρά. Η χρήση πολλών CPU για την επίτευξη υψηλών υπολογιστικών ποσοστών απαιτείται από τα φυσικά όρια της τεχνολογίας κυκλωμάτων. Τα ηλεκτρονικά σήματα δεν μπορούν να ταξιδεύουν γρηγορότερα από την ταχύτητα του φωτός, το οποίο συνεπώς αποτελεί θεμελιώδες όριο ταχύτητας για μετάδοση σήματος και εναλλαγή κυκλώματος. Αυτό το όριο έχει σχεδόν επιτευχθεί, λόγω της μικρογραφίας των εξαρτημάτων κυκλώματος, της δραματικής μείωσης του μήκους των καλωδίων που συνδέουν τις πλακέτες κυκλώματος και της καινοτομίας στις τεχνικές ψύξης (π.χ., σε διάφορα συστήματα υπερυπολογιστών, τα κυκλώματα επεξεργαστών και μνήμης βυθίζονται σε ένα κρυογονικό υγρό για να επιτευχθούν χαμηλές θερμοκρασίες στις οποίες λειτουργούν ταχύτερα). Απαιτείται γρήγορη ανάκτηση αποθηκευμένων δεδομένων και εντολών για την υποστήριξη της εξαιρετικά υψηλής υπολογιστικής ταχύτητας των CPU. Επομένως, οι περισσότεροι υπερυπολογιστές έχουν πολύ μεγάλη χωρητικότητα αποθήκευσης, καθώς και πολύ γρήγορη ικανότητα εισόδου / εξόδου.

Ακόμα ένα άλλο χαρακτηριστικό των υπερυπολογιστών είναι η χρήση αριθμητικής διανύσματος - δηλαδή, μπορούν να λειτουργούν σε ζεύγη λιστών αριθμών και όχι σε απλά ζεύγη αριθμών. Για παράδειγμα, ένας τυπικός υπερυπολογιστής μπορεί να πολλαπλασιάσει μια λίστα ωριαίων μισθών για μια ομάδα εργαζομένων στο εργοστάσιο με μια λίστα ωρών που εργάζονται από τα μέλη αυτής της ομάδας για να παράγει μια λίστα με το ποσό που κερδίζει κάθε εργαζόμενος περίπου στο ίδιο χρονικό διάστημα που χρειάζεται κανονικός υπολογιστής για τον υπολογισμό του ποσού που κερδίζει ένας μόνο εργαζόμενος.

Οι υπερυπολογιστές αρχικά χρησιμοποιήθηκαν σε εφαρμογές που σχετίζονται με την εθνική ασφάλεια, συμπεριλαμβανομένου του σχεδιασμού πυρηνικών όπλων και της κρυπτογραφίας. Σήμερα χρησιμοποιούνται επίσης τις αεροδιαστημικές, πετρελαϊκές και αυτοκινητοβιομηχανίες. Επιπλέον, οι υπερυπολογιστές έχουν βρει ευρεία εφαρμογή σε τομείς που περιλαμβάνουν μηχανική ή επιστημονική έρευνα, όπως, για παράδειγμα, σε μελέτες της δομής των υποατομικών σωματιδίων και της προέλευσης και της φύσης του σύμπαντος. Οι υπερυπολογιστές έχουν γίνει απαραίτητο εργαλείο στην πρόγνωση καιρού: οι προβλέψεις βασίζονται τώρα σε αριθμητικά μοντέλα. Καθώς το κόστος των υπερυπολογιστών μειώθηκε, η χρήση τους εξαπλώθηκε και στον κόσμο του διαδικτυακού παιχνιδιού. Συγκεκριμένα, ο 5ος έως 10ος ταχύτερος Κινέζικος υπερυπολογιστής το 2007 ανήκε σε μια εταιρεία με διαδικτυακά δικαιώματα στην Κίνα για το ηλεκτρονικό παιχνίδι World of Warcraft, το οποίο μερικές φορές είχε περισσότερα από ένα εκατομμύριο άτομα να παίζουν μαζί στον ίδιο κόσμο του παιχνιδιού.

Η απόδοση ενός υπερυπολογιστή μετριέται συνήθως σε λειτουργίες κινητής υποδιαστολής ανά δευτερόλεπτο (FLOPS) αντί για εκατομμύρια οδηγίες ανά δευτερόλεπτο (MIPS) που μετριέται η απόδοση των mainframes.

2.6. Διαφορές Mainframes από Super Computers

Τόσο τα mainfames όσο και οι υπερυπολογιστές ωθούν τα όρια του τι μπορεί να επιτευχθεί μέσω του υπολογιστή. Είναι και οι δύο μεγάλες και ισχυρές μηχανές, αλλά δεν είναι το ίδιο πράγμα. Λόγω της ομοιότητάς τους (μεγάλα μαύρα κουτιά που κρύβονται

μακριά σε κλειδωμένα κέντρα δεδομένων), οι όροι συχνά συγχέονται. Ωστόσο, αναφέρονται σε πολύ διαφορετικά είδη υλικού και τύπων υπολογιστών.

Η μεγαλύτερη διάκριση μεταξύ των mainframes και των υπερυπολογιστών είναι ο τύπος των προβλημάτων που αντιμετωπίζουν. Κάθε ένας από αυτούς τους τύπους μεγάλων υπολογιστών είναι ειδικά σχεδιασμένος και βελτιστοποιημένος για να εκτελεί έναν συγκεκριμένο τύπο εργασίας και να το κάνει καλύτερα από οποιονδήποτε άλλο υπολογιστή. Όχι μόνο οι υπερυπολογιστές και τα mainframes εκτελούν τις εργασίες τους πιο αποτελεσματικά από άλλους τύπους υπολογιστών, αλλά κάνουν πράγματα που κανένας άλλος υπολογιστής δεν μπορεί να κάνει.

Οι υπερυπολογιστές έχουν σχεδιαστεί για να εργάζονται σε τύπους προβλημάτων των οποίων ο πρωταρχικός περιορισμός είναι η ταχύτητα υπολογισμού. Τα mainframes, από την άλλη πλευρά, αντιμετωπίζουν προβλήματα που περιορίζονται από την είσοδο / έξοδο και τα οποία απαιτούν αξιοπιστία πάνω απ' 'όλα. Έτσι, ενώ οι υπερυπολογιστές είναι ιδανικοί για την εκτέλεση σύνθετων υπολογισμών σε ένα μεγάλο σύνολο δεδομένων, τα mainframes είναι κατάλληλα για την εκτέλεση χιλιάδων υπολογισμών με χιλιάδες ταυτόχρονες συναλλαγές.

Οι υπερυπολογιστές εκτελούν μεγάλες ποσότητες πολύ γρήγορων και πολύπλοκων υπολογισμών σε δεδομένα που είναι αποθηκευμένα στη μνήμη. Αυτοί οι υπολογιστές είναι σχεδιασμένοι για να εκτελούν πολύπλοκες προσομοιώσεις. Τα mainframes επεξεργάζονται τις μεγάλες ποσότητες δεδομένων που εισέρχονται σε αυτές από εξωτερικές πηγές, όπως συναλλαγές με πιστωτική κάρτα ή επεξεργασία μισθοδοσίας.

Οι υπερυπολογιστές ωθούν τα όρια της υπολογιστικής ταχύτητας, ανακαλύπτοντας τι είναι δυνατό για έναν υπολογιστή. Είναι οι εξερευνητές του κόσμου των υπολογιστών. Αντίθετα, τα mainframes είναι οι εργαζόμενοι. Αντί να σπρώχνουν τα όρια του δυνατού, εστιάζουν στην αξιόπιστη ολοκλήρωση μεγάλων εργασιών και την επεξεργασία συναλλαγών.

Μερικές από τις κύριες διαφορές είναι οι εξής:

Mainframes:

- Εκτέλεση πολλών προγραμμάτων ταυτόχρονα
- Υποστήριξη πολλών ταυτόχρονων χρηστών
- Υποστήριξη νέου και παλαιού λογισμικού (συμβατότητα προς τα πίσω)
- Εκτέλεση πολλά διαφορετικών ειδών λειτουργικών συστημάτων (z / OS, Linux κ.λπ.)
- Αδιάλειπτη λειτουργία
- Η απόδοση μετράτε σε εκατομμύρια οδηγίες ανά δευτερόλεπτο (MIPS).
- Εκτέλεση εργασιών σε τεράστιες ποσότητες εξωτερικών δεδομένων
- Είναι αρκετά ευέλικτα για να εκτελούν πολλά είδη εφαρμογών και να αντιμετωπίζουν ευρείες επιχειρηματικές εργασίες

Υπερυπολογιστές:

- Εστιάζουν στη δύναμη επεξεργασίας για την εκτέλεση μερικών προγραμμάτων ή εντολών το συντομότερο δυνατό
- Επικεντρώνονται στην ταχύτητα και την επιταχυνόμενη απόδοση
- Ωθούν τα όρια για το τι μπορεί να επιτύχει το υλικό και το λογισμικό
- Συνήθως εκτελούν μια παραλλαγή του Linux ως λειτουργικό σύστημα

- Τυπικά εκτελούνται με τη μέγιστη ικανότητα, θέτοντας τους πλήρεις πόρους επεξεργασίας του υπολογιστή προς την επίλυση ενός συγκεκριμένου προβλήματος
- Η απόδοση μετράτε σε λειτουργίες κινητής υποδιαστολής ανά δευτερόλεπτο (FLOPS)
- Εκτελούν περίπλοκους υπολογισμούς χρησιμοποιώντας μεγάλη εσωτερική μνήμη
- Έχουν ειδικούς σκοπούς για εργασίες όπως επιστημονική έρευνα ή μηχανικά μοντέλα

Αυτά τα δύο μεγαθήρια του κόσμου των υπολογιστών, mainframes και υπερυπολογιστές, θα συνεχίσουν να κυριαρχούν στις βαριές υπολογιστικές ανάγκες των επιχειρήσεων, της επιστήμης, της κυβέρνησης και πολλών άλλων τομέων. Η δύναμη και οι εξειδικευμένες δυνατότητές τους τα καθιστούν κατάλληλα για τις συγκεκριμένες εργασίες τους.

3. Αρχιτεκτονικές υλικού των server

3.1. Εισαγωγή

Το υλικό του διακομιστή μοιράζεται πολλά από τα ίδια βασικά στοιχεία όπως η μνήμη, η χωρητικότητα και οι CPU με έναν επιτραπέζιο υπολογιστή. Αλλά οι ομοιότητες τελειώνουν εκεί καθώς τα στοιχεία του διακομιστή είναι πολύ πιο εξειδικευμένα επειδή έχουν μια πιο εντατική, αποκλειστική λειτουργία από ό, τι μια τυπική επιφάνεια εργασίας.

Οι διακομιστές χρησιμοποιούνται γενικά για τη διαχείριση των πόρων ενός δικτύου και την παροχή υπηρεσιών στους χρήστες σε αυτό το δίκτυο. Ο τύπος υλικού διακομιστή ενδέχεται να εξαρτάται από την ειδική υπηρεσία που παρέχει ο διακομιστής, καθώς κάποιο υλικό είναι πιο κατάλληλο για συγκεκριμένους σκοπούς.

Διακομιστές πύργων (Tower Servers), διακομιστές ραφιών (Rack Servers), διακομιστές blade (Blade Servers) και Mainframes είναι τύποι διακομιστών που προσφέρουν διαφορετικά πλεονεκτήματα ο καθένας.

Rack Servers

Ο διακομιστής rack μοιάζει με το διακομιστή blade. Περιλαμβάνει 1U rack, 2U rack, 4U rack κ.λπ. Συνήθως, το 1U rack-mount servers παρέχει την καλύτερη εξοικονόμηση χώρου, αλλά κακή απόδοση και επεκτασιμότητα. Είναι κατάλληλο για κάποιο σχετικά σταθερό πεδίο μιας επιχείρησης. Οι διακομιστές 4U παρέχουν υψηλότερη απόδοση, επεκτασιμότητα και γενικά υποστηρίζουν περισσότερους από 4 επεξεργαστές υψηλής απόδοσης και μεγάλο αριθμό τυπικών εξαρτημάτων με δυνατότητα εναλλαγής. Η διαχείρισή του είναι επίσης αρκετά εύκολη και αυτό γιατί οι κατασκευαστές συνήθως παρέχουν τα κατάλληλα εργαλεία διαχείρισης και παρακολούθησης, τα οποία είναι κατάλληλα για τις μεγάλες εφαρμογές κυκλοφορίας (Εικόνα 3.1).

Εικόνα 3.1

Ωστόσο, σε μεγαλύτερους διακομιστές, η χρήση του χώρου είναι πιο μικρή.

Ο διακομιστής rack είναι εγκατεστημένος μέσα σε μια τυπική θήκη 19 ιντσών. Το μεγαλύτερο μέρος αυτής της δομής είναι ένας πολυλειτουργικός διακομιστής.

Οι πιο δημοφιλείς διακομιστές rack το 2019 είναι οι διακομιστές σειράς HPE ProLiant DL380 Gen10 και οι διακομιστές σειράς Dell PowerEdge R740.

Blade Servers

Ο διακομιστής blade είναι η μονάδα διακομιστή που μπορεί να συνδεθεί στο βασικό πλαίσιο rack. Κάθε μονάδα διακομιστή είναι ένα κεντρικό σύστημα συστήματος, όπως ένας ανεξάρτητος διακομιστής. Σε αυτήν τη λειτουργία, κάθε mainboard εκτελεί το δικό του σύστημα και εξυπηρετεί διαφορετικές ομάδες χρηστών που καθορίζονται και δεν συνδέεται μεταξύ τους. Επομένως η απόδοση μιας μητρικής πλακέτας ενός chip είναι χαμηλότερη, σε σύγκριση με αυτούς τους διακομιστές που είναι τοποθετημένοι σε rack.
Ωστόσο, οι διαχειριστές μπορούν να χρησιμοποιήσουν λογισμικό συστήματος για να συγκεντρώσουν αυτές τις κεντρικές κάρτες σε ένα σύμπλεγμα διακομιστή (εικόνα 3.2).

Εικόνα 3.2

Σε λειτουργία συμπλέγματος, όλες οι κύριες μονάδες μπορούν να συνδεθούν για να παρέχουν ένα περιβάλλον δικτύου υψηλής ταχύτητας, ενώ μοιράζονται πόρους και εξυπηρετούν την ίδια βάση χρηστών. Καθώς κάθε "λεπίδα" (blade) μπορεί να αλλάξει, το σύστημα μπορεί εύκολα να αντικατασταθεί και να ελαχιστοποιηθεί ο χρόνος συντήρησης. Ένας από τους πιο δημοφιλείς διακομιστές σε αυτούς τους τύπους διακομιστών είναι ο Blade HPE ProLiant BL460c.

Tower Servers

Οι διακομιστές Tower είναι stand alone υπολογιστές με αποκλειστικό σκοπό τη λειτουργία σε επίπεδο ενός μόνο διακομιστή. Τοποθετούνται σε αυτόνομο κατακόρυφο ντουλάπι ή «πύργο», σαν τον πύργο ενός προσωπικού επιτραπέζιου υπολογιστή.
Οι διακομιστές Tower παρέχουν τα δικά τους μοναδικά πλεονεκτήματα.
Λόγω της χαμηλής πυκνότητας εσωτερικών στοιχείων, είναι πιο εύκολο να κρυώσουν από τους διακομιστές rack ή blade Ο εγκλεισμένος σχεδιασμός επιτρέπει χώρο για περισσότερο υλικό ή εγκατάσταση μονάδας δίσκου, εάν είναι απαραίτητο (εικόνα 3.3).

Εικόνα 3.3

Ενώ οι διακομιστές blade και οι διακομιστές rack διαθέτουν τακτοποιημένα, αρθρωτά σχέδια rack, οι διακομιστές πύργων είναι πολύ λιγότερο αποδοτικοί ως προς το χώρο λόγω του όγκου που καταλαμβάνουν.

Ένα σύνολο διακομιστών πύργων θα είναι πολύ βαρύτερο και χρονοβόρο από τους λεπτότερους Blade ή Rack διακομιστές τους. Η διαχείριση καλωδίων μπορεί να είναι περίπλοκη και ογκώδης και η ψύξη του αέρα από τους ανεμιστήρες πύργου μπορεί να είναι θορυβώδης.

Mainframes

Ένα Mainframe είναι ένας μεγάλης κλίμακας υπολογιστής με εκλεπτυσμένο σχεδιασμό και υψηλή χωρητικότητα φόρτου εργασίας. Τα κύρια πλαίσια είναι μεγάλα μηχανήματα περίπου στο μέγεθος ενός ψυγείου ή ενός στοιβαγμένου πλυντηρίου και στεγνωτηρίου. Διαθέτουν πληθώρα ανταλλακτικών και είναι πολύ διαμορφώσιμα.

Τα κεντρικά πλαίσια διαχωρίζονται τεχνικά κατηγορηματικά από τους κανονικούς διακομιστές κέντρων δεδομένων, καθώς λειτουργούν γενικά με τα δικά τους μοναδικά λειτουργικά συστήματα και έχουν πολύ μεγαλύτερη ικανότητα απόδοσης (εικόνα 3.4).

Γενικά, τα mainframe χρησιμοποιούνται από βιομηχανίες με υψηλό όγκο δεδομένων λόγω της μεγάλης ανάγκης για αξιόπιστο και ασφαλή υπολογισμό.

Οι κεντρικοί διακομιστές είναι πολύ πιο ακριβοί από οποιονδήποτε άλλο διακομιστή, αλλά είναι απαράμιλλοι στην ανθεκτικότητά τους και στην καθαρή υπολογιστική τους δύναμη.

Λόγω του μεγέθους και της πολυπλοκότητάς τους, οι διακομιστές Mainframe απαιτούν συνεπή συντήρηση από έναν ειδικό τεχνικό. Τα υψηλά κόστη συντήρησης μπορεί να αποτρέψουν έναν οργανισμό να προβεί σε υλοποίηση ενός τέτοιου project. Επομένως είναι πολύ σημαντικό να εκτιμηθεί η κλίμακα των λειτουργιών που θα εκτελέσει για να προσδιοριστεί εάν ένας διακομιστής Mainframe θα είναι επωφελής για την εταιρία.

Εικόνα 3.4

3.2. Αρχιτεκτονικές CPU

Η αρχιτεκτονική της CPU ορίζεται από τα βασικά χαρακτηριστικά και τα κύρια χαρακτηριστικά της CPU. Η αρχιτεκτονική της CPU ονομάζεται μερικές φορές και αρχιτεκτονική σετ εντολών (Instruction Set Architecture - ISA). Στα χαρακτηριστικά της αρχιτεκτονικής των CPU συμπεριλαμβάνονται πράγματα όπως ο αριθμός και οι τύποι των καταχωρητών, οι μέθοδοι αντιμετώπισης της μνήμης και ο βασικός σχεδιασμός και η διάταξη του συνόλου οδηγιών. Δεν περιλαμβάνονται η υλοποίηση, η ταχύτητα εκτέλεσης εντολών, οι λεπτομέρειες της διεπαφής μεταξύ της CPU και των συσχετισμένων κυκλωμάτων υπολογιστών και διάφορες προαιρετικές δυνατότητες. Αυτές οι λεπτομέρειες αναφέρονται συνήθως ως οργανισμός του υπολογιστή. Η αρχιτεκτονική μπορεί να

περιλαμβάνει ή να μην περιλαμβάνει την απουσία ή παρουσία συγκεκριμένων οδηγιών, το μέγεθος της διευθύνσιμης μνήμης ή τα πλάτη δεδομένων που υποβάλλονται σε τακτική επεξεργασία από την CPU. Ορισμένες αρχιτεκτονικές ορίζονται πιο αυστηρά από άλλες. Σημαντικές αρχιτεκτονικές οικογένειες CPU περιλαμβάνουν τη σειρά mainframe της IBM, η οικογένεια Intel x86, η αρχιτεκτονική IBM POWER / PowerPC, η ARM αρχιτεκτονική και η οικογένεια Oracle SPARC. Κάθε ένα από αυτά χαρακτηρίζεται από διάρκεια ζωής άνω των είκοσι ετών. Το πρωτότυπο, η αρχιτεκτονική Mainframe της IBM είναι άνω των σαράντα πέντε ετών.

Οι αρχιτεκτονικές CPU στην αγορά σήμερα είναι παραλλαγές στον παραδοσιακό σχεδιασμό. Αυτές κατηγοριοποιούνται βασικά σε έναν από τους δύο τύπους, το CISC συγκρότημα υπολογιστών με σετ εντολών (Complex Instruction Set Computers) ή RISC υπολογιστές με μειωμένες οδηγίες (Reduced Instruction Set Computers). Στη σύγχρονη εποχή, η διαχωριστική γραμμή μεταξύ των αρχιτεκτονικών CISC και RISC έχει γίνει ολοένα και πιο ασαφής, πολλά από τα χαρακτηριστικά του καθενός έχουν μεταναστεύσει στη διαχωριστική γραμμή. Στην παραπάνω λίστα, το IBM mainframe και x86 CPUs θεωρούνται CISCs. Οι άλλοι θεωρούνται RISCs.

Έχουν γίνει μερικές ενδιαφέρουσες προσπάθειες για τη δημιουργία άλλων τύπων, συμπεριλαμβανομένης μιας στοίβας CPU χωρίς καταχωρητές γενικού σκοπού, αρχιτεκτονική με πολύ μεγάλες λέξεις διδασκαλίας και μια αρχιτεκτονική με σαφείς παράλληλες οδηγίες. Καμία όμως από αυτές τις προσπάθειες δεν ολοκληρώθηκε με επιτυχία. Καθεμία από αυτές τις αρχιτεκτονικές είναι σύμφωνη με τα ευρεία χαρακτηριστικά που ορίζουν έναν υπολογιστή von Neumann.

Ο νόμος του Amdahl

Ο Gene Myron Amdahl, ο οποίος ήταν ένας από τους αρχιτέκτονες των υπολογιστών Mainframe, συμπεριλαμβανομένου του διάσημου IBM System 360, καθόρισε ένα φαινόμενο που με τα χρόνια έγινε ο ακρογωνιαίος λίθος για την αξιολόγηση και την απόδοση επεξεργαστών. Ωστόσο, μπορεί να εφαρμοστεί και σε άλλους κλάδους, όπως μηχανική συστημάτων γενικά.

Ο νόμος του Amdahl δηλώνει ότι οι βελτιώσεις απόδοσης που πρέπει να αποκτηθούν από κάποιο στοιχείο περιορίζεται από το ποσοστό χρόνου χρήσης του στοιχείου αυτού. Αυτός ο νόμος χρησιμοποιείται συνήθως σε καταστάσεις όπου πρέπει να εκτιμήσουμε τις βελτιώσεις απόδοσης που πρέπει να επιτευχθούν προσθέτοντας επιπλέον επεξεργαστές στο σύστημα ή στα σύγχρονα συστήματα που χρησιμοποιούν πολλούς πυρήνες. Ωστόσο, ο νόμος δεν περιορίζεται μόνο σε υπολογιστές και είναι δυνατή η χρήση του σε άλλες ρυθμίσεις που δεν σχετίζονται με υπολογιστές.

Ο τύπος που αντιπροσωπεύει το νόμο είναι:

Υποθέτοντας:

Το F_E είναι το κλάσμα του χρόνου που μπορεί να χρησιμοποιηθεί η βελτίωση.

Το P_E είναι η απόδοση που αποκτά η ενίσχυση.

Τότε ο νέος αναμενόμενος χρόνος εκτέλεσης δίνεται από την παρακάτω σχέση:

$$Execution\ Time_{new} = Execution\ Time_{old} * \left((1 - F_E) + \frac{F_E}{P_E} \right)$$

Χρησιμοποιώντας αυτή τη σχέση είναι εύκολο να υπολογίσουμε την απόδοση

$$Speedup = \frac{Execution\ Time_{old}}{Execution\ Time_{new}} = \frac{1}{\left((1 - F_E) + \frac{F_E}{P_E} \right)}$$

Τύποι επεξεργαστών

Παρόλο που η αφαίρεση (abstraction) χρησιμοποιείται στο σχεδιασμό των επεξεργαστών που στοχεύει στη μείωση του κόστους ενώ διατηρεί κάποιες δυνατότητες, οι οικονομικοί πόροι που εξακολουθούν να απαιτούνται για το σχεδιασμό μιας νέας γενιάς επεξεργαστών είναι τεράστιοι. Αυτό σημαίνει ότι η επιβίωση σε αυτήν την εξαιρετικά ανταγωνιστική αγορά δεν είναι εύκολη και οι κατασκευαστές έπρεπε να αναζητήσουν τρόπους να πουλήσουν όσο το δυνατόν περισσότερους επεξεργαστές για να κερδίσουν κέρδη μέσα από τις επενδύσεις τους. Αυτός είναι ένας από τους κύριους λόγους που πολλές από τις παλιές εταιρείες Mainframe εξαφανίστηκαν και αυτοί που εξακολουθούν να υπάρχουν χρησιμοποιούν επεξεργαστές ευρέως κοινού.
Για να κατανοηθούν καλύτερα αυτές οι τάσεις, πρέπει να ακολουθήσουμε τις τεχνολογικές εξελίξεις από το 1990. Κατά τα πρώτα χρόνια αυτής της δεκαετίας, σημειώθηκε αύξηση του αριθμού των νεοεμφανιζόμενων εταιρειών υπολογιστών. Πολλοί σταθμοί εργασίας σχεδιάστηκαν και πουλήθηκαν σε UNIX και βασίστηκαν σε επεξεργαστές σχεδιασμένους χρησιμοποιώντας μια «νέα» τεχνολογία που ονομάζεται υπολογιστής μειωμένων οδηγιών (Reduced Instruction Set Computer -RISC). Η καινοτομία που εισήγαγε η RISC είναι κυρίως η ικανότητα σχεδιασμού και ανάπτυξης εναλλακτικών επεξεργαστών που είναι γρήγοροι αλλά απλοί και σχετικά φθηνοί στον σχεδιασμό.
Αν και υπήρχαν δεκάδες τέτοιες εταιρείες κατά τη διάρκεια της δεκαετίας του 1990, καθεμία προσπάθησε να επικεντρωθεί σε συγκεκριμένο τμήμα της αγοράς. Οl κυρίαρχες εταιρίες ήταν:

- ✓ Η IBM, η οποία σχεδίασε και κατασκεύασε το PowerPC που αποτελεί μέρος της Power αρχιτεκτονικής, αλλά αρχικά προοριζόταν να τρέξει συστήματα που βασίζονται σε UNIX. Το τσιπ σχεδιάστηκε σε συνεργασία μεταξύ Apple, IBM και Motorola. Χρησιμοποιήθηκε σε συστήματα σχεδιασμένα και κατασκευασμένα και από τις τρεις εταιρείες. Δυστυχώς, στην κύρια αγορά προσωπικών υπολογιστών κυριαρχούν επεξεργαστές της Intel και το νέο chip δεν κατάφερε να αποκτήσει σημαντικό μερίδιο. Παρ 'όλα αυτά, το σύστημα Apple Macintosh χρησιμοποίησε το τσιπ μέχρι το 2006 (όταν η Apple άλλαξε Επεξεργαστές της Intel). Επί του παρόντος, το τσιπ εφαρμόζεται κυρίως σε διάφορες ενσωματωμένες συσκευές υψηλών επιδόσεων (εικόνα 3.5).

- ✓ Η Digital Equipment Corporation (γνωστή ως DEC ή Digital) ήταν μία επιτυχημένη εταιρεία υπολογιστών που εισήγαγε την έννοια των μικροϋπολογιστών. Η DEC εξαγοράστηκε από την Compaq (μια μεγάλη παραγωγός προσωπικών υπολογιστών: συστήματα συμβατά με IBM PC) το 1998. Πριν από αυτήν την απόκτηση, Η DEC σχεδίασε και ανέπτυξε ένα γρήγορο τσιπ 64-bit που ονομάζεται Alpha.

Χρησιμοποιήθηκε κυρίως από συστήματα DEC και δεν υπήρξαν σημαντικές συνεργασίες με άλλους κατασκευαστές συστημάτων υπολογιστών. Αυτό σήμαινε ότι το υψηλό κόστος σχεδιασμού δεν μπορούσε να μοιραστεί με άλλους κατασκευαστές, που μπορεί να συνέβαλαν στα οικονομικά προβλήματα της DEC. Η ίδια η Compaq αγοράστηκε από την HP το 2002, η οποία ακόμη διατηρεί το εμπορικό σήμα κυρίως για τα συστήματα χαμηλού επιπέδου. Πριν από αυτό, λόγω της ύπαρξης της Compaq ένας πελάτης Intel, η τεχνολογία Alpha και τα δικαιώματα πνευματικής ιδιοκτησίας πωλήθηκαν στην Intel, που σηματοδότησε το τέλος της τεχνολογίας.

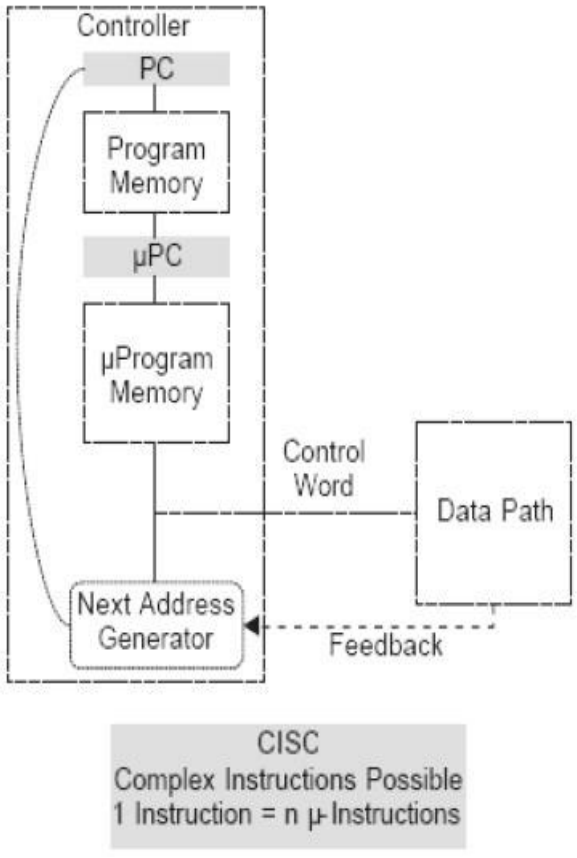
Εικόνα 3.5

- ✓ Η MIPS Computer Systems ήταν μια εταιρεία που σχεδίασε μια οικογένεια τσιπ επεξεργαστών που προορίζονταν τόσο για εμπορικά συστήματα όσο και για διάφορες ενσωματωμένες συσκευές. Οι επεξεργαστές της εταιρείας χρησιμοποιήθηκαν από την SGI (Silicon Graphics, Inc.) μια εταιρεία που κατασκεύαζε τρισδιάστατες λύσεις υψηλών επιδόσεων υπολογιστικών γραφικών. Ως αποτέλεσμα, το 1992 η SGI απέκτησε το MIPS. Δυστυχώς, αρκετά χρόνια αργότερα, η SGI αποφάσισε να αλλάξει σε επεξεργαστές Intel ως κινητήρα για τα συστήματά τους. Το 2013, εξαγοράστηκε από την εταιρεία Imagination προσφέρει ενσωματωμένους επεξεργαστές.
- ✓ Η Sun Microsystems, Inc. ήταν μια άλλη επιτυχημένη εταιρεία που άνοιξε τη βιομηχανία υπολογιστών. Η Sun Microsystems ήταν ένας σημαντικός παράγοντας στην παραγωγή μερικών από τις επί του παρόντος πολύ χρησιμοποιούμενες τεχνολογίες όπως το UNIX, η ιδέα προγραμματισμού Java, το σύστημα αρχείων δικτύου (NFS), η εικονικοποίηση (Virtualization) και διάφορα άλλα. Παρά την επιτυχημένη συμβολή της, η Sun Microsystems αποκτήθηκε από την Oracle Corporation για να παρέχει ένα ολοκληρωμένο σύστημα (hardware / software) βελτιστοποιημένο για μεγάλες επιχειρήσεις, καθώς και συστήματα που βασίζονται σε cloud.
- ✓ Η Intel είναι μια εταιρεία ημιαγωγών που εφηύρε την οικογένεια μικροεπεξεργαστών x86, που είναι η καρδιά των περισσότερων προσωπικών υπολογιστών 32-bit παγκοσμίως. Η γρήγορη τεχνολογική ανάπτυξη στη βιομηχανία προσωπικών υπολογιστών και η παρουσία της Intel σε υλικό επηρέασε εν μέρει τη δραματική επιτυχία της. Αν και υπήρχαν αρκετοί ανταγωνιστές, όπως η AMD, κατά τη διάρκεια της δεκαετίας του 1990, η Intel καθιερώθηκε ως ο κορυφαίος προμηθευτής επεξεργαστών.
- ✓ Η Hewlett-Packard (HP) είναι κατασκευαστής συστημάτων υπολογιστών και περιφερειακών που ιδρύθηκε το 1939. Αν και η εταιρεία είχε τη δική της σειρά επεξεργαστών, αποφάσισε να συνεργαστεί με την Intel για μια νέα σειρά επεξεργαστών (Itanium).

3.2.1.Τεχνολογία CISC

Η τεχνολογία CISC ήταν η κυρίαρχη τεχνολογία στα πρώτα στάδια της πληροφορικής. Η εφαρμογή των μικροοδηγιών παρείχε έναν εύκολο τρόπο καθορισμού και εφαρμογής πρόσθετων νέων οδηγιών. Μερικές από αυτές τις οδηγίες ήταν αρκετά περίπλοκες. Η σύμβαση εκείνη την εποχή ήταν ότι όσο περισσότερο περίπλοκες ήταν οι οδηγίες θα ήταν ευκολότερο για τον μεταγλωττιστή κατά τη μετάφραση των οδηγιών προγραμματισμού υψηλού επιπέδου. Σαφές ήταν ότι όσο περνάει ο χρόνος, οι εφαρμογές θα γίνονται όλο και περισσότερο πολύπλοκες και οι προγραμματιστές θα χρειαστούν πιο στιβαρές οδηγίες. Η έννοια της μικροεκπαίδευσης αποδείχθηκε χρήσιμη. Για το λόγο αυτό, πολλοί κατασκευαστές εφάρμοζαν πολύπλοκες και μερικές φορές περιττές εντολές, με βάση την υπόθεση ότι θα βοηθήσει τους προγραμματιστές και τον μεταγλωττιστή. Στην πραγματικότητα, αυτές οι περίπλοκες εντολές παρείχαν καλύτερη υποστήριξη για υψηλό επίπεδο γλωσσών προγραμματισμού. Λόγω της σχετικής απλότητας στον καθορισμό νέων εντολών, οι υπολογιστές που βασίζονταν στην τεχνολογία CISC είχαν εκατοντάδες διαφορετικές εντολές μηχανής και πολλούς τρόπους αντιμετώπισης. Αυτοί οι τρόποι αντιμετώπισης που καθορίζουν τον τρόπο με τον οποίο οι εντολές διευθύνουν τη μνήμη είναι ένα από τα κύρια χαρακτηριστικά που συμβάλλουν στην πολυπλοκότητα της μεταγλώττισης.

Η εφαρμογή της τεχνολογίας CISC παρείχε έναν καλύτερο τρόπο από την υψηλού επιπέδου γλώσσα προγραμματισμού στις εντολές του μηχανήματος, παρέχοντας έτσι τα μέσα για απλούστερο σχεδιασμό μεταγλωττιστών. Αυτές οι πολύπλοκες εντολές προσέφεραν έναν πιο συμπαγή κώδικα και, ως εκ τούτου, το ποσό της μνήμης που απαιτείται για το πρόγραμμα μειώθηκε. Αυτό ήταν ένα σημαντικό όφελος όταν οι τιμές μνήμης ήταν πολύ υψηλές. Καθώς το κόστος μνήμης μειώθηκε απότομα, αυτό δεν ήταν καθόλου πλεονέκτημα. Η CISC δημιούργησε ορισμένα σοβαρά προβλήματα, τόσο ως προς το κόστος όσο και για την τεχνολογική πρόοδο.



Εικόνα 3.6

Ο επεξεργαστής περιέχει δύο κύρια μέρη. Η ALU (Arithmetic Logic Unit) που είναι υπεύθυνη για εκτέλεση της εντολής και την CU (Control Unit) που είναι υπεύθυνη για τον έλεγχο και τον προγραμματισμό. Η CU παίρνει εντολή από τη μνήμη, την αποκωδικοποιεί, φέρνει τους απαραίτητους τελεστές και μόνο τότε τις στέλνει προς εκτέλεση στην ALU. Με το CISC, η CU πρέπει να γνωρίζει όλες τις εντολές και τους διάφορους τρόπους αντιμετώπισης, καθώς και γνώση του χρόνου που απαιτείται για την εκτέλεση κάθε εντολής.

Ως εκ τούτου η επόμενη εντολή δεν μπορεί να ξεκινήσει πριν από την ολοκλήρωση της προηγούμενης εντολής (εικόνα 3.6).

Αν και η CISC παρείχε κάποια πλεονεκτήματα εκείνη τη στιγμή, η περίπλοκη φύση των εντολών και ο τρόπος αντιμετώπισή τους οδήγησαν την ίδια την CU να γίνει πολύ περίπλοκη. Το μεγαλύτερο μέρος της λογικής των επεξεργαστών ήταν στην CU και κάθε νέα εντολή που εφαρμόστηκε πρόσθεσε νέα επίπεδα πολυπλοκότητας. Ακόμα και τα μήκη των εντολών, σε όρους χρήσης μνήμης, προκάλεσαν κάποιο βαθμό πολυπλοκότητας. Μια εντολή που χρησιμοποιεί καταχωρητές ως τελεστές μπορεί να είναι πολύ σύντομη (μόνο 2-3 byte), ενώ οι εντολές που περιέχουν άμεσο τελεστή (που αποθηκεύεται ως μέρος της εντολής) πρέπει να είναι μεγαλύτερη. Επιπλέον, ορισμένες εντολές, όπως η εντολή Scaled, περιέχει δύο άμεσους τελεστές, οπότε εξ ορισμού θα πρέπει να είναι ακόμη μεγαλύτερη. Αυτό σημαίνει ότι η CU πρέπει να υπολογίσει τον αριθμό των byte που χρειάζεται για κάθε εντολή. Αρχίζει διαβάζοντας την εντολή, την αποκωδικοποιεί και μόνο μετά την ολοκλήρωση του σταδίου αποκωδικοποίησης, η CU γνωρίζει τη μορφή της μεταγλώττισης και πόσα byte απαιτεί.

Η ίδια διαδικασία επαναλαμβάνεται με την προετοιμασία των απαιτούμενων τελεστών. Μερικές φορές οι τελεστές ήταν σε μητρώα, και σε τέτοιες περιπτώσεις, η λήψη είναι απλή. Ωστόσο, σε κάποιες άλλες φορές, οι τελεστές ήταν στη μνήμη και η CU έπρεπε να υπολογίσει τις θέσεις τους. Αυτό αντιφάσκει με την αρχική ιδέα ότι η ALU είναι υπεύθυνη για τους υπολογισμούς και η CU ελέγχει τις λειτουργίες, αφού η CU έπρεπε να έχει απλές δυνατότητες υπολογισμών επίσης. Αποδεικνύεται ότι η πλειονότητα της λογικής και της πολυπλοκότητας των επεξεργαστών CISC ήταν στην CU. Αυτή η πολυπλοκότητα εκδηλώθηκε με υψηλότερο κόστος που σχετίζεται με το σχεδιασμό νέων επεξεργαστών, οι οποίοι επιβράδυναν τις τεχνολογικές εξελίξεις. Αυτά τα προβλήματα πυροδότησαν την ανάπτυξη μιας νέας τεχνολογίας υπολογιστών - RISC.

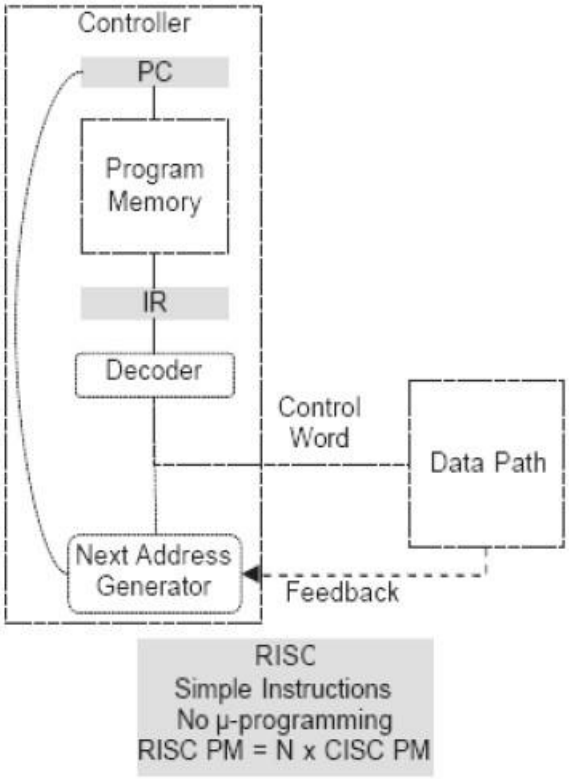
3.3.2.Τεχνολογία RISC

Η τεχνολογία RISC συζητείται εδώ και πολύ καιρό και ορισμένα από τα mainframe της δεκαετίας του 1960 το χρησιμοποίησαν μερικώς. Ωστόσο, άνθισε μόνο κατά τη δεκαετία του 1990. Αφορμή για τη χρήση αυτής της «νέας» τεχνολογίας οφείλεται κυρίως στα προβλήματα που σχετίζονται με τη CISC και την κατανόηση ότι το οι σύνθετες οδηγίες CISC χρησιμοποιήθηκαν σπάνια. Επιπλέον, λόγω των γενικών εξόδων που προκύπτουν από αυτές τις περίπλοκες εντολές, δεν ήταν σαφές εάν είναι πραγματικά πιο γρήγορες σε σύγκριση με έναν απλούστερο βρόχο εντολών (εικόνα 3.7).

Η τεχνολογία RISC βασίζεται σε διάφορες αρχές:

- ✓ Υπάρχει περιορισμένος αριθμός εντολών (αρκετές δεκάδες).
- ✓ Οι εντολές είναι απλές
- ✓ Όλες οι εντολές έχουν το ίδιο μήκος (byte στη μνήμη)
- ✓ Οι χρόνοι εκτέλεσης όλων των εντολών είναι ίδιοι
- ✓ Υπάρχουν πολλοί καταχωρητές για την ελαχιστοποίηση της σχετικά βραδύτερης πρόσβασης στη μνήμη
- ✓ Υπάρχουν μόνο λίγες ελάχιστες λειτουργίες διευθύνσεων
- ✓ Οι μεταγλωττιστές πρέπει να είναι πιο εξελιγμένοι για την εκτέλεση βελτιστοποιήσεων κώδικα και τη χρήση καταχωρητών με έξυπνο τρόπο.

Η ιδέα που προώθησε την τεχνολογία RISC ήταν ότι το λογισμικό παρέχει πολύ πιο γρήγορα πορεία ανάπτυξης. Αν και οι σχεδιαστές υλικού έχουν δανειστεί αρχές που χρησιμοποιούνται από τους μηχανικούς λογισμικού, όπως η αρθρωτή σχεδίαση και η απλότητα, είναι συνήθως πιο γρήγορο να χειριστείς ορισμένα από αυτά τα ζητήματα με λογισμικό.



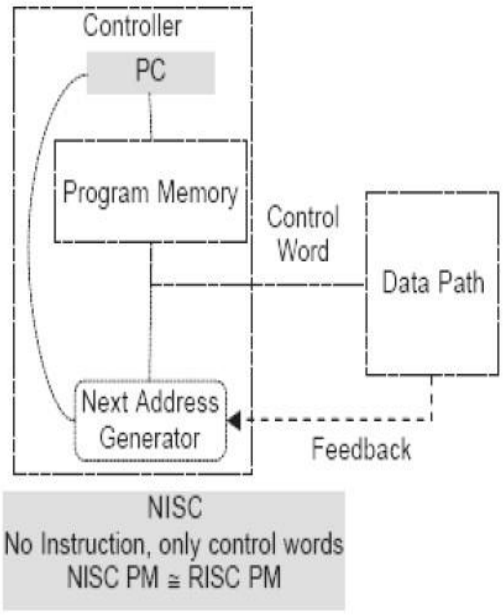
Εικόνα 3.7

Όταν ήταν σαφές ότι η CU έγινε πολύπλοκη και επιβραδύνει την τεχνολογία ανάπτυξης, ήρθε η ώρα για μια αλλαγή. Ενεργοποιήθηκαν νέες εξελίξεις στη μηχανική λογισμικού, απλοποίηση της αρχιτεκτονικής, ειδικά της CU, και ενίσχυση της ευελιξίας του μεταγλωττιστή και της πολυπλοκότητας. Η εφαρμογή της τεχνολογίας RISC παράγει περισσότερες οδηγίες ανά πρόγραμμα που καταρτίζεται. Αυτό σημαίνει ότι το πρόγραμμα θα απαιτήσει περισσότερη μνήμη. Ωστόσο, ο σχεδιασμός των επεξεργαστών είναι απλούστερος και φθηνότερος, ειδικά όσον αφορά τη CU. Οι ομοιόμορφοι χρόνοι εκτέλεσης παρέχουν έναν μηχανισμό για την εκτέλεση της εντολής σε αγωγό (pipeline). Η ιδέα του αγωγού είναι ένα σημαντικό ενισχυτικό απόδοσης, το οποίο παρέχει τη δυνατότητα εκτέλεσης μιας εντολής σε κάθε κύκλο ρολογιού. Δυστυχώς, για αντικειμενικούς λόγους, υπάρχει ένα κενό μεταξύ των προγραμματισμένων αρχών και αυτών εκτέλεση. Για παράδειγμα, είναι αδύνατο να υπάρχουν παρόμοιοι χρόνοι εκτέλεσης όταν ορισμένες εντολές είναι πολύ απλές, όπως IF ή πρόσθεση ακεραίων ADD και άλλες είναι πιο περίπλοκες όπως το DIVIDE.
Αυτά τα προβλήματα ξεπεράστηκαν με το διαχωρισμό των εκτελέσιμων εντολών εκτέλεσης σε διάφορα τμήματα για να επίτευξη του ίδιου αποτελέσματος.

3.2.3. Τεχνολογία NISC

Οι προηγμένες αρχιτεκτονικές υπολογιστών για επεξεργαστές σε συγκεκριμένες εφαρμογές στοχεύουν στην προσαρμογή της αναδυόμενης απαίτησης ευελιξίας καθώς και στην επίτευξη της καλύτερης απόδοσης. Ένας τέτοιος συνδυασμός ευελιξίας και συνεχώς αυξανόμενων απαιτήσεων απόδοσης απαιτεί προσέγγιση σχεδιασμού που παρέχει καλύτερους τρόπους ελέγχου και διαχείρισης των πόρων υλικού.
Πρόσφατα, η ιδέα ενός επεξεργαστή αφιερωμένου σε μια εφαρμογή που δεν χρησιμοποιεί ένα σύνολο εντολών έχει εισαχθεί με το όνομα No-Instruction-Set-Computer (NISC). Η κύρια πρόταση της προσέγγισης NISC είναι ότι δεν υπάρχει ανάγκη χρήσης ενός συνόλου εντολών όταν το υλικό προγραμματίζεται από τους σχεδιαστές του και όχι από τους χρήστες του. Το NISC απλοποιεί την προσέγγιση Application Specific Instruction Set Processor – ASIP(Η προσέγγιση του σχεδιασμού προσαρμοσμένων

επεξεργαστών βασίζεται στην έννοια του Επεξεργαστή σετ συγκεκριμένων οδηγιών) καταργώντας το πλήρες έργο εύρεσης και σχεδιασμού «πιο κερδοφόρων» προσαρμοσμένων οδηγιών. Η εξάλειψη του συνόλου οδηγιών αυξάνει την παραγωγικότητα του σχεδιαστή και συρρικνώνει το χρόνο προς την αγορά. Το υλικό απλοποιείται λόγω της παράλειψης του αποκωδικοποιητή εντολών που μειώνει την πολυπλοκότητα και βελτιώνει την απόδοση. Όλες οι σημαντικές εργασίες του τυπικού ελεγκτή επεξεργαστή (αποκωδικοποίηση εντολών, ανάλυση εξάρτησης, προγραμματισμός εντολών κ.λπ.) εκτελούνται από τον μεταγλωττιστή στατικά κατά το χρόνο σύνταξης. Ο μεταγλωττιστής, ο οποίος δεν περιορίζεται από το μέγεθος, τους πόρους των chip ή τους περιορισμούς χρονισμού, δημιουργεί τις λέξεις ελέγχου (CWs) που πρέπει να εφαρμόζονται σε στοιχεία datapath κατά το χρόνο εκτέλεσης σε κάθε κύκλο ρολογιού και τα φορτώνει σε μια μνήμη ελέγχου. Κατά τον χρόνο εκτέλεσης, ο ελεγκτής φορτώνει μόνο τα CW και τα εφαρμόζει στο datapath.



Εικόνα 3.8

Η ιδέα της NISC προσφέρει μια εντελώς νέα προσέγγιση για το σχεδιασμό προσαρμοσμένων επεξεργαστών. Όπως φαίνεται στην εικόνα 3.8 σχήμα η τεχνολογία NISC διαγράφει εντελώς το στάδιο αποκωδικοποίησης και αποθηκεύει τη λέξη ελέγχου στο PM.

Η τεχνολογία NISC είναι παραμετροποιήσιμη και αναδιαμορφώσιμη, το οποίο επιτρέπει πολύ καλό συντονισμό σε οποιαδήποτε εφαρμογή και απόδοση. Εξαλείφει τις οδηγίες για να διευκολύνει την ταχύτερη εκτέλεση και την καλύτερη προσαρμογή της διαδικασίας. Ο μεταγλωττιστής NISC, χωρίς instruction, έχει πλήρη έλεγχο όλων των εξαρτημάτων και συνδέσεων στο datapath που του επιτρέπει να επιτύχει καλύτερη χρήση πόρων και ένα σύνολο εργαλείων NISC κατάλληλο για όλα τα πιθανά δεδομένα κατά την επεξεργασία.

3.2.4. Πλεονεκτήματα – Μειονεκτήματα τεχνολογιών CISC, RISC, NISC

Στους παρακάτω πίνακες αναφέρονται επιγραμματικά τα πλεονεκτήματα και τα μειονεκτήματα της εκάστοτε τεχνολογίας στις αρχιτεκτονικές επεξεργαστών.

Τεχνολογία CISC	
Πλεονεκτήματα	***Μειονεκτήματα***
Έμφαση στο υλικό	Για την ενσωμάτωση παλαιότερων instructions sets σε νέες γενιές του οι επεξεργαστές τείνουν να δείχνουν αυξανόμενη πολυπλοκότητα

Περιλαμβάνει πολυλειτουργικό συγκρότημα οδηγιών (instructions)	Πολλές εξειδικευμένες οδηγίες CISC δεν χρησιμοποιήθηκαν αρκετά συχνά για να δικαιολογήσουν την ύπαρξή τους
Μνήμη σε μνήμη: LOAD και STORE ενσωματωμένες στις οδηγίες	Επειδή κάθε εντολή CISC πρέπει να μεταφραστεί από τον επεξεργαστή σε δεκάδες ή ακόμη και εκατοντάδες γραμμές μικροκώδικα, τείνει να λειτουργεί πιο αργά από μια αντίστοιχη σειρά απλούστερων εντολών που δεν απαιτούν τόσο μεγάλη μετάφραση
Μικρά μεγέθη κώδικα και υψηλούς κύκλους ανά δευτερόλεπτο	
Τρανζίστορ τα οποία χρησιμοποιούνται για την αποθήκευση σύνθετων οδηγιών	

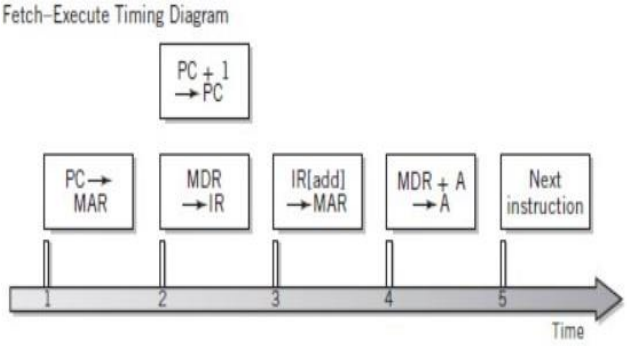
Τεχνολογία RISC	
Πλεονεκτήματα	***Μειονεκτήματα***
Σχετικά λίγες εντολές	Απαιτούνται λίγες εντολές
Σχετικά λίγες διευθύνσεις	Απαιτείται λογική αποκωδικοποίησης
Πρόσβαση στη μνήμη που περιορίζεται στις εντολές LOAD και STORE	Η Control Unit επειδή είναι σε επίπεδο hardware δεν αλλάζει δυναμικά
Όλες οι λειτουργίες πραγματοποιούνται με τους καταχωρητές της CPU	
Μορφή εντολών σταθερού μήκους, εύκολα αποκωδικοποιημένη	
Εκτέλεση εντολών ενός κύκλου	
Καλύτερος έλεγχος σε επίπεδο hardware από ότι σε μικροπρογραμματισμένο έλεγχο	

Τεχνολογία NISC	
Πλεονεκτήματα	***Μειονεκτήματα***
Επιτρέπει την εξαφάνιση της διάκρισης μεταξύ SW και HW υλοποίησης. Για υλοποίηση HW οι λέξεις ελέγχου είναι σε λογική ROM ή πύλης, ενώ για υλοποίηση σε SW βρίσκονται στη μνήμη RAM	Η τεχνολογία NISC δεν υποστηρίζει τις τυπικές βιβλιοθήκες της εφαρμογής C
Γρηγορότερη δυνατή εκτέλεση, δεδομένου ότι το datapath μπορεί να πραγματοποιηθεί μέσω τεχνικής pipelining σε οποιουδήποτε αριθμό στάδια και δεδομένου ότι το datapath μπορεί να έχει οποιοδήποτε επίπεδο παραλληλισμού	Ο προγραμματισμός είναι σε ANSI C
Επειδή δεν υπάρχει σύνολο εντολών, το NISC μειώνει το τελευταίο στάδιο ερμηνείας μεταξύ κώδικα μηχανής και HW. Εδώ ο κωδικός μηχανής εκτελείται απευθείας στο HW, δηλαδή datapath	Η ύπαρξη λίγων περιορισμών στο πρόγραμμα εισόδου C, τους pointers λειτουργίας και τον global pointer.
Η τεχνολογία NISC μπορεί μιμηθεί οποιοδήποτε σύνολο εντολών, δεδομένου ότι η λέξη ελέγχου NISC μπορεί να εκτελέσει οποιαδήποτε λειτουργία εφόσον οι πόροι του datapath στο datapath είναι διαθέσιμοι. Επομένως οποιοσδήποτε κώδικας παλαιού τύπου μπορεί να εκτελεστεί σε ένα σωστά καθορισμένο NISC με τη μετατροπή παλαιού τύπου εντολών σε λέξεις ελέγχου NISC μέσω πίνακα κλήσεων	Οι αρχικοποιήσεις δεν υποστηρίζονται επί του παρόντος στο NISC για συντήρηση, δοκιμές και πολλές άλλες πτυχές σχεδιασμού του συστήματος με παρόμοιο τρόπο όπως οι βιβλιοθήκες πύλης οδήγησαν στην τυποποίηση του ψηφιακού σχεδιασμού στο παρελθόν
Ο μεταγλωττιστής NISC χρησιμοποιεί τη σύνθεση αλγορίθμων υψηλού επιπέδου για την κάλυψη του δέντρου ανάλυσης με λέξεις ελέγχου	
Καθώς η τεχνολογία NISC είναι μία επαρκής τεχνολογία για κάθε	

υπολογισμό χρειάζεται μόνο ένας μεταγλωττιστής παγκοσμίως	
Μόνο ένας επεξεργαστής τεχνολογίας NISC, ακόμη και σε διαφορετικές εκδόσεις και με διαφορετικές παραμέ-τρους, χρειάζεται παγκοσμίως και έτσι μια τέτοια μοναδικότητα θα μπορούσε να απλοποιήσει την εκπαίδευση, το σχεδιασμό, το εμπόριο, συντήρηση, τις δοκιμές και πολλές άλλες πτυχές του σχεδιασμού συστήματος, με παρόμοιο τρόπο όπως οδήγησαν οι βιβλιοθήκες πύλης στην τυποποίηση του ψηφιακού σχεδιασμού πρόσφατα	

3.2.5. Τεχνική Pipelining

Στην εικόνα 3.9 υπάρχουν δύο στάδια για την εκτέλεση των φάσεων του κύκλου μεταγλώττισης. Εάν κάθε στάδιο εφαρμόζεται ξεχωριστά, έτσι ώστε η κάθε εντολή να περνά απλά από το ένα στάδιο στο άλλο καθώς εκτελείται, μόνο ένα στάδιο χρησιμοποιείται σε κάθε δεδομένο χρόνο. Εάν υπάρχουν περισσότερα βήματα στον κύκλο, το ίδιο ισχύει ακόμα.



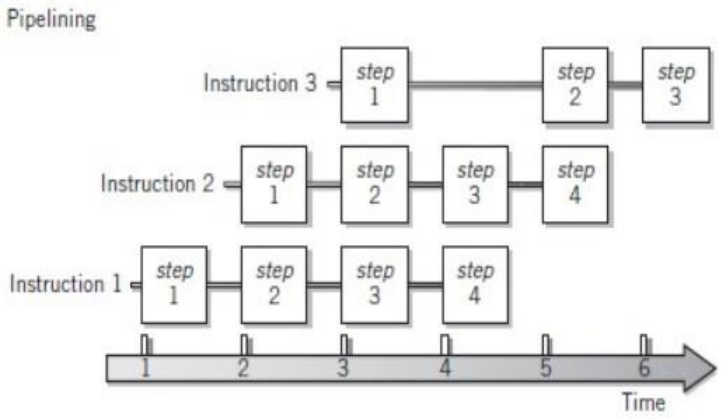
Εικόνα 3.9

Έτσι, για να επιταχυνθεί η επεξεργασία ακόμη περισσότερο, οι σύγχρονοι υπολογιστές αλληλεπικαλύπτονται με εντολές, ώστε να υπάρχουν περισσότερες από μία εντολές που τρέχουν κάθε φορά. Αυτή η μέθοδος είναι γνωστή ως αγωγός. Η ιδέα των σωληνώσεων είναι μία από τις σημαντικές εξελίξεις στον σύγχρονο σχεδιασμό υπολογιστών. Ήταν υπεύθυνη για μεγάλες αυξήσεις στο ταχύτητα εκτέλεσης προγράμματος. Στην απλούστερη μορφή του, η ιδέα της σωληνώσεως είναι ότι καθώς κάθε εντολή ολοκληρώνει ένα βήμα, οι ακόλουθες εντολές μετακινούνται στο στάδιο που μόλις ελευθερώθηκε. Έτσι, όταν είναι η πρώτη εντολή ολοκληρωθεί, το επόμενο είναι ήδη ένα στάδιο πριν από την ολοκλήρωση. Εάν υπάρχουν πολλά βήματα στον κύκλο λήψης-εκτέλεσης, μπορούμε να έχουμε πολλές εντολές σε διάφορα σημεία του κύκλου. Η τεχνική των σωληνώσεων οδηγεί σε μια μεγάλη συνολική αύξηση του μέσου όρου αριθμού εντολών που εκτελέστηκαν σε δεδομένο χρόνο.

Μια εντολή κλάδου μπορεί να ακυρώσει όλες τις εντολές που βρίσκονται σε εξέλιξη στιγμιαία εάν ο κλάδος έχει ληφθεί και ο υπολογιστής πρέπει να έχει τα δεδομένα από προηγούμενη εντολή, εάν η επόμενη εντολή το απαιτεί για να προχωρήσει. Οι σύγχρονοι υπολογιστές χρησιμοποιούν μια ποικιλία τεχνικών για την αντιστάθμιση του προβλήματος διακλάδωσης.

Μια κοινή προσέγγιση είναι η διατήρηση δύο ή περισσοτέρων ξεχωριστών αγωγών έτσι ώστε οι εντολές και από τα δύο πιθανά αποτελέσματα να μπορούν να υποστούν επεξεργασία έως ότου η κατεύθυνση του κλάδου είναι σαφής. Μια άλλη προσέγγιση ,που προσπαθεί να προβλέψει το πρόβλημα της αναμονής για αποτελέσματα δεδομένων από προηγούμενες εντολές μπορεί να μετριαστεί με το διαχωρισμό των εντολών έτσι ώστε να μην εκτελούνται η μία μετά την άλλη.

Πολλοί σύγχρονοι υπολογιστές σχεδιάζονται ώστε να περιέχουν λογική που να μπορούν να αναδιατάξουν τις εντολές καθώς εκτελούνται για να διατηρήσουν τους αγωγούς πλήρης και για ελαχιστοποίηση καταστάσεων όπου απαιτείται καθυστέρηση. Η αναδιάταξη των εντολών δίνει την δυνατότητα επίσης να παρέχονται παράλληλοι αγωγοί, με διπλή λογική CPU, έτσι ώστε πολλές εντολές να μπορούν να εκτελεστούν ταυτόχρονα (εικόνα 3.10).



Εικόνα 3.10

Ο σωληνώσεις και η αναδιάταξη των εντολών περιπλέκουν τα ηλεκτρονικά κυκλώματα που απαιτούνται για το υπολογιστή και επίσης απαιτούν προσεκτική σχεδίαση για να εξαλειφθεί η πιθανότητα να εμφανιστούν σφάλματα και ασυνήθιστες ακολουθίες εντολών.

3.2.6. Οργάνωση επεξεργαστών Scalar και Superscalar

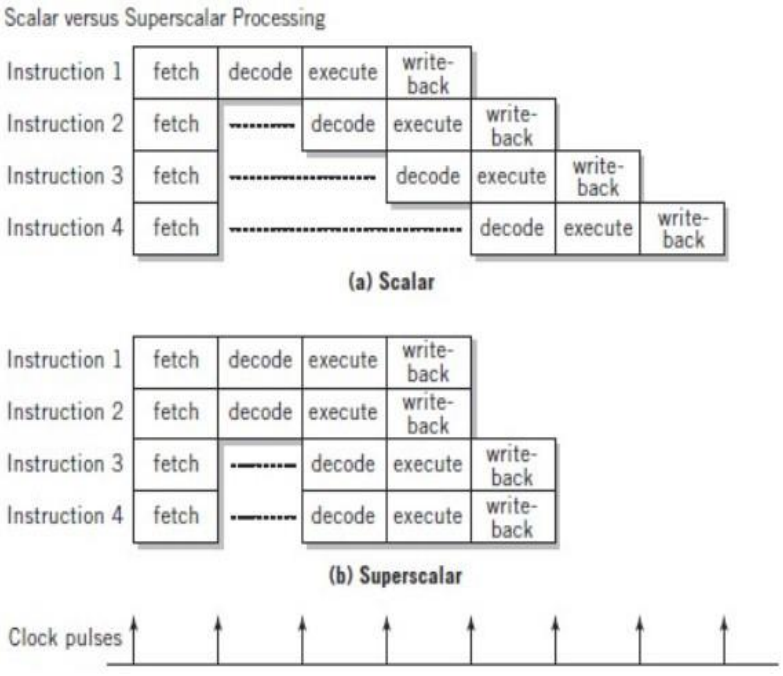
Όπως αναφέρθηκε και στην προηγούμενη ενότητα οι σύγχρονοι επεξεργαστές επιτυγχάνουν υψηλή απόδοση έως διαχωρίζοντας τις δύο κύριες φάσεις του κύκλου λήψης-εκτέλεσης σε ξεχωριστά στοιχεία, στη συνέχεια διαχωρίζοντας περαιτέρω τη φάση εκτέλεσης σε έναν αριθμό ανεξάρτητων μονάδων εκτέλεσης, καθεμία με ικανότητα αγωγού. Μόλις γεμίσει ένας αγωγός, μια μονάδα εκτέλεσης μπορεί να ολοκληρώσει μια εντολή με κάθε ρολόι. Με έναν αγωγό μονάδας εκτέλεσης, αγνοούνται οι τρύπες στον αγωγό από διαφορετικούς τύπους εντολών και συνθήκες διακλάδωσης. Η CPU μπορεί κατά μέσο όρο εντολή εκτέλεση περίπου ίση με την ταχύτητα ρολογιού του μηχανήματος. Ένας επεξεργαστής που έχει αυτή τη δυνατότητα ονομάζεται επεξεργαστής κλιμάκωσης (Scalar Processor).

Με πολλαπλές μονάδες εκτέλεσης είναι δυνατή η επεξεργασία εντολών παράλληλα, με μέσο ρυθμό περισσότερες από μία οδηγίες ανά κύκλο ρολογιού. Η ικανότητα εκτέλεσης περισσοτέρων από μία εντολών ανά κύκλο ρολογιού είναι γνωστή ως υπερβαθμική επεξεργασία (Superscalar Processor).

Η Superscalar επεξεργασία είναι ένα τυπικό χαρακτηριστικό των σύγχρονων CPU. Η δυνατότητα επεξεργασίας Superscalar αυξάνει την απόδοση στο διπλάσιο ή και περισσότερο. Συνήθως, οι σημερινές CPU παράγουν ταχύτητες μεταξύ δύο και πέντε φορές παραπάνω (εικόνα 3.11).

Είναι σημαντικό το ότι οι τεχνικές επεξεργασίας σωληνώσεων και υπερβαθμών δεν επηρεάζουν τον χρόνο κύκλου οποιασδήποτε μεμονωμένης εντολής.

Μια εντολή ανάκτησης - εκτέλεση κύκλου που απαιτεί έξι κύκλους ρολογιού από την αρχή έως το τέλος θα απαιτήσει έξι κύκλους ρολογιού είτε εκτελούνται εντολές μία κάθε φορά ή σωληνώνονται παράλληλα με δώδεκα άλλες εντολές. Έτσι ο μέσος χρόνος κύκλου μεταγλώττισης βελτιώνεται εκτελώντας κάποια μορφή παράλληλης εκτέλεσης.



Εικόνα 3.11

Εάν μια μεμονωμένη εντολή πρέπει να ολοκληρωθεί για οποιονδήποτε λόγο προτού εκτελεστεί άλλη, η CPU πρέπει να σταματήσει για ολόκληρο τον κύκλο της πρώτης εντολής.

Η Superscalar επεξεργασία περιπλέκει σημαντικά το σχεδιασμό μιας CPU. Υπάρχει ένας αριθμός δύσκολων τεχνικών ζητημάτων που πρέπει να επιλυθούν για να είναι δυνατή η εκτέλεση πολλαπλών εντολών ταυτόχρονα. Τα πιο σημαντικά από αυτά είναι:

- Προβλήματα που προκύπτουν από οδηγίες που συμπληρώνονται με λάθος σειρά
- Αλλαγές στη ροή του προγράμματος λόγω των εντολών του κλάδου
- Συγκρούσεις για εσωτερικούς πόρους CPU, ιδιαίτερα για καταχωρητές γενικού σκοπού.

3.2.7. Η εξέλιξη της αρχιτεκτονικής Intel x86

Η αρχιτεκτονική x86 ενσωματώνει τις εξελιγμένες αρχές σχεδίασης που βρίσκονταν μόνο σε Mainframes και υπερυπολογιστές και χρησιμεύει ως ένα εξαιρετικό παράδειγμα σχεδιασμού CISC. Η Intel κατατάσσεται ως ο νούμερο ένα κατασκευαστής μικροεπεξεργαστών για μη ενσωματωμένα συστήματα. για δεκαετίες, μια θέση που φαίνεται απίθανο να αποδώσει. Οι μικροεπεξεργαστές χρησιμεύουν ως ένας καλός δείκτης της εξέλιξης της τεχνολογίας των υπολογιστών γενικά.
Μερικά από τα κυριότερα σημεία της εξέλιξης της σειράς προϊόντων Intel:

- **8080**: Ο πρώτος μικροεπεξεργαστής γενικού σκοπού στον κόσμο. Αυτό ήταν ένα μηχάνημα 8-bit, με 8-bit διαδρομή δεδομένων (datapath) στη μνήμη. Το 8080 χρησιμοποιήθηκε στον πρώτο προσωπικό υπολογιστή, το Altair.

- **8086**: Ένα πολύ πιο ισχυρό μηχάνημα των 16-bit. Εκτός από μια ευρύτερη διαδρομή δεδομένων και μεγαλύτερους καταχωρητές, το 8086 εμφάνισε μια κρυφή μνήμη εντολών (cache) ή μια ουρά, που προκαθορίζει μερικές οδηγίες πριν εκτελεστούν. Μια

παραλλαγή αυτού του επεξεργαστή, το 8088, χρησιμοποιήθηκε στον πρώτο προσωπικό υπολογιστή της IBM, διασφαλίζοντας την επιτυχία της Intel. Το 8086 είναι η πρώτη εμφάνιση της αρχιτεκτονικής x86.

- **80286**: Αυτή η επέκταση του 8086 ενεργοποίησε τη διεύθυνση μνήμης 16 MB αντί για 1 MB.

- **80386**: Η πρώτη μηχανή 32-bit της Intel και μια σημαντική αναθεώρηση του προϊόντος της. Με αρχιτεκτονική 32-bit, το 80386 ανταγωνίστηκε την πολυπλοκότητα και τη δύναμη των μικροϋπολογιστών και των Mainframes που εισήχθησαν μόλις ένα στην αγορά λίγα χρόνια νωρίτερα. Αυτός ήταν ο πρώτος επεξεργαστής Intel που υποστήριζε πολλαπλές εργασίες, που σημαίνει ότι θα μπορούσε να εκτελέσει πολλαπλά προγράμματα ταυτόχρονα.

- **80486**: Το 80486 εισήγαγε τη χρήση πολύ πιο εξελιγμένης και ισχυρής τεχνολογίας cache και εξελιγμένες εντολές pipelining. Το 80486 προσέφερε επίσης έναν ενσωματωμένο μαθηματικό συνεπεξεργαστή, ο οποίος εκτελούσε σύνθετες μαθηματικές λειτουργίες από την κύρια CPU.

- **Pentium**: Με τον Pentium, η Intel εισήγαγε τη χρήση τεχνικών superscalar, οι οποίες επιτρέπουν πολλαπλές εντολές για παράλληλη εκτέλεση.

- **Pentium Pro**: Ο Pentium Pro συνέχισε τη μετάβαση σε οργάνωση superscalar που ξεκίνησε με το Pentium, με επιθετική χρήση της μετονομασίας μητρώου, πρόβλεψη κλάδου και ανάλυση ροής δεδομένων.

- **Pentium II**: Ο Pentium II ενσωμάτωσε την τεχνολογία Intel MMX, η οποία σχεδιάστηκε ειδικά για να επεξεργάζεται αποτελεσματικά τα δεδομένα βίντεο, ήχου και γραφικών.

- **Pentium III**: Ο Pentium III ενσωματώνει επιπλέον οδηγίες κινητής υποδιαστολής: Το Streaming SIMD Extensions (SSE) πρόσθεσε 70 νέες οδηγίες σχεδιασμένες για αύξηση απόδοσης όταν ακριβώς οι ίδιες λειτουργίες πρόκειται να εκτελεστούν σε πολλά αντικείμενα δεδομένων. Τυπικές εφαρμογές είναι η επεξεργασία ψηφιακού σήματος και η επεξεργασία γραφικών.

- **Pentium 4**: Το Pentium 4 περιλαμβάνει επιπλέον κινητά σημεία και άλλες βελτιώσεις για πολυμέσα.

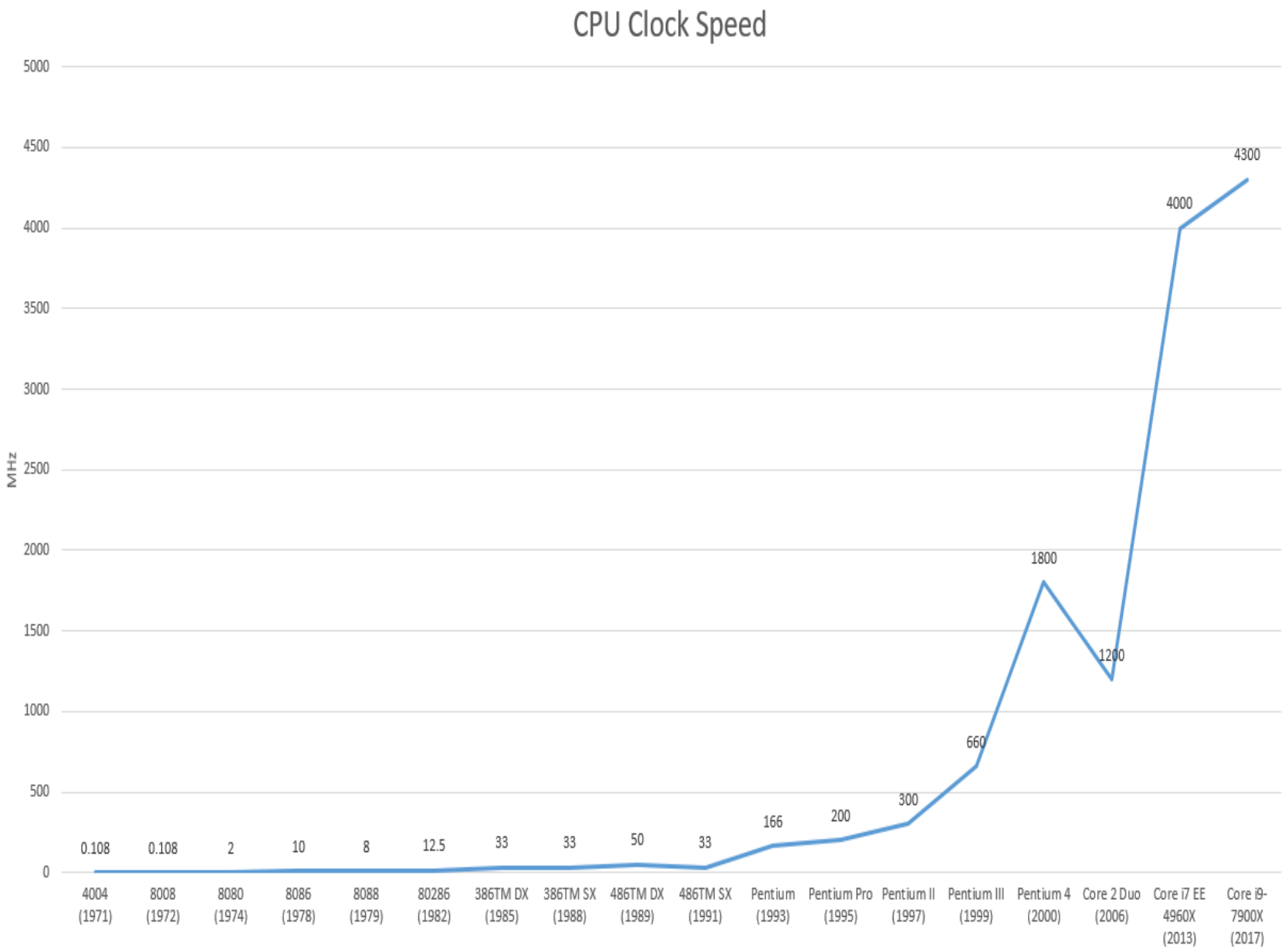
- **Core**: Αυτός είναι ο πρώτος μικροεπεξεργαστής Intel x86 με διπλό πυρήνα, όπου ενσωμάτωνε στην υλοποίησή του δύο πυρήνες σε ένα μόνο τσιπ.

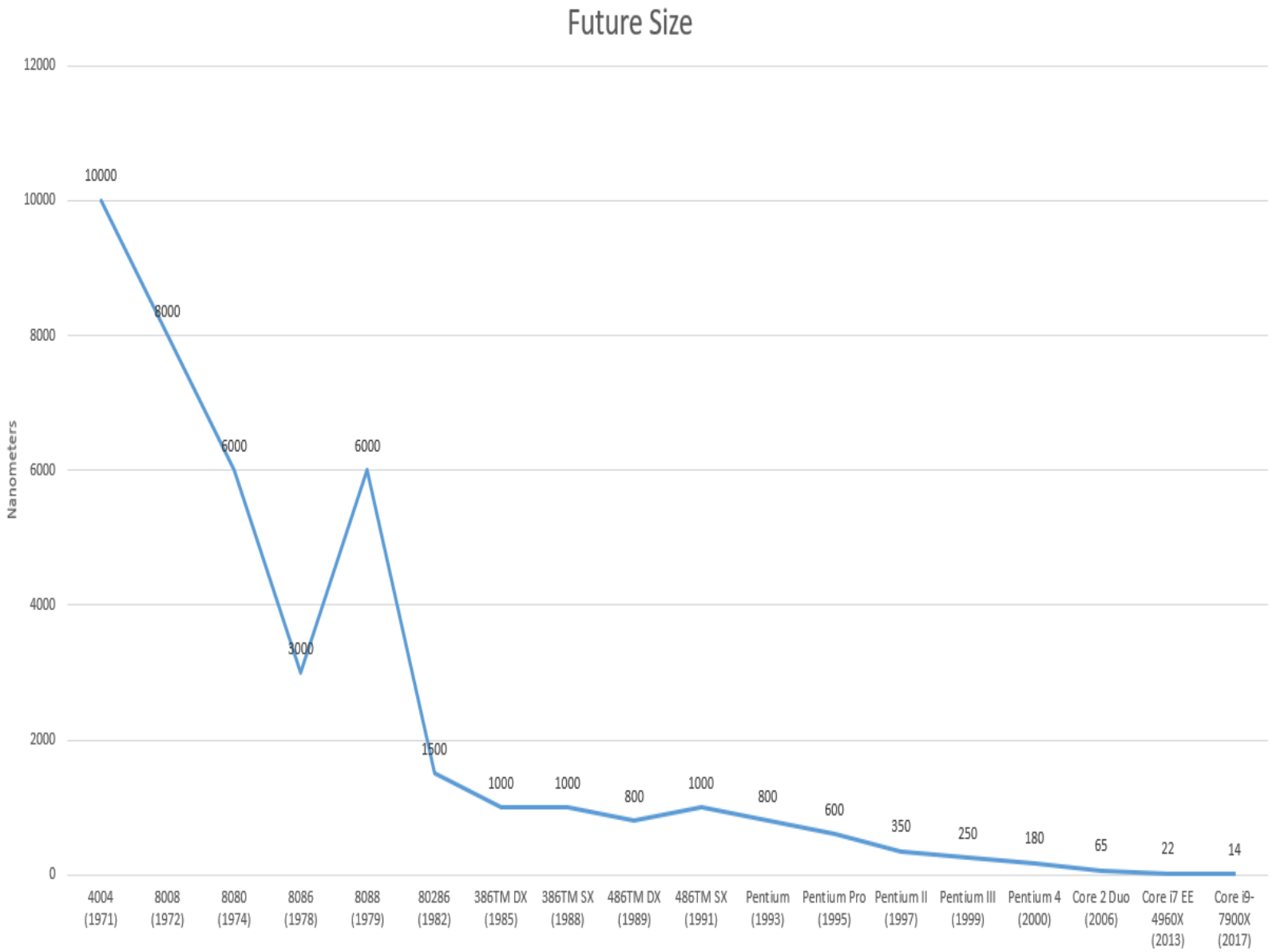
- **Core 2**: Ο Core 2 επεκτείνει την αρχιτεκτονική Core σε 64 bit. Το Core 2 Quad παρέχει τέσσερις πυρήνες σε ένα μόνο τσιπ. Οι πιο πρόσφατες υλοποιήσεις Core έχουν έως και 10 πυρήνες ανά τσιπ. Μια σημαντική προσθήκη στην αρχιτεκτονική ήταν το

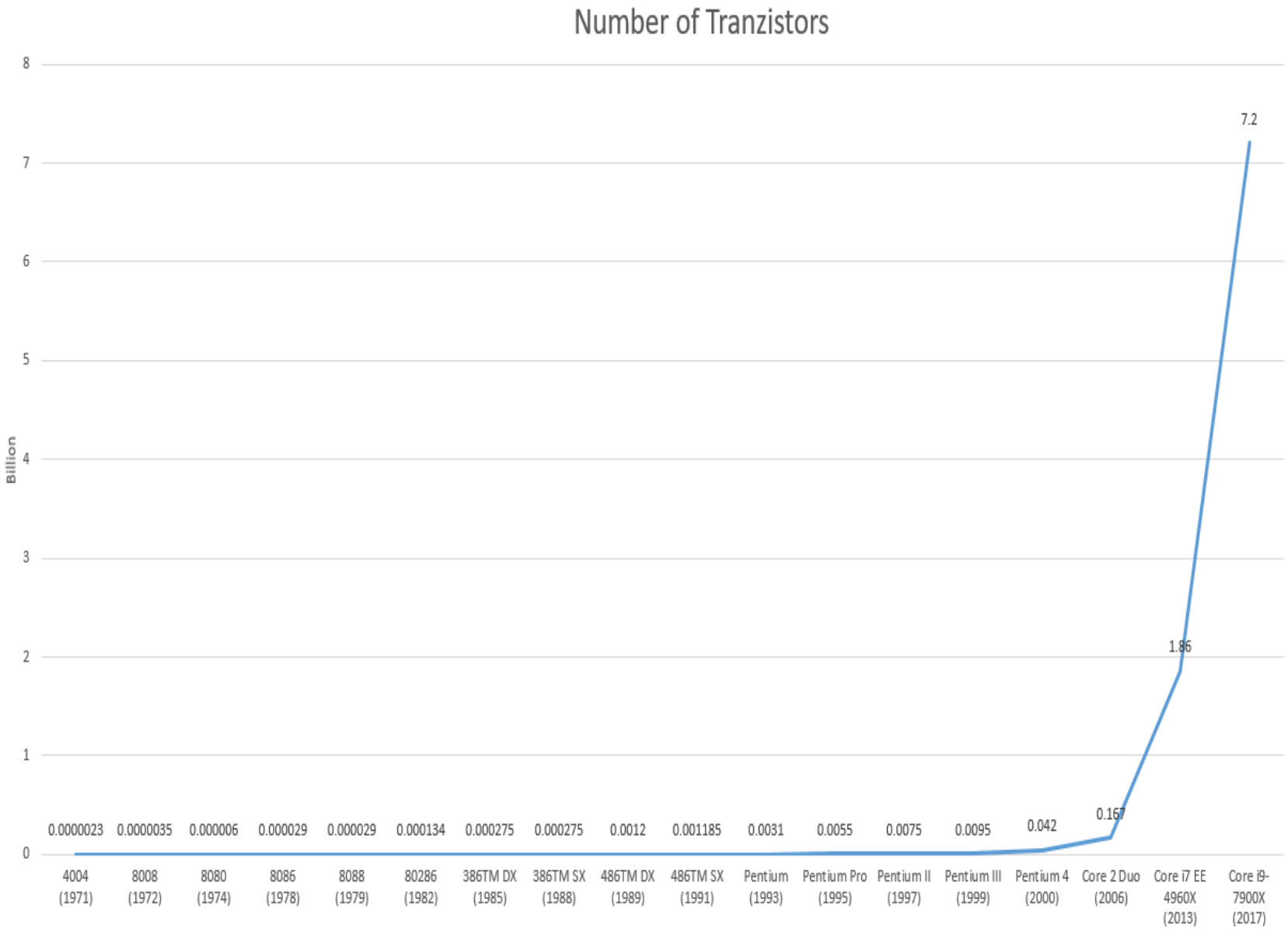
σύνολο εντολών Advanced Vector Extensions που παρείχε ένα σύνολο 256-bit, και στη συνέχεια 512-bit, instructions για αποτελεσματική επεξεργασία δεδομένων πίνακα.

Σχεδόν 40 χρόνια μετά την εισαγωγή της το 1978, η αρχιτεκτονική x86 συνεχίζει να κυριαρχεί στην αγορά επεξεργαστών εκτός των ενσωματωμένων συστημάτων. Η οργάνωση και η τεχνολογία του x86 στα μηχανήματα έχουν αλλάξει δραματικά κατά το πέρασμα των δεκαετιών, η αρχιτεκτονική του σετ εντολών παρόλο που έχει εξελιχθεί παραμένει συμβατή με παλαιότερες εκδόσεις. Έτσι, οποιοδήποτε πρόγραμμα είναι γραμμένο σε παλαιότερη έκδοση η αρχιτεκτονική x86 μπορεί να εκτελεστεί σε νεότερες εκδόσεις. Όλες οι αλλαγές στην αρχιτεκτονική του συνόλου των εντολών έχουν συμπεριλάβει προσθήκες στο σύνολο εντολών, χωρίς να γίνουν αφαιρέσεις από τις προηγούμενες εκδόσεις. Το ποσοστό αλλαγής ήταν η προσθήκη περίπου μιας εντολής το μήνα που προστίθεται στην αρχιτεκτονική [ANTH08], έτσι ώστε να υπάρχουν τώρα χιλιάδες εντολές επί του συνόλου των εντολών.

Η αρχιτεκτονική x86 παρέχει μια εξαιρετική απεικόνιση των εξελίξεων στο υλικό του υπολογιστή τα τελευταία 35 χρόνια. Το 1978 κυκλοφόρησε ο 8086 με ταχύτητα ρολογιού 5 MHz και είχε 29.000 τρανζίστορ. Ένας 6-πύρηνοςi7 EE 4960X που κυκλοφόρησε το 2013 λειτουργεί στα 4 GHz, επιτάχυνση συντελεστή (FSB) 800 και έχει 1,86 δισεκατομμύρια τρανζίστορ, περίπου 64.000 φορές περισσότερα από τον 8086. Ωστόσο, ο Core i7 EE 4960X περιλαμβάνει ένα ελαφρώς μεγαλύτερο πακέτο από τον 8086 και έχει συγκρίσιμο κόστος. Παρακάτω παρουσιάζονται σε γραφήματα η εξέλιξη κατά τις δεκαετίες 1970 έως και 2010 η ταχύτητα των επεξεργαστών, η αρχιτεκτονική νανομέτρων και ο αριθμός των τρανζίστορ.


CPU Clock Speed
MHz
5000
4500
4000
3500
3000
2500
2000
1500
1000
500
0
0.108
0.108
2
10
8
12.5
33
33
50
33
166
200
300
660
1800
1200
4000
4300
4004 (1971)
8008 (1972)
8080 (1974)
8086 (1978)
8088 (1979)
80286 (1982)
386TM DX (1985)
386TM SX (1988)
486TM DX (1989)
486TM SX (1991)
Pentium (1993)
Pentium Pro (1995)
Pentium II (1997)
Pentium III (1999)
Pentium 4 (2000)
Core 2 Duo (2006)
Core i7 EE 4960X (2013)
Core i9-7900X (2017)


Future Size
Nanometers
12000
10000
8000
6000
4000
2000
0
10000
8000
6000
3000
6000
1500
1000
1000
800
1000
800
600
350
250
180
65
22
14
4004 (1971)
8008 (1972)
8080 (1974)
8086 (1978)
8088 (1979)
80286 (1982)
386TM DX (1985)
386TM SX (1988)
486TM DX (1989)
486TM SX (1991)
Pentium (1993)
Pentium Pro (1995)
Pentium II (1997)
Pentium III (1999)
Pentium 4 (2000)
Core 2 Duo (2006)
Core i7 EE 4960X (2013)
Core i9-7900X (2017)


Number of Tranzistors
Billion
8
7
6
5
4
3
2
1
0
0.0000023
0.0000035
0.000006
0.000029
0.000029
0.000134
0.000275
0.000275
0.0012
0.001185
0.0031
0.0055
0.0075
0.0095
0.042
0.167
1.86
7.2
4004 (1971)
8008 (1972)
8080 (1974)
8086 (1978)
8088 (1979)
80286 (1982)
386TM DX (1985)
386TM SX (1988)
486TM DX (1989)
486TM SX (1991)
Pentium (1993)
Pentium Pro (1995)
Pentium II (1997)
Pentium III (1999)
Pentium 4 (2000)
Core 2 Duo (2006)
Core i7 EE 4960X (2013)
Core i9-7900X (2017)

3.2.8. Οι επεξεργαστές Xeon των διακομιστών

Οι επεξεργαστές κατηγορίας Xeon είναι μια μάρκα μικροεπεξεργαστών x86 που σχεδιάστηκαν, κατασκευάστηκαν και διατέθηκαν στην αγορά από την Intel, με στόχο τους σταθμούς εργασίας, τους διακομιστές και τα ενσωματωμένα συστήματα. Παρουσιάστηκε για πρώτη φορά τον Ιούνιο του 1998.

Οι επεξεργαστές Xeon βασίζονται στην ίδια αρχιτεκτονική με τους κανονικούς επεξεργαστές επιτραπέζιου επιπέδου, αλλά διαθέτουν προηγμένες δυνατότητες όπως υποστήριξη για μνήμη ECC, υψηλότερες μετρήσεις πυρήνων, υποστήριξη για μεγαλύτερες ποσότητες RAM, μεγαλύτερη μνήμη cache και επιπλέον παροχή για λειτουργίες αξιοπιστίας, διαθεσιμότητας και δυνατότητας συντήρησης (Reliability Availability Serviceability – RAS) εταιρικού επιπέδου που είναι υπεύθυνες για τον χειρισμό εξαιρέσεων υλικού μέσω της αρχιτεκτονικής Machine Check. Συχνά είναι σε θέση να συνεχίσουν με ασφάλεια την εκτέλεση εργασιών όπου ένας κανονικός επεξεργαστής δεν μπορεί και αυτό οφείλεται σε αυτές τις επιπλέον δυνατότητες RAS, ανάλογα με τον τύπο και τη σοβαρότητα της εξαίρεσης ελέγχου μηχανής (MCE).

Ορισμένοι υποστηρίζουν επίσης συστήματα πολλαπλών υποδοχών με δύο, τέσσερις ή οκτώ υποδοχές μέσω της χρήσης του διαύλου Quick Path Interconnect (QPI). Ορισμένες αδυναμίες που καθιστούν τους επεξεργαστές Xeon ακατάλληλους για τους περισσότερους επιτραπέζιους υπολογιστές, που χρησιμοποιούνται από την πληθώρα των καταναλωτών είναι:

- Περιλαμβάνουν χαμηλότερους ρυθμούς ρολογιού στο ίδιο εύρος τιμής (δεδομένου ότι οι διακομιστές εκτελούν περισσότερες εργασίες παράλληλα από τους επιτραπέζιους υπολογιστές καθώς ο αριθμός των πυρήνων είναι πιο σημαντικός από τους ρυθμούς ρολογιού)
- Απουσία ενσωματωμένης μονάδα επεξεργασίας γραφικών (GPU)
- Έλλειψη υποστήριξης για overclocking

Παρά τα μειονεκτήματα αυτά, οι επεξεργαστές Xeon είχαν πάντα δημοτικότητα μεταξύ ορισμένων χρηστών επιτραπέζιων υπολογιστών (επεξεργαστές βίντεο και άλλων χρηστών ισχύος), κυρίως λόγω του υψηλότερου δυναμικού μέτρησης πυρήνα και της υψηλότερης αναλογίας απόδοσης προς τιμή έναντι του Core i7 όσον αφορά τη συνολική υπολογιστική ισχύ όλων των πυρήνων. Δεδομένου ότι οι περισσότεροι επεξεργαστές Intel Xeon δεν διαθέτουν ενσωματωμένη GPU, τα συστήματα που είναι κατασκευασμένα με αυτούς τους επεξεργαστές απαιτούν μια ξεχωριστή κάρτα γραφικών ή μια ξεχωριστή GPU.

3.2.9. Nehalem based Xeon

3400-series "Clarkdale": Οι επεξεργαστές της σειράς Clarkdale βρίσκονται στο χαμηλότερο σημείο της σειράς 3400. Χρησιμοποιούνται στους επεξεργαστές Core i3-500 και Core i5-600 καθώς και στις σειρές Celeron G1000 και G6000 Pentium. Ένα ενιαίο μοντέλο κυκλοφόρησε τον Μάρτιο του 2010, το Xeon L3406. Σε σύγκριση με όλα τα άλλα προϊόντα που βασίζονται στο Clarkdale, αυτό δεν υποστηρίζει ενσωματωμένα γραφικά, προσφέρει μόνο δύο πυρήνες, αλλά έχει πολύ χαμηλότερη ισχύ θερμικής σχεδίασης μόλις 30 W.

3400-series "Lynnfield": Οι επεξεργαστές Xeon 3400-series που βασίζονται στο Lynnfield είναι επεξεργαστές τεσσάρων πυρήνων βασισμένοι στη μικροαρχιτεκτονική Nehalem παρουσιάστηκαν τον Σεπτέμβριο του 2009. Οι ίδιοι επεξεργαστές διατίθενται στην αγορά για επιτραπέζιους υπολογιστές μεσαίου εύρους έως υψηλού επιπέδου όπως Core i5 και Core i7. Έχουν δύο ενσωματωμένα κανάλια μνήμης, καθώς και συνδέσεις PCI Express και Direct Media Interface (DMI), αλλά χωρίς διασύνδεση QuickPath Interconnect (QPI).

Εικόνα 3.12

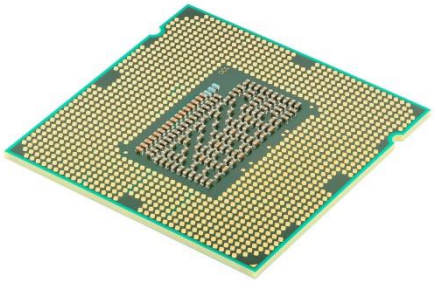
3600/5600-series "Gulftown" & "Westmere-EP": Οι επεξεργαστές της σειράς Gulftown ή Westmere-EP, είναι επεξεργαστές έξι πυρήνων βασισμένοι στο Westmere με αρχιτεκτονική 32 nm. Αποτελούν τη βάση για τις σειρές Xeon 36xx και 56xx και το Core i7-980X. Κυκλοφόρησαν το πρώτο τρίμηνο του 2010. Η σειρά 36xx ακολουθεί το μοντέλο uni-επεξεργαστή Bloomfield της σειράς 35xx, ενώ η σειρά 56xx ακολουθεί το μοντέλο διπλού επεξεργαστή Gainestown της σειράς 55xx όπου και οι δύο είναι υποδοχές συμβατές με τους προκατόχους τους.

6500/7500-series "Beckton": Η σειρά Beckton ή Nehalem-EX (EXpandable server market) είναι ένας επεξεργαστής που βασίζεται στην αρχιτεκτονική Nehalem με έως και οκτώ πυρήνες και χρησιμοποιεί buffering μέσα στο chipset για υποστήριξη έως 16 τυπικών DDR3 DIMMS ανά υποδοχή CPU χωρίς να απαιτείται η χρήση FB-DIMMS. Σε αντίθεση με όλους τους προηγούμενους επεξεργαστές Xeon MP, ο Nehalem-EX χρησιμοποιεί το νέο Socket LGA 1567, αντικαθιστώντας το Socket 604 που χρησιμοποιήθηκε στα προηγούμενα μοντέλα, μέχρι το Xeon 7400 "Dunnington". Τα μοντέλα 75xx έχουν τέσσερις διεπαφές QuickPath, οπότε μπορούν να χρησιμοποιηθούν σε διαμορφώσεις έως και οκτώ υποδοχών, ενώ τα μοντέλα 65xx είναι μόνο για έως και δύο διεπαφές. Σχεδιασμένο από την ομάδα Digital Enterprise Group (DEG) Santa Clara και Hudson Design, η Beckton κατασκευάζεται με την τεχνολογία P1266 (45 nm). Το λανσάρισμά του έγινε τον Μάρτιο του 2010 όπου και συνέπεσε με αυτό του άμεσου ανταγωνιστή της, τον AMD Opteron 6xxx "Magny-Cours".
Τα περισσότερα μοντέλα περιορίζουν τον αριθμό των πυρήνων και των συνδέσμων QPI, καθώς και το μέγεθος της προσωρινής μνήμης L3, προκειμένου να αποκτήσουν μια ευρύτερη γκάμα προϊόντων από τη σχεδίαση ενός τσιπ.

E7-x8xx-series "Westmere-EX": Το Westmere-EX είναι συνέχεια του Beckton / Nehalem-EX και του πρώτου Intel Chip που έχει δέκα πυρήνες CPU. Η μικροαρχιτεκτονική είναι η ίδια με τον εξαπύρηνο επεξεργαστή Gulftown / Westmere-EP, αλλά χρησιμοποιεί το socket LGA 1567 όπως το Beckton για να υποστηρίξει έως και οκτώ διεπαφές.
Ξεκινώντας με το Westmere-EX, το σχήμα ονομάτων άλλαξε για άλλη μια φορά, με το "E7-xxxx" να σηματοδοτεί τώρα τη γραμμή προηγμένων επεξεργαστών Xeon χρησιμοποιώντας ένα πακέτο που υποστηρίζει διαμορφώσεις μεγαλύτερες από δύο CPU, πρώην σειρά 7xxx. Ομοίως, οι σειρές διπλού επεξεργαστή 3xxx και 5xxx μετατράπηκαν σε E3-xxxx και E5-xxxx, αντίστοιχα, για μεταγενέστερους επεξεργαστές.

3.2.10. Sandy Bridge– and Ivy Bridge–based Xeon

E3-12xx-series "Sandy Bridge": Η σειρά επεξεργαστών Xeon E3-12xx, που παρουσιάστηκε τον Απρίλιο του 2011, χρησιμοποιεί τα τσιπ Sandy Bridge που αποτελούν επίσης τη βάση για τα προϊόντα Core i3 / i5 / i7-2xxx και Celeron / Pentium Gxxx που χρησιμοποιούν την ίδια υποδοχή LGA 1155, αλλά με απενεργοποιημένο διαφορετικό σύνολο λειτουργιών. Συγκεκριμένα, οι παραλλαγές Xeon περιλαμβάνουν υποστήριξη για μνήμη ECC, VT-d και αξιόπιστη εκτέλεση που δεν υπάρχουν στα μοντέλα καταναλωτών, ενώ μόνο ορισμένα Xeon E3 επιτρέπουν την ενσωματωμένη GPU που υπάρχει στο Sandy Bridge. Όπως και οι προκάτοχοί της σειράς Xeon 3400, το Xeon E3 υποστηρίζει λειτουργία μόνο με μία υποδοχή CPU και στοχεύει σε σταθμούς εργασίας και διακομιστές εισόδου.



Εικόνα 3.13

E3-12xx v2-series "Ivy Bridge": Το Xeon E3-12xx v2 είναι μια μικρή ενημέρωση του Sandy Bridge που βασίζεται στο E3-12xx, χρησιμοποιώντας τη συρρίκνωση των 22 nm και παρέχει ελαφρώς καλύτερη απόδοση ενώ παραμένει συμβατή προς τα πίσω. Κυκλοφόρησαν τον Μάιο του 2012 και αντικατοπτρίζουν τους επιτραπέζιους Core i3 / i5 / i7-3xxx στην επιφάνεια εργασίας.

E5-14xx/24xx series "Sandy Bridge-EN" and E5-16xx/26xx/46xx-series "Sandy Bridge-EP": Οι επεξεργαστές Xeon E5-16xx ακολουθούν τα προηγούμενα προϊόντα της σειράς Xeon 3500/3600 ως την πλατφόρμα ενιαίου socket τελευταίας τεχνολογίας, χρησιμοποιώντας το πακέτο LGA 2011 που παρουσιάστηκε με αυτόν τον επεξεργαστή. Μοιράζονται την πλατφόρμα Sandy Bridge-E με τους επεξεργαστές Core i7-38xx και i7-39xx με μία υποδοχή. Τα τσιπ CPU δεν έχουν ενσωματωμένη GPU αλλά οκτώ πυρήνες CPU, μερικοί από τους οποίους είναι απενεργοποιημένοι στα προϊόντα entry-level. Η σειρά Xeon E5-26xx έχει τα ίδια χαρακτηριστικά αλλά επιτρέπει επίσης τη λειτουργία πολλαπλών υποδοχών, όπως οι προηγούμενοι επεξεργαστές Xeon 5000-series και Xeon 7000-series.

E5-14xx v2/24xx v2 series "Ivy Bridge-EN" and E5-16xx v2/26xx v2/46xx v2 series "Ivy Bridge-EP": Η σειρά Xeon E5 v2 ήταν μια ενημέρωση, που κυκλοφόρησε τον Σεπτέμβριο του 2013 για να αντικαταστήσει τους αρχικούς επεξεργαστές Xeon E5 με μια παραλλαγή που βασίζεται στην συρρίκνωση του Ivy Bridge Ο μέγιστος αριθμός πυρήνων CPU αυξήθηκε σε 12 ανά μονάδα επεξεργαστή και η συνολική προσωρινή μνήμη L3 αυξήθηκε στα 30 MB. Η καταναλωτική έκδοση του επεξεργαστή Xeon E5-16xx v2 είναι οι Core i7-48xx και 49xx.

E7-28xx v2/48xx v2/88xx v2 series "Ivy Bridge-EX": Η σειρά Xeon E7 v2 ήταν μια ενημέρωση, η οποία κυκλοφόρησε τον Φεβρουάριο του 2014 για να αντικαταστήσει τους αρχικούς επεξεργαστές Xeon E7 με μια παραλλαγή που βασίζεται στη συρρίκνωση του Ivy Bridge. Δεν υπήρχε έκδοση Sandy Bridge αυτών των επεξεργαστών.

3.2.11. Haswell-based Xeon

E3-12xx v3 series "Haswell-WS": Το Xeon E3-12xx v3 που παρουσιάστηκε τον Μάιο του 2013 είναι η πρώτη σειρά Xeon που βασίζεται στη μικροαρχιτεκτονική Haswell. Χρησιμοποιεί τη νέα υποδοχή LGA 1150, η οποία παρουσιάστηκε με τους επεξεργαστές Core i5 / i7 Haswell, ασυμβίβαστη με την LGA 1155 που χρησιμοποιήθηκε στα Xeon E3 και E3 v2. Όπως και πριν, η κύρια διαφορά μεταξύ των εκδόσεων επιτραπέζιου και διακομιστή είναι η προσθήκη υποστήριξης για μνήμη ECC στα parts με επωνυμία Xeon. Το κύριο όφελος της νέας μικροαρχιτεκτονικής είναι η καλύτερη απόδοση ισχύος.

Εικόνα 3.14

E5-16xx/26xx v3 series "Haswell-EP": Οι σειρές Xeon E5-16xx v3 και Xeon E5-26xx v3 που παρουσιάστηκαν τον Σεπτέμβριο του 2014 χρησιμοποιούν τη νέα υποδοχή LGA 2011-v3, η οποία είναι ασυμβίβαστη με την υποδοχή LGA 2011 που χρησιμοποιήθηκε από προηγούμενες γενιές Xeon E5 και E5 v2 με βάση την Sandy Bridge και την Ivy Bridge μικροαρχιτεκτονικές. Μερικά από τα κύρια οφέλη αυτής της γενιάς, σε σύγκριση με την προηγούμενη, είναι η βελτιωμένη απόδοση ισχύος, οι υψηλότερες μετρήσεις πυρήνων και οι μεγαλύτερες προσωρινές μνήμες τελευταίου επιπέδου (LLC). Ακολουθώντας την ήδη χρησιμοποιούμενη ονοματολογία, η σειρά Xeon E5-26xx v3 επιτρέπει τη λειτουργία διπλής διεπαφής.

Ένα από τα νέα χαρακτηριστικά αυτής της γενιάς είναι ότι τα μοντέλα Xeon E5 v3 με περισσότερους από 10 πυρήνες υποστηρίζουν τη λειτουργία λειτουργίας συμπλέγματος σε μήτρα (COD), επιτρέποντας στις πολλαπλές στήλες των πυρήνων της CPU και των φετών LLC να χωρίζονται λογικά σε αυτό που παρουσιάζεται ως μη Ομοιόμορφη πρόσβαση μνήμης (NUMA) CPU στο λειτουργικό σύστημα. Διατηρεί τοπικά δεδομένα και οδηγίες στο "διαμέρισμα" της CPU που τα επεξεργάζεται, μειώνοντας έτσι τον λανθάνοντα χρόνο πρόσβασης LLC, το COD φέρνει βελτιώσεις απόδοσης σε λειτουργικά συστήματα και εφαρμογές που υποστηρίζουν NUMA.

E7-48xx/88xx v3 series "Haswell-EX": Παρουσιάστηκαν τον Μάιο του 2015, οι σειρές Xeon E7-48xx v3 και Xeon E7-88xx v3 παρέχουν υψηλότερες μετρήσεις πυρήνων, υψηλότερη απόδοση ανά πυρήνα και βελτιωμένες δυνατότητες αξιοπιστίας, σε σύγκριση με την προηγούμενη γενιά Xeon E7 v2. Ακολουθώντας τη συνήθη ονοματολογία SKU, οι σειρές Xeon E7-48xx v3 και E7-88xx v3 επιτρέπουν τη λειτουργία πολλαπλών υποδοχών, υποστηρίζοντας έως και τετραπλές και οκτώ υποδοχές, αντίστοιχα. Αυτοί οι επεξεργαστές χρησιμοποιούν την υποδοχή LGA 2011 (R1).

Οι σειρές Xeon E7-48xx v3 και E7-88xx v3 περιέχουν έναν ενσωματωμένο ελεγκτή μνήμης quad-channel (IMC), που υποστηρίζει μονάδες μνήμης DDR3 και DDR4 LRDIMM ή RDIMM μέσω της χρήσης μνήμης Jordan Creek (DDR3) ή Jordan Creek 2 (DDR4) buffer chips. Και οι δύο εκδόσεις του chip buffer μνήμης συνδέονται στον επεξεργαστή χρησιμοποιώντας την έκδοση 2.0 της διεπαφής Intel Scalable Memory Interconnect (SMI), ενώ υποστηρίζουν διατάξεις μνήμης lockstep για βελτιωμένη αξιοπιστία. Μπορούν να συνδεθούν έως τέσσερα τσιπ μνήμης σε έναν επεξεργαστή, με έως και έξι υποδοχές DIMM για κάθε τσιπ μνήμης.

Οι σειρές Xeon E7-48xx v3 και E7-88xx v3 περιέχουν επίσης λειτουργική υποστήριξη χωρίς σφάλματα για επεκτάσεις συγχρονισμού συναλλαγών (TSX), η οποία απενεργοποιήθηκε μέσω ενημέρωσης μικροκώδικα τον Αύγουστο του 2014 για Haswell-E, Haswell-WS (E3-12xx v3) και μοντέλα Haswell-EP (E5-16xx / 26xx v3), λόγω ενός σφάλματος που ανακαλύφθηκε κατά την εφαρμογή TSX.

3.2.12. Broadwell-based Xeon

Σειρά E3-12xx v4 "Broadwell-WS": Παρουσιάστηκε τον Ιούνιο του 2015, το Xeon E3-12xx v4 είναι η πρώτη σειρά Xeon που βασίζεται στην μικροαρχιτεκτονική του Broadwell. Χρησιμοποιεί υποδοχή LGA 1150, η οποία παρουσιάστηκε με τους επεξεργαστές Core i5 / i7 Haswell. Όπως και πριν, η κύρια διαφορά μεταξύ των εκδόσεων επιτραπέζιου και διακομιστή είναι η προσθήκη υποστήριξης για μνήμη ECC στα parts με επωνυμία Xeon. Το κύριο πλεονέκτημα της νέας μικροαρχιτεκτονικής είναι η νέα διαδικασία λιθογραφίας, η οποία οδηγεί σε καλύτερη απόδοση ισχύος.

Εικόνα 3.15

3.2.13. Skylake-based Xeon

E3-12xx v5 series "Skylake-WS": Το Xeon E3-12xx v5 παρουσιάστηκε τον Οκτώβριο του 2015 και είναι η πρώτη σειρά Xeon που βασίζεται στη μικροαρχιτεκτονική του Skylake. Χρησιμοποιεί νέα υποδοχή LGA 1151, η οποία παρουσιάστηκε με τους επεξεργαστές Core i5 / i7 Skylake στην επιφάνεια εργασίας. Παρόλο που χρησιμοποιεί την ίδια υποδοχή με τους επεξεργαστές καταναλωτών, περιορίζεται στη σειρά chipset διακομιστή C200 και δεν θα λειτουργεί με chipset καταναλωτή όπως το Z170. Όπως και πριν, η κύρια διαφορά μεταξύ των εκδόσεων επιτραπέζιου και διακομιστή είναι η προσθήκη υποστήριξης για μνήμη ECC στα parts με επωνυμία Xeon.

Εικόνα 3.16

3.2.14. Kaby Lake-based Xeon

E3-12xx v6 series: Το Xeon E3-12xx v6 που παρουσιάστηκε τον Ιανουάριο του 2017 είναι η πρώτη σειρά Xeon που βασίζεται στη μικροαρχιτεκτονική Kaby Lake. Χρησιμοποιεί την ίδια υποδοχή LGA 1151, η οποία παρουσιάστηκε με τους επεξεργαστές Core i5 / i7 Skylake στους επιτραπέζιους. Όπως και πριν, η κύρια διαφορά μεταξύ των εκδόσεων επιτραπέζιου και διακομιστή είναι η πρόσθετη υποστήριξη για μνήμη ECC και βελτιωμένη ενεργειακή απόδοση στα parts με επωνυμία Xeon.

Εικόνα 3.17

3.2.15. Coffee Lake-based Xeon

Ο Coffee Lake είναι το όνομα της Intel για την οικογένεια μικροεπεξεργαστών Core της όγδοης γενιάς, που ανακοινώθηκε στις 25 Σεπτεμβρίου 2017. Κατασκευάστηκε χρησιμοποιώντας τον δεύτερο κόμβο επεξεργασίας 14 nm της Intel. Οι επεξεργαστές Desktop Coffee Lake παρουσίασαν CPU i5 και i7 με έξι πυρήνες (μαζί με υπερ-σπείρωμα στην περίπτωση του τελευταίου) και Core i3 CPU με τέσσερις πυρήνες και χωρίς υπερθέματα.

Στις 8 Οκτωβρίου 2018, η Intel ανακοίνωσε αυτό που χαρακτηρίζει την ένατη γενιά επεξεργαστών Core, την οικογένεια Coffee Lake Refresh. Για να αποφευχθεί η αντιμετώπιση θερμικών προβλημάτων σε υψηλές ταχύτητες ρολογιού, η Intel συγκολλήσε το ενσωματωμένο θερμοδιακόπτη (IHS) στη μήτρα της CPU αντί να χρησιμοποιεί θερμική πάστα όπως στους επεξεργαστές Coffee Lake. Η γενιά καθορίστηκε από την πρώτη αύξηση πυρήνων στο mainstream chip από το 2011. Τα i7s και i5s Quad-Core έγιναν Hexa-Cores και τα i3s dual core έγιναν quad core.

Το Coffee Lake χρησιμοποιείται με το chipset 300 σειρών και επίσημα δεν λειτουργεί με τις μητρικές κάρτες chipset 100 και 200. Αν και οι επιτραπέζιοι επεξεργαστές Coffee Lake χρησιμοποιούν την ίδια φυσική υποδοχή LGA 1151 με τους Skylake και Kaby Lake, το pinout είναι ηλεκτρικά ασύμβατο με αυτούς τους παλαιότερους επεξεργαστές και μητρικές κάρτες. Στις 2 Απριλίου 2018, η Intel κυκλοφόρησε επιπλέον επιτραπέζιους υπολογιστές Core i3, i5, i7, Pentium Gold, Celeron CPU, τους πρώτους 6-core Core i7 και i9 mobile CPUs, υπερ-νήμα τεσσάρων πυρήνων Core i5 mobile CPUs και τον πρώτο Coffee Lake CPU υψηλής ισχύος με γραφικά Intel Iris Plus.

Εικόνα 3.18

Στις 8 Ιουνίου 2018, για τον εορτασμό της 40ης επετείου της αρχιτεκτονικής επεξεργαστή Intel 8086, η Intel κυκλοφόρησε το i7-8086K ως CPU περιορισμένης έκδοσης, μια αρίθμηση και ελαφρώς υψηλότερη χρονική παρτίδα των i7-8700K.

3.2.16. Cascade Lake-based Xeon

Ο Cascade Lake είναι ένα όνομα κωδικού Intel για διακομιστή 14 νανομέτρων, σταθμό εργασίας και ενθουσιώδη μικροαρχιτεκτονική επεξεργαστή, που κυκλοφόρησε τον Απρίλιο του 2019. Στο μοντέλο Process-Architecture-Optimization της Intel, το Cascade Lake είναι μια βελτιστοποίηση του Skylake. Η Intel δηλώνει ότι θα είναι η πρώτη μικροαρχιτεκτονική τους που θα υποστηρίζει μονάδες μνήμης που βασίζονται σε 3D XPoint. Περιλαμβάνει επίσης οδηγίες Deep Learning Boost και μετριασμούς για το Meltdown και το Specter. Η Intel ξεκίνησε επίσημα τους νέους Xeon Scalable SKU στις 24 Φεβρουαρίου 2020.

Εικόνα 3.19

Συνολικά, οι αλλαγές στους επεξεργαστές μεταξύ της πρώτης και της δεύτερης γενιάς φαίνονται στον παρακάτω πίνακα.

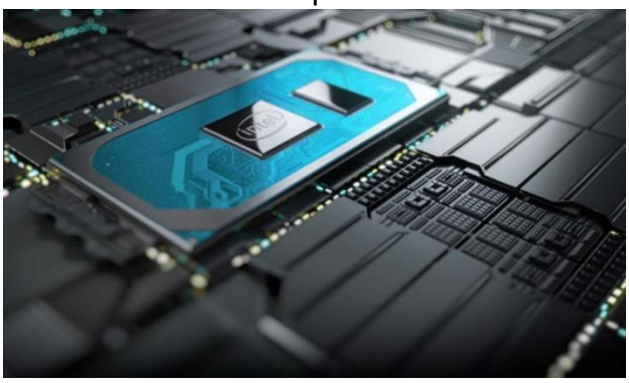
Intel Xeon Scalable		
2nd Gen Cascade Lake	**AnandTech**	**1st Gen Skylake-SP**
Απρίλιος 2019	Κυκλοφόρησαν	Ιούλιος 2017
[8200] Έως 28 [9200] Έως 56	Πυρήνες	[8100] Έως 28
1 MB L2 ανά πυρήνα Κοινόχρηστο L3 έως 38,5 MB	Προσωρινή μνήμη	1 MB L2 ανά πυρήνα Κοινόχρηστο L3 έως 38,5 MB
Έως 48 λωρίδες	PCIe 3.0	Έως 48 λωρίδες
Έξι κανάλια Έως DDR4-2933 Πρότυπο 1,5 TB	Υποστήριξη DRAM	Έξι κανάλια Έως DDR4-2666 Πρότυπο 768 GB
Έως 4,5 TB ανά επεξεργαστή	Υποστήριξη Optane	-
AVX-512 VNNI με INT8	Διάνυσμα υπολογισμού	AVX-512
Παραλλαγή 2, 3, 3a, 4, και L1TF	Specter / Meltdown Διορθώσεις	-
[8200] Έως 205 W [9200] Έως 400 W	θερμικό σημείο σχεδιασμού (TDP)	[8200] Έως 205 W

Πίνακας 3.1

3.2.17. Ice Lake-based Xeon

Ο Ice Lake είναι το κωδικό όνομα της Intel για τους επεξεργαστές Intel Core 10ης γενιάς που βασίζονται στη νέα μικροαρχιτεκτονική Sunny Cove Core. Το Ice Lake αντιπροσωπεύει ένα βήμα Αρχιτεκτονικής στο μοντέλο διαδικασίας-αρχιτεκτονικής-βελτιστοποίησης της Intel. Οι επεξεργαστές Ice Lake πωλούνται μαζί με τους επεξεργαστές Comet Lake των 14 nm ως οικογένεια προϊόντων "10ης γενιάς Core" της Intel.

Παράγεται στη δεύτερη γενιά της διαδικασίας 10 nm της Intel, 10 nm +, η Ice Lake είναι η δεύτερη μικροαρχιτεκτονική της Intel που θα κατασκευαστεί στη διαδικασία των 10 nm, μετά την περιορισμένη κυκλοφορία του Cannon Lake το 2018. Ωστόσο, η Intel άλλαξε το σχήμα ονομασίας τους το 2020 για τη διαδικασία των 10 nm. Σε αυτό το νέο σχήμα ονομασίας, η διαδικασία κατασκευής της Ice Lake ονομάζεται απλά 10 nm, χωρίς συνημμένα πλεονεκτήματα. Από τον Σεπτέμβριο του 2020, κυκλοφόρησε μια σειρά επεξεργαστών κινητής τηλεφωνίας Ice Lake, αλλά δεν έχουν ανακοινωθεί ή κυκλοφορήσει επεξεργαστές επιτραπέζιου ή φορητού υπολογιστή Ice Lake.



Εικόνα 3.20

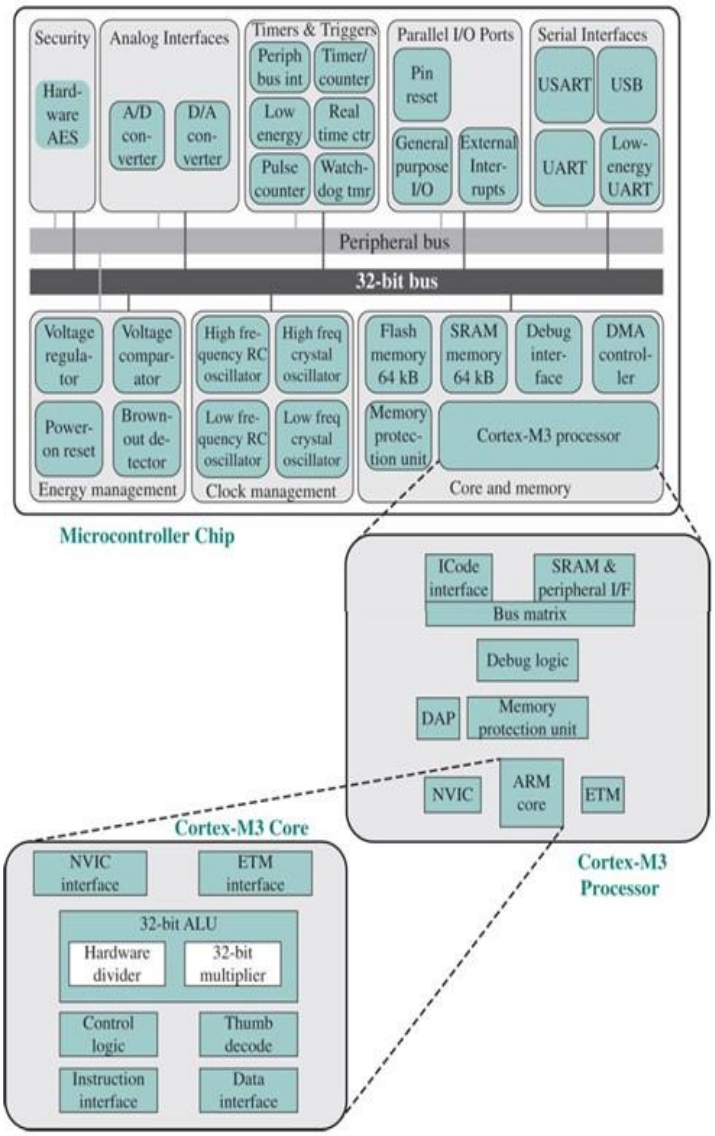
3.4. Η αρχιτεκτονική ARM

Η αρχιτεκτονική ARM αναφέρεται σε αρχιτεκτονική επεξεργαστή που έχει εξελιχθεί από τις αρχές σχεδιασμού RISC και χρησιμοποιείται σε ενσωματωμένα συστήματα.
Η ARM είναι μια οικογένεια μικροεπεξεργαστών και μικροελεγκτών βασισμένων σε αρχιτεκτονική RISC που σχεδιάστηκαν από την ARM Holdings, Κέιμπριτζ, Αγγλία. Η εταιρεία δεν κατασκευάζει επεξεργαστές αλλά αντ' αυτού σχεδιάζει μικροεπεξεργαστές και αρχιτεκτονικές πολλαπλών πυρήνων και τις άδειες σε κατασκευαστές. Η ARM Holdings έχει δύο τύπους προϊόντων με άδεια χρήσης: επεξεργαστές και αρχιτεκτονικές επεξεργαστών. Για τους επεξεργαστές, ο πελάτης αγοράζει τα δικαιώματα χρήσης του σχεδιασμού που παρέχεται από την ARM στις δικές τους μάρκες. Για αρχιτεκτονικές επεξεργαστή, ο πελάτης αγοράζει τα δικαιώματα σχεδιασμού του δικού τους επεξεργαστή σύμφωνα με την αρχιτεκτονική του ARM.
Τα ARM τσιπ είναι επεξεργαστές υψηλής ταχύτητας που είναι γνωστοί για το μικρό τους μέγεθος και τις απαιτήσεις σε χαμηλή ισχύ. Χρησιμοποιούνται ευρέως σε smartphone και άλλες φορητές συσκευές, συμπεριλαμβανομένου συστήματα παιχνιδιών, καθώς και μια μεγάλη ποικιλία καταναλωτικών προϊόντων.
Οι επεξεργαστές της Apple είναι ARM στις δημοφιλείς συσκευές iPod και iPhone, και χρησιμοποιούνται σχεδόν σε όλα τα smartphone Android επίσης. Το 2016 στάλθηκαν 16,7 δισεκατομμύρια τσιπ βασισμένα σε ARM αρχιτεκτονική. Η ARM είναι πιθανώς η πιο ευρέως χρησιμοποιούμενη ενσωματωμένη αρχιτεκτονική επεξεργαστών και πράγματι η πιο ευρέως χρησιμοποιούμενη αρχιτεκτονική επεξεργαστών οποιουδήποτε είδους στον κόσμο.
Η προέλευση της τεχνολογίας ARM αρχιτεκτονικής εντοπίζεται στην εταιρεία Acorn Computers με έδρα τη Βρετανία. Στις αρχές της δεκαετίας του 1980, η Acorn ανέλαβε συμβόλαιο από την British Broadcasting Corporation (BBC) να αναπτύξει μια νέα αρχιτεκτονική μικροϋπολογιστών για το BBC Computer Literacy Project. Η επιτυχία αυτού του project επέτρεψε στην Acorn να συνεχίσει να αναπτύσσει τον πρώτο εμπορικό επεξεργαστή RISC, τον Acorn RISC Machine (ARM). Η πρώτη έκδοση, ARM1, τέθηκε σε λειτουργία το 1985 και χρησιμοποιήθηκε για εσωτερική έρευνα και ανάπτυξη, καθώς και να χρησιμοποιείται ως συνεπεξεργαστής στο μηχάνημα BBC (εικόνα 3.21) .

Εικόνα 3.21

Σε αυτό το πρώιμο στάδιο, η Acorn χρησιμοποίησε την εταιρεία VLSI Technology για να κάνει την πραγματική κατασκευή στους επεξεργαστές της. Η VLSI έλαβε άδεια για την αγορά του chip από μόνη της

και είχε κάποια επιτυχία στο να πάρει άλλες εταιρείες να χρησιμοποιούν το ARM στα προϊόντα τους, ιδίως ως ενσωματωμένος επεξεργαστής. Ο σχεδιασμός ARM ταιριάζει με την αυξανόμενη εμπορική ανάγκη για κατανάλωση υψηλής απόδοσης και χαμηλής κατανάλωσης, επεξεργαστές μικρού μεγέθους και χαμηλού κόστους για ενσωματωμένες εφαρμογές. Η περαιτέρω ανάπτυξη ήταν πέρα από το πεδίο των δυνατοτήτων του Acorn. Κατά συνέπεια, οργανώθηκε μια νέα εταιρεία με την συμμετοχή των εταιριών Acorn, VLSI και Apple Computer ως ιδρυτικοί συνεργάτες, γνωστοί ως ARM Ltd. Οι Acorn RISC Machine (ARM) έγιναν προηγμένες μηχανές RISC (Advanced RISC Machine). Η ARM αποκτήθηκε το 2016 από τις ιαπωνικές τηλεπικοινωνίες από την εταιρεία SoftBank Group. Στην εικόνα 3.22 φαίνεται η αρχιτεκτονική ARM του προϊόντος Cortex-M3.



Εικόνα 3.22

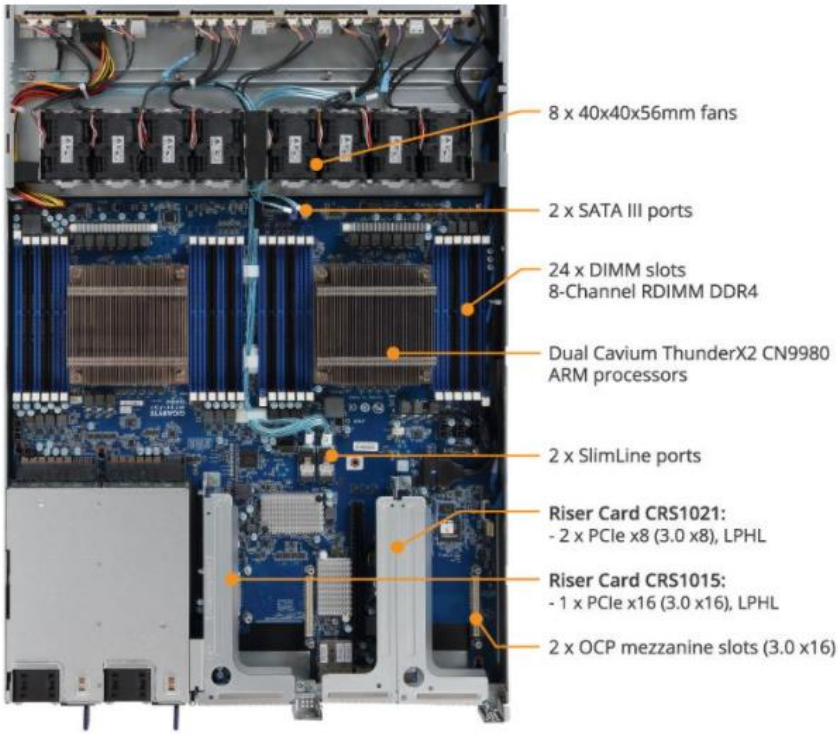
3.5. Διακομιστές σε ARM αρχιτεκτονική

Παρόλο που οι επεξεργαστές x86 υπήρξαν το βασικό στοιχείο στα κέντρα δεδομένων των επιχειρήσεων και των παρόχων cloud, οι διακομιστές που βασίζονται σε ARM εμφανίστηκαν στα τέλη της δεκαετίας του 2010. Για παράδειγμα, η AMD άρχισε να προσφέρει τους διακομιστές ARM Opteron A1100 το 2016. Το 2018, η Ampere ξεκίνησε τους πρώτους επεξεργαστές που βασίζονται σε ARM για διακομιστές. Αν και η αρχιτεκτονική x86 της Intel κυριαρχεί σχεδόν αποκλειστικά στον κόσμο των διακομιστών, σήμερα οι διακομιστές ARM καλούνται να παρέχουν παρόμοια ή μεγαλύτερη ισχύ επεξεργασίας από τους αντίστοιχους διακομιστές x86 ενώ καταναλώνουν λιγότερη ενέργεια και παράγουν λιγότερη θερμότητα, έτσι αναμένεται να κερδίσουν κάποιο μερίδιο αγοράς.

Στην διάρκεια των τελευταίων ετών πολλές εταιρίες έχουν επενδύσει τεράστια ποσά για να προωθήσουν τη βιομηχανία διακομιστών ARM, άλλες είδαν τις προσπάθειές τους να λήγουν σύντομα, όπως η Broadcom (με τα chip διακομιστή Vulcan ARM) ή η Qualcomm με τα σχέδια επεξεργαστών Amberwing, ενώ άλλες εταιρείες όπως η AWS με το τσιπ διακομιστή Graviton ARM, η Huawei Technlogies, με τη θυγατρική της HiSilicon ή η Gigabyte προωθούν την αγορά διακομιστών ARM.

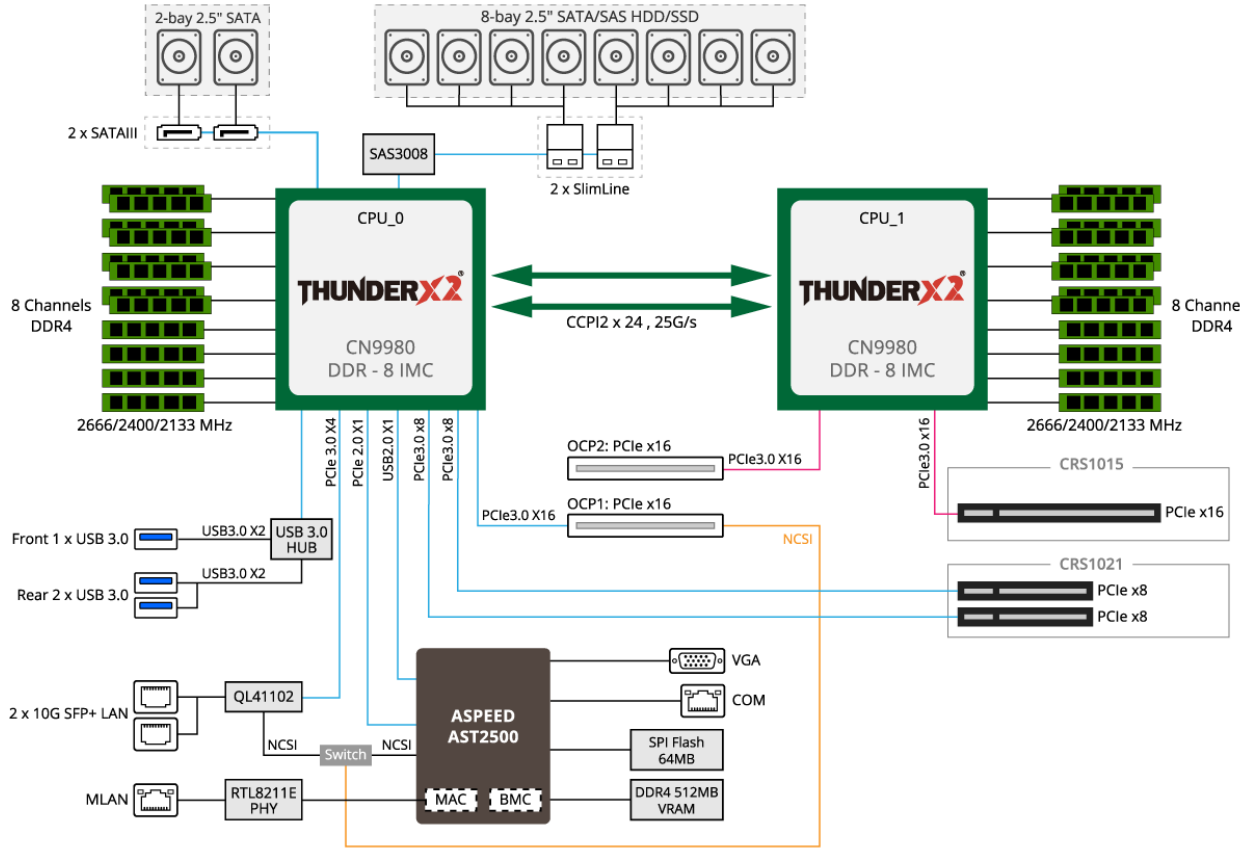
3.5.1. Οι διακομιστές ARM της Gigabyte

R181-T92 1U 2P ThunderX2: Είναι ένας διακομιστής διπλού επεξεργαστή 1U (ο διακομιστής 1U είναι ένας επίπεδος διακομιστής που καταλαμβάνει μία μονάδα χώρου όταν είναι τοποθετημένος σε ένα πλαίσιο διακομιστή βάσης). Αυτό σημαίνει ότι μπορεί κανείς να πάρει έως 64 πυρήνες και 256 νήματα ανά U χρησιμοποιώντας 4-way SMT στο ThunderX2. Αυτές οι CPU είναι τοποθετημένες στη μητρική κάρτα κάτι που εξοικονομεί σημαντικά το κόστος της. Μερικές από τις αξιοσημείωτες δυνατότητες είναι οι ενσωματωμένες διεπαφές Broadcom SAS3008 HBA και QLogic SFP + 10GbE. Ο Gigabyte R181-T92 φαίνεται να μοιράζεται την ίδια μητρική πλακέτα με τον Gigabyte R281-T94 2U.



Εικόνα 3.23

Το διάγραμμα μπλοκ δείχνει τις κύριες δυνατότητες, όπως η συνδεσιμότητα PCIe και OCP, η συνδεσιμότητα αποθήκευσης και η διαμόρφωση μνήμης 24x DDR4 σε 8-κανάλια.



Εικόνα 3.24

Τα λειτουργικά συστήματα που υποστηρίζει είναι:

- RHEL 7.5 64bit (ARM64)
- Ubuntu 18.04 (ARM64)
- SUSE SLES 15 (ARM64)
- CentOS 7.6 64bit (ARM64)
- Oracle Linux 7.4 (ARM64)

Μια άλλη εναλλακτική λύση είναι ο **R281-T94 2U 2P.** Οι διαφορές του με τον παραπάνω μοντέλο, εκτός από το μέγεθος του καθώς είναι 2U, είναι ότι έχει περισσότερες θέσεις για τοποθέτηση αποθηκευτικών μέσων, περισσότερες θύρες καρτών επέκτασης και περισσότερες θύρες συνδεσιμότητας όπως USB και LAN.

3.5.2. Ο διακομιστής Ampere Altra σε ARM αρχιτεκτονική

Ο πρώτος διακομιστής για cloud υπηρεσίες σε ARM αρχιτεκτονική

Η Ampere παρουσίασε στις 3 Μαρτίου 2020 τον πρώτο επεξεργαστή διακομιστή 64-bit που βασίζεται σε ARM αρχιτεκτονική 80-core στον κλάδο, σε μια προσπάθεια να ξεπεράσει την Intel και την AMD σε CPU για data center.

Η Ampere ανακοίνωσε ότι άρχισε να παρέχει δείγματα του επεξεργαστή Ampere Altra για σύγχρονα κέντρα δεδομένων cloud και edge computing. Ο επεξεργαστής Ampere Altra λειτουργεί με 210 watts και στοχεύει σε εφαρμογές διακομιστή όπως ανάλυση δεδομένων, τεχνητή νοημοσύνη, βάσεις δεδομένων, αποθήκευση, στοίβες telco, υπολογιστές αιχμής, φιλοξενία ιστοσελίδων και εφαρμογές εγγενών cloud.

Εικόνα 3.25

Η Intel κυριαρχεί στο 95,5% της αγοράς chip για server με τους επεξεργαστές που βασίζονται σε x86 και η AMD έχει τα υπόλοιπα. Ωστόσο, η Ampere στοχεύει σε λειτουργίες υψηλής απόδοσης και υψηλής χωρητικότητας μνήμης.

Η Ampere Computing, που ιδρύθηκε το 2017 από την πρώην πρόεδρο της Intel, Renee James, βασίστηκε στην αρχική IP και το ταλέντο σχεδιασμού των CPU X-Gene της AppliedMicro και με την Arm Holdings να γίνει επενδυτής το 2019, είναι αυτή τη στιγμή ο μοναδικός προμηθευτής σχεδιασμού και προσφορά σχεδίων διακομιστή Neoverse-N1.

Η Renee James δήλωσε σε συνέντευξή της στη VentureBeat ότι το τσιπ είναι ταχύτερο από έναν επεξεργαστή AMD Epyc 64 πυρήνων και από έναν Xeon “Cascade Lake” της Intel με 28 πυρήνες.

Η Santa Clara, Ampere με έδρα την Καλιφόρνια υποστηρίζεται από την ιδιωτική εταιρεία επενδύσεων μετοχών, την Carlyle Group. Η James ελπίζει να πάρει την Intel με την αρχιτεκτονική ARM που χρησιμοποιείται στα smartphones του κόσμου και γνωστή για την αποτελεσματικότητά της στην απόδοση σε πολύ χαμηλά επίπεδα ισχύος. Η εταιρία Ampere δημιουργήθηκε από τις στάχτες της εταιρίας Applied Micro Circuits. Η εταιρία Ampere βγήκε στην αγορά περίπου το 2019 και συνεργάζεται με μεγάλους κατασκευαστές υπολογιστών γνήσιων συσκευών παγκόσμιας κλάσης και κατασκευαστές γνήσιου εξοπλισμού.

Η κατηγορία των τσιπ διακομιστών ARM 64-bit πέρασε από τον δικό της κύκλο διαφημίσεων πριν από μερικά χρόνια, με εταιρείες όπως οι Advanced Micro Devices και η Applied Micro που προσπαθούν να σχεδιάσουν τσιπ βασισμένα σε ARM αντί για την αρχιτεκτονική x86 της Intel, η οποία τροφοδοτεί σχεδόν όλο τον κόσμο υπολογιστές και Mac για Windows. Αλλά αυτές οι εταιρείες απέτυχαν. Η AMD έκλεισε το έργο της για ARM αρχιτεκτονικές και η Macom απέκτησε την Applied Micro το 2016. Ο όμιλος Carlyle αγόρασε το τμήμα της κεντρικής μονάδας επεξεργασίας (CPU) της Applied Micro από τη Macom το 2017. Η εξαγορά ολοκληρώθηκε στα τέλη του περασμένου έτους και η James ανέλαβε CEO, αφήνοντας τη θέση της ως εκτελεστικό στέλεχος στο Carlyle Group.

Ο Jeff Wittich, ανώτερος αντιπρόεδρος προϊόντων, δήλωσε σε συνέντευξή του ότι το Ampere Altra σχεδιάστηκε για να παρέχει τα χαρακτηριστικά που απαιτούν όλο και περισσότερο οι πελάτες και ειδικά βελτιστοποιημένα για τη χρήση cloud. Ο τρόπος με τον οποίο το cloud χρησιμοποιεί την απόδοση, την ασφάλεια και την απόδοση ισχύος είναι

πολύ διαφορετικός από τα πιο παραδοσιακά περιβάλλοντα εταιρικών κέντρων δεδομένων.
Η κατανάλωση ενέργειας είναι επίσης μια αυξανόμενη πρόκληση για όλα τα σύγχρονα κέντρα δεδομένων, ειδικά εκείνα που λειτουργούν σε μεγάλη κλίμακα. Λόγω της αύξησης των περιπτώσεων χρήσης κέντρων δεδομένων, η κατανάλωση ενέργειας συνεχίζει να αυξάνεται. Εκτιμάται ότι τα κέντρα δεδομένων χρησιμοποιούν επί του παρόντος το 3% της παγκόσμιας ηλεκτρικής ενέργειας και αυτό αναμένεται να αυξηθεί στο 11% έως το 2030. Η απλή αναβάθμιση των υφιστάμενων CPU δεν αρκεί για να αντιμετωπίσει την ανάγκη για περισσότερους υπολογιστές για την τροφοδοσία της έκρηξης δεδομένων .
Οι πυρήνες ενός σπειρώματος της Ampere Altra και οι πυκνοί, αποδοτικοί διακομιστές που κάνουν εφικτοί, θα επιτρέψουν στους πελάτες να μεγιστοποιήσουν τον αριθμό των υπηρεσιών που μπορούν να αναπτύξουν στο cloud και στο edge, δήλωσε η εταιρεία.
Ο επεξεργαστής Ampere Altra βασίζεται στην πλατφόρμα Arm Neoverse N1 και αντιπροσωπεύει μια σημαντική ανακάλυψη στην απόδοση και την αποδοτικότητα ισχύος για υπολογισμούς σε υψηλές κλίμακες. Η Ampere συνεργάστηκε επίσης στενά με την TSMC για να χρησιμοποιήσει την τεχνολογία επεξεργασίας 7 νανομέτρων για την υψηλότερη απόδοση, τα πιο αποδοτικά και πιο πυκνά τρανζίστορ. Σε μια διαδικασία 7 νανομέτρων, τα τσιπ κυκλώματα έχουν πλάτος επτά δισεκατομμυρίων μέτρων. Το Ampere Altra τρέχει στα 3 gigahertz.
Η Ampere ξεκίνησε να παρέχει ήδη δείγματα για τον διακομιστή Ampere Altra το Μάρτιο του 2020 σε πελάτες σε όλο τον κόσμο, συμπεριλαμβανομένων πολλών από τους κορυφαίους παρόχους υπηρεσιών cloud, με διαθέσιμες πλατφόρμες 2-socket και 1-socket. Η πλήρης παραγωγή ξεκίνησε στα μέσα του 2020.

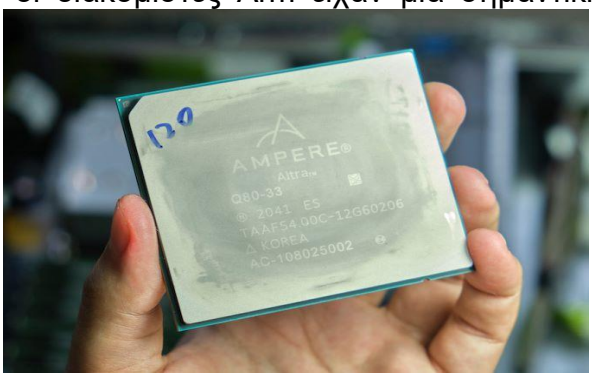
Εικόνα 3.26

Ο Leendert van Doorn, μηχανικός της Microsoft Azure, δήλωσε ότι το Ampere Altra βοηθά στην ενίσχυση της επεξεργασίας κέντρου δεδομένων μεγάλης κλίμακας γύρω από την απόδοση ισχύος, την ανθεκτικότητα, την τηλεμετρία και την ασφάλεια. Η Ampere είχε επίσης υποστηρικτικές δηλώσεις από Oracle, Canonical, VMware, Kinvolk, Packet, Lenovo, Gigabyte, Wiwynn και Micron. Σύμφωνα με τον Jeff Wittich,ανώτερο αντιπρόεδρο προϊόντων της εταιρίας Ampere δήλωσε «Το μεγάλο πράγμα τώρα είναι ότι αν κοιτάξετε σε όλα τα επίπεδα, το επίπεδο λειτουργικού συστήματος - από το Linux έως το BSD στα Windows - όλα υποστηρίζουν την ARM».
Στην τυποποίηση εικονικοποίησης, υπάρχει υποστήριξη από Kubernetes, Docker, VMware και KBM. Όλα υποστηρίζονται εκεί. Σε επίπεδο εφαρμογής, όλα όσα τρέχουν στο cloud σήμερα τρέχουν ήδη και στον νέο server της Ampere.
Ο Wittich ανέφερε επίσης ότι το τσιπ της Ampere είναι 14% καλύτερο από το γρηγορότερο τσιπ Epyc της AMD για αποδοτικότητα ισχύος και 4% γρηγορότερο σε ακατέργαστη απόδοση. Αναφέρει επίσης ότι ήταν 2,11 φορές καλύτερο από το ανταγωνιστικό τσιπ της

Intel για απόδοση ισχύος και 2,23 φορές καλύτερο στην πρώτη απόδοση. Συνεχίζοντας ανέφερε ότι αυτό σημαίνει ότι μπορούμε να βάλουμε σε ένα RACK διακομιστή 42 μονάδων χωρίς να εξαντληθεί.

Παρουσίαση του Ampere Altra Arm διακομιστή με 2 socket των 80 πυρήνων

Το έτος 2020 ήταν πράγματι το έτος όπου οι διακομιστές Arm είχαν μια σημαντική ανακάλυψη. Ο νέος πυρήνας του Neoverse-N1 CPU της Arm ήταν ο πρώτος αληθινός αφιερωμένος πυρήνας διακομιστή των σχεδιαστών IP, που υπόσχεται εστιασμένη απόδοση και αποδοτικότητα για τα κέντρο δεδομένων. Νωρίτερα μέσα στη χρονιά δοκιμάστηκε το πρώτο πυρίτιο Neoverse-N1 με τη μορφή του Graviton2 του Amazon μέσα από την προσφορά υπολογιστικού νέφους AWS EC2. Το Graviton2 φάνηκε σαν ένα πολύ εντυπωσιακό σχέδιο, αλλά ήταν μάλλον συντηρητικό στους στόχους του, και είναι επίσης ένα κομμάτι υλικού στο οποίο το ευρύ κοινό δεν μπορεί να έχει πρόσβαση εκτός των υπηρεσιών cloud της Amazon.



Εικόνα 3.27

Η εταιρεία είχε μερικά προϊόντα με τη μορφή τσιπ eMAG, αλλά με μάλλον απογοητευτικά στοιχεία απόδοσης - κατανοητό δεδομένου ότι αυτά ήταν ουσιαστικά προϊόντα παλαιού τύπου βασισμένα στην παλιά μικρο-αρχιτεκτονική X-Gene.

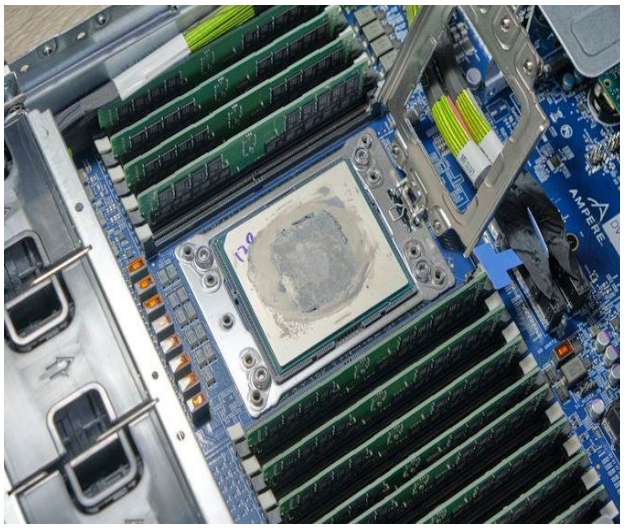

Εικόνα 3.28

Η νέα σειρά προϊόντων Altra της Ampere, από την άλλη πλευρά, είναι το αποκορύφωμα πολλών ετών εργασίας και στενής συνεργασίας με την Arm - και το πρώτο "αληθινό" προϊόν της εταιρείας που μπορεί να θεωρηθεί ως γενεαλογικό Ampere.

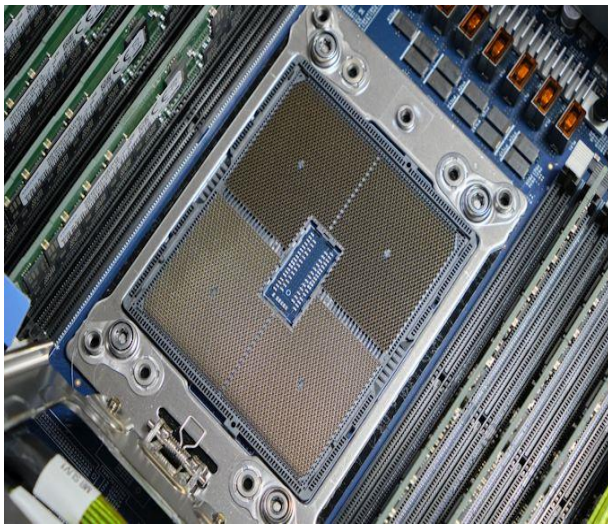
Η Ampere παράσχει τον σχεδιασμό αναφοράς διακομιστή της εταιρείας, που ονομάζεται «Mount Jade», ένα διακομιστή 2-υποδοχών socket. Ο διακομιστής εφοδιάστηκε με δύο επεξεργαστές Altra Q80-33, τον κορυφαίο SKU της Ampere, ο καθένας με 80 πυρήνες που λειτουργούν στα 3.3GHz, με το Thermal Design Power (TDP) να φτάνει τα 250W ανά υποδοχή.

Ο διακομιστής σχεδιάστηκε με στενή συνεργασία με τη Wiwynn για την υλοποίηση του διπλού socket και με την GIGABYTE για την παραλλαγή του ενός socket. Η μητρική

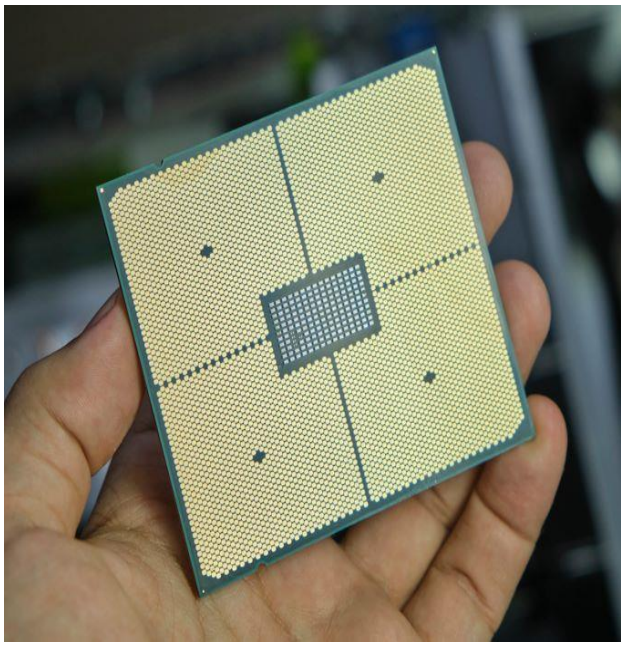
πλακέτα αναφοράς Mount Jade DVT με την επωνυμία Ampere διατίθεται σε ένα τυπικό συνδυασμό μπλε χρώματος διακομιστή και διαθέτει 2 socket με έως και 16 υποδοχές DIMM ανά socket, φτάνοντας έως και χωρητικότητα DRAM 4 TB ανά socket.
Αυτή επίσης είναι η πρώτη ματιά στον σχεδιασμό socket πρώτης γενιάς του Ampere. Η εταιρεία δεν εμπορεύεται κανένα συγκεκριμένο όνομα στο socket, αλλά είναι ένα τεράστιο socket LGA4926 με αριθμό pin που υπερβαίνει οποιαδήποτε άλλο εμπορικό socket διακομιστή από την AMD ή την Intel. Ο μηχανισμός συγκράτησης είναι κάπως παρόμοιος με αυτόν του συστήματος SP3 της AMD, με έναν μηχανισμό συγκράτησης που τεντώνεται από ένα σύστημα βιδών 5 σημείων όπως φαίνεται στις παρακάτω εικόνες.



Εικόνα 3.29


Εικόνα 3.30

Το ίδιο το τσιπ είναι απολύτως τεράστιο και μεταξύ των τωρινών διαθέσιμων στο κοινό επεξεργαστών είναι ο μεγαλύτερος στη βιομηχανία, με μέγεθος συσκευασίας SP3 τύπου AMD, με διαστάσεις 77 x 66,8 mm περίπου - περίπου του ίδιου μήκους αλλά σημαντικά μεγαλύτερο από τους αντίστοιχους της AMD.

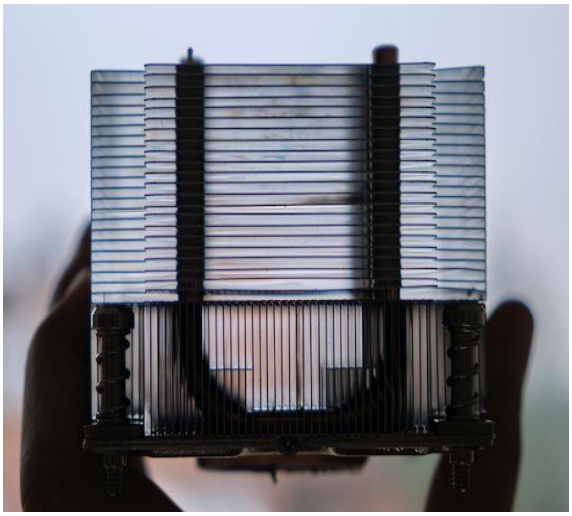


Εικόνα 3.31

Εικόνα 3.32

Παρόλο που είναι ένα τεράστιο τσιπ με τεράστιο IHS, ο διακομιστής Mount Jade έχει μικρή ψύκτρα κάνοντας επαφή με περίπου το 1/4 της επιφάνειας του επεξεργαστή. Αυτό φαίνεται και στις παρακάτω εικόνες.

Εικόνα 3.33



Εικόνα 3.34

3.6. Αρχιτεκτονικές Motherboard

Αρχιτεκτονική von Neumann

Οι περισσότεροι σύγχρονοι υπολογιστές εξακολουθούν να χρησιμοποιούν την αρχιτεκτονική von Neumann. Η ιδέα του διαχωρισμού του επεξεργαστή και της μνήμης ήταν από τις πιο σημαντικές ανακαλύψεις στον σχεδιασμό της αρχιτεκτονικής. Αυτός ο διαχωρισμός οδήγησε στην ιδέα της φόρτωσης ενός προγράμματος, δηλαδή την έννοια ότι ο υπολογιστής μπορεί να χρησιμοποιηθεί για την εκτέλεση διαφόρων εργασιών. Αυτό είναι ένα από τα μοναδικά χαρακτηριστικά των υπολογιστών και προήλθε από αυτόν τον διαχωρισμό. Το υλικό παραμένει αμετάβλητο, αλλά με φόρτωση και εκτελώντας διαφορετικά προγράμματα, ο υπολογιστής συμπεριφέρεται διαφορετικά.

Ο John von Neumann σχεδίασε μια αρχιτεκτονική υπολογιστών που χρησιμοποιείται ακόμη και σήμερα στο σχεδιασμό σύγχρονων υπολογιστών. Στην πραγματικότητα, εφαρμόστηκε αργότερα η αρχή της αρθρωτότητας. Η αρχιτεκτονική von Neumann αποτελείται από μια κοινόχρηστη μνήμη (ισοδύναμη στη βραχυπρόθεσμη μνήμη σε ανθρώπους) που χρησιμοποιείται για την αποθήκευση τόσο οδηγιών όσο και δεδομένων. Το μοντέλο ορίζει πολλά διαφορετικά αλλά διασυνδεδεμένα συστατικά που περιλαμβάνουν την αρχιτεκτονική υπολογιστή. Το μοντέλο αναφέρεται ως αποθηκευμένο μοντέλο προγράμματος, καθώς επιτρέπει διαφορετικά προγράμματα να φορτωθούν στη μνήμη του υπολογιστή, σε αντίθεση με τα μονά προγράμματα που ήταν διαθέσιμο στα πρώτα μοντέλα. Μια σημαντική αρχή που προήλθε από την αρχιτεκτονική von Neumann και προχώρησε στη χρήση υπολογιστών μειώνοντας ταυτόχρονα τις τιμές τους είναι η αρθρωτότητα. Το μοντέλο ορίζει πολλές λειτουργικές μονάδες με ξεχωριστό διαχωρισμό μεταξύ τους. Για παράδειγμα:

- *Διαχωρισμός της κεντρικής μονάδας επεξεργασίας από τη μνήμη*. Η κεντρική μονάδα επεξεργασίας (ή ο επεξεργαστής) είναι υπεύθυνος για την εκτέλεση των εντολών και δεν σχετίζεται με κανέναν τρόπο με την τοποθεσία των εντολών ή των δεδομένων. Ο επεξεργαστής είναι το ηλεκτρονικό ισοδύναμο του εγκεφάλου στο ανθρώπινο σώμα. Ένα ειδικό συστατικό στοιχείο της μονάδας ελέγχου στο εσωτερικό του επεξεργαστή είναι υπεύθυνο για ανάκτηση των οδηγιών και των τελεστών που απαιτούνται για την εκτέλεσή του. Ένα παρόμοιο συστατικό είναι υπεύθυνο για τη συλλογή του αποτελέσματος της εκτελεσμένης εντολής και την αποθήκευσή του σε καθορισμένη τοποθεσία.
- *Ορισμός ενός μοναδικού μηχανισμού αποθήκευσης δεδομένων και ανάκτησης δεδομένων από τη μνήμη*. Το βασικό νόημα είναι ότι το σύστημα υπολογιστή μπορεί να θεωρήσει τα προγράμματα ως δεδομένα και να φορτώσει το

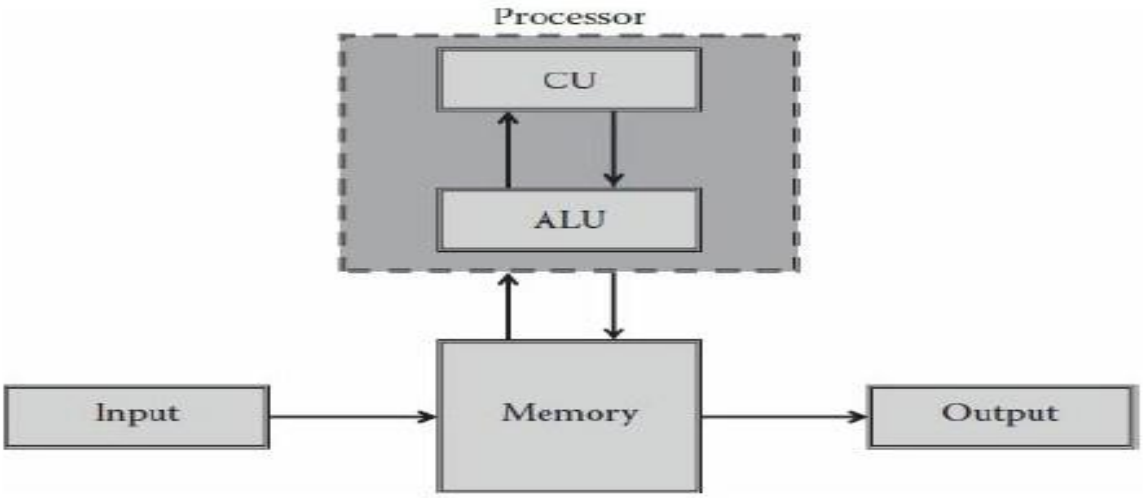
πρόγραμμα στη μνήμη του για εκτέλεση. Αυτός ο μηχανισμός είναι η βάση για το αποθηκευμένο πρόγραμμα μοντέλο. Ο διαχωρισμός της μνήμης από τον επεξεργαστή και η κατανόηση αυτών των δεδομένων και των προγραμμάτων ότι είναι μεταβλητές που μπορούν να αλλάξουν, άνοιξαν το δρόμο για τους σύγχρονους υπολογιστές. Τέτοιοι υπολογιστές είναι ικανοί να εκτελούν παράλληλα πολλά προγράμματα. Αυτά τα προγράμματα αλλάζουν τη λειτουργικότητα του συστήματος όπως ορίζεται από κάθε πρόγραμμα. Επιπλέον, η ικανότητα εκτέλεσης αρκετών προγραμμάτων / εφαρμογών παράλληλα επιτρέπουν στον υπολογιστή να παρέχει διαφορετικές λειτουργίες σε διαφορετικούς χρήστες, καθώς και διαφορετικές λειτουργίες του ίδιου χρήστη σε διαφορετικά παράθυρα.

❖ *Διαχωρισμός της μονάδας εκτέλεσης από τη μονάδα ελέγχου*. Αρχικά, οι δύο μονάδες συνδυάστηκαν στη μονάδα εκτέλεσης, η οποία είναι υπεύθυνη για την εκτέλεση των οδηγιών των προγραμμάτων. Μετά τον διαχωρισμό, η μονάδα ελέγχου είναι υπεύθυνη για τον προγραμματισμό της εκτέλεσης καθώς και για την παροχή όλων των απαραίτητων για την εκτέλεση (εντολές, τελεστές), ενώ μόνο η μονάδα εκτέλεσης εκτελεί τις εντολές.

❖ *Διαχωρισμός των μονάδων εισόδου και εξόδου από άλλα στοιχεία του συστήματος διαχωρίζοντας κάθε μονάδα από τις άλλες μονάδες*. Το αποτέλεσμα, για παράδειγμα, είναι ο υψηλός βαθμός αρθρωτότητας όπου όλοι απολαμβάνουμε με τον προσωπικό υπολογιστή. Λόγω αυτού του διαχωρισμού, μπορεί κάποιος να αγοράσει έναν υπολογιστή από κάποιον κατασκευαστή, ενώ το ποντίκι και το πληκτρολόγιο μπορούν να ληφθούν ξεχωριστά και να συνδεθούν στον υπολογιστή, μαζί με άλλες συσκευές εισόδου και εξόδου.

Αυτός ο υψηλός βαθμός αρθρωτότητας σπάνια απαντάται σε άλλες ηλεκτρονικές συσκευές, εκτός εάν αυτές οι συσκευές χρησιμοποιούν ενσωματωμένους υπολογιστές. Στις ηλεκτρονικές συσκευές, κάποιος μπορεί να αντικαταστήσει ηλεκτρονικά εξαρτήματα, αλλά συνήθως χρησιμοποιεί άλλα πρωτότυπα ή συμβατά στοιχεία. Αυτά τα αντικατασταθέντα εξαρτήματα πρέπει να είναι πλήρως συμβατά και να παρέχουν την ίδια λειτουργικότητα. Ο υπολογιστής, μέσω των τυπικών διεπαφών του, επιτρέπει στο χρήστη να αντικαταστήσει ένα στοιχείο, για παράδειγμα έναν σκληρό δίσκο, με έναν άλλο εντελώς διαφορετικό κατασκευαστή. Αντί για περιστρεφόμενο σκληρό δίσκο, μπορεί κάποιος να εγκαταστήσει έναν Solid State Disk (SSD) που λειτουργεί πολύ πιο γρήγορα ή, εναλλακτικά, έναν άλλο περιστρεφόμενο σκληρό δίσκο με σημαντικά μεγαλύτερη χωρητικότητα.

Παρακάτω στην εικόνα 3.35 παρουσιάζεται η αρχιτεκτονική von Neumann με τα κύρια στοιχεία της :



Εικόνα 3.35

➢ Η ALU (αριθμητική και λογική μονάδα) είναι υπεύθυνη για την εκτέλεση της εντολής βάσει των δεδομένων που λαμβάνονται από τη μονάδα ελέγχου.

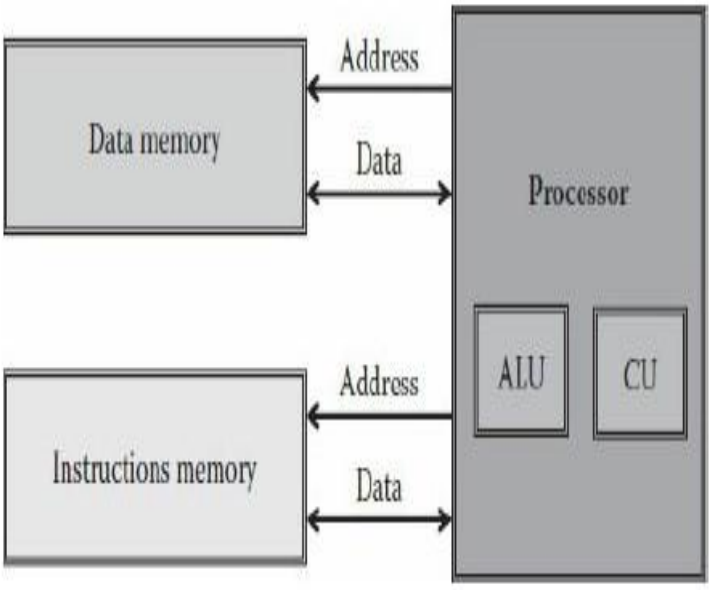
➢ Η CU (μονάδα ελέγχου) είναι υπεύθυνη για τον προγραμματισμό των εντολών εκτέλεσης, τη λήψη των εντολών, την αποκωδικοποίηση και ανάκτηση των τελεστών, εάν υπάρχουν.

- Οι μονάδες εισόδου και εξόδου παρέχουν το μηχανισμό σύνδεσης με τον έξω κόσμο (χρήστες, άλλα συστήματα, διάφορες συσκευές).
- Η μνήμη προορίζεται για την αποθήκευση των εντολών και των δεδομένων.

Η πρώτη εφαρμογή της αρχιτεκτονικής von Neumann πραγματοποιήθηκε στο Ινστιτούτο Προηγμένων Τεχνολογιών (IAS) στο Πανεπιστήμιο του Princeton. Ο υπολογιστής IAS είχε τη δυνατότητα να φορτώνει προγράμματα, σε αντίθεση με τις προηγούμενες χειροκίνητες ρυθμίσεις διακοπτών. Ο υπολογιστής σχεδιάστηκε ειδικά για πολύπλοκους μαθηματικούς υπολογισμούς, χρησιμοποιώντας δυαδικούς αριθμούς και είχαν και αρκετούς καταχωρητές.

Αρχιτεκτονική Harvad

Παράλληλα με την ανάπτυξη της αρχιτεκτονικής von Neumann, μία άλλη ελαφρώς διαφορετική αρχιτεκτονική αναπτύχθηκε στο Χάρβαρντ που βασίστηκε στην εμπειρία που συγκεντρώθηκε από την ανάπτυξη του Mark I. Στην αρχιτεκτονική του Χάρβαρντ δόθηκε ιδιαίτερη έμφαση σε έναν επιπλέον διαχωρισμό μεταξύ δύο τύπων μνήμης. Ένας τύπος είναι η μνήμη που χρησιμοποιείται για εντολές και ο άλλος τύπος χρησιμοποιείται για δεδομένα. Αυτός ο διαχωρισμός απαιτούσε πρόσθετα κανάλια ικανά να μεταφέρουν δεδομένα και εντολές ταυτόχρονα. Αυτό το επιπλέον επίπεδο παραλληλισμού παρέχει καλύτερη και περισσότερη απόδοση. Ενώ ο επεξεργαστής λαμβάνει την επόμενη εντολή, μπορεί να φέρει τον τελεστή που απαιτείται για τις εκτελέσεις. Αυτές οι δύο μεταφορές μπορούν να πραγματοποιηθούν ταυτόχρονα χρησιμοποιώντας δύο διακριτά κανάλια. Ο διαχωρισμός των μνημών, σε συνδυασμό με το γεγονός ότι η καθεμία έχει ένα διαφορετικό κανάλι, παρέχει πρόσθετες δυνατότητες. Αυτά μπορεί να είναι ετερογενή κανάλια με διαφορετικά χαρακτηριστικά που μπορεί να είναι χρήσιμα κατά την ανάπτυξη αρχιτεκτονικών που ταιριάζουν καλύτερα σε συγκεκριμένες ανάγκες (εικόνα 3.36).



Εικόνα 3.36

Για το λόγο αυτό, πολλά συστήματα επεξεργασίας σήματος βασίζονται στην αρχιτεκτονική του Χάρβαρντ, η οποία είναι πιο προβλέψιμη από άποψη εκτέλεσης.

Αυτό επιτυγχάνεται λόγω των λιγότερο πιθανών συγκρούσεων στο κανάλι. Αυτή η υψηλότερη προβλεψιμότητα είναι ένας λόγος που αυτή η αρχιτεκτονική χρησιμοποιείται και για πολλά συστήματα σε πραγματικό χρόνο. Σε αντίθεση με τα «συνηθισμένα» συστήματα, τα συστήματα σε πραγματικό χρόνο πρέπει να διασφαλίζουν την εκτέλεση σε ένα περιβάλλον με επαναπροσδιορισμένο χρονικό παράθυρο.

3.7. Αρχιτεκτονικές κύριας μνήμης

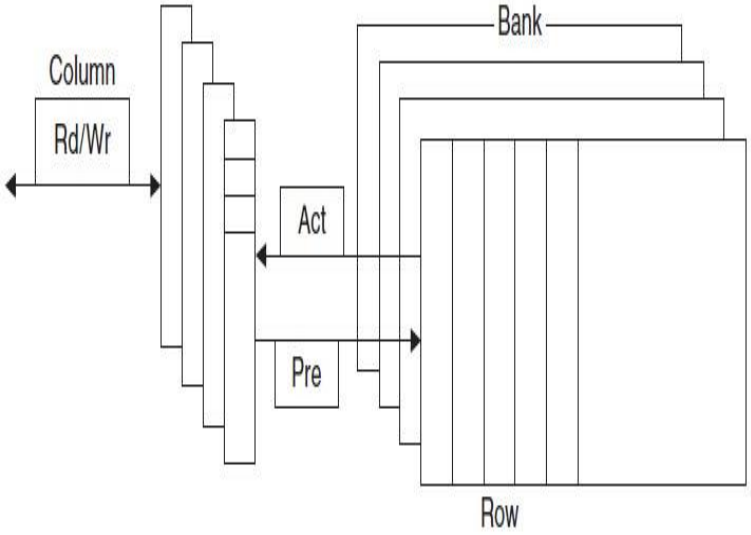
Η κύρια μνήμη είναι το επόμενο επίπεδο κάτω στην ιεραρχία μετά από την κεντρική μονάδα επεξεργασίας και την μητρική. Η κύρια μνήμη ικανοποιεί τις απαιτήσεις σε cache μνήμη και χρησιμεύει ως διεπαφή Εισόδου/Εξόδου, καθώς είναι ο προορισμός της πηγής εισαγωγής καθώς και η πηγής εξόδου. Δίνεται ιδιαίτερη έμφαση στην απόδοση της κύριας μνήμης τόσο στην καθυστέρηση όσο και στο εύρος ζώνης. Η καθυστέρηση της κύριας μνήμης είναι το κύριο μέλημα της προσωρινής μνήμης (cache), ενώ το εύρος ζώνης της κύριας μνήμης είναι το κύριο μέλημα των πολυεπεξεργαστών και του I / O.
Στο παρελθόν, η καινοτομία ήταν πώς να οργανωθούν τα πολλά chips DRAM, από τα οποία αποτελείται η κύρια μνήμη, σε πολλές τράπεζες μνήμης. Το υψηλότερο εύρος ζώνης επιτυγχάνονταν χρησιμοποιώντας τράπεζες μνήμης. Όμως καθώς αυξάνεται η χωρητικότητα ανά τσιπ μνήμης, υπάρχουν λιγότερα chip με το ίδιο μέγεθος μνήμης, μειώνοντας τις δυνατότητες για ευρύτερα συστήματα μνήμης με την ίδια χωρητικότητα.
Για να επιτρέπεται στα συστήματα μνήμης να συμβαδίζουν με τις απαιτήσεις του σύγχρονου εύρους ζώνης των επεξεργαστών, άρχισαν να υλοποιούνται νέες καινοτομίες μνήμης μέσα στα ίδια τα DRAM chip.
Σχεδόν όλοι οι υπολογιστές από το 1975 έχουν χρησιμοποιήσει DRAM για κύρια μνήμη και SRAM για προσωρινή μνήμη, με ένα έως τρία ενσωματωμένα επίπεδα στο τσιπ επεξεργαστή στην CPU.

Τεχνολογία SRAM

Το πρώτο γράμμα του SRAM (Random Access Memory) σημαίνει Static (στατική). Η δυναμική φύση των κυκλωμάτων στην DRAM (Dynamic Random Access Memory) απαιτεί την εγγραφή δεδομένων μετά την ανάγνωση - εξ ου και η διαφορά μεταξύ του χρόνου πρόσβασης και του χρόνου κύκλου καθώς και της ανάγκης ανανέωσης. Οι SRAM δεν χρειάζεται να ανανεώνονται, επομένως ο χρόνος πρόσβασης είναι πολύ κοντά στον χρόνο κάθε κύκλου.
Συνήθως στις SRAM χρησιμοποιούνται έξι τρανζίστορ ανά bit για να αποτραπεί η παρενόχληση των πληροφοριών κατά την ανάγνωση. Οι SRAM χρειάζονται ελάχιστη ισχύ για να διατήρηση της φόρτισης στην κατάσταση αναμονής.
Παλαιότερα, τα περισσότερα συστήματα επιτραπέζιων υπολογιστών και διακομιστών χρησιμοποιούσαν SRAM chip για τις κύριες, δευτερογενείς ή τριτογενείς κρυφές μνήμες. Σήμερα, και τα τρία επίπεδα cache είναι ενσωματωμένα στο chip του επεξεργαστή.
Η μεγαλύτερη cache τρίτου επιπέδου on-chip μέχρι σήμερα είναι 12 MB, ενώ το σύστημα μνήμης για έναν τέτοιο επεξεργαστή είναι πιθανό να έχει 4 έως 16 GB DRAM. Οι χρόνοι πρόσβασης για μεγάλα, τρίτου επιπέδου, cache on-chip είναι συνήθως δύο έως τέσσερις φορές μεγαλύτερη από αυτήν της προσωρινής μνήμης δευτέρου επιπέδου, η οποία εξακολουθεί να είναι τρεις έως πέντε φορές πιο γρήγορη σε σχέση με τον χρόνο πρόσβασης στη μνήμη DRAM.

Τεχνολογία DRAM

Καθώς οι πρώτες Dynamic Random Access Memory (DRAM) αυξήθηκαν σε χωρητικότητα, το κόστος ενός πακέτου με όλες τις απαραίτητες γραμμές διευθύνσεων ήταν ένα πρόβλημα. Η λύση ήταν η πολυπλεξία στις γραμμές διευθύνσεων, μειώνοντας έτσι τον αριθμό των pin διευθύνσεων στο μισό. Στην εικόνα 3.37 φαίνεται η βασική οργάνωση μίας μνήμης DRAM.



Εικόνα 3.37

Το πρώτο μισό της διεύθυνσης αποστέλλεται κατά τη διάρκεια της RAS (Row Access Strobe) πρόσβασης. Το άλλο μισό της διεύθυνσης, αποστέλλεται κατά τη διάρκεια του CAS (Column Access Strobe), το οποίο το ακολουθεί. Αυτά τα ονόματα προέρχονται από την εσωτερική οργάνωση του chip καθώς η μνήμη οργανώνεται ως ορθογώνιος πίνακας που αντιμετωπίζεται από σειρές και στήλες.

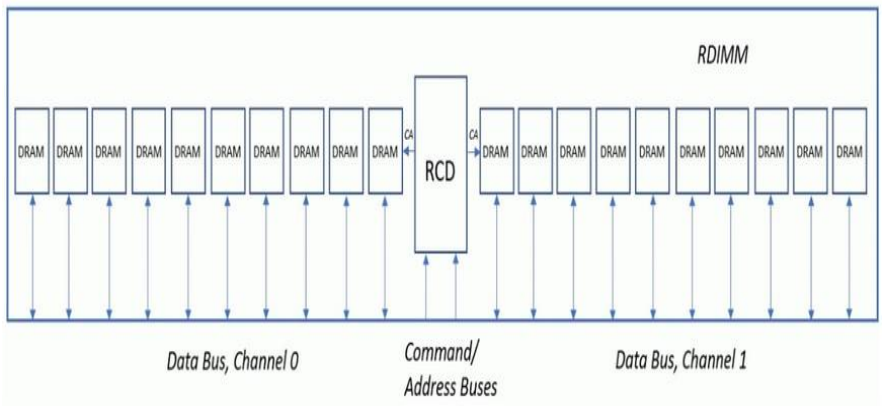
Μια πρόσθετη απαίτηση της μνήμης DRAM απορρέει από την ιδιότητας της να είναι δυναμική. Προκειμένου να συσκευασθούν περισσότερα bit ανά chip, οι μνήμες DRAM χρησιμοποιούν μόνο ένα τρανζίστορ για αποθήκευση. Η ανάγνωση αυτού του bit καταστρέφει την πληροφορία, οπότε θα πρέπει να αποκατασταθεί. Αυτός είναι ένας λόγος για τον οποίο ο χρόνος κύκλου των μνημών DRAM είναι παραδοσιακά μεγαλύτερος από τον χρόνο πρόσβασης. Πιο πρόσφατα, τα DRAM έχουν εισαγάγει πολλές τράπεζες, που επιτρέπουν την απόκρυψη του τμήματος επανεγγραφής του κύκλου. Επιπλέον, για την πρόληψη απώλειας πληροφοριών, όταν ένα bit δεν διαβάζεται ή γράφεται, το bit πρέπει να "ανανεώνεται" περιοδικά. Όλα τα κομμάτια στη σειρά μπορούν να ανανεωθούν ταυτόχρονα απλά διαβάζοντας αυτή τη σειρά. Ως εκ τούτου, κάθε DRAM στο σύστημα μνήμης πρέπει να έχει πρόσβαση σε κάθε σειρά μέσα σε ένα συγκεκριμένο χρονικό παράθυρο, όπως 8 ms. Ελεγκτές μνήμης εκτελούν τη ανανέωση των DRAM περιοδικά. Αυτή η απαίτηση σημαίνει ότι το σύστημα μνήμης είναι περιστασιακά μη διαθέσιμο γιατί στέλνει ένα σήμα που λέει σε κάθε τσιπ να ανανεώνεται. Ο χρόνος για ανανέωση είναι συνήθως μια πλήρης πρόσβαση στη μνήμη (RAS και CAS) για κάθε σειρά του DRAM. Δεδομένου ότι η μήτρα μνήμης σε ένα DRAM είναι εννοιολογικά τετράγωνο, ο αριθμός των βημάτων σε μια ανανέωση είναι συνήθως η τετραγωνική ρίζα της χωρητικότητας DRAM. Οι σχεδιαστές των μνημών DRAM προσπαθούν να διατηρήσουν τον χρόνο ανανέωσης σε λιγότερο από 5% του συνολικού χρόνου.

Ο Amdahl πρότεινε κατά κανόνα ότι η χωρητικότητα μνήμης πρέπει να αυξάνεται γραμμικά με την ταχύτητα επεξεργαστή προκειμένου να διατηρείται ένα ισορροπημένο σύστημα, έτσι ώστε ένας επεξεργαστής 1000 MIPS θα πρέπει να έχει 1000 MB μνήμης. Οι σχεδιαστές επεξεργαστών βασίζονται στις μνήμες DRAM για να ικανοποιήσουν αυτή

την απαίτηση. Στο παρελθόν, ανέμεναν τετραπλή βελτίωση της χωρητικότητας κάθε τρία χρόνια, ή 55% ετησίως. Δυστυχώς, η απόδοση των DRAM αναπτύσσονταν με πολύ πιο αργό ρυθμό.
Αν και μιλάμε για μεμονωμένα τσιπ, τα DRAM συνήθως πωλούνται σε μικρές πλακέτες που ονομάζονται μονάδες μνήμης διπλής γραμμής (Dual Inline Memory Modules – DIMM). Τα DIMM συνήθως περιέχουν 4 έως 16 DRAM και κανονικά είναι οργανωμένα σε 8 byte κατά πλάτος (+ ECC) για συστήματα επιτραπέζιων υπολογιστών και διακομιστών. Όμως οι μνήμες DRAM υπακούν στον νόμο του Moore για 20 χρόνια, παρουσιάζοντας ένα νέο chip με τετραπλάσια χωρητικότητα κάθε τρία χρόνια. Λόγω των κατασκευαστικών προκλήσεων ενός μονού-bit DRAM, τα νέα chip εμφανίζονται από το 1998 μόνο με διπλή χωρητικότητα κάθε δύο χρόνια. Το 2006, ο ρυθμός επιβραδύνθηκε περαιτέρω, με τα τέσσερα χρόνια από το 2006 έως το 2010 να βλέπουμε μόνο διπλασιασμό της χωρητικότητας.

Registered DIMM (R-DIMM)

Οι καταχωρημένες (οι οποίες καλούνται και buffered) μονάδες μνήμης (RDIMM) έχουν έναν καταχωρητή μεταξύ των μονάδων DRAM και του ελεγκτή μνήμης του συστήματος. Τοποθετούν λιγότερο ηλεκτρικό φορτίο στον ελεγκτή μνήμης και επιτρέπουν στα μεμονωμένα συστήματα να παραμένουν σταθερά με περισσότερες μονάδες μνήμης από ότι θα είχαν διαφορετικά. Σε σύγκριση με την καταχωρημένη μνήμη, η συμβατική μνήμη αναφέρεται συνήθως ως μνήμη χωρίς καταχωρητή ή μη καταχωρημένη μνήμη (UDIMM). Όταν κατασκευάζεται ως μονάδα μνήμης διπλής γραμμής (Dual In-line Memory Module – DIMM) μια καταχωρημένη μονάδα μνήμης ονομάζεται RDIMM, ενώ η μη καταχωρημένη μνήμη ονομάζεται Unregistered DIMM ή απλά DIMM. Η καταχωρημένη μνήμη είναι συχνά πιο ακριβή λόγω του χαμηλότερου αριθμού μονάδων που πωλούνται και απαιτούνται πρόσθετα κυκλώματα, οπότε απαντάται συνήθως μόνο σε εφαρμογές όπου η ανάγκη για επεκτασιμότητα και αντοχή υπερτερεί της ανάγκης για χαμηλή τιμή - για παράδειγμα, χρησιμοποιείται συνήθως καταχωρημένη μνήμη σε διακομιστές. Αν και οι περισσότερες καταχωρημένες μονάδες μνήμης διαθέτουν επίσης μνήμη κώδικα διόρθωσης σφαλμάτων (ECC), είναι επίσης πιθανό οι καταχωρημένες μονάδες μνήμης να μην διορθώνουν σφάλματα ή το αντίστροφο. Η μη καταχωρημένη μνήμη ECC υποστηρίζεται και χρησιμοποιείται σε μητρικές κάρτες διακομιστών σταθμών εργασίας ή entry-level που δεν υποστηρίζουν πολύ μεγάλες ποσότητες μνήμης.



Εικόνα 3.38

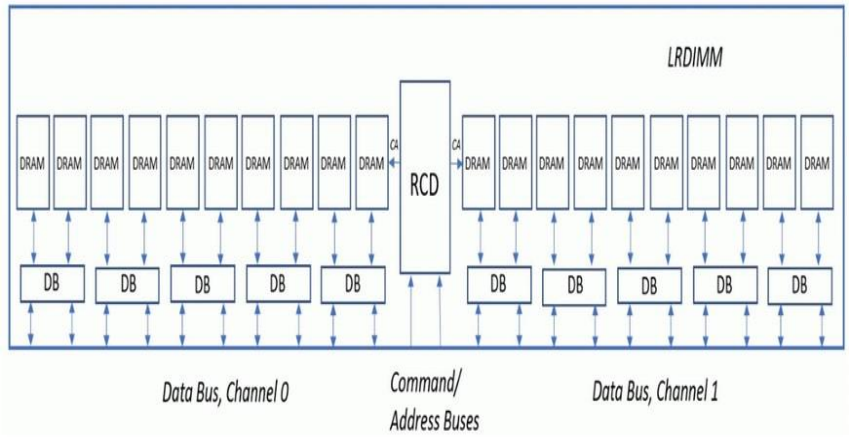
Όπως φαίνεται και στην εικόνα, ένα RDIMM έχει ένα πρόγραμμα οδήγησης ρολογιού εγγραφής (Registering Clock Driver – RCD) σε αυτό. Το RCD παίρνει το δίαυλο διεύθυνσης εντολών, τα σήματα ελέγχου και τα σήματα ρολογιού από τον κεντρικό

ελεγκτή μνήμης και στη συνέχεια τα προωθεί εκεί που βρίσκονται στο DRAM στο DIMM. Ο δίαυλος δεδομένων για τα σήματα DQ (Data Signals) και τα strobe DQ (DQS) πηγαίνει απευθείας από τον ελεγκτή μνήμης στα πακέτα DRAM. Οι μόνες λειτουργίες που είναι αποθηκευμένες στο RCD είναι ο δίαυλος εντολών/διευθύνσεων, τα σήματα ελέγχου και το ρολόι εισόδου στο DIMM. Όλοι αυτοί βγαίνουν σε όλο το DRAM στο RDIMM αφού περάσουν από το RCD και επανενεργοποιηθούν και καθαριστούν. Το RDIMM επιτρέπει μεγαλύτερη ταχύτητα σε σύγκριση με τον σχεδιασμό DIMM (UDIMM) παλαιότερης γενιάς. Η τοποθέτηση του RCD στο RDIMM βοηθά στην αύξηση του φορτίου σε σύγκριση με τα UDIMMs επειδή ρυθμίζει τα σήματα ρολογιού και τις γραμμές εντολών/διευθύνσεων. Στις μνήμες RDIMMs, τα σήματα ρολογιού και οι γραμμές εντολών/διευθύνσεων χρειάζονται επιπλέον ισχύ μονάδας δίσκου επειδή μεταβαίνουν σε όλα τα πακέτα DRAM στο DIMM. Συγκριτικά, τα σήματα DQ και DQS δεν χρειάζονται αυτήν την πρόσθετη ισχύ μονάδας δίσκου, επειδή πηγαίνουν απευθείας από τον ελεγκτή μνήμης σε ένα μόνο πακέτο DRAM ή σε πολλές σειρές πακέτων DRAM. Επίσης είναι σημαντικό να γνωρίζουμε ότι ο δίαυλος εντολών/διευθύνσεων και το ρολόι εισόδου στο RCD είναι μονοκατευθυνόμενοι από τον ελεγκτή μνήμης στο DIMM. Συγκριτικά, το δίαυλο DQ και το DQS είναι αμφίδρομα μεταξύ του ελεγκτή μνήμης και του DRAM στο RDIMM.
Όταν ένας διακομιστής έχει ρυθμιστεί με RDIMM, ο δίαυλος μνήμης λειτουργεί σε παράλληλη λειτουργία και όλα τα DRAM ελέγχονται από τον ελεγκτή μνήμης του επεξεργαστή. Καθώς όλο και περισσότερα DRAM είναι ενσωματωμένα σε ένα καταχωρημένο DIMM, η ηλεκτρική φόρτωση της μονάδας μνήμης αυξάνεται (αυτά είναι γνωστά ως Ranks - οι μονάδες μνήμης έρχονται ως Single Rank, Dual Rank και Quad Rank). Καθώς εγκαθίστανται περισσότερες τάξεις σε ένα κανάλι μνήμης, η ταχύτητα μνήμης μειώνεται ή / και η χρήση πρόσθετων υποδοχών μνήμης είναι περιορισμένη. Χρησιμοποιώντας RDIMM σε πλατφόρμες που βασίζονται σε επεξεργαστές Intel Xeon 5500, 5600 και E5, οι χρήστες περιορίζονται σε μέγιστο αριθμό 2 DIMM ανά διαμόρφωση καναλιού καθώς η ταχύτητα μνήμης μειώνεται με τη χρήση της τρίτης τράπεζας. Σήμερα, οι μονάδες Dual Rank είναι διαθέσιμες σε χωρητικότητα 16 GB, αλλά 32 GB RDIMM είναι Quad Rank, οι οποίες περιορίζονται σε 2 DIMM ανά κανάλι με πολύ χαμηλότερες ταχύτητες.

Load Reduced DIMM (LR-DIMM)

Τα LRDIMM είναι παρόμοια με τα RDIMM που χρησιμοποιούνται στη συντριπτική πλειονότητα των διακομιστών σήμερα. Όπως φαίνεται στην εικόνα, αυτό έχει επίσης ένα μόνο RCD σε αυτό και χρησιμοποιεί πολλαπλά buffer δεδομένων (DBs) για να αποθηκεύσει τα εισερχόμενα σήματα DQ και DQS μεταξύ του ελεγκτή μνήμης κεντρικού υπολογιστή και του DRAM. Το DDR5 LRDIMM έχει 10 DB και κάθε DB χειρίζεται μόνο 8 bit του διαύλου δεδομένων. Είναι ενσωματωμένα σε μονάδα μνήμης Printed Circuit Board που ταιριάζει στις ίδιες υποδοχές μνήμης διακομιστή και χρησιμοποιούν τον ίδιο τύπο τσιπ DRAM. Εκεί τελειώνουν οι ομοιότητες, καθώς τα LRDIMM λειτουργούν διαφορετικά από τα καταχωρημένα DIMM. Οι LRDIMM μπορούν να υπάρξουν εκτός αυτών των περιορισμών μέσω της χρήσης των chip μνήμης Buffer. Όταν ένας διακομιστής έχει διαμορφωθεί αποκλειστικά με LRDIMM, οι ελεγκτές μνήμης στους επεξεργαστές μεταβαίνουν αυτόματα σε Σειριακή Λειτουργία - όλα τα σήματα δεδομένων, εντολών και ελέγχου γίνονται πακέτα και μεταδίδονται στη μνήμη των LRDIMMs.

Στη συνέχεια, το Memory Buffer χειρίζεται όλα τα Reads and Writes στα DRAM chip. Οι LRDIMMs μειώνουν σημαντικά την ηλεκτρική φόρτωση των τσιπ DRAM στο δίαυλο μνήμης και μέσω μιας διαδικασίας που ονομάζεται «Rank Multiplication», μετατρέπεται ένα Quad Rank LRDIMM σε μονάδα μνήμης Dual Rank για τον ελεγκτή μνήμης. Μέσω της μείωσης των ηλεκτρικών τάξεων του LRDIMM, ο διακομιστής μπορεί στη συνέχεια να υποστηρίζει LRDIMM σε υψηλότερες ταχύτητες από τις RDIMM, και με λιγότερους περιορισμούς στα socket. Για παράδειγμα, στα 1.5V ανά μονάδα μνήμης, ένας επεξεργαστής Xeon E5 μπορεί να υποστηρίξει έως και 12 LRDIMM ή έως και 768 GB ανά διακομιστή 2 κατευθύνσεων, σε ταχύτητες μνήμης 1066MHz. Συγκριτικά, δεδομένου ότι τα 32 GB RDIMM είναι διαθέσιμα μόνο ως Quad Rank, υπάρχει όριο 8 μονάδων ανά επεξεργαστή Xeon E5 που περιορίζεται σε ταχύτητες 800MHz.



Εικόνα 3.39

Η φόρτωση των μειωμένων DIMM αντικαθιστά τον καταχωρητή με ένα στοιχείο Isolation Memory Buffer (iMB ™ by Inphi). Το iMB αποθηκεύει τα σήματα εντολών, διευθύνσεων και δεδομένων. Το iMB απομονώνει όλη την ηλεκτρική φόρτωση (συμπεριλαμβανομένων των σημάτων δεδομένων) των τσιπ μνήμης στο (LR) DIMM από τον κεντρικό ελεγκτή μνήμης. Και πάλι, οι ελεγκτές κεντρικού υπολογιστή βλέπουν μόνο το iMB και όχι τα μεμονωμένα τσιπ μνήμης. Ως αποτέλεσμα, μπορούμε να γεμίσουμε όλες τις υποδοχές DIMM με τετραπλή κατάταξη DIMM. Στην πραγματικότητα αυτό σημαίνει ότι έχουμε 50% έως 100% περισσότερη χωρητικότητα μνήμης.

R-DIMM vs LR-DIMM

Οι περισσότερες πλατφόρμες Intel E5 μπορούν να υποστηρίξουν 2 LRDIMM ανά κανάλι έως 1333MHz στα 1,5V και 3 LRDIMM ανά κανάλι στα 1066MHz, με αποτέλεσμα 12 LRDIMM ανά διαμόρφωση επεξεργαστή. Όταν χρησιμοποιούνται Quad Rank RDIMMs, χρησιμοποιούνται μόνο 8 υποδοχές ανά επεξεργαστή με προκύπτουσα ταχύτητα μνήμης 800MHz. Συγκρίνοντας 32 GB LRDIMM και 32 GB Quad Rank RDIMM, μπορούμε να δούμε ότι ένας αμφίδρομος διακομιστής E5-2600 v2 με 24 υποδοχές μνήμης μπορεί να διαμορφωθεί ως εξής:

- LRDIMMs: 32 GB x 24 = 768 GB στα 1066MHz και 1,5V και 1,35V
- RDIMMs: 32 GB x 16 = 512 GB στα 800MHz στα 1.5V

Τα LRDIMM παρέχουν υψηλότερες ταχύτητες σε υψηλότερες χωρητικότητες για χρήστες που δεν μπορούν να ικανοποιήσουν τις απαιτήσεις τους χρησιμοποιώντας 16 GB Dual Rank ή 32 GB Quad Rank RDIMMs.

Ο παρακάτω πίνακας δείχνει τις επιλογές διαμόρφωσης μνήμης για έναν διακομιστή Intel Xeon E5 v2 (Ivy Bridge) με έως και τρία DIMM(s) per Channel (3DPC) χρησιμοποιώντας τυπικές και χαμηλής τάσης μνήμες.

Standard Voltage 1.5V				**Low Voltage 1.35V**		
DIMM Type	**1 DPC**	**2 DPC**	**3 DPC**	**1 DPC**	**2 DPC**	**3 DPC**
Single-Rank RDIMM	1866	1600	1066	1600 1333	1333	800
Dual-Rank RDIMM	1866	1600	1066	1600	1333	800
Quad-Rank RDIMM	1066	800		800	800	
Quad-Rank LRDIMM	1866	1600	1066	1600	1600	1066

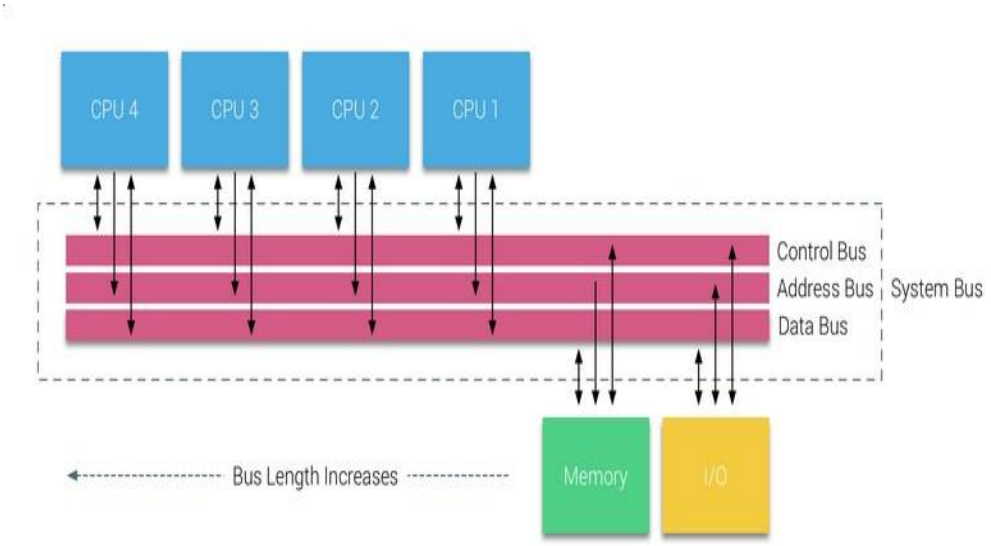
Πίνακας 3.1 Μέγιστες ταχύτητες μνήμης ανά διαμόρφωση μνήμης. Η πραγματική ταχύτητα μνήμης μιας πλατφόρμας (που ονομάζεται επίσης ρυθμός δεδομένων) είναι ένας παράγοντας της ονομαστικής ταχύτητας μνήμης του επεξεργαστή, των τάξεων και της ταχύτητας των μονάδων μνήμης και της διαμόρφωσης της πλατφόρμας σε 1DPC, 2DPC και 3DPC.

3.8. Αρχιτεκτονική Κύριας Μνήμης NUMA

Η μη ομοιόμορφη πρόσβαση στη μνήμη (Non-Uniform Memory Access - NUMA) είναι μια αρχιτεκτονική κοινόχρηστης μνήμης που χρησιμοποιείται στα σημερινά συστήματα πολλαπλής επεξεργασίας. Σε κάθε CPU εκχωρείται η δική της τοπική μνήμη και μπορεί να έχει πρόσβαση στη μνήμη από άλλες CPU του συστήματος. Η τοπική πρόσβαση στη μνήμη παρέχει χαμηλή καθυστέρηση - υψηλή απόδοση εύρους ζώνης. Η πρόσβαση στη μνήμη που ανήκει στην άλλη CPU έχει υψηλότερη καθυστέρηση και χαμηλότερη απόδοση εύρους ζώνης. Σύγχρονες εφαρμογές και λειτουργικά συστήματα όπως το ESXi (το VMware ESXi ,πρώην ESX, είναι ένας hypervisor εταιρικού τύπου, τύπου-1 που αναπτύχθηκε από την VMware για ανάπτυξη και εξυπηρέτηση εικονικών υπολογιστών) υποστηρίζουν το NUMA από προεπιλογή, αλλά για να παρέχουν την καλύτερη απόδοση, η διαμόρφωση της εικονικής μηχανής θα πρέπει να γίνει λαμβάνοντας υπόψη την αρχιτεκτονική NUMA. Εάν δεν έχει σχεδιαστεί σωστά, εμφανίζεται ασυνεπής συμπεριφορά ή υποβάθμιση της συνολικής απόδοσης για τη συγκεκριμένη εικονική μηχανή ή στη χειρότερη περίπτωση για όλα τα VM που εκτελούνται σε αυτόν τον κεντρικό υπολογιστή ESXi. Αυτή η σειρά στοχεύει στην παροχή πληροφοριών για την αρχιτεκτονική της CPU, το υποσύστημα μνήμης και τον επεξεργαστή ESXi και τον προγραμματιστή μνήμης. Επιτρέπει να δημιουργήσουμε μια πλατφόρμα υψηλής απόδοσης που θέτει τα θεμέλια για τις υψηλότερες υπηρεσίες και τις αυξημένες αναλογίες ενοποίησης.

Η εξέλιξη της αρχιτεκτονικής πολλαπλών επεξεργαστών μνήμης τις τελευταίες δεκαετίες

Μια αρχιτεκτονική που ονομαζόταν Uniform Memory Access φαινόταν ότι θα ταίριαζε καλύτερα όταν γινόταν ο σχεδιασμός για μια σταθερή πλατφόρμα χαμηλού λανθάνοντος χρόνου και υψηλού εύρους ζώνης. Ωστόσο, οι σύγχρονες αρχιτεκτονικές συστήματος θα περιορίζονταν στο να είναι πραγματικά ομοιόμορφο. Για να κατανοήσουμε τον λόγο πίσω από αυτό, πρέπει να επιστρέψουμε στην ιστορία για να εντοπίσουμε τους βασικούς οδηγούς της παράλληλης πληροφορικής.
Με την εισαγωγή σχεσιακών βάσεων δεδομένων στις αρχές της δεκαετίας του εβδομήντα, η ανάγκη για συστήματα που θα μπορούσαν να εξυπηρετήσουν πολλαπλές ταυτόχρονες λειτουργίες χρηστών και υπερβολική παραγωγή δεδομένων αποτελούσε κοινή τάση για όλους. Παρά τον εντυπωσιακό ρυθμό απόδοσης του μονού επεξεργαστή, τα συστήματα πολλαπλών επεξεργαστών ήταν καλύτερα εξοπλισμένα για να χειριστούν αυτόν τον φόρτο εργασίας.
Προκειμένου να παρέχουν ένα οικονομικά αποδοτικό σύστημα, ο κοινόχρηστος χώρος διευθύνσεων μνήμης έγινε το επίκεντρο της έρευνας. Νωρίς υποστηρίχθηκαν συστήματα που χρησιμοποιούν διακόπτη εγκάρσιας ράβδου, όπως φαίνεται στην εικόνα 3.40. Ωστόσο με αυτήν την κλιμακωτή πολυπλοκότητα σχεδιασμού και μαζί με την αύξηση των επεξεργαστών καθιστούσαν το σύστημα που βασίζεται σε bus πιο ελκυστικό. Οι επεξεργαστές σε ένα σύστημα διαύλου μπορούν να έχουν πρόσβαση σε ολόκληρο το χώρο μνήμης στέλνοντας αιτήματα στο bus, έναν πολύ οικονομικό τρόπο για να χρησιμοποιήσουμε τη διαθέσιμη μνήμη όσο το δυνατόν βέλτιστα.
Τα βασιζόμενα συστήματα σε bus είχαν τα δικά τους προβλήματα επεκτασιμότητας. Το κύριο ζήτημα είναι το περιορισμένο ποσό εύρους ζώνης, το οποίο περιορίζει τον αριθμό των επεξεργαστών που μπορεί να φιλοξενήσει το bus.



Εικόνα 3.40

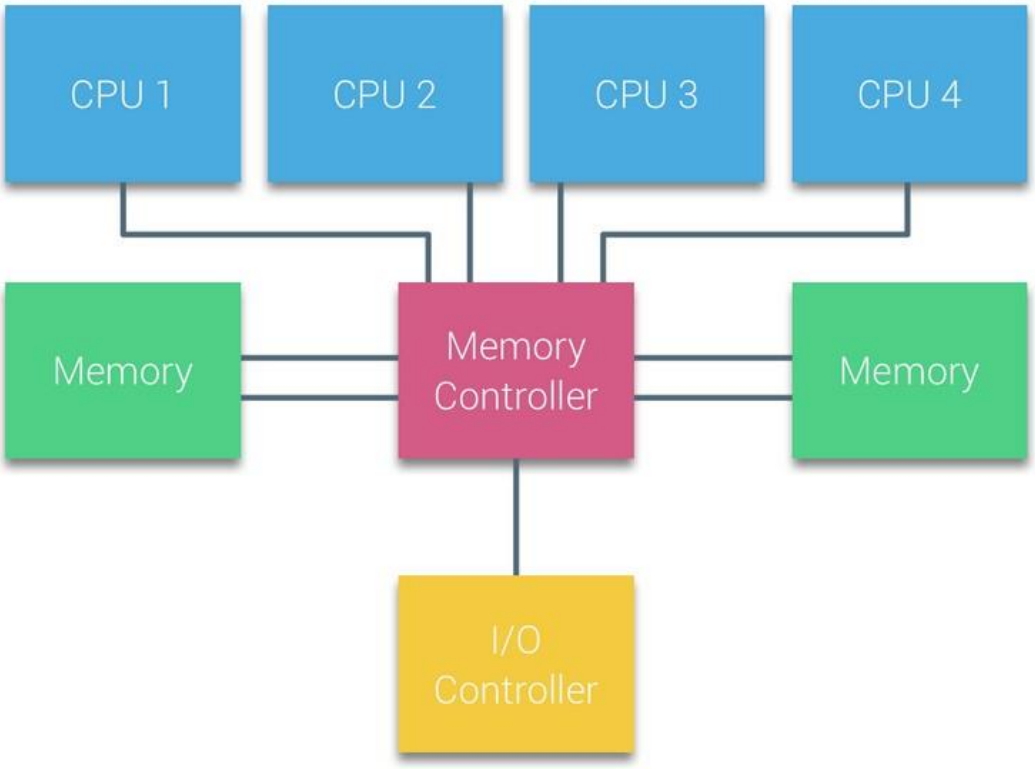
Η προσθήκη CPU στο σύστημα εισάγει δύο σημαντικούς τομείς ανησυχίας:

- Το διαθέσιμο εύρος ζώνης ανά κόμβο μειώνεται καθώς προστίθεται κάθε CPU
- Το μήκος του διαύλου αυξάνεται κατά την προσθήκη περισσότερων επεξεργαστών, αυξάνοντας έτσι την καθυστέρηση.

Η αύξηση της απόδοσης της CPU και συγκεκριμένα το χάσμα ταχύτητας μεταξύ του επεξεργαστή και της απόδοσης της μνήμης ήταν, και στην πραγματικότητα εξακολουθεί να είναι καταστροφικό για τους πολυεπεξεργαστές. Δεδομένου ότι το κενό μνήμης μεταξύ επεξεργαστή και μνήμης αναμενόταν να αυξηθεί, πολλή προσπάθεια κατέληξε στην ανάπτυξη αποτελεσματικών στρατηγικών για τη διαχείριση των συστημάτων μνήμης. Μία από αυτές τις στρατηγικές ήταν η προσθήκη μνήμης cache, η οποία εισήγαγε πολλές προκλήσεις. Η επίλυση αυτών των προκλήσεων εξακολουθεί να αποτελεί το επίκεντρο των σημερινών ομάδων σχεδιασμού CPU, έχει γίνει πολλή έρευνα για δομές προσωρινής αποθήκευσης και εξελιγμένους αλγορίθμους για την αποφυγή απώλειας προσωρινής μνήμης.

Ομοιόμορφη Αρχιτεκτονική Πρόσβασης στη Μνήμη (Uniform Memory Access Architecture)

Οι επεξεργαστές πολυεπεξεργαστών βασισμένων σε Bus που έχουν τον ίδιο ομοιόμορφο χρόνο πρόσβασης σε οποιαδήποτε μονάδα μνήμης στο σύστημα αναφέρονται συχνά ως συστήματα Uniform Memory Access (UMA) ή Symmetric Multi-Processors (SMPs), εικόνα 3.41.
Με τα συστήματα UMA, οι CPU συνδέονται μέσω ενός διαύλου συστήματος (Front-Side Bus) στο Northbridge. Το Northbridge περιέχει τον ελεγκτή μνήμης και κάθε επικοινωνία από και προς τη μνήμη πρέπει να περάσει μέσω του Northbridge. Ο ελεγκτής I / O, ο οποίος είναι υπεύθυνος για τη διαχείριση του I / O σε όλες τις συσκευές, είναι συνδεδεμένος στο Northbridge. Επομένως, κάθε I / O πρέπει να περάσει από το Northbridge για να φτάσει στη CPU.



Εικόνα 3.41

Πολλά bus και κανάλια μνήμης χρησιμοποιούνται για να διπλασιάσουν το διαθέσιμο εύρος ζώνης και να μειώσουν τη συμφόρηση του Northbridge. Για να αυξήσουν ακόμη περισσότερο το εύρος ζώνης της μνήμης, ορισμένα συστήματα συνδέουν εξωτερικούς ελεγκτές μνήμης με το Northbridge, βελτιώνοντας το εύρος ζώνης και υποστηρίζοντας περισσότερη μνήμη. Ωστόσο, λόγω του εσωτερικού εύρους ζώνης του Northbridge και της φύσης εκπομπής των πρωτόκολλων snoopy cache, το UMA θεωρήθηκε ότι έχει περιορισμένη επεκτασιμότητα. Με τη σημερινή χρήση συσκευών flash υψηλής ταχύτητας, ωθώντας εκατοντάδες χιλιάδες I/O ανά δευτερόλεπτο, είχαν απόλυτο δίκιο ότι αυτή η αρχιτεκτονική δεν θα κλιμακώνονταν για μελλοντικούς φόρτους εργασίας.

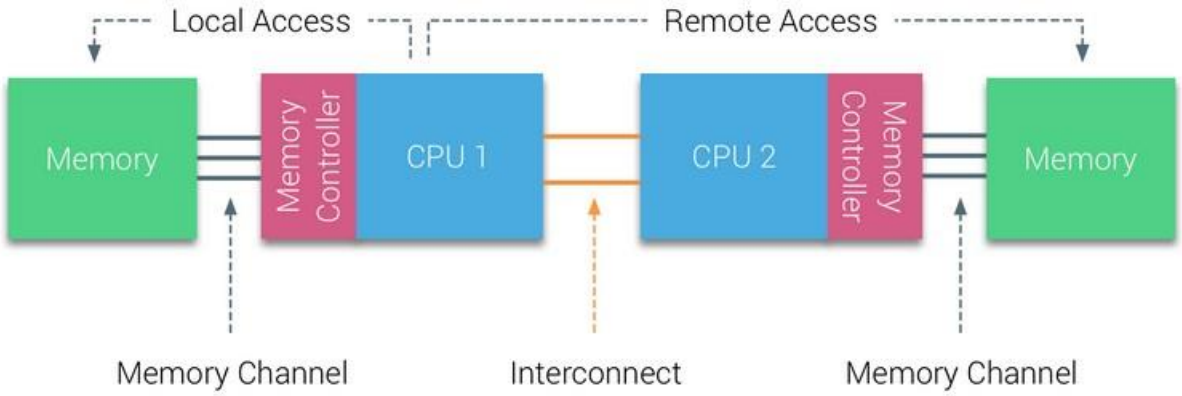
Μη ομοιόμορφη αρχιτεκτονική πρόσβασης στη μνήμη (Non-Uniform Memory Access Architecture)

Για τη βελτίωση της επεκτασιμότητας και της απόδοσης, πραγματοποιούνται τρεις κρίσιμες αλλαγές στην αρχιτεκτονική των πολλαπλών επεξεργαστών κοινής μνήμης

1. Μη ομοιόμορφη οργάνωση πρόσβασης μνήμης
2. Τοπολογία διασύνδεσης από σημείο σε σημείο
3. Επεκτάσιμες λύσεις συνοχής προσωρινής μνήμης

Μη ομοιόμορφη οργάνωση πρόσβασης μνήμης

Το NUMA απομακρύνεται από ένα συγκεντρωτικό απόθεμα μνήμης και εισάγει τοπολογικές ιδιότητες. Με την ταξινόμηση των βάσεων θέσης μνήμης στο μήκος της διαδρομής σήματος από τον επεξεργαστή στη μνήμη, μπορεί να αποφευχθεί η καθυστέρηση και το εύρος ζώνης. Αυτό γίνεται με τον επανασχεδιασμό ολόκληρου του συστήματος επεξεργαστή και chipset. Οι αρχιτεκτονικές NUMA κέρδισαν δημοτικότητα στα τέλη της δεκαετίας του '90 όταν χρησιμοποιήθηκαν σε υπερυπολογιστές SGI όπως το Cray Origin 2000. Το NUMA βοήθησε στον εντοπισμό της θέσης της μνήμης, σε αυτήν την περίπτωση αυτών των συστημάτων. Έπρεπε να αναρωτηθούν ποια ήταν η περιοχή μνήμης στην οποία το πλαίσιο κρατούσε τα κομμάτια μνήμης.



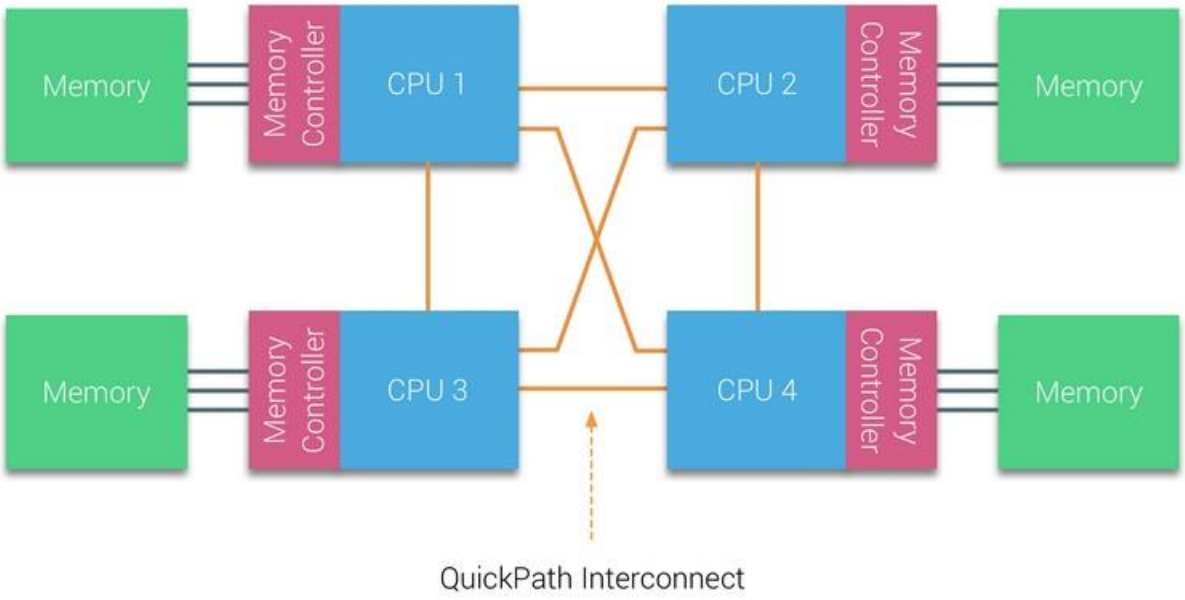
Εικόνα 3.42

Στο πρώτο μισό της δεκαετίας της χιλιετίας, η AMD έφερε το NUMA στο επιχειρηματικό τοπίο όπου τα συστήματα UMA βασίλευαν υπέρτατα. Το 2003 παρουσιάστηκε η οικογένεια AMD Opteron, με ενσωματωμένους ελεγκτές μνήμης με κάθε CPU να διαθέτει συγκεκριμένες τράπεζες μνήμης. Κάθε CPU έχει πλέον το δικό της χώρο διευθύνσεων μνήμης. Ένα βελτιστοποιημένο λειτουργικό σύστημα NUMA όπως το ESXi επιτρέπει στον φόρτο εργασίας να καταναλώνει μνήμη και από τους δύο χώρους διευθύνσεων μνήμης, ενώ βελτιστοποιείται για τοπική πρόσβαση στη μνήμη.
Για παράδειγμα σε ένα σύστημα με δύο CPU μπορούμε να διακρίνουμε τη διαφορά μεταξύ τοπικής και απομακρυσμένης πρόσβασης μνήμης σε ένα μόνο σύστημα, εικόνα 3.42. Η μνήμη που είναι συνδεδεμένη στον ελεγκτή μνήμης του CPU1 θεωρείται τοπική μνήμη. Η μνήμη που είναι συνδεδεμένη σε άλλη υποδοχή CPU (CPU2) θεωρείται ξένη ή απομακρυσμένη για CPU1. Η απομακρυσμένη πρόσβαση στη μνήμη έχει επιπλέον καθυστέρηση στην τοπική πρόσβαση στη μνήμη, καθώς πρέπει να διασχίσει μια διασύνδεση (σύνδεσμος από σημείο σε σημείο) και να συνδεθεί στον απομακρυσμένο ελεγκτή μνήμης. Ως αποτέλεσμα των διαφορετικών θέσεων μνήμης, αυτό το σύστημα αντιμετωπίζει «μη ομοιόμορφο» χρόνο πρόσβασης στη μνήμη.

Διασύνδεση από σημείο σε σημείο

Η AMD παρουσίασε τη σύνδεση Point-to-Point HyperTransport με τη μικροαρχιτεκτονική AMD Opteron. Η Intel απομακρύνθηκε από τη διπλή ανεξάρτητη αρχιτεκτονική bus το 2007, εισάγοντας την αρχιτεκτονική QuickPath στην οικογενειακή σχεδίαση Nehalem Processor.

Η αρχιτεκτονική Nehalem ήταν μια σημαντική αλλαγή στο σχεδιασμό της μικροαρχιτεκτονικής της Intel και θεωρείται η πρώτη πραγματική γενιά της σειράς Intel Core. Η τρέχουσα αρχιτεκτονική Broadwell είναι η 4η γενιά της μάρκας Intel Core (Intel Xeon E5 v4. Μέσα στην αρχιτεκτονική QuickPath, οι ελεγκτές μνήμης μετακινήθηκαν στην CPU και εισήγαγαν το QuickPath σημείο-προς-σημείο Interconnect (QPI) ως συνδέσμους δεδομένων μεταξύ CPUs στο σύστημα.

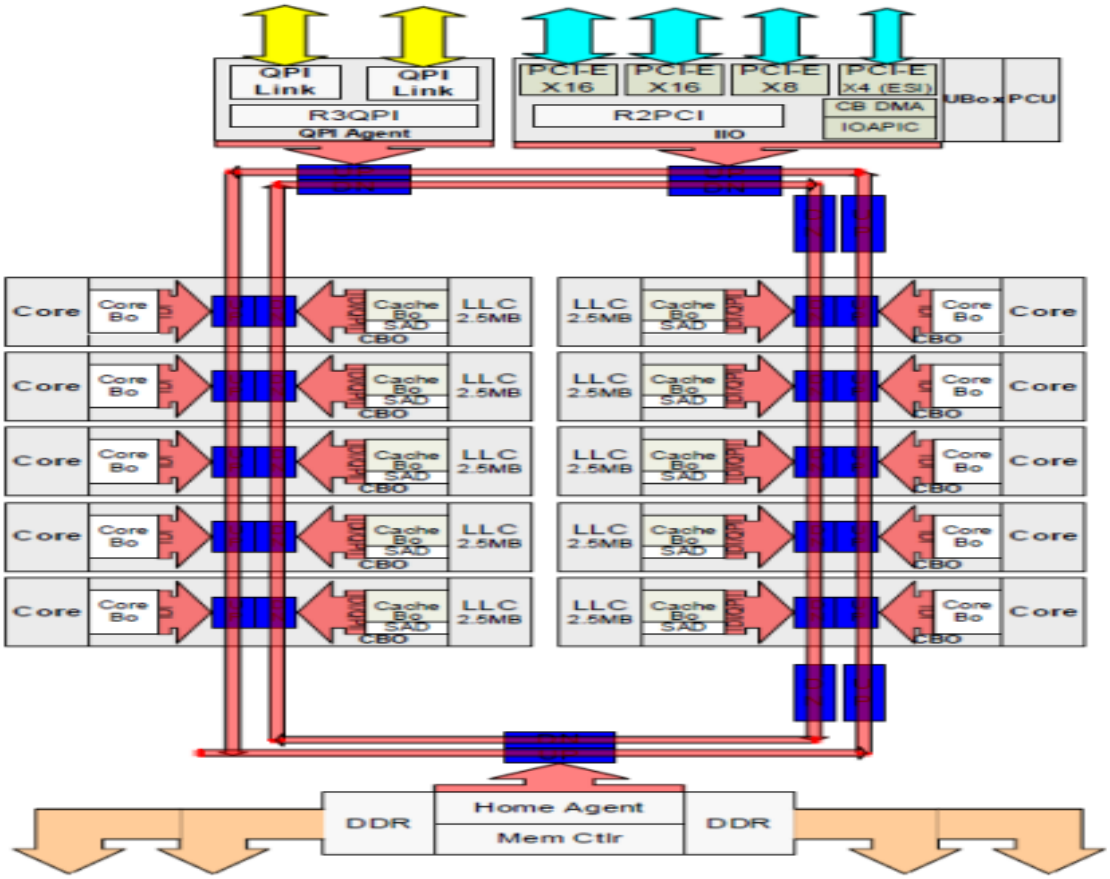


Εικόνα 3.43

Η μικροαρχιτεκτονική Nehalem όχι μόνο αντικατέστησε το κλασικό μπροστινό bus αλλά αναδιοργάνωσε ολόκληρο το υποσύστημα σε μια αρθρωτή σχεδίαση για CPU διακομιστή. Αυτή η αρθρωτή σχεδίαση εισήχθη ως "Uncore" και δημιουργεί μια βιβλιοθήκη δομικών μονάδων για αποθήκευση cache και διασύνδεση. Η αφαίρεση του διαύλου μπροστινής πλευράς βελτιώνει τα ζητήματα κλιμάκωσης εύρους ζώνης, αλλά η επικοινωνία μεταξύ των επεξεργαστών πρέπει να επιλυθεί όταν αντιμετωπίζονται ζητήματα με τεράστιες ποσότητες χωρητικότητας μνήμης και εύρους ζώνης. Τόσο ο ενσωματωμένος ελεγκτής μνήμης όσο και οι διασυνδέσεις QuickPath αποτελούν μέρος του Uncore και είναι Model Specific Registers (MSR). Συνδέονται με ένα MSR που παρέχει την επικοινωνία μεταξύ των επεξεργαστών. Η αρθρωτότητα του Uncore επιτρέπει επίσης στην Intel να προσφέρει διαφορετικές ταχύτητες QPI, κατά τη στιγμή της σύνταξης, η μικροαρχιτεκτονική Intel Broadwell-EP (2016) προσφέρει 6,4 Giga-transfer ανά δευτερόλεπτο (GT / s), 8,0 GT / s και 9,6 GT / s . Αντίστοιχα, παρέχεται ένα θεωρητικό μέγιστο εύρος ζώνης 25,6 GB / s, 32 GB / s και 38,4 GB / s μεταξύ των CPU. Για να το θέσουμε σε προοπτική, ο τελευταίος μπροστινός δίαυλος που χρησιμοποιήθηκε παρείχε 1,6 GT / s ή 12,8 GB / s εύρους ζώνης πλατφόρμας. Κατά την εισαγωγή του Sandy Bridge η Intel μετονομάζει το Uncore στο System Agent, ωστόσο ο όρος Uncore εξακολουθεί να χρησιμοποιείται στην τρέχουσα τεκμηρίωση.

Επεκτάσιμη συνοχή προσωρινής μνήμης

Κάθε πυρήνας έχει μια ιδιωτική διαδρομή προς την προσωρινή μνήμη L3. Κάθε διαδρομή αποτελείται από χίλια καλώδια και μπορούμε να φανταστούμε ότι αυτό δεν κλιμακώνεται καλά εάν θέλουμε να μειώσουμε τη διαδικασία κατασκευής του νανομέτρου, ενώ ταυτόχρονα αυξάνουμε τους πυρήνες που θέλουν να έχουν πρόσβαση στην προσωρινή μνήμη. Προκειμένου να είναι δυνατή η κλιμάκωση, η Αρχιτεκτονική Sandy Bridge μετακίνησε την προσωρινή μνήμη L3 από το Uncore και εισήγαγε τον επεκτάσιμο δακτύλιο on-die Interconnect. Αυτό επέτρεψε στην Intel να χωρίσει και να διανείμει την προσωρινή μνήμη L3 σε ίσες φέτες. Αυτό παρέχει υψηλότερο εύρος ζώνης και συνάφεια. Κάθε κομμάτι είναι 2,5 MB και ένα κομμάτι συνδέεται με κάθε πυρήνα. Ο δακτύλιος επιτρέπει σε κάθε πυρήνα να έχει πρόσβαση σε κάθε άλλη φέτα επίσης. Παρακάτω απεικονίζεται η διαμόρφωση μήτρας ενός επεξεργαστή χαμηλού πυρήνα (LCC) Xeon CPU της Broadwell Microarchitecture (v4) (2016).



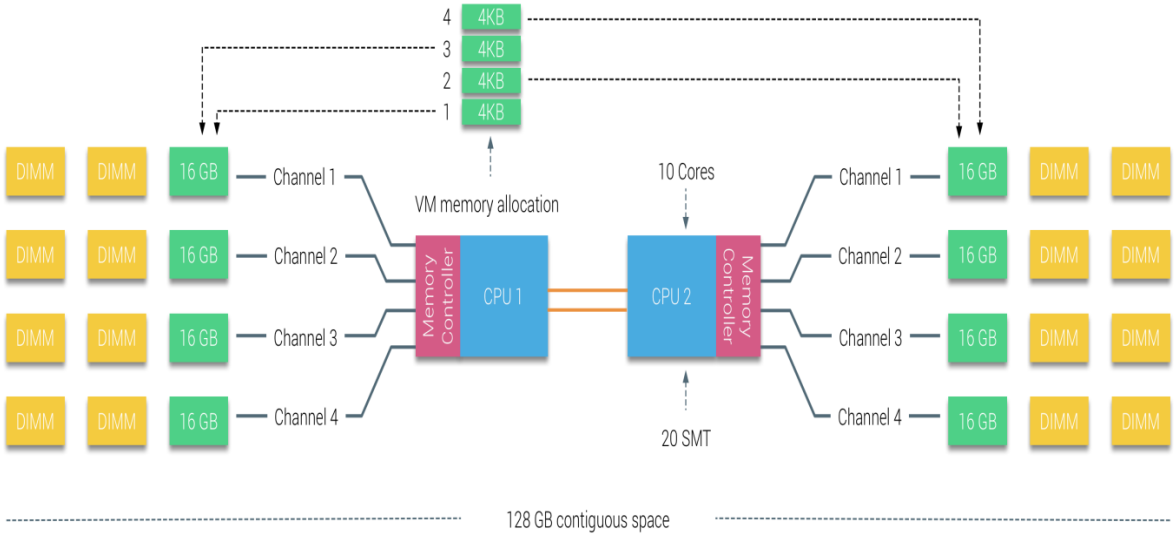
Εικόνα 3.44

Αυτή η αρχιτεκτονική προσωρινής αποθήκευσης απαιτεί ένα πρωτόκολλο ελέγχου που ενσωματώνει τόσο την κατανεμημένη τοπική προσωρινή μνήμη όσο και τους άλλους επεξεργαστές στο σύστημα για να διασφαλιστεί η συνοχή της προσωρινής μνήμης. Με την προσθήκη περισσότερων πυρήνων στο σύστημα, αυξάνεται η ποσότητα ελέγχου της κίνησης, καθώς κάθε πυρήνας έχει τη δική του σταθερή ροή ελλείψεων cache. Αυτό

επηρεάζει την κατανάλωση των συνδέσμων QPI και των cache τελευταίου επιπέδου, απαιτώντας συνεχή ανάπτυξη πρωτοκόλλων συνοχής.

Μη παρεμβαλλόμενη ενεργοποίηση NUMA = SUMA

Η φυσική μνήμη κατανέμεται σε ολόκληρη τη μητρική πλακέτα, ωστόσο, το σύστημα μπορεί να παρέχει έναν μοναδικό χώρο διευθύνσεων μνήμης παρεμβάλλοντας τη μνήμη μεταξύ των δύο κόμβων NUMA. Αυτό ονομάζεται Node-interleaving. Όταν είναι ενεργοποιημένη η παρεμβολή κόμβου, το σύστημα γίνεται επαρκώς ομοιόμορφη αρχιτεκτονική μνήμης (Non-interleaved enabled NUMA = SUMA). Αντί να μεταδίδει τις πληροφορίες τοπολογίας και τη φύση των επεξεργαστών και της μνήμης στο σύστημα του λειτουργικού συστήματος, το σύστημα κατανέμει ολόκληρο το εύρος μνήμης σε περιοχές που διευθύνονται από 4KB και τις χαρτογραφεί με τρόπο round robin από κάθε κόμβο. Αυτό παρέχει μια «παρεμβαλλόμενη» δομή μνήμης όπου ο χώρος διευθύνσεων μνήμης κατανέμεται στους κόμβους. Όταν το ESXi εκχωρεί μνήμη σε εικονική μηχανή, εκχωρεί φυσική μνήμη που βρίσκεται από δύο διαφορετικούς κόμβους όταν η φυσική CPU που βρίσκεται στον κόμβο 0 πρέπει να ανακτήσει τη μνήμη από τον κόμβο 1, η μνήμη θα διασχίσει τους συνδέσμους QPI.



Εικόνα 3.45

Το ενδιαφέρον είναι ότι το σύστημα SUMA παρέχει έναν ομοιόμορφο χρόνο πρόσβασης στη μνήμη. Όχι μόνο το πιο βέλτιστο αλλά και εξαρτώμενο σε μεγάλο βαθμό από τα επίπεδα διαμάχης στην αρχιτεκτονική QPI.
Το Intel Memory Latency Checker χρησιμοποιήθηκε για να δείξει τις διαφορές μεταξύ των παραμέτρων NUMA και SUMA στο ίδιο σύστημα. Αυτή η δοκιμή μετρά τους χρόνους αδράνειας (σε νανοδευτερόλεπτα) από κάθε socket, από το ένα socket στο άλλο του συστήματος. Η καθυστέρηση που αναφέρεται στο Memory Node 0 από το Socket 0 είναι τοπική πρόσβαση στη μνήμη, η πρόσβαση στη μνήμη από την υποδοχή 0 του κόμβου μνήμης 1 είναι απομακρυσμένη πρόσβαση στη μνήμη στο σύστημα που έχει διαμορφωθεί ως NUMA.

Όπως αναμενόταν το interleaving επηρεάζεται από τη συνεχή διέλευση των συνδέσμων QPI. Το τεστ σε αδράνεια μνήμης είναι το καλύτερο σενάριο. Μια πιο ενδιαφέρουσα δοκιμή είναι η μέτρηση των καθυστερημένων φορτίων. Θα ήταν κακή επένδυση εάν οι διακομιστές ESXi είναι σε αδράνεια, γι' αυτό μπορούμε να υποθέσουμε ότι ένα σύστημα ESXi επεξεργάζεται δεδομένα. Η μέτρηση των καθυστερημένων φορτίων παρέχει καλύτερη εικόνα σχετικά με την απόδοση του συστήματος υπό κανονικό φορτίο. Κατά τη διάρκεια της δοκιμής, οι καθυστερήσεις έγχυσης φορτίου αλλάζουν αυτόματα κάθε 2 δευτερόλεπτα και μετράται τόσο το εύρος ζώνης όσο και το αντίστοιχο λανθάνοντα χρόνο σε αυτό το επίπεδο. Αυτή η δοκιμή χρησιμοποιεί 100% επισκεψιμότητα ανάγνωσης. Τα αποτελέσματα της δοκιμής φαίνονται στον παρακάτω πίνακα.

NUMA	Memory Node 0	Memory Node 1	SUMA	Memory Node 0	Memory Node 1
Socket 0	75.7	132.0	Socket 0	105.5	106.4
Socket 1	131.9	75.8	Socket 1	106.0	104.6

Πίνακας 3.2

Το αναφερόμενο εύρος ζώνης για το σύστημα SUMA είναι χαμηλότερο διατηρώντας παράλληλα υψηλότερο λανθάνοντα χρόνο από το σύστημα που έχει διαμορφωθεί ως NUMA. Επομένως, πρέπει να δοθεί έμφαση στη βελτιστοποίηση του μεγέθους VM για την αξιοποίηση των χαρακτηριστικών του NUMA συστήματος.

3.9. Αρχιτεκτονικές μέσων αποθήκευσης

Κάθε σύστημα υπολογιστή περιλαμβάνει τα μέσα για την αποθήκευση και την ανάκτηση δεδομένων όποτε αυτό χρειαστεί. Υπάρχουν διάφορα επίπεδα αποθήκευσης. Σε γενικές γραμμές, η μνήμη, είτε η κύρια μνήμη είτε τα διάφορα επίπεδα της προσωρινής μνήμης, θεωρείται ως το κύριο επίπεδο. Ωστόσο, τα δεδομένα αυτά είναι ασταθή και προσωρινά και διατηρούνται για όσο διάστημα δεν αντικαταστάθηκαν ή για όσο διάστημα το σύστημα είναι λειτουργικό. Για το λόγο αυτό, απαιτούνται πρόσθετες συσκευές για μακροχρόνια αποθήκευση. Τα ακόλουθα επίπεδα ιεραρχίας προορίζονται για αποθήκευση μέσων που δεν χρειάζεται να συνδεθούν σε πηγή ηλεκτρικής για να διατηρηθούν τα δεδομένα αποθηκευμένα. Επιπλέον, τα δεδομένα αποθηκεύονται ακόμη και αν το σύστημα δεν λειτουργεί. Οι πρόσθετες συσκευές αποθήκευσης μπορούν να χωριστούν σε διάφορους τύπους, με βάση την πρόσβαση στα αποθηκευμένα δεδομένα και εάν είναι διαδικτυακά ή όχι.

Η πρόσβαση στις συσκευές μπορεί να είναι:

- ✓ Σειριακή πρόσβαση, που σημαίνει ότι για την ανάγνωση ενός στοιχείου δεδομένων, όλα τα προηγούμενα στοιχεία πρέπει να διαβαστούν ή να παραλειφθούν. Αυτός ο τύπος μέσων χρησιμοποιήθηκε κατά πολύ στο παρελθόν, κυρίως για σκοπούς δημιουργίας αντιγράφων ασφαλείας, αλλά τα τελευταία χρόνια, η χρήση τους ήταν περιορισμένη. Ο κύριος περιορισμός τέτοιων συσκευών είναι ότι ο χρόνος αναζήτησης επηρεάζεται από τη θέση του αντικειμένου που αναζητήθηκε.
- ✓ Τυχαία (ή άμεση) πρόσβαση, στην οποία είναι δυνατή η απευθείας πρόσβαση στο απαιτούμενο αντικείμενο. Η μνήμη, για παράδειγμα, είναι μια συσκευή άμεσης πρόσβασης. Ο χρόνος πρόσβασης για τη λήψη ενός στοιχείου δεδομένων χρησιμοποιώντας απευθείας πρόσβαση είναι σχεδόν παρόμοιος για όλα τα στοιχεία, ανεξάρτητα από την τοποθεσία τους.

Μια άλλη ταξινόμηση για συσκευές αποθήκευσης είναι το διαδικτυακό τους επίπεδο:

- ➢ Πλήρως συνδεδεμένο, πράγμα που σημαίνει ότι η συσκευή είναι πάντα συνδεδεμένη και όλα τα δεδομένα της είναι συνεχώς διαθέσιμα. Οι περισσότεροι μαγνητικοί δίσκοι που είναι εγκατεστημένοι σε ένα σύστημα υπολογιστή είναι πλήρως συνδεδεμένοι.
- ➢ Εν μέρει στο διαδίκτυο, το οποίο συνήθως περιλαμβάνει ένα ρομποτικό σύστημα που περιέχει μια βιβλιοθήκη δίσκων (π.χ. οπτικοί δίσκοι). Όταν απαιτείται ένας δίσκος, θα εκδώσει τις εντολές για να τον σταματήσει. Αυτός ο τύπος συσκευής

παρέχει απεριόριστη αποθήκευση. Ωστόσο, η πρώτη πρόσβαση μπορεί να απαιτεί χρόνο, και μερικές φορές ακόμη και ένα σημαντικό χρονικό διάστημα (σε περιπτώσεις όπου απασχολούνται όλοι οι αναγνώστες δίσκων).

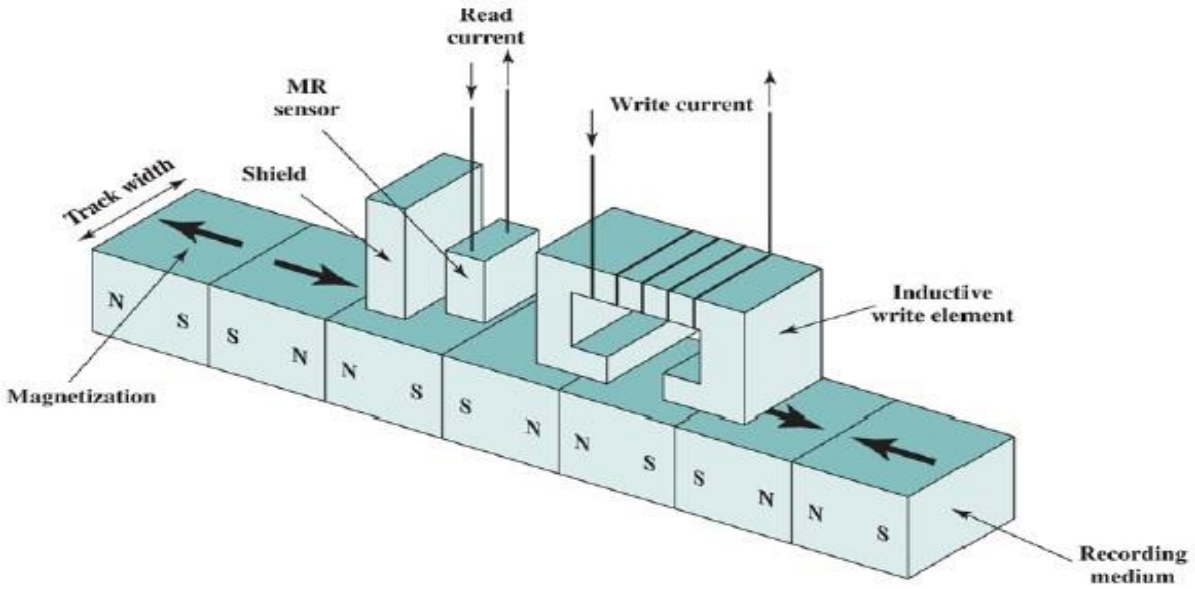
- ➢ Off-line, που σημαίνει ότι η συσκευή δεν είναι συνδεδεμένη στο σύστημα και τα δεδομένα της δεν είναι διαθέσιμα. Ένα παράδειγμα μπορεί να είναι ένας δίσκος ο οποίος διατηρεί το κλειδί από τα δεδομένα που βρίσκονται εκτός σύνδεσης και όταν χρειάζεται ο δίσκος συνδέεται με το σύστημα και το περιεχόμενό του καθίσταται διαθέσιμο. Υπάρχουν οργανισμούς που, για λόγους ασφαλείας, χρησιμοποιούν την ίδια μέθοδο αλλά με αφαιρούμενους σκληρούς δίσκους. Και στις δύο περιπτώσεις, αυτές είναι συσκευές εκτός σύνδεσης.

Μαγνητικοί Δίσκοι

Ένας δίσκος είναι μια κυκλική πιατέλα κατασκευασμένη από μη μαγνητικό υλικό, που ονομάζεται υπόστρωμα, επικαλυμμένο με μαγνητίσιμο υλικό. Παραδοσιακά, το υπόστρωμα ήταν υλικό από αλουμίνιο ή κράμα αλουμινίου. Πιο πρόσφατα, έχουν εισαχθεί γυάλινα υποστρώματα. Το γυάλινο υπόστρωμα έχει πολλά οφέλη, συμπεριλαμβανομένων των ακόλουθων:

- ✓ Βελτίωση της ομοιομορφίας της επιφάνειας του μαγνητικού φιλμ για αύξηση της αξιοπιστίας του δίσκου.
- ✓ Σημαντική μείωση των συνολικών επιφανειακών ελαττωμάτων για τη μείωση των σφαλμάτων ανάγνωσης.
- ✓ Ικανότητα να υποστηρίζει χαμηλότερα ύψη πτήσης
- ✓ Καλύτερη ακαμψία για μείωση της δυναμικής του δίσκου.
- ✓ Μεγαλύτερη ικανότητα αντοχής σε ζημιές από πτώσεις.

Τα δεδομένα καταγράφονται και αργότερα ανακτώνται από το δίσκο μέσω ενός αγώγιμου πηνίου που ονομάζεται κεφαλή. Σε πολλά συστήματα, υπάρχουν δύο κεφαλές, μια κεφαλή ανάγνωσης και μια κεφαλή εγγραφής. Κατά τη διάρκεια μιας λειτουργίας ανάγνωσης ή εγγραφής, η κεφαλή είναι ακίνητη ενώ ο δίσκος περιστρέφεται κάτω από αυτήν. Ο μηχανισμός εγγραφής εκμεταλλεύεται το γεγονός ότι η ηλεκτρική ενέργεια που ρέει μέσω ενός πηνίου παράγει ένα μαγνητικό πεδίο. Ηλεκτρικοί παλμοί αποστέλλονται στην κεφαλή εγγραφής και τα προκύπτοντα μαγνητικά μοτίβα καταγράφονται στην επιφάνεια κάτω, με διαφορετικά μοτίβα για θετικά και αρνητικά ρεύματα. Η ίδια η κεφαλή εγγραφής είναι φτιαγμένη από εύκολα μαγνητίσιμο υλικό και έχει σχήμα ορθογώνιου ντόνατ με διάκενο κατά μήκος μιας πλευράς και μερικές στροφές αγώγιμου σύρματος κατά μήκος της αντίθετης πλευράς. Ένα ηλεκτρικό ρεύμα στο καλώδιο προκαλεί ένα μαγνητικό πεδίο στο κενό, το οποίο με τη σειρά του μαγνητίζει μια μικρή περιοχή στο μέσο εγγραφής. Η αναστροφή της κατεύθυνσης του ρεύματος αντιστρέφει την κατεύθυνση του μαγνητισμού στο μέσο εγγραφής. Στην εικόνα 3.32 φαίνεται μία κεφαλή ανάγνωσης και εγγραφής.



Εικόνα 3.46

Ο παραδοσιακός μηχανισμός ανάγνωσης εκμεταλλεύεται το γεγονός ότι ένα μαγνητικό πεδίο όταν κινείται σε σχέση με ένα πηνίο παράγει ηλεκτρικό ρεύμα στο πηνίο. Όταν η επιφάνεια του δίσκου περιστρέφεται κάτω από την κεφαλή, δημιουργεί ένα ρεύμα της ίδιας πολικότητας με αυτό που έχει ήδη καταγραφεί. Η δομή της κεφαλής ανάγνωσης είναι σε αυτήν την περίπτωση ουσιαστικά η ίδια με της γραφής, και επομένως μπορεί να χρησιμοποιηθεί η ίδια κεφαλή και για τις δύο περιπτώσεις. Τέτοιες μονές κεφαλές χρησιμοποιούνταν σε συστήματα δισκέτας και σε παλαιότερα άκαμπτα συστήματα δίσκων. Τα σύγχρονα συστήματα άκαμπτων δίσκων χρησιμοποιούν διαφορετικό μηχανισμό ανάγνωσης, που απαιτεί ξεχωριστή κεφαλή ανάγνωσης, η οποία είναι τοποθετημένη για ευκολία κοντά στην κεφαλή εγγραφής. Η κεφαλή ανάγνωσης αποτελείται από ένα μερικώς θωρακισμένο μαγνητοανθεκτικό (MagnetoResistive - MR) αισθητήρα. Το υλικό MR έχει ηλεκτρική αντίσταση που εξαρτάται από την κατεύθυνση του μαγνητισμού του μέσου που κινείται κάτω από αυτό. Περνώντας ένα ρεύμα μέσω του MR αισθητήρα, οι αλλαγές αντίστασης ανιχνεύονται ως σήματα τάσης. Ο σχεδιασμός MR επιτρέπει υψηλότερη συχνότητα λειτουργία, η οποία ισοδυναμεί με μεγαλύτερες πυκνότητες αποθήκευσης και ταχύτητες λειτουργίας.

Τεχνολογία RAID

Ο ρυθμός βελτίωσης της απόδοσης δευτερεύουσας αποθήκευσης ήταν πολύ μικρότερος σε σχέση με τον ρυθμό για τους επεξεργαστές και την κύρια μνήμη. Αυτή η αναντιστοιχία έκανε το σύστημα αποθήκευσης με τη χρήση δίσκων ίσως το επίκεντρο της ανησυχίας για τη βελτίωση της εκτέλεσης του συνολικού συστήματος υπολογιστών. Όπως και σε άλλους τομείς απόδοσης υπολογιστή, οι σχεδιαστές αποθήκευσης δίσκων αναγνωρίζουν ότι εάν ένα στοιχείο μπορεί να προωθηθεί μονό μέχρι τώρα, επιπρόσθετα κέρδη στην απόδοση πρέπει να επιτευχθούν με τη χρήση πολλαπλών παράλληλων συστατικών. Στην περίπτωση αποθήκευσης δίσκου, αυτό οδηγεί στην ανάπτυξη συστοιχιών δίσκων που λειτουργούν ανεξάρτητα και παράλληλα. Με πολλαπλούς

δίσκους, μπορούν να αντιμετωπιστούν παράλληλα ξεχωριστά αιτήματα εισόδου / εξόδου, εφόσον τα απαιτούμενα δεδομένα βρίσκονται σε ξεχωριστούς δίσκους. Επιπλέον, ένα μόνο αίτημα εισόδου / εξόδου μπορεί να εκτελεστεί παράλληλα εάν το μπλοκ των δεδομένων προς πρόσβαση κατανέμεται σε πολλούς δίσκους.
Με τη χρήση πολλαπλών δίσκων, υπάρχει μια μεγάλη ποικιλία τρόπων με τους οποίους τα δεδομένα μπορούν να οργανωθούν και στην οποία μπορεί να προστεθεί πλεονασμός για τη βελτίωση της αξιοπιστίας. Αυτό θα μπορούσε να είναι δύσκολο να αναπτυχθεί σε σχήματα βάσεων δεδομένων που μπορούν να χρησιμοποιηθούν σε διάφορες πλατφόρμες και λειτουργικά συστήματα. Η βιομηχανία έχει συμφωνήσει σε ένα τυποποιημένο σχέδιο για το σχεδιασμό βάσεων δεδομένων πολλαπλών δίσκων, γνωστό ως RAID (Redundant Array of Independent Disks - Πλεονάζουσα σειρά ανεξάρτητων δίσκων). Το σχήμα RAID αποτελείται από επτά επίπεδα, μηδέν έως έξι. Αυτά τα επίπεδα δεν συνεπάγονται ιεραρχική σχέση, αλλά προσδιορίζουν διαφορετικές αρχιτεκτονικές σχεδιασμού που μοιράζονται τρία κοινά χαρακτηριστικά:

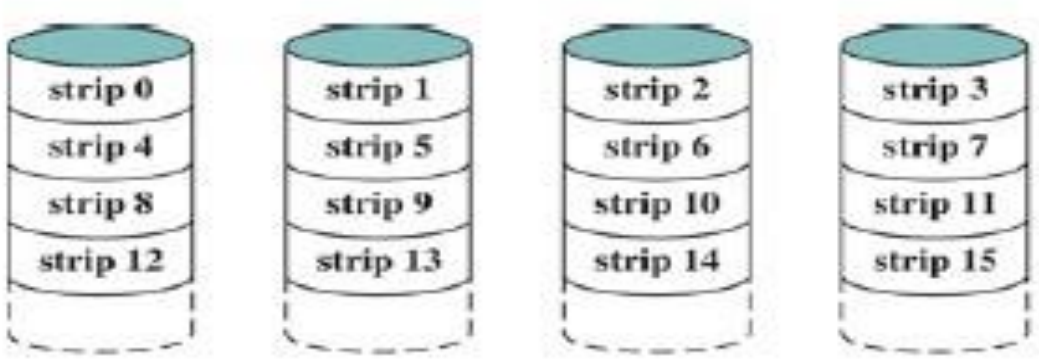
i. Το RAID είναι ένα σύνολο φυσικών δίσκων που βλέπει το λειτουργικό σύστημα ως μία λογική μονάδα δίσκου.
ii. Τα δεδομένα κατανέμονται σε όλες τις φυσικές μονάδες δίσκου σε ένα σχήμα γνωστό ως striping.
iii. Η πλεονάζουσα χωρητικότητα δίσκου χρησιμοποιείται για την αποθήκευση πληροφοριών ισοτιμίας, οι οποίες εγγυώνται τα δεδομένα με δυνατότητα ανάκτησης σε περίπτωση βλάβης του δίσκου.

Οι λεπτομέρειες του δεύτερου και του τρίτου χαρακτηριστικού διαφέρουν για τα διαφορετικά επίπεδα RAID. Το RAID 0 και το RAID 1 δεν υποστηρίζει το τρίτο χαρακτηριστικό.
Ο όρος RAID δημιουργήθηκε αρχικά σε μια εργασία από μια ομάδα ερευνητών στο Πανεπιστήμιο του Καλιφόρνια στο Μπέρκλεϋ. Το έγγραφο περιγράφει διάφορες διαμορφώσεις και εφαρμογές RAID και εισήγαγε τους ορισμούς των επιπέδων RAID που εξακολουθούν να χρησιμοποιούνται. Η στρατηγική RAID χρησιμοποιεί πολλαπλές μονάδες δίσκου και διανέμει δεδομένα με τέτοιο τρόπο ώστε να επιτρέπεται ταυτόχρονη πρόσβαση σε δεδομένα από πολλαπλές μονάδες δίσκου, βελτιώνοντας έτσι την απόδοση I / O και επιτρέποντας ευκολότερες αυξήσεις στο χωρητικότητα.
Η μοναδική συμβολή της πρότασης RAID είναι η αποτελεσματική αντιμετώπιση της ανάγκης για πλεονάζοντα χώρο. Παρόλο που η ταυτόχρονη λειτουργία πολλαπλών κεφαλών και ενεργοποιητών επιτυγχάνει υψηλότερα I / O και ρυθμούς μεταφοράς, η χρήση πολλαπλών συσκευών αυξάνει την πιθανότητα αστοχίας. Για να αντισταθμίσει η μειωμένη αξιοπιστία, το RAID χρησιμοποιεί αποθηκευμένες πληροφορίες ισοτιμίας που επιτρέπουν την ανάκτηση δεδομένων που χάθηκαν λόγω αστοχίας δίσκου.

RAID Επίπεδο 0

Το επίπεδο RAID 0 δεν είναι αληθινό μέλος της οικογένειας RAID επειδή δεν περιλαμβάνει πλεονασμό για βελτίωση της απόδοσης. Ωστόσο, υπάρχουν μερικές εφαρμογές, όπως μερικές σε υπερυπολογιστές, στις οποίες η απόδοση και χωρητικότητα αποτελούν πρωταρχικές ανησυχίες και το χαμηλό κόστος είναι πιο σημαντικό από την βελτιωμένη αξιοπιστία. Για το RAID 0, τα δεδομένα χρήστη και συστήματος κατανέμονται σε όλους τους δίσκους του πίνακα. Αυτό έχει αξιοσημείωτο πλεονέκτημα έναντι της

χρήσης ενός μεγάλου δίσκου: Εάν εκκρεμούν δύο διαφορετικά αιτήματα εισόδου / εξόδου για δύο διαφορετικά μπλοκ δεδομένων, τότε υπάρχει μια καλή πιθανότητα τα ζητούμενα μπλοκ να βρίσκονται σε διαφορετικούς δίσκους. Έτσι, τα δύο αιτήματα μπορούν να εκδοθούν παράλληλα, μειώνοντας τον χρόνο αναμονής I / O. Αλλά το RAID 0, όπως και με όλα τα επίπεδα RAID, προχωρά πέρα από την απλή διανομή των δεδομένων σε έναν πίνακα δίσκων: Τα δεδομένα είναι κατανεμημένα στους διαθέσιμους δίσκους. Όλα τα δεδομένα χρήστη και συστήματος θεωρούνται αποθηκευμένα σε έναν λογικό δίσκο. Ο λογικός δίσκος είναι χωρίζεται σε λωρίδες. Αυτές οι ταινίες μπορεί να είναι φυσικά μπλοκ, τομείς ή κάποια άλλη μονάδα. Το πλεονέκτημα αυτής της διάταξης είναι ότι εάν ένα μεμονωμένο αίτημα εισόδου / εξόδου αποτελείται από πολλές λογικά συνεχόμενες ταινίες, τότε έως ότου βρεθεί η n ταινία για αυτό το αίτημα μπορούν να αντιμετωπιστούν παράλληλα όλες οι ταινίες, μειώνοντας σημαντικά το χρόνο μεταφοράς I / O. Στην παρακάτω εικόνα 3.47 φαίνεται η υλοποίηση του RAID 0.



Εικόνα 3.47

RAID Επίπεδο 1

Το RAID 1 διαφέρει από τα επίπεδα RAID 2 έως 6 στον τρόπο με τον οποίο επιτυγχάνεται ο πλεονασμός. Στα άλλα σχήματα RAID, κάποια μορφή υπολογισμού ισοτιμίας χρησιμοποιείται για την εισαγωγή πλεονασμού, ενώ στο επίπεδο RAID 1, ο πλεονασμός επιτυγχάνεται με την απλή λύση της αντιγραφής όλων των δεδομένων. Κάθε λογικός δίσκος αντιστοιχίζεται σε δύο διαφορετικούς φυσικούς δίσκους έτσι ώστε κάθε δίσκος στη συστοιχία να έχει έναν δίσκο καθρέφτη που περιέχει τα ίδια δεδομένα. Το RAID 1 μπορεί επίσης να εφαρμοστεί χωρίς πλεονασμό δεδομένων.
Υπάρχουν ορισμένες θετικές πτυχές στην υλοποίηση του RAID 1:

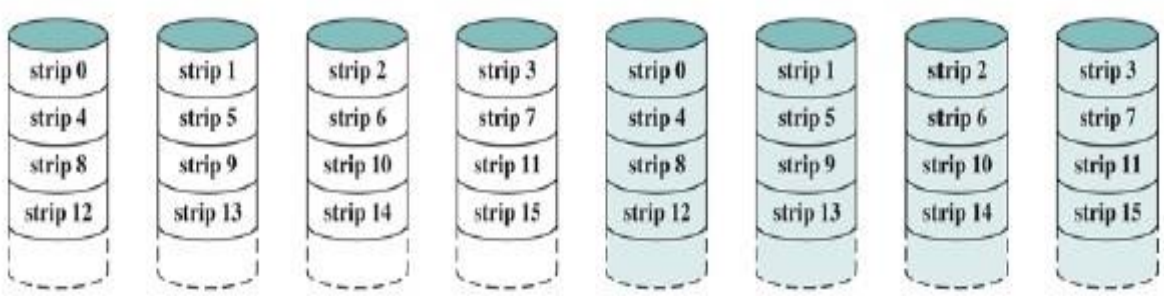
1. Ένα αίτημα ανάγνωσης μπορεί να εξυπηρετηθεί από έναν από τους δύο δίσκους που περιέχει τα ζητούμενα δεδομένα, όποιο από τα δύο συνεπάγεται τον ελάχιστο χρόνο αναζήτησης και τον λανθάνοντα χρόνο περιστροφής.
2. Ένα αίτημα εγγραφής απαιτεί και οι δύο αντίστοιχες ταινίες να ενημερώνονται, αλλά αυτό μπορεί να γίνει παράλληλα. Έτσι, η απόδοση εγγραφής υπαγορεύεται από την πιο αργή από τις δύο εγγραφές (δηλαδή, αυτή που περιλαμβάνει τον μεγαλύτερο χρόνο αναζήτησης και την περιστροφική καθυστέρηση). Ωστόσο, δεν υπάρχει «ποινή γραφής» με RAID 1. Τα επίπεδα RAID 2 έως 6 περιλαμβάνουν τη χρήση bit ισοτιμίας. Επομένως, όταν είναι μία μόνο ταινία

ενημερωμένη, το λογισμικό διαχείρισης πίνακα πρέπει πρώτα να υπολογίσει και να ενημερώσει τα bit ισοτιμίας ως ενημέρωση της πραγματικής εν λόγω ταινίας.

3. Η ανάκτηση από αποτυχία είναι απλή. Όταν μια μονάδα δίσκου αποτύχει, τα δεδομένα ενδέχεται να εξακολουθούν να είναι προσβάσιμα από τον δεύτερο δίσκο.

Το κύριο μειονέκτημα του RAID 1 είναι το κόστος απαιτεί διπλάσιο χώρο στο δίσκο του λογικού δίσκου που υποστηρίζει. Εξαιτίας αυτού, μια διαμόρφωση RAID 1 είναι πιθανό να περιορίζεται σε μονάδες δίσκου που αποθηκεύουν λογισμικό και δεδομένα συστήματος, και άλλα εξαιρετικά κρίσιμα αρχεία. Σε αυτές τις περιπτώσεις, το RAID 1 παρέχει σε πραγματικό χρόνο αντίγραφο όλων των δεδομένων, ώστε σε περίπτωση βλάβης του δίσκου, όλα τα κρίσιμα δεδομένα να παραμένουν αμέσως διαθέσιμα.

Σε ένα περιβάλλον προσανατολισμένο στις συναλλαγές, το RAID 1 μπορεί να επιτύχει υψηλά ποσοστά αιτήσεων εισόδου / εξόδου εάν το μεγαλύτερο μέρος από τα αιτήματα διαβάζονται. Σε αυτήν την περίπτωση, η απόδοση του RAID 1 μπορεί να προσεγγίσει διπλάσια από εκείνη του RAID 0. Ωστόσο, εάν ένα σημαντικό μέρος των αιτημάτων εισόδου / εξόδου είναι αιτήματα εγγραφής, τότε ενδέχεται να μην υπάρχει σημαντικό κέρδος απόδοσης έναντι RAID 0. Το RAID 1 μπορεί επίσης να προσφέρει βελτιωμένη απόδοση έναντι RAID 0 για εφαρμογές εντατικής μεταφοράς δεδομένων με υψηλό ποσοστό αναγνώσεων. Η βελτίωση συμβαίνει εάν η εφαρμογή μπορεί να χωρίσει κάθε αίτημα ανάγνωσης έτσι ώστε να συμμετέχουν και τα δύο μέλη του δίσκου. Στην εικόνα 3.48 φαίνεται το RAID 1.



Εικόνα 3.48

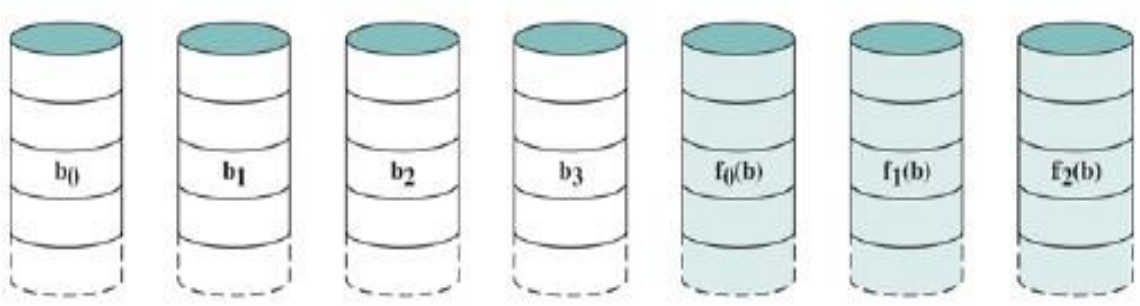
RAID Επίπεδο 2

Τα επίπεδα RAID 2 και 3 κάνουν χρήση μιας παράλληλης τεχνικής πρόσβασης. Σε έναν παράλληλο πίνακα πρόσβασης, όλα τα μέλη δίσκων συμμετέχουν στην εκτέλεση κάθε αιτήματος εισόδου / εξόδου. Συνήθως, οι άξονες των μεμονωμένων δίσκων συγχρονίζονται έτσι ώστε κάθε κεφαλή δίσκου να βρίσκεται στην ίδια θέση σε κάθε δίσκο ανά πάσα στιγμή.

Όπως και στα άλλα σχήματα RAID, χρησιμοποιείται λωρίδες δεδομένων. Στην περίπτωση RAID 2 και 3, οι λωρίδες είναι πολύ μικρές, συχνά τόσο μικρές όσο ένα byte ή λέξη. Με το RAID 2, υπολογίζεται ένας κωδικός διόρθωσης σφαλμάτων (Hamming code) σε αντίστοιχα bit σε κάθε δίσκο δεδομένων, και τα bit του κώδικα αποθηκεύονται στις αντίστοιχες θέσεις bit σε πολλαπλούς δίσκους ισοτιμίας. Συνήθως, χρησιμοποιείται ένας κωδικός Hamming, ο οποίος μπορεί να διορθώσει σφάλματα ενός bit και να εντοπίσει σφάλματα διπλού bit.

Αν και το RAID 2 απαιτεί λιγότερους δίσκους από το RAID 1, εξακολουθεί να είναι αρκετά δαπανηρό. Ο αριθμός των περιττών δίσκων είναι ανάλογος με το αρχείο καταγραφής του αριθμού των δίσκων δεδομένων. Σε μία μόνο ανάγνωση, όλοι οι δίσκοι έχουν ταυτόχρονη

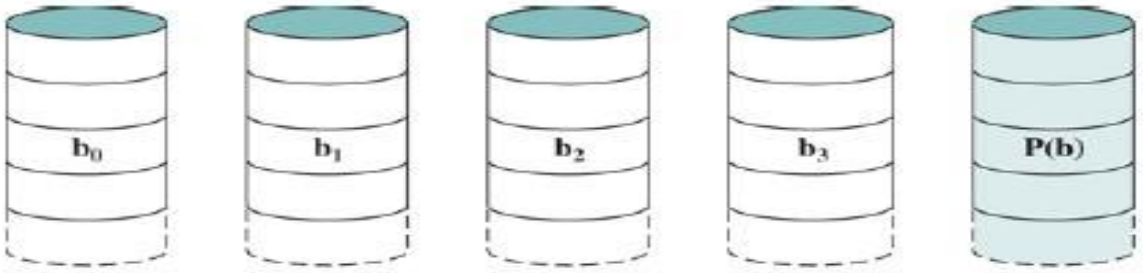
πρόσβαση. Τα απαιτούμενα δεδομένα και ο σχετικός κώδικας διόρθωσης σφαλμάτων παραδίδονται στον πίνακα ελέγχου. Εάν υπάρχει σφάλμα ενός bit, ο ελεγκτής μπορεί να αναγνωρίσει και να διορθώσει το σφάλμα αμέσως, έτσι ώστε ο χρόνος πρόσβασης ανάγνωσης να μην επιβραδύνεται. Σε μία μόνο εγγραφή, όλοι οι δίσκοι δεδομένων και οι δίσκοι ισοτιμίας πρέπει να έχουν πρόσβαση για τη λειτουργία εγγραφής.
Το RAID 2 θα ήταν μόνο μια αποτελεσματική επιλογή σε ένα περιβάλλον στο οποίο παρουσιάζονται πολλά σφάλματα δίσκου. Δεδομένου ότι υπάρχει υψηλή αξιοπιστία μεμονωμένων δίσκων και μονάδων δίσκου, το RAID 2 είναι υπερβολικό και δεν εφαρμόζεται. Στην εικόνα 3.49 φαίνεται το RAID 2.



Εικόνα 3.49

RAID Επίπεδο 3

Το RAID 3 είναι οργανωμένο με παρόμοιο τρόπο με το RAID 2. Η διαφορά είναι ότι το RAID 3 απαιτεί μόνο ένα περιττό δίσκο, ανεξάρτητα από το πόσο μεγάλος είναι ο πίνακας δίσκων. Το RAID 3 χρησιμοποιεί παράλληλη πρόσβαση, με τα δεδομένα να κατανέμονται σε μικρές λωρίδες. Αντί για κώδικα διόρθωσης σφαλμάτων, ένα απλό bit ισοτιμίας υπολογίζεται για το σύνολο μεμονωμένων bits στην ίδια θέση σε όλους τους δίσκους δεδομένων. Σε περίπτωση βλάβης του δίσκου, όλα τα δεδομένα εξακολουθούν να είναι διαθέσιμα σε αυτό που αναφέρεται ως μειωμένη λειτουργία. Σε αυτήν τη λειτουργία, για ανάγνωση, τα δεδομένα που λείπουν αναδημιουργούνται εν κινήσει χρησιμοποιώντας τον αποκλειστικό - OR υπολογισμό. Όταν τα δεδομένα γράφονται σε έναν μειωμένο πίνακα RAID 3, πρέπει να διατηρείται η συνέπεια της ισοτιμίας για μεταγενέστερη αναγέννηση. Η επιστροφή σε πλήρη λειτουργία απαιτεί την αντικατάσταση του αποτυχημένου δίσκου και ολόκληρο το περιεχόμενο του αποτυχημένου δίσκου θα αναγεννηθεί στον νέο δίσκο. Επειδή τα δεδομένα είναι κατανεμημένα σε πολύ μικρές ταινίες, το RAID 3 μπορεί να επιτύχει πολύ υψηλούς ρυθμούς μεταφοράς δεδομένων. Οποιοδήποτε αίτημα I / O θα περιλαμβάνει την παράλληλη μεταφορά δεδομένων από όλους τους δίσκους δεδομένων. Σε μεγάλες μεταφορές, η βελτίωση της απόδοσης είναι ιδιαίτερα αισθητή. Από την άλλη πλευρά, μπορεί να είναι μόνο ένα αίτημα εισόδου / εξόδου το οποίο εκτελείται κάθε φορά. Έτσι, σε ένα περιβάλλον προσανατολισμένο στις συναλλαγές, η απόδοση υποφέρει. Στην εικόνα 3.50 φαίνεται το RAID 3.

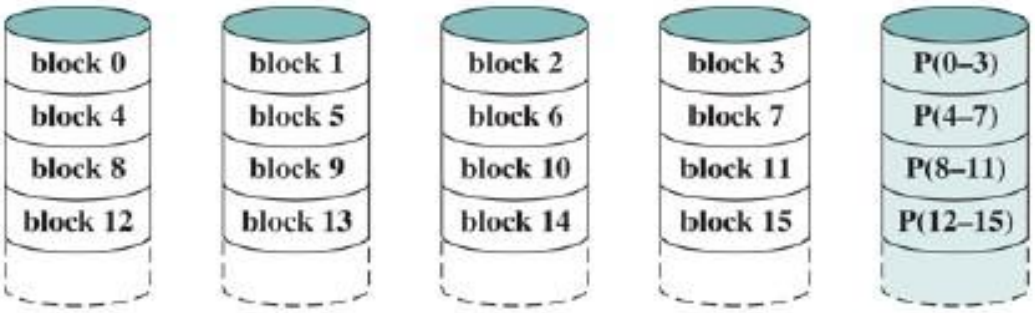


Εικόνα 3.50

RAID Επίπεδο 4

Τα επίπεδα RAID 4 έως 6 κάνουν χρήση μιας ανεξάρτητης τεχνικής πρόσβασης. Με την ανεξάρτητη πρόσβαση πίνακα, κάθε δίσκος μέλους λειτουργεί ανεξάρτητα, έτσι ώστε να μπορούν να ικανοποιηθούν ξεχωριστά αιτήματα εισόδου / εξόδου παράλληλα. Εξαιτίας αυτού, οι ανεξάρτητες συστοιχίες πρόσβασης είναι πιο κατάλληλες για εφαρμογές που απαιτούν υψηλά ποσοστά αιτήσεων εισόδου / εξόδου και είναι σχετικά λιγότερο κατάλληλα για εφαρμογές που απαιτούν υψηλές τιμές μεταφοράς δεδομένων.
Όπως και στα άλλα σχήματα RAID, χρησιμοποιείται λωρίδα δεδομένων. Στην περίπτωση RAID 4 έως 6, οι ταινίες είναι σχετικά μεγάλες. Με το RAID 4, μια ταινία ισοτιμίας bit-by-bit υπολογίζεται σε αντίστοιχες ταινίες σε κάθε ένα δίσκο δεδομένων και τα bit ισοτιμίας αποθηκεύονται στην αντίστοιχη ταινία του δίσκου ισοτιμίας. Το RAID 4 περιλαμβάνει ποινή γραφής όταν πραγματοποιείται αίτηση εγγραφής I / O μικρού μεγέθους. Κάθε φορά που γίνεται εγγραφή, το λογισμικό διαχείρισης πίνακα πρέπει να ενημερώνει όχι μόνο τα δεδομένα χρήστη αλλά και τα αντίστοιχα bits ισοτιμίας. Για τον υπολογισμό της νέας ισοτιμίας, το λογισμικό διαχείρισης πίνακα πρέπει να διαβάσει την παλιά ταινία χρήστη και την παλιά ισοτιμία. Στη συνέχεια, μπορεί να ενημερώσει αυτές τις δύο λωρίδες με τα νέα δεδομένα και την πρόσφατα υπολογισμένη ισοτιμία. Έτσι, κάθε ταινία γράφει δύο αναγνώσεις και δύο εγγραφές.

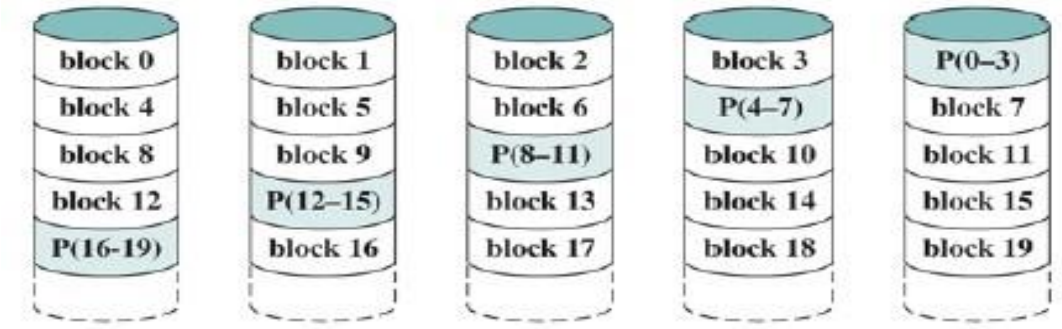
Στην περίπτωση εγγραφής I / O μεγαλύτερου μεγέθους που περιλαμβάνει ταινίες σε όλες τις μονάδες δίσκου, η ισοτιμία υπολογίζεται εύκολα χρησιμοποιώντας μόνο τα νέα bit δεδομένων. Έτσι, η μονάδα δίσκου ισοτιμίας μπορεί να ενημερωθεί παράλληλα με τα δεδομένα των δίσκων και δεν υπάρχουν επιπλέον αναγνώσεις ή εγγραφές. Σε κάθε περίπτωση, κάθε εγγραφή πρέπει να περιλαμβάνει το δίσκο ισοτιμίας το οποίο μπορεί να δημιουργήσει το λεγόμενο bottle-neck. Στην εικόνα 3.51 φαίνεται το RAID 4.



Εικόνα 3.51

RAID Επίπεδο 5

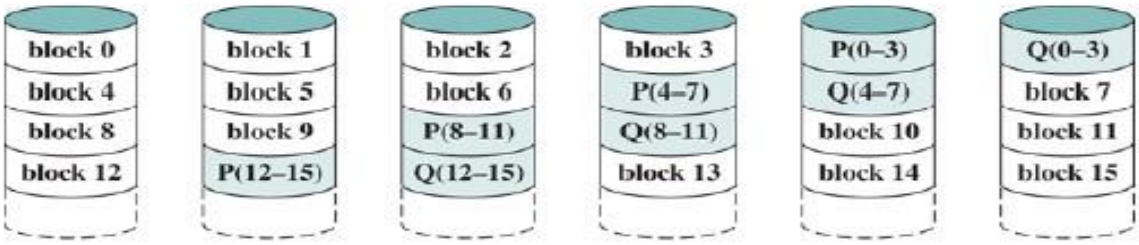
Το RAID 5 είναι οργανωμένο με παρόμοιο τρόπο με το RAID 4. Η διαφορά είναι ότι το RAID 5 διανέμει την ισοτιμία με λωρίδες σε όλους τους δίσκους. Μια τυπική κατανομή είναι ένα σχήμα round-robin, το οποίο φαίνεται στην παρακάτω εικόνα. Για
μια συστοιχία n - δίσκου, η ταινία ισοτιμίας βρίσκεται σε διαφορετικό δίσκο για τις πρώτες λ λωρίδες, και το μοτίβο στη συνέχεια επαναλαμβάνεται. Η κατανομή των ταινιών ισοτιμίας σε όλους τους δίσκους αποφεύγει τον πιθανό bottle-neck I / O που βρίσκεται στο RAID 4. Στην εικόνα 3.52 φαίνεται το RAID 5.



Εικόνα 3.52

RAID Επίπεδο 6

Το RAID 6 παρουσιάστηκε σε επόμενο έγγραφο από τους ερευνητές του Berkeley. Στο RAID 6 σχήμα, δύο διαφορετικοί υπολογισμοί ισοτιμίας πραγματοποιούνται και αποθηκεύονται σε ξεχωριστά μπλοκ σε διαφορετικούς δίσκους. Έτσι, ένας πίνακας RAID 6 του οποίου τα δεδομένα χρήστη απαιτούν δίσκους N αποτελείται από N+2 δίσκους.
Το πλεονέκτημα του RAID 6 είναι ότι παρέχει εξαιρετικά υψηλή διαθεσιμότητα δεδομένων. Τρεις δίσκοι θα πρέπει να αποτύχουν εντός του διαστήματος MTTR (μέσος χρόνος επιδιόρθωσης) για να χαθούν τα δεδομένα. Από την άλλη πλευρά, το RAID 6 επιβάλλει σημαντική ποινή γραφής, επειδή κάθε εγγραφή επηρεάζει δύο ομάδες ισοτιμίας. Αναφορές δείχνουν ότι ένας ελεγκτής RAID 6 μπορεί να επιφέρει περισσότερο από 30% πτώση στη συνολική απόδοση εγγραφής σε σύγκριση με μια εφαρμογή RAID 5. Η απόδοση ανάγνωσης RAID 5 και RAID 6 είναι συγκρίσιμες. Στην εικόνα 3.53 φαίνεται το RAID 6.



Εικόνα 3.53

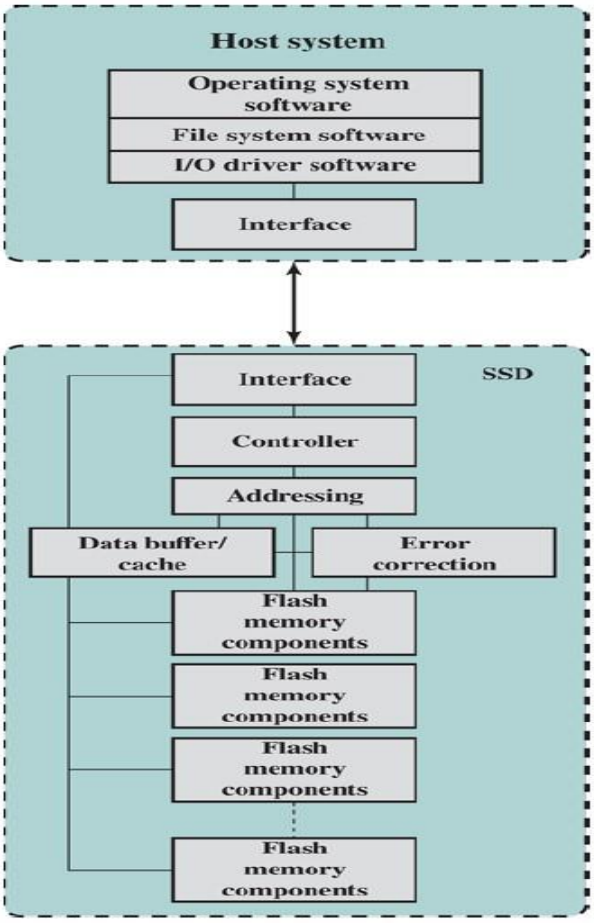
Τεχνολογία Solid State Drive

Μία από τις πιο σημαντικές εξελίξεις στην αρχιτεκτονική των υπολογιστών τα τελευταία χρόνια είναι η αύξηση χρήσης μονάδων στερεάς κατάστασης (Solid State Drive - SSD) για τη συμπλήρωση ή ακόμη και την αντικατάσταση μονάδων σκληρού δίσκου (HDD) και τη χρήση τους ως εσωτερική και εξωτερική δευτερεύουσα μνήμη. Ο όρος στερεά κατάσταση αναφέρεται σε ηλεκτρονικά κυκλώματα με ενσωματωμένους ημιαγωγούς. Ένας SSD είναι μια συσκευή μνήμης κατασκευασμένη με στοιχεία στερεάς κατάστασης που μπορούν να χρησιμοποιηθούν ως αντικατάσταση της μονάδας σκληρού δίσκου. Τα SSD που κυκλοφορούν τώρα στην αγορά και έρχονται σε απευθείας σύνδεση χρησιμοποιούν φλας μνήμη τύπου NAND.

Καθώς το κόστος των SSD που βασίζονται σε φλας μνήμη έχει μειωθεί και η απόδοση και η πυκνότητα bit αυξάνονται, οι SSD έχουν γίνει όλο και πιο ανταγωνιστικοί με τους σκληρούς δίσκους.

Οι SSD έχουν τα ακόλουθα πλεονεκτήματα έναντι των σκληρών δίσκων:

- ✓ *Λειτουργίες εισόδου / εξόδου υψηλής απόδοσης ανά δευτερόλεπτο*: σημαντική αύξηση της επίδοσης των υποσυστημάτων I / O.
- ✓ *Ανθεκτικότητα*: Λιγότερο ευαίσθητοι σε πτώσεις και κραδασμούς.
- ✓ *Μεγαλύτερη διάρκεια ζωής*: Οι SSD δεν είναι ευαίσθητοι σε μηχανική φθορά.
- ✓ *Χαμηλότερη κατανάλωση ενέργειας*: Οι SSD χρησιμοποιούν πολύ λιγότερη ισχύ από τους συγκρίσιμους μεγέθους HDD.
- ✓ *Αθόρυβες και ψυχρότερες δυνατότητες λειτουργίας*: Απαιτείται λιγότερος χώρος, χαμηλότερο ενεργειακό κόστος και πιο καλοί για το περιβάλλον.
- ✓ *Χαμηλότεροι χρόνοι πρόσβασης και ρυθμοί καθυστέρησης*: Πάνω από 10 φορές γρηγορότερος σε σχέση με τους κλασικούς σκληρούς δίσκους. Επί του παρόντος, οι σκληροί δίσκοι έχουν πλεονέκτημα κόστους ανά bit και πλεονέκτημα χωρητικότητας, αλλά αυτές οι διαφορές συνεχώς μειώνονται.



Εικόνα 3.54

Στην εικόνα 3.54 απεικονίζεται μια γενική άποψη της αρχιτεκτονικής συστήματος που σχετίζεται με οποιοδήποτε σύστημα SSD. Στο σύστημα κεντρικού υπολογιστή, το λειτουργικό σύστημα ζητά πρόσβαση στο λογισμικό συστήματος αρχείων των δεδομένων στο δίσκο.

Το σύστημα αρχείων, με τη σειρά του, επικαλείται λογισμικό προγράμματος

οδήγησης εισόδου / εξόδου. Το λογισμικό προγράμματος οδήγησης I / O παρέχει πρόσβαση στον
κεντρικό υπολογιστή στο συγκεκριμένο προϊόν SSD.Εάν η συσκευή είναι ένας εσωτερικός σκληρός δίσκος, μια κοινή διεπαφή είναι το PCIe. Για εξωτερικές συσκευές, μια κοινή η διεπαφή είναι USB.
Εκτός από τη διασύνδεση με το κεντρικό σύστημα, ο SSD περιέχει τα ακόλουθα στοιχεία:

- *Ελεγκτής*: Παρέχει διεπαφή επιπέδου συσκευής SSD και εκτέλεσης υλικολογισμικού.
- *Διεύθυνση*: Λογική που εκτελεί τη λειτουργία επιλογής μεταξύ των στοιχείων της μνήμης flash.
- *Buffer δεδομένων / προσωρινή μνήμη*: Υψηλής ταχύτητας μνήμη RAM που χρησιμοποιείται για την αντιστοίχιση της ταχύτητας και την αυξημένη απόδοση δεδομένων.
- *Διόρθωση σφαλμάτων*: Λογική για ανίχνευση και διόρθωση σφαλμάτων.
- *Στοιχεία μνήμης flash*: Μεμονωμένα τσιπ NAND.

Υπάρχουν δύο πρακτικά ζητήματα που αφορούν τα SSD που δεν αντιμετωπίζουν οι σκληροί δίσκοι.

Πρώτον, η απόδοση SSD έχει την τάση να επιβραδύνεται καθώς χρησιμοποιείται η συσκευή. Τα αρχεία αποθηκεύονται στο δίσκο ως σύνολο σελίδων, συνήθως μήκους 4 KB. Αυτές οι σελίδες δεν είναι απαραίτητο να είναι αποθηκευμένες ως συνεχόμενο σύνολο σελίδων στο δίσκο. Ωστόσο, η μνήμη flash είναι προσβάσιμη σε μπλοκ, με τυπικό μέγεθος μπλοκ 512 KB, έτσι ώστε να υπάρχουν συνήθως 128 σελίδες ανά μπλοκ. Η διαδικασία που υλοποιείται προκειμένου να διαγραφεί μια σελίδα σε μια μνήμη flash είναι:

A. Ολόκληρο το μπλοκ πρέπει να διαβαστεί από τη μνήμη flash και να τοποθετηθεί σε μνήμη RAM. Μετά ενημερώνεται η κατάλληλη σελίδα στο buffer RAM.
B. Πριν από την εγγραφή του μπλοκ στη μνήμη flash, πρέπει ολόκληρο το μπλοκ της μνήμης flash να έχει διαγραφεί - δεν είναι δυνατή η διαγραφή μόνο μιας σελίδας της μνήμης flash.
C. Ολόκληρο το μπλοκ από το buffer γράφεται τώρα πίσω στη μνήμη flash.

Όταν μια μονάδα flash είναι σχετικά κενή και δημιουργείται ένα νέο αρχείο, γράφονται οι σελίδες αυτού του αρχείου στη μονάδα δίσκου συνεχόμενα, έτσι ώστε να επηρεάζονται ένα ή μόνο μερικά μπλοκ. Ωστόσο, με την πάροδο του χρόνου, λόγω του τρόπου λειτουργίας της εικονικής μνήμης, τα αρχεία κατακερματίζονται, σε σελίδες διάσπαρτες με πολλαπλά μπλοκ. Καθώς η μονάδα γίνεται όλο και πιο απασχολημένη, υπάρχει περισσότερος κατακερματισμός, το γράψιμο ενός νέου αρχείου μπορεί να επηρεάσει πολλά μπλοκ. Έτσι, η συγγραφή πολλαπλών σελίδων από ένα μπλοκ γίνεται πιο αργή, όσο γεμίζει ο δίσκος.

Ένα δεύτερο πρακτικό πρόβλημα με τις μονάδες μνήμης flash είναι ότι η μνήμη flash δεν μπορεί να χρησιμοποιηθεί μετά από έναν ορισμένο αριθμό εγγραφών. Καθώς τα κελιά μνήμης πιέζονται, χάνουν την ικανότητά τους να καταγράφουν και να διατηρούν τιμές. Ένα τυπικό όριο είναι 100.000 εγγραφές. Οι τεχνικές για την παράταση της διάρκειας ζωής μιας μονάδας SSD περιλαμβάνουν διαγραφή της μνήμης flash με προσωρινή μνήμη για καθυστέρηση και ομαδοποίηση εγγραφών, χρησιμοποιώντας αλγόριθμους ισοπέδωσης φθοράς που διανέμουν ομοιόμορφα εγγραφές σε μπλοκ κελιών, και εξελιγμένες τεχνικές διαχείρισης κακών μπλοκ. Επιπλέον, οι κατασκευαστές αναπτύσσουν SSD σε διαμορφώσεις RAID για περαιτέρω μείωση της πιθανότητας

απώλειας δεδομένων. Επίσης περισσότερες συσκευές flash είναι σε θέση να εκτιμήσουν το υπόλοιπο της διάρκεια ζωής τους, έτσι ώστε τα συστήματα να μπορούν να προβλέψουν την αποτυχία και να λάβουν μέτρα πρόληψης.

3.10. Επικρατέστεροι κατασκευαστές server

3.10.1. Supermicro

Η Super Micro Computer, Inc, που δραστηριοποιείται ως Supermicro, είναι εταιρεία πληροφορικής με έδρα το Σαν Χοσέ της Καλιφόρνια. Τα κεντρικά γραφεία της Supermicro βρίσκονται στη Silicon Valley, με χώρο κατασκευής στις Κάτω Χώρες και Επιστημονικό και Τεχνολογικό Πάρκο στην Ταϊβάν.

Ιδρύθηκε από τους Charles Liang, Wally Liaw και Sara Liu την 1η Νοεμβρίου 1993, και ειδικεύεται σε διακομιστές, αποθήκευση, blades servers, λύσεις rack, συσκευές δικτύωσης, λογισμικό διαχείρισης διακομιστών και σταθμούς εργασίας προηγμένης τεχνολογίας για κέντρο δεδομένων, υπολογιστικά νέφη, εταιρική πληροφορική, μεγάλα δεδομένα και υπολογιστές υψηλής απόδοσης.

Εικόνα 3.55

Το 2016, η εταιρεία ανέπτυξε χιλιάδες διακομιστές σε ένα ενιαίο κέντρο δεδομένων και κατατάχθηκε στην 18η ταχύτερα αναπτυσσόμενη εταιρεία στη λίστα των 100 κορυφαίων εταιρειών του κόσμου που κυκλοφόρησε το 2016 στο Fortune Magazine και την ταχύτερα αναπτυσσόμενη εταιρεία υποδομής πληροφορικής.

Τον Σεπτέμβριο του 2014, η Supermicro μετακίνησε την εταιρική έδρα της στα πρώην κεντρικά γραφεία της Mercury News στο Βόρειο Σαν Χοσέ της Καλιφόρνια ονομάζοντας την πανεπιστημιούπολη Supermicro Green Computing Park. Το 2017, η εταιρεία ολοκλήρωσε ένα νέο κτίριο κατασκευής 16.900 τετραγωνικών μέτρων στην πανεπιστημιούπολη. Το κύριο κτίριο σχεδιάστηκε από τον Warren B. Heid σε μοντέρνο

στιλ, το οποίο ήταν κοινό για εμπορικά κτίρια τη δεκαετία του 1960, και κατασκευάστηκε από την εταιρεία Carl N. Swenson. Κατά τη διάρκεια της περιόδου που χρησίμευσε ως έδρα της Mercury News, το κεντρικό κτίριο επεκτάθηκε από 17.200 m^2 σε 29.000 m^2.

Στις 4 Οκτωβρίου 2018, το Bloomberg Businessweek δημοσίευσε μια έκθεση, επικαλούμενη ανώνυμες εταιρικές και κυβερνητικές πηγές, οι οποίες ισχυρίστηκαν ότι ο Κινεζικός Λαϊκός Απελευθερωτικός Στρατός ανάγκασε τους Κινέζους υπεργολάβους της Supermicro να προσθέσουν μικροτσίπ με hardware backdoors στους διακομιστές του. Η έκθεση ισχυρίστηκε ότι οι παραβιασμένοι διακομιστές είχαν πωληθεί σε κυβερνητικά τμήματα των ΗΠΑ (συμπεριλαμβανομένης της CIA και του Υπουργείου Άμυνας), σε εργολάβους και τουλάχιστον σε 30 εμπορικούς πελάτες (συμπεριλαμβανομένης της Apple). Σύμφωνα με τις πληροφορίες, η πίσω πόρτα ανακαλύφθηκε από την Amazon κατά την ανασκόπηση της Elemental Technologies, ενός πελάτη της Supermicro.

Ο Supermicro αρνήθηκε την έκθεση, δηλώνοντας ότι δεν είχαν επικοινωνήσει με κυβερνητικές υπηρεσίες και δεν γνώριζαν καμία έρευνα. Η Amazon και η Apple αρνήθηκαν επίσης τους ισχυρισμούς του Bloomberg και το άρθρο αντιμετώπισε σκεπτικισμό σχετικά με την εγκυρότητά του. Στις 22 Οκτωβρίου η Supermicro ανακοίνωσε ότι "παρά την έλλειψη αποδείξεων ότι υπάρχει κακόβουλο τσιπ υλικού", εξέταζε τις μητρικές της για πιθανά κακόβουλο υλικό σε απάντηση στο άρθρο.

Στις 9 Οκτωβρίου 2018, το Bloomberg εξέδωσε μια δεύτερη έκθεση, ισχυριζόμενο ότι οι διακομιστές δεδομένων που κατασκευάζονται από Supermicro για μια ανώνυμη εταιρεία τηλεπικοινωνιών των ΗΠΑ είχαν παραβιαστεί από ένα εμφύτευμα υλικού σε μια υποδοχή Ethernet. Η έκθεση ανέφερε τον πρώην αξιωματικό πληροφοριών του Ισραήλ Yossi Appleboum, ο οποίος είχε αναλύσει και τεκμηριώσει το εμφύτευμα. Η έκθεση Bloomberg δεν συνέδεσε αυτά τα ευρήματα με την προηγούμενη έκθεση. Ο Appleboum έκτοτε είπε ότι η εταιρεία του είχε βρει τέτοια εμφυτεύματα σε διαφορετικούς προμηθευτές, όχι μόνο στην Supermicro.

Η Supermicro υπέβαλε επιστολή στην Επιτροπή Κεφαλαιαγοράς δηλώνοντας ότι ήταν σίγουρη ότι δεν είχε εμφυτευτεί κακόβουλο υλικό κατά τη διάρκεια της κατασκευής των μητρικών της. Αναφέρθηκε επίσης ότι τα διευθυντικά στελέχη της Apple και της Amazon Web Services απέρριψαν τους ισχυρισμούς σχετικά με τις αναφορές για backdoor υλικού σε διακομιστές της Supermicro.

3.10.2. DELL

Η Dell Inc. (Dell Computer Corporation) είναι μία παγκόσμια εταιρεία που σχεδιάζει, αναπτύσσει και κατασκευάζει προσωπικούς υπολογιστές (PC), servers και μια ποικιλία προϊόντων που σχετίζονται με τον υπολογιστή. Η εταιρεία είναι ένας από τους κορυφαίους προμηθευτές υπολογιστών στον κόσμο και εδρεύει στο Round Rock του Τέξας.

Η εταιρεία, που η αρχική της ονομασία ήταν PC's Limited, ιδρύθηκε το 1984 από τον Αμερικανό Michael Dell, ο οποίος ήταν τότε φοιτητής στο Πανεπιστήμιο του Τέξας στο Ώστιν. Αρχικά διευθυνε την επιχείρηση από το δωμάτιο του. Η Dell ξεκίνησε την παροχή προσαρμοσμένων αναβαθμίσεων για υπολογιστές. Το εγχείρημα αποδείχθηκε κερδοφόρο, και ο Dell εγκατέλειψε το κολέγιο την ίδια χρονιά για να αρχίσει να κατασκευάζει υπολογιστές. Το 1985 η εταιρεία κυκλοφόρησε τον Turbo PC, τον πρώτο υπολογιστή με το δικό του σχέδιο. Βασισμένη στην αρχή της δημιουργίας και πώλησης

προσαρμοσμένων υπολογιστών απευθείας σε καταναλωτές, η εταιρεία πούλησε αρχικά τα προϊόντα της μέσω διαφημίσεων και καταλόγων αλληλογραφίας.

Αποφεύγοντας το κόστος που σχετίζεται με τις παραδοσιακές αγορές λιανικής και μπόρεσε να προσφέρει υψηλής ποιότητας υπολογιστές σε ανταγωνιστικές τιμές. Η Dell έδωσε έμφαση την υποστήριξη πελατών, την αποστολή τεχνικών για service σε υπολογιστές και την εφαρμογή μιας πολιτικής επιστροφών χωρίς κίνδυνο. Αυτό το επιχειρηματικό μοντέλο αποδείχτηκε επιτυχές και η εταιρεία μεγάλωσε γρήγορα και επεκτάθηκε στις διεθνείς αγορές. Η εταιρεία, μετονομάστηκε σε Dell Computer Corporation το 1988.

Η Dell κυκλοφόρησε τον πρώτο φορητό υπολογιστή, τον 316LT, το 1989. Το 1991 κυκλοφόρησε ο πρώτος έγχρωμος φορητός υπολογιστής της Dell και το 1994 η Dell ήταν η πρώτη εταιρεία που προσέφερε μπαταρίες ιόντων λιθίου μεγάλης διάρκειας. Το 1996 η Dell άρχισε να πωλεί ηλεκτρονικούς υπολογιστές online και επίσης χρησιμοποίησε το Διαδίκτυο για υποστήριξη πελατών. Οι διαδικτυακές πωλήσεις βοήθησαν την Dell να ξεπεράσει την Compaq Computer Corporation και το 1999 αναδείχθηκε ως ο μεγαλύτερος πωλητής υπολογιστών στις Ηνωμένες Πολιτείες.

Στις αρχές του 21ου αιώνα, η Dell επέκτεινε τη σειρά προϊόντων της για να συμπεριλάβει τηλεοράσεις, ψηφιακές φωτογραφικές μηχανές και μια ποικιλία προϊόντων που σχετίζονται με τον υπολογιστή. Το 2003 η εταιρεία μετονομάστηκε σε Dell Inc. για να υποδηλώσει τη μετάβαση στην ευρύτερη αγορά ηλεκτρονικών ειδών ευρείας κατανάλωσης.

Εικόνα 3.56

Ωστόσο, η κυριαρχία της Dell στην αγορά άρχισε να εξασθενεί και η εταιρεία επέστρεψε στην ιδιωτική ιδιοκτησία το 2013, όταν ο Michael Dell και η ιδιωτική εταιρεία Silver Lake Partners την αγόρασαν για 25 δισεκατομμύρια δολάρια. Το 2016 η εταιρεία και μια εταιρεία επενδύσεων απέκτησαν την EMC, μια αμερικανική εταιρεία που ειδικεύεται στην αποθήκευση δεδομένων. Η συγχώνευση, αξίας περίπου 60 δισεκατομμυρίων δολαρίων, ήταν η μεγαλύτερη συμφωνία τεχνολογίας εκείνη την εποχή.

Αν και στην πορεία των χρόνων πολλά εργοστάσια της Dell έχουν ανοίξει και έχουν κλείσει η Dell συνεχίζει να παράγει τους διακομιστές της (τα πιο κερδοφόρα προϊόντα της) στο Ώστιν του Τέξας.

3.10.3. Hewlett-Packard

Η Hewlett-Packard Company είναι Αμερικάνικη εταιρία κατασκευαστής λογισμικού και υπηρεσιών υπολογιστών. Χωρίστηκε το 2015 σε δύο εταιρείες: HP Inc. και Hewlett Packard Enterprise. Τα κεντρικά γραφεία ήταν στο Palo Alto της Καλιφόρνια.
Η εταιρεία ιδρύθηκε την 1η Ιανουαρίου 1939 από τους William R. Hewlett και David Packard, δύο πρόσφατους πτυχιούχους ηλεκτρολόγων μηχανικών του Πανεπιστημίου του Στάνφορντ. Ήταν η πρώτη από πολλές εταιρείες τεχνολογίας που επωφελήθηκε από τις ιδέες και την υποστήριξη του καθηγητή μηχανικού Frederick Terman, ο οποίος πρωτοστάτησε στην ισχυρή σχέση μεταξύ του Στάνφορντ και αυτού που τελικά εμφανίστηκε ως Silicon Valley. Η εταιρεία καθιέρωσε τη φήμη της ως κατασκευαστής εξελιγμένων οργάνων. Ο πρώτος πελάτης της ήταν η Walt Disney Productions, η οποία αγόρασε οκτώ ταλαντωτές ήχου για χρήση στην παραγωγή της ταινίας Fantasia πλήρους μήκους (1940). Κατά τη διάρκεια του Β 'Παγκοσμίου Πολέμου, η εταιρεία ανέπτυξε προϊόντα για στρατιωτικές εφαρμογές που ήταν αρκετά σημαντικά για να αξίζουν στον Packard ένα σχέδιο εξαίρεσης, ενώ ο Hewlett υπηρέτησε στο Στρατιωτικό Σώμα Στρατού. Καθ' όλη τη διάρκεια του πολέμου η εταιρεία συνεργάστηκε με το Naval Research Laboratory για την κατασκευή τεχνολογίας αντι-ραντάρ και προηγμένων ασφάλειών πυροβολικού.

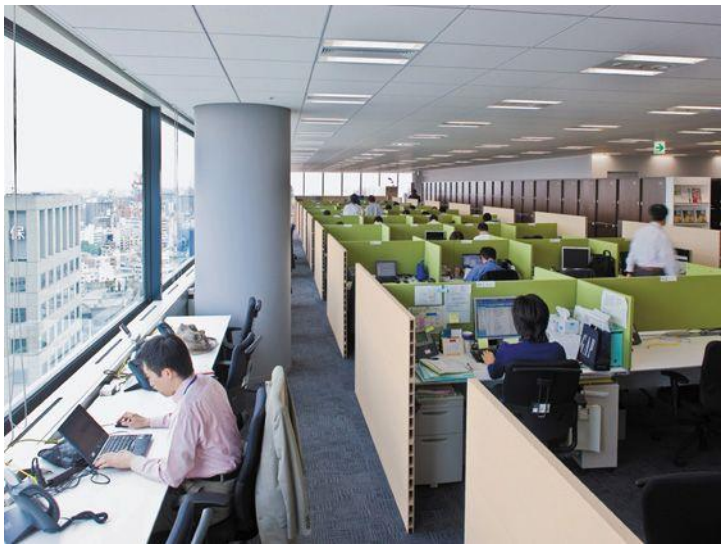
Μετά τον πόλεμο, ο Packard έγινε υπεύθυνος για την επιχείρηση της εταιρείας, ενώ ο Hewlett ηγήθηκε των προσπαθειών έρευνας και ανάπτυξης. Μετά από μια μεταπολεμική πτώση των αμυντικών συμβολαίων, το 1947 η Hewlett-Packard επέστρεψε στα επίπεδα των εσόδων που είχε κατά την διάρκεια των πολέμων και στη συνέχεια αυξήθηκε συνεχώς μέσω μιας στρατηγικής διαφοροποίησης των προϊόντων. Ένα από τα πιο δημοφιλή πρώιμα προϊόντα ήταν ένας μετρητής συχνοτήτων υψηλής ταχύτητας που εισήγαγε το 1951. Χρησιμοποιήθηκε στην ταχέως αναπτυσσόμενη αγορά ραδιοφωνικών και τηλεοπτικών σταθμών FM για τον ακριβή καθορισμό συχνοτήτων σήματος σύμφωνα με τους κανονισμούς της Ομοσπονδιακής Επιτροπής Επικοινωνιών. Οι στρατιωτικές πωλήσεις κατά τη διάρκεια του Κορεατικού Πολέμου αύξησαν επίσης τα έσοδα της εταιρείας.

Για να βοηθήσει στη χρηματοδότηση της ανάπτυξης νέων προϊόντων, η Hewlett-Packard συγκέντρωσε χρήματα εκδίδοντας δημόσιο απόθεμα το 1957. Επιπλέον, ξεκίνησε μια μακρά εκστρατεία επέκτασης της σειράς προϊόντων της με την απόκτηση εταιρειών, ξεκινώντας το έτος αφότου δημοσιοποιήθηκε με την αγορά της F.L. Moseley Company. Το 1961 άρχισε να ανεβαίνει σε κατάταξη ως κατασκευαστής ιατρικών οργάνων με την αγορά της Sanborn Company.

Το 1964 τα όργανα Hewlett-Packard απέκτησαν διεθνή αναγνώριση στο τεχνολογικό βάθρο. Οι μηχανικοί της εταιρείας πέταξαν σε όλο τον κόσμο με το όργανο δέσμης καισίου HP 5060A για να συγχρονίσουν τα ατομικά ρολόγια του πλανήτη σε ένα εκατομμυριοστό του δευτερολέπτου. Τέσσερα χρόνια αργότερα, η εταιρεία παρουσίασε την πρώτη αριθμομηχανή γραφείου. Το 1972, χρησιμοποιώντας προηγμένη τεχνολογία ολοκληρωμένου κυκλώματος, η Hewlett-Packard παρουσίασε την πρώτη αριθμομηχανή τσέπης. Πουλώντας την στο ένα έκτο της αρχικής τιμής της αριθμομηχανής γραφείου την αντικατέστησε πλήρως.

Παρόλο που η εταιρεία δεν ανέπτυξε ποτέ οπλικά συστήματα, εξαρτιόταν σε μεγάλο βαθμό από την ιστορία της στις στρατιωτικές δαπάνες, επειδή τα εργαλεία της

χρησιμοποιήθηκαν για την ανάπτυξη και τον έλεγχο στρατιωτικών προϊόντων, ιδίως καθώς τα οπλικά συστήματα έχουν εξαρτηθεί περισσότερο από τις τεχνολογίες ηλεκτρονικών και ημιαγωγών. Η στρατιωτική εμπειρογνωμοσύνη της Hewlett-Packard υπογραμμίστηκε το 1969 όταν ο Ρίτσαρντ Μ. Νίξον όρισε αναπληρωτή γραμματέα Άμυνας τον Packard, σε μία θέση από την οποία επέβλεψε τα αρχικά σχέδια για την ανάπτυξη δύο από τα πιο επιτυχημένα προγράμματα μαχητικών αεροσκαφών της χώρας, το F-16 και το A-10.



Εικόνα 3.57

Ο πρώτος υπολογιστής της Hewlett-Packard, ο HP 2116A, αναπτύχθηκε το 1966 ειδικά για τη διαχείριση των συσκευών δοκιμής και μέτρησης της εταιρείας. Το 1972 η εταιρεία κυκλοφόρησε τον HP 3000 γενικού σκοπού μικρού υπολογιστή - μια σειρά προϊόντων που παραμένει σε χρήση ακόμη και σήμερα - για χρήση στις επιχειρήσεις. Το 1976 ένας μηχανικός της εταιρεία, ο Stephen G. Wozniak, δημιούργησε ένα πρωτότυπο για τον πρώτο προσωπικό υπολογιστή (PC) και το πρόσφερε στην εταιρεία. Η Hewlett-Packard αρνήθηκε και έδωσε στον Wozniak όλα τα δικαιώματα στην ιδέα του. αργότερα εντάχθηκε με τον Steven P. Jobs για να δημιουργήσει την Apple Computer, Inc. (τώρα Apple Inc.).

Η Hewlett-Packard παρουσίασε τον πρώτο επιτραπέζιο υπολογιστή της, τον HP-85, το 1980. Επειδή ήταν ασύμβατος με τον υπολογιστή IBM, ο οποίος έγινε το βιομηχανικό πρότυπο, ήταν μια αποτυχία. Η επόμενη σημαντική εισβολή της εταιρείας στην αγορά υπολογιστών ήταν με το HP-150, ένα σύστημα συμβατό με υπολογιστή IBM που είχε οθόνη αφής. Αν και τεχνικά ενδιαφέρον, απέτυχε επίσης στην αγορά. Το πρώτο επιτυχημένο προϊόν της εταιρείας για την αγορά Η / Υ ήταν στην πραγματικότητα ένας εκτυπωτής. Το HP LaserJet εμφανίστηκε το 1984 για να κερδίσει κριτικές και τεράστιες πωλήσεις, καθιστώντας το πιο επιτυχημένο προϊόν της Hewlett-Packard.

Στα μέσα της δεκαετίας του 1980, η Hewlett-Packard μείωσε τις δραστηριότητές της στους βασικούς τομείς της επιστήμης και της μηχανικής για να ανταγωνιστεί εταιρείες που κατασκεύαζαν workstations όπως η Sun Microsystems, Inc., η Silicon Graphics, Inc. και η Apollo Computer. Το 1989 η Hewlett-Packard αγόρασε την Apollo για να γίνει ο νούμερο ένα κατασκευαστής workstations, μια θέση που μοιράστηκε με την Sun και αργότερα την Dell Inc.

Καθώς ξεκίνησε η δεκαετία του 1990, η εταιρεία έχασε ορισμένους στόχους εσόδων και κερδών, προκαλώντας μια απότομη πτώση της τιμής της μετοχής της. Ως αποτέλεσμα, ο Packard βγήκε από τη συνταξιοδότησή του για να αναλάβει ενεργό ρόλο στη διοίκηση της εταιρείας. Οι πιο δραματικές αλλαγές ήρθαν στην ομάδα του PC με την εισαγωγή νέων υπολογιστών, έγχρωμων εκτυπωτών και περιφερειακών σε χαμηλές τιμές που κατέστησαν την εταιρεία έναν από τους τρεις κορυφαίους κατασκευαστές υπολογιστών στον κόσμο. Το 1993, με την ολοκλήρωση της ανάκαμψης της εταιρείας, ο Packard

αποσύρθηκε ξανά. Το 1997 η Hewlett-Packard έγινε μία από τις 30 εταιρείες των οποίων η τιμή της μετοχής διαμορφώνει τον Dow Jones, του Χρηματιστηρίου της Νέας Υόρκης. Κατά τη δεκαετία του 1990, η Hewlett-Packard συνεργάστηκε με την Intel Corporation, για το σχεδιασμό και την κατασκευή του μικροεπεξεργαστή 64-bit Itanium, που κυκλοφόρησε το 2001.

Κατά τη διάρκεια της δεκαετίας του 2000, η Hewlett-Packard επέκτεινε τις παγκόσμιες δραστηριότητές της ανοίγοντας ερευνητικά εργαστήρια στο Μπανγκαλόρ Ινδία (2002), Πεκίνο Κίνα (2005) και Αγία Πετρούπολη Ρωσία (2007). Αυτά εντάχθηκαν σε μια λίστα που περιελάμβανε εργαστήρια στο Μπρίστολ Αγγλία (1984), Τόκιο Ιαπωνία (1990) και Χάιφα Ισραήλ (1994).

Το 2002 εξαγόρασε την Compaq Computer Corporation, μια μεγάλη αμερικανική εταιρία κατασκευής υπολογιστών. Η κίνηση έγινε μετά από έκκληση του πρόσφατα προσληφθέντος διευθύνοντος συμβούλου (CEO), Carly Fiorina, της πρώτης γυναίκας που ηγείται μιας εταιρείας που είναι εισηγμένη στον Dow Jones. Αντιτάχθηκαν σκληρά ορισμένα μέλη του διοικητικού συμβουλίου της εταιρείας και ορισμένοι μεγάλοι μέτοχοι, συμπεριλαμβανομένου του Walter Hewlett, γιου του συνιδρυτή της εταιρείας. Όταν τα υποτιθέμενα οφέλη της συγχώνευσης απέτυχαν να υλοποιηθούν, αναγκάστηκε να αποχωρήσει το 2005. Ωστόσο, η εταιρεία σύντομα γύρισε τον ισολογισμό της και το 2007 η Hewlett-Packard έγινε η πρώτη εταιρεία τεχνολογίας που ξεπέρασε τα 100 δισεκατομμύρια δολάρια σε έσοδα από πωλήσεις ενός έτους.

Η Fiorina αντικαταστάθηκε ως CEO και πρόεδρος από τον Mark Hurd, ο οποίος ήταν διευθύνων σύμβουλος της NCR Corporation. (Ο Hurd πήρε τον τίτλο του προέδρου το 2006.) Κατά τη διάρκεια της θητείας του Hurd, η εταιρεία ξεκίνησε μια στρατηγική πρωτοβουλία για επέκταση στον χώρο των φορητών υπολογιστών. Για το σκοπό αυτό, το 2010 η Hewlett-Packard εξαγόρασε την Palm, Inc., μια εταιρία κατασκευής PDA και smartphone. Η θέση της Palm στην εξαιρετικά ανταγωνιστική αγορά smartphone ήταν αδύναμη, αλλά το λειτουργικό της σύστημα πολλαπλών εργασιών, γνωστό ως webOS ("επόμενη γενιά" διάδοχος του αρχικού Palm OS), θεωρήθηκε από τους αναλυτές ως ένα κορυφαίο σύστημα για smartphone. Η εξαγορά θα συμπληρώσει τις δύο σειρές smartphone iPAQ της Hewlett-Packard, μία για επιχειρηματικούς χρήστες και μία για καταναλωτές, που διέθεσε το Windows Mobile OS της Microsoft Corporation.

Ωστόσο, ο Hurd απομακρύνθηκε από την εταιρεία το 2010 μετά από σκάνδαλο που αφορούσε αμφισβητήσιμες σχέσεις με έναν εργολάβο. Αντικαταστάθηκε από τον Léo Apotheker, ο οποίος ήταν διευθύνων σύμβουλος του γερμανικού γίγαντα λογισμικού SAP. Τον Αύγουστο του 2011, η Hewlett-Packard ανακοίνωσε ότι θα σταματήσει να κατασκευάζει smartphone και τον υπολογιστή tablet της, το TouchPad (το οποίο είχε κάνει ντεμπούτο μόλις επτά εβδομάδες νωρίτερα τον Ιούλιο) και ότι σκέφτεται να διαχωρίσει την επιχείρηση υπολογιστών της σε ξεχωριστή εταιρεία. Στο εξής, η Hewlett-Packard επικεντρώθηκε στο λογισμικό και τις υπηρεσίες για επιχειρήσεις και εξαγόρασε τη βρετανική εταιρεία λογισμικού επιχειρήσεων Autonomy Corporation για 11,1 δισεκατομμύρια δολάρια. Ο Apotheker αντικαταστάθηκε ως Διευθύνων Σύμβουλος τον Σεπτέμβριο του 2011 από το μέλος του διοικητικού συμβουλίου Meg Whitman, ο οποίος ήταν διευθύνων σύμβουλος της διαδικτυακής εταιρείας δημοπρασιών eBay. Τον Νοέμβριο του 2012, η Hewlett-Packard κατηγόρησε τη διοίκηση της Autonomy ότι διογκώνει την αξία της εταιρείας μέσω «λογιστικών ανωμαλιών» και ανακοίνωσε ότι θα μειώσει την αξία της Autonomy κατά 8,8 δισεκατομμύρια δολάρια.

Το 2015 η Hewlett-Packard χωρίστηκε σε δύο εταιρείες: την HP Inc., η οποία δημιούργησε προσωπικούς υπολογιστές και εκτυπωτές και την Hewlett Packard Enterprise, η οποία παρείχε προϊόντα και υπηρεσίες για επιχειρήσεις.
Από νωρίς στην ιστορία της εταιρείας, οι δύο ιδρυτές ενέκριναν επίσημες διαδικασίες διαχείρισης και η Hewlett-Packard ήταν μία από τις πρώτες εταιρείες που χρησιμοποίησαν την προσέγγιση «management by objective». Δημιούργησαν επίσης έναν ανεπίσημο χώρο εργασίας, ενθαρρύνοντας τη χρήση των ονομάτων μεταξύ των εργαζομένων, ακόμη και για τον εαυτό τους. Οι Packard και Hewlett ήταν επίσης γνωστοί για τη «διοίκηση με το περπάτημα», επισκέπτονταν όσο το δυνατόν περισσότερα τμήματα χωρίς ραντεβού ή προγραμματισμένες συναντήσεις για συνομιλία με τους υπαλλήλους της γραμμής, τόσο συχνά όσο και με τους διευθυντές για να καταλάβουν πώς λειτουργεί η εταιρεία. Η Hewlett-Packard έγινε μια από τις πρώτες επιχειρήσεις στις Ηνωμένες Πολιτείες που ενέκρινε την ιδέα ότι οι εργαζόμενοι, οι πελάτες και η κοινότητα έχουν εξίσου ισχυρό ενδιαφέρον για την απόδοση της εταιρείας, όπως και οι μέτοχοι. Ως αποτέλεσμα, κατατάσσεται σταθερά μεταξύ των καλύτερων χώρων εργασίας για γυναίκες και μειονότητες. Έγινε επίσης ένας από τους κορυφαίους συνεισφέροντες σε φιλανθρωπικούς οργανισμούς, δωρίζοντας έως και 4,4% των προ φόρων κερδών της.

3.10.4. Intel

Η Intel Corporation, μία Αμερικάνικη εταιρία κατασκευής κυκλωμάτων υπολογιστών. Έχει την έδρα της στη Σάντα Κλάρα της Καλιφόρνια. Το όνομα της εταιρείας προέρχεται από το "Integrated electronics".

Η Intel ιδρύθηκε τον Ιούλιο του 1968 από τους Αμερικανούς μηχανικούς Robert Noyce και Gordon Moore. Σε αντίθεση με τον συνηθισμένο τύπο επιχειρήσεων της Silicon Valley που ξεκίνησαν σε ένα γκαράζ , η Intel άνοιξε τις πόρτες της με χρηματοδότηση 2,5 εκατομμυρίων δολαρίων που διοργανώθηκε από τον Arthur Rock, τον Αμερικανό χρηματοδότη που επινόησε τον όρο επιχειρηματικός καπιταλιστής. Οι ιδρυτές της Intel ήταν έμπειροι, μεσήλικες τεχνολόγοι που είχαν καθιερωμένη φήμη. Ο Noyce ήταν ο συν-εφευρέτης του ολοκληρωμένου κυκλώματος πυριτίου το 1959 όταν ήταν γενικός διευθυντής του Fairchild Semiconductor, ενός τμήματος της Fairchild Camera and Instrument. Ο Moore ήταν ο επικεφαλής της έρευνας και ανάπτυξης στο Fairchild Semiconductor. Αμέσως μετά την ίδρυση της Intel, η Noyce και ο Moore στρατολόγησαν άλλους υπαλλήλους της Fairchild, συμπεριλαμβανομένου του Αμερικάνου επιχειρηματία γεννημένου στην Ουγγαρία Andrew Grove. Οι Noyce, Moore και Grove υπηρέτησαν διαδοχικά ως πρόεδρος και διευθύνων σύμβουλος (CEO) κατά τις τρεις πρώτες δεκαετίες της ιστορίας της εταιρείας.

Τα αρχικά προϊόντα της Intel ήταν τσιπ μνήμης, συμπεριλαμβανομένου του πρώτου ημιαγωγού μεταλλικού οξειδίου του κόσμου, τον 1101, ο οποίος δεν είχε καλές πωλήσεις. Ωστόσο, ο «αδελφός» του, ένα Dynamic Random-Access Memory (DRAM) του ενός kilobit, ήταν επιτυχές και ήταν το πρώτο τσιπ που αποθηκεύει σημαντική ποσότητα πληροφοριών. Αγοράστηκε πρώτα από την αμερικανική εταιρεία τεχνολογίας Honeywell Incorporated το 1970 για να αντικαταστήσει την βασική τεχνολογία μνήμης στους υπολογιστές της. Επειδή τα DRAM ήταν φθηνότερα και χρησιμοποιούσαν λιγότερη ισχύ από τη βασική μνήμη, γρήγορα έγιναν οι τυπικές συσκευές μνήμης σε υπολογιστές παγκοσμίως.

Μετά την επιτυχία της στο DRAM, η Intel έγινε διάσημη το 1971. Την ίδια χρονιά η Intel παρουσίασε το programmable read-only memory (EPROM), το οποίο ήταν η πιο επιτυχημένη σειρά προϊόντων της εταιρείας μέχρι το 1985. Επίσης το 1971 οι μηχανικοί της Intel Ted Hoff, Federico Faggin, και Stan Mazor εφήυραν ένα μικροεπεξεργαστή γενικής χρήσης τεσσάρων bit και ένας από τους πρώτους μικροεπεξεργαστές single-chip, τον 4004, με σύμβαση με τον ιαπωνικό κατασκευαστή αριθμομηχανών Nippon Calculating Machine Corporation, οι οποίοι επέτρεψαν στην Intel να διατηρήσει όλα τα δικαιώματα στην τεχνολογία.

Δεν ήταν όλες οι πρώτες προσπάθειες της Intel επιτυχημένες. Το 1972 η διοίκηση αποφάσισε να εισέλθει στην αναπτυσσόμενη αγορά ψηφιακών ρολογιών αγοράζοντας το Microma. Αλλά η Intel δεν είχε πραγματική κατανόηση των καταναλωτών και πούλησε την εταιρεία ωρολογοποιίας το 1978 με απώλεια 15 εκατομμυρίων δολαρίων. Το 1974 η Intel ελέγχει το 82,9% της αγοράς του τσιπ DRAM, αλλά, με την άνοδο των ξένων εταιρειών ημιαγωγών, το μερίδιο αγοράς της εταιρείας μειώθηκε στο 1,3% έως το 1984. Μέχρι τότε, η Intel είχε μετατοπιστεί από τα τσιπ μνήμης και είχε επικεντρωθεί στην επιχείρηση μικροεπεξεργαστών. Το 1972 κατασκεύασε τον 8008, μια CPU 8-bit. Ο 8080, ο οποίος ήταν 10 φορές γρηγορότερος από το 8008, ήρθε δύο χρόνια αργότερα και το 1978 η εταιρεία δημιούργησε τον πρώτο μικροεπεξεργαστή 16-bit, τον 8086.

Το 1981 η IBM επέλεξε τον Intel 16-bit 8088 για να είναι ο CPU στον πρώτο μαζικής παραγωγής προσωπικό υπολογιστή (PC). Η Intel παρείχε επίσης τους μικροεπεξεργαστές της σε άλλους κατασκευαστές που δημιούργησαν «κλώνους» υπολογιστή που ήταν συμβατοί με το προϊόν της IBM. Ο υπολογιστής IBM και οι κλώνοι του πυροδότησαν τη ζήτηση για επιτραπέζιους και φορητούς υπολογιστές. Η IBM είχε συνάψει σύμβαση με μια μικρή εταιρεία στο Redmond, Washington, Microsoft Corporation, για την παροχή του λειτουργικού συστήματος δίσκου (DOS) για τον υπολογιστή της. Τελικά η Microsoft εγκατέστησε το λειτουργικό της σύστημα Windows σε υπολογιστές IBM, οι οποίοι, με συνδυασμό με το λογισμικό Windows και το Intel chip, ονομάστηκαν μηχανήματα "Wintel" και κυριάρχησαν στην αγορά από την ίδρυσή τους.
Από τους πολλούς μικροεπεξεργαστές που έχει παράγει η Intel, ίσως ο πιο σημαντικός ήταν το 80386, ένα τσιπ 32-bit που κυκλοφόρησε το 1985 και ξεκίνησε τη δέσμευση της εταιρείας να κάνει όλους τους μελλοντικούς μικροεπεξεργαστές συμβατούς με τους προηγούμενους. Οι προγραμματιστές εφαρμογών και οι ιδιοκτήτες υπολογιστών θα μπορούσαν τότε να είναι σίγουροι ότι το λογισμικό που δούλευε σε παλαιότερα μηχανήματα Intel θα λειτουργούσε στα νεότερα μοντέλα.

Με την εισαγωγή του μικροεπεξεργαστή Pentium το 1993, η Intel άφησε πίσω τις συμβάσεις ονομασίας προϊόντων με βάση τον αριθμό για τους μικροεπεξεργαστές της. Ο Pentium ήταν το πρώτο τσιπ της Intel που χρησιμοποίησε παράλληλη ή υπερκατευθυνόμενη επεξεργασία, η οποία αύξησε σημαντικά την ταχύτητά του. Είχε 3,1 εκατομμύρια τρανζίστορ, σε σύγκριση με τα 1,2 εκατομμύρια τρανζίστορ του προκατόχου του, το 80486. Σε συνδυασμό με το λειτουργικό σύστημα Windows 3.x της Microsoft, το πολύ πιο γρήγορο τσιπ Pentium βοήθησε στο να προωθηθεί η σημαντική επέκταση της εταιρίας στην αγορά υπολογιστών. Παρόλο που οι επιχειρήσεις αγόρασαν ακόμη περισσότερους υπολογιστές, οι υπολογιστές με Pentium κατέστησαν δυνατό για τους καταναλωτές να χρησιμοποιούν υπολογιστές για εφαρμογές γραφικών πολυμέσων, όπως παιχνίδια που απαιτούσαν περισσότερη ισχύ επεξεργασίας.

Η επιχειρηματική στρατηγική της Intel βασίστηκε στο να καταστήσει τους νεότερους μικροεπεξεργαστές δραματικά ταχύτερους από τους προηγούμενους για να προσελκύσει τους αγοραστές να αναβαθμίσουν τους υπολογιστές τους. Ένας τρόπος για να επιτευχθεί αυτό ήταν η κατασκευή τσιπ με πολύ περισσότερα τρανζίστορ σε κάθε έκδοση. Για παράδειγμα, ο 8088 που βρέθηκε στον πρώτο υπολογιστή IBM είχε 29.000 τρανζίστορ, ενώ το 80386 που παρουσιάστηκε τέσσερα χρόνια αργότερα περιελάμβανε 275.000, και το Core 2 Quad που παρουσιάστηκε το 2008 είχε περισσότερα από 800.000.000 τρανζίστορ. Το Itanium 9500, το οποίο κυκλοφόρησε το 2012, είχε 3.100.000.000 τρανζίστορ. Αυτή η αύξηση του αριθμού των τρανζίστορ έγινε γνωστή ως νόμος του Μουρ, που πήρε το όνομά του από τον συνιδρυτή της εταιρείας Gordon Moore.

Εικόνα 3.58

Προκειμένου να αυξηθεί η ευαισθητοποίηση των καταναλωτών, το 1991 η Intel άρχισε να επιδοτεί διαφημίσεις υπολογιστή με την προϋπόθεση ότι οι διαφημίσεις περιλάμβαναν την ετικέτα της εταιρείας "Intel inside". Στο πλαίσιο του προγράμματος συνεργασίας, η Intel διέθεσε ένα μέρος των χρημάτων που κάθε κατασκευαστής υπολογιστών ξόδευε κάθε χρόνο σε μάρκες Intel, από το οποίο η Intel συνεισέφερε το μισό κόστος των εντύπων και τηλεοπτικών διαφημίσεων της εταιρείας κατά τη διάρκεια του έτους. Αν και το πρόγραμμα κόστισε άμεσα στην Intel εκατοντάδες εκατομμύρια δολάρια κάθε χρόνο, είχε το επιθυμητό αποτέλεσμα να καθιερώσει την Intel ως εμφανές εμπορικό σήμα.

Η φημισμένη τεχνική ικανότητα της Intel δεν ήταν χωρίς ατυχήματα. Το μεγαλύτερο λάθος ήταν το λεγόμενο «Pentium flaw», στο οποίο ένα σκοτεινό τμήμα μεταξύ των 3,1 εκατομμυρίων τρανζίστορ της Pentium CPU έδινε λανθασμένη διαίρεση. Οι μηχανικοί της εταιρείας ανακάλυψαν το πρόβλημα μετά την κυκλοφορία του προϊόντος το 1993, αλλά αποφάσισαν να παραμείνουν σιωπηλοί και να διορθώσουν το πρόβλημα στις ενημερώσεις του chip. Ωστόσο, ο μαθηματικός Thomas Nicely του Lynchburg College στη Δυτική Βιρτζίνια ανακάλυψε επίσης το ελάττωμα. Αρχικά ο Grove (τότε CEO) αντιστάθηκε στα αιτήματα ανάκλησης του προϊόντος. Αλλά όταν η IBM ανακοίνωσε ότι δεν θα στέλνει υπολογιστές με την CPU, ανάγκασε την ανάκληση που κόστισε την Intel 475 εκατομμύρια δολάρια.

Παρόλο το φιάσκο των Pentium, ο συνδυασμός τεχνολογίας Intel με λογισμικό Microsoft συνέχισε να καταστρέφει τον ανταγωνισμό. Ανταγωνιστικά προϊόντα από την εταιρεία ημιαγωγών Advanced Micro Devices (AMD), την εταιρεία ασύρματων επικοινωνιών Motorola, τον κατασκευαστή σταθμών εργασίας Sun Microsystems, και άλλα σπάνια απειλούσαν το μερίδιο αγοράς της Intel. Ως αποτέλεσμα, το ντουέτο Wintel ήταν μονοπώλιο. Το 1999, η Microsoft κρίθηκε ένοχη σε ένα περιφερειακό δικαστήριο των ΗΠΑ

ότι ήταν μονοπώλιο μετά από μήνυση από το Υπουργείο Δικαιοσύνης, ενώ το 2009 η Ευρωπαϊκή Ένωση επέβαλε πρόστιμο στην Intel 1,45 δισεκατομμυρίων δολαρίων για φερόμενες μονοπωλιακές ενέργειες. Το 2009 η Intel πλήρωσε επίσης 1,25 δισεκατομμύρια δολάρια για να επιλύσει μια δεκαετή νομική διαμάχη στην οποία η AMD κατηγόρησε την Intel ότι πιέζει τους κατασκευαστές υπολογιστών να μην χρησιμοποιούν τα chip της.

Μέχρι τα μέσα της δεκαετίας του 1990, η Intel είχε επεκταθεί τόσο που οι μεγάλοι κατασκευαστές υπολογιστών, όπως η IBM και η Hewlett-Packard, μπόρεσαν να σχεδιάσουν και να κατασκευάσουν υπολογιστές που βασίζονται στην Intel για τις αγορές τους. Ωστόσο, η Intel ήθελε και άλλους, μικρότερους κατασκευαστές υπολογιστών να αποκτήσουν τα προϊόντα της και, επομένως, τα chip της Intel να κυκλοφορήσουν γρηγορότερα, έτσι άρχισε να σχεδιάζει και να κατασκευάζει Motherboards που περιείχαν όλα τα βασικά μέρη του υπολογιστή, συμπεριλαμβανομένων γραφικών και chip δικτύωσης. Μέχρι το 1995, η εταιρεία πούλησε περισσότερα από 10 εκατομμύρια motherboards σε κατασκευαστές υπολογιστών, περίπου το 40% της συνολικής αγοράς υπολογιστών. Στις αρχές του 21ου αιώνα, ο κατασκευαστής ASUSTeK με έδρα την Ταϊβάν ξεπέρασε την Intel ως ο κορυφαίος κατασκευαστής μητρικών καρτών PC.

Μέχρι το τέλος του αιώνα, Intel και συμβατά chip από εταιρείες όπως η AMD βρέθηκαν σε κάθε υπολογιστή, εκτός από το Macintosh της Apple Inc., το οποίο είχε χρησιμοποιήσει CPU από τη Motorola από το 1984. Ο Craig Barrett, ο οποίος διαδέχθηκε την Grove ως CEO της Intel το 1998, ήταν ικανός να καλύψει αυτό το κενό. Το 2005, ο Διευθύνων Σύμβουλος της Apple, Steven Jobs, συγκλόνισε τη βιομηχανία όταν ανακοίνωσε ότι οι μελλοντικοί υπολογιστές Apple θα χρησιμοποιούν επεξεργαστές Intel. Ως εκ τούτου μικροεπεξεργαστές της Intel βρίσκονται σχεδόν σε κάθε υπολογιστή και η εταιρεία κυριάρχησε στην αγορά CPU στις αρχές του 21ου αιώνα.

3.10.5. IBM

Η International Business Machines, IBM, ιδρύθηκε το 1911 με το όνομα Computing-Tabulation-Recording Company (C-T-R).

Ο ιδρυτής Charles Ranlett Flint δεν δημιούργησε την εταιρεία C-T-R με τη συγχώνευση τριών εταιρειών που υπήρχαν από τα τέλη του 1800, των Computing Scale Company, Tabulating Machine Company και Time Recording Company. Η νέα συγχωνευθείσα εταιρεία είχε έδρα την Νέα Υόρκη με περίπου 1.300 υπαλλήλους. (Συγκριτικά, σήμερα η IBM απασχολεί περίπου 350.000 άτομα.)

Αυτά τα πρώτα χρόνια η εταιρεία C-T-R επικεντρώθηκε σε προϊόντα όπως μηχανές λογιστικής και υπολογισμού, συσκευές καταγραφής χρόνου για επιχειρήσεις και μηχανικά συστήματα καρτών διάτρησης. Βασιζόταν κυρίως σε τυποποιημένα προϊόντα γραφείου όχι στην εφεύρεση όπως εξελίχθηκε αργότερα.

Το 1924, ο Thomas Watson ανέλαβε την εταιρεία η οποία και μετονομάστηκε σε International Business Machines (IBM). Στα πρώτα του χρόνια ο Watson δημιούργησε την επιτυχία της IBM μέσω επιχειρηματικών και εμπορικών στρατηγικών, δημιουργώντας προϊόντα που χτίστηκαν γύρω από τις ανάγκες των μεμονωμένων πελατών και επενδύοντας σε μεγάλο βαθμό στο δυναμικό πωλήσεων της εταιρείας.

Τη δεκαετία του 1920 και του 1930, η IBM ξεκίνησε ξεκίνησε να εδραιώνει το όνομα της. Δημιούργησε το σύστημα δημόσιων διευθύνσεων που χρησιμοποιούν τα σχολεία, το οποίο γρήγορα έγινε βασικό στην αμερικανική κοινωνία. Η Υπηρεσία Κοινωνικής

Ασφάλισης υιοθέτησε τα μηχανήματα καρτών διάτρησης της εταιρείας για να βοηθήσει στη δημιουργία του νέου δικτύου αριθμών κοινωνικής ασφάλισης για όλους τους πολίτες. Και το 1928 εφηύρε την πρώτη αριθμομηχανή που μπορούσε να κάνει αφαίρεση άμεσα. Παρά το εντυπωσιακό επιχειρηματικό ρεκόρ, η IBM είναι μία από τις πιο αξιοσημείωτες εταιρίες για τα τεχνολογικά της επιτεύγματα.

Το 1943 η εταιρεία ανέπτυξε την πρώτη πλήρως ηλεκτρονική υπολογιστική μηχανή, το Vacuum Tube Multiplier. Αυτό οδήγησε το 1944 στην ανάπτυξη του Automatic Sequence Controlled Calculator, (Mark I), το οποίο η IBM ανέπτυξε μαζί με το Harvard. Αυτή ήταν η πρώτη συσκευή που θα αναγνωριζόταν ως σύγχρονος υπολογιστής. Καταλάμβανε ένα μικρό δωμάτιο, σε μήκος 16 μέτρα και ύψος 2,4 μέτρα περίπου, και πραγματοποιούσε αυτόματα ηλεκτρομηχανικούς υπολογισμούς. Το Πολεμικό Ναυτικό των ΗΠΑ χρησιμοποίησε το Mark I για να υπολογίσει τις τροχιές των όπλων στα πλοία του.
Ωστόσο, η εταιρεία δεν προώθησε αυτήν την επιχείρηση μέχρι τη δεκαετία του 1950 όταν και ανέλαβε ο γιος του Thomas Watson, Thomas Watson Jr. Σε αυτήν την εποχή η επιχείρηση υπολογιστών της IBM εγκατέλειψε τους μηχανικούς διακόπτες του Mark I και στράφηκε στους σωλήνες κενού του Vacuum Tube Multiplier, καθώς αυτοί ήταν πιο εύκολο να συντηρηθούν και να αντικατασταθούν.

Κατά τη διάρκεια της δεκαετίας του 1950 και του 1960, η IBM εφηύρε πολλές από τις βασικές τεχνολογίες που βοήθησαν ώστε οι υπολογιστές να γίνουν βασικά εργαλεία στον επιχειρηματικό κόσμο. Ανέπτυξε τον υπολογιστή σωλήνων κενού εργασίας, ο οποίος έγινε η βάση για όλους τους υπολογιστές μέχρι την εφεύρεση του μικροτσίπ. Η IBM εφηύρε επίσης τον σκληρό δίσκο, δημιουργώντας τον πρώτο υπολογιστή που αποθηκεύει δεδομένα σε περιστρεφόμενες πιατέλες και ανακτά αυτά τα δεδομένα με μαγνητικό βραχίονα. Επίσης, ανέπτυξε την FORTRAN, τον πρόδρομο για τις περισσότερες σύγχρονες γλώσσες προγραμματισμού.

Την εποχή αυτή η κυριαρχία της IBM στην αγορά υπολογιστών ήταν σχεδόν πλήρης, με την εταιρεία να κατασκευάζει το 60% έως 70% όλων των επιχειρηματικών υπολογιστών παγκοσμίως.

Η σύγχρονη εποχή της IBM ξεκίνησε αναμφισβήτητα το 1981 με τον προσωπικό υπολογιστή 5150 ή αλλιώς PC. Αυτός ήταν ένας από τους πρώτους υπολογιστές που προορίζονται για χρήση από τους καταναλωτές και δεν ήταν αφιερωμένος στην επιχείρηση ή την κυβέρνηση. Η IBM συνεργάστηκε με τη Microsoft, τότε ήταν μια σχετικά νέα εταιρεία, για την εκτέλεση του MS-DOS ως λειτουργικού συστήματος σε αυτά τα μηχανήματα.

Στην ίδια εποχή, η IBM εφηύρε την αρχιτεκτονική για τοπικά δίκτυα. Αυτό εφαρμόστηκε πρώτα στα δίκτυα γραφείων στα οποία βασίστηκαν οι χρήστες, και στη συνέχεια έγινε η βάση για τα παγκόσμια δίκτυα που συνδέουν τους χρήστες στο Διαδίκτυο και τέλος τα οικιακά δίκτυα που χρησιμοποιούν τα περισσότερα νοικοκυριά σήμερα. Δημιούργησε επίσης ένα από τα σύγχρονα σημεία αναφοράς για την τεχνητή νοημοσύνη με το σύστημα σκέψης Deep Blue. Αυτό το AI έγινε το πιο διάσημο για τη σειρά σκακιστικών παιχνιδιών εναντίον του παγκόσμιου πρωταθλητή Garry Kasparov στη δεκαετία του 1990, με αποκορύφωμα την ήττα του Kasparov το 1997.

Ωστόσο, την ίδια στιγμή, καθώς η δεκαετία του 1980 και του 1990 η υπολογιστική μονάδα της IBM ήταν πρωτοπόρος, η εταιρεία έχασε επίσης το καθεστώς της ως ηγέτης της αγοράς. Οι κλώνοι της μηχανής IBM και του επιχειρηματικού μοντέλου ξεπήδησαν γρήγορα σε όλη την καταναλωτική αγορά, με πολλές άλλες εταιρείες που πωλούν

μηχανήματα υπολογιστών να χρησιμοποιούν το λειτουργικό σύστημα της Microsoft. Αν και για αρκετά χρόνια η πολιτιστική παρουσία της IBM ήταν αρκετά ισχυρή ώστε αυτά τα μηχανήματα ήταν γνωστά ως «κλώνοι IBM», τελικά η εταιρεία έγινε απλά ένας άλλος ανταγωνιστής σε μια μεγάλη αγορά.

Εικόνα 3.59

Ταυτόχρονα, η ιστορική κυριαρχία της στην αγορά μεγάλων, εγκατεστημένων mainframes άρχισε να πλήττει την IBM καθώς τεχνολογικά εξελισσόταν και οι υπολογιστικές μηχανές έγιναν μικρότερες και γρηγορότερες. Η εταιρεία δεν ήταν καλά εξοπλισμένη για να ανταποκριθεί σε μια εποχή κατά την οποία τα mainframe αντικαταστάθηκαν από μικρούς διακομιστές. Κατά τη διάρκεια της δεκαετίας του 1990, το βασικό επιχειρηματικό μοντέλο της IBM και τα κέντρα κέρδους απομακρύνθηκαν από την τεχνολογία. Μέχρι το τέλος της δεκαετίας, η εταιρεία είχε μεγάλο μέρος, αν όχι το μεγαλύτερο μέρος, της ανάπτυξής της σε επιχειρηματικές υπηρεσίες, όπως η παροχή βοήθειας στους πελάτες για τη δημιουργία δικτύων και την εγκατάσταση διακομιστών.

Το 2005, η Lenovo αγόρασε το τμήμα προσωπικών υπολογιστών της IBM, μετατοπίζοντας το επιχειρηματικό της μοντέλο ακόμη περισσότερο προς επιχειρηματικές υπηρεσίες και μακριά από υλικό. Ωστόσο, ενώ η IBM δεν έχει την πολιτιστική φήμη για την καινοτομία που κάποτε έκανε, συνέχισε να επενδύει σε μεγάλο βαθμό σε αυτόν τον τομέα. Το ερευνητικό σκέλος της εταιρείας υπερυπολογιστών συνεχίζει να παράγει μερικά από τα πιο ισχυρά μηχανήματα στον κόσμο και η IBM συνεχίζει να χορηγεί νέα σχέδια σε επιχειρήσεις, κυβέρνηση και στρατό μέχρι σήμερα.

4. Ιστορική εξέλιξη λειτουργικών συστημάτων εξυπηρετητών

4.1. Ιστορική εξέλιξη των Linux

Το Unix είναι ένα από τα πιο δημοφιλή λειτουργικά συστήματα παγκοσμίως λόγω της μεγάλης βάσης και της διανομής του. Αρχικά αναπτύχθηκε από την ανάπτυξη του έργου Multics στο Κέντρο Ερευνών Επιστημών Υπολογιστών Bell Laboratories. Οι προγραμματιστές που εργάζονταν στο Multics στα Bell Labs και αλλού ενδιαφέρονταν να δημιουργήσουν ένα λειτουργικό σύστημα πολλαπλών χρηστών και με δυναμική σύνδεση (στην οποία μια τρέχουσα διεργασία μπορεί να ζητήσει να προστεθεί ένα άλλο τμήμα κώδικα στον χώρο διευθύνσεών της, επιτρέποντάς της να εκτελέσει τον κώδικα αυτού του τμήματος) και ένα ιεραρχικό σύστημα αρχείων.

Η Bell Labs σταμάτησε να χρηματοδοτεί το έργο Multics το 1969, αλλά μια ομάδα ερευνητών, συμπεριλαμβανομένων των Ken Thompson και Dennis Ritchie, συνέχισαν να εργάζονται με τις βασικές αρχές του έργου. Το 1972-3 αποφάσισαν να ξαναγράψουν το σύστημα σε C, κάτι το οποίο έκανε το Unix μοναδικά φορητό: σε αντίθεση με άλλα σύγχρονα λειτουργικά συστήματα, θα μπορούσε να μεταφερθεί και να μην εξαρτάται από το υλικό του.

Η έρευνα και η ανάπτυξη στα Bell Labs (αργότερα AT&T) συνεχίστηκε, με τα Unix System Laboratories να αναπτύσσουν εκδόσεις του Unix, σε συνεργασία με την Sun Microsystems, και υιοθετήθηκαν ευρέως από εμπορικούς προμηθευτές του Unix. Η έρευνα συνεχίστηκε σε ακαδημαϊκούς κύκλους, κυρίως στην Ομάδα Έρευνας Συστημάτων Υπολογιστών στο Πανεπιστήμιο της Καλιφόρνια στο Μπέρκλεϋ. Αυτή η ομάδα παρήγαγε το Berkeley Software Distribution (BSD), το οποίο ενέπνευσε μια σειρά λειτουργικών συστημάτων, πολλά από τα οποία εξακολουθούν να χρησιμοποιούνται ακόμη και σήμερα. Δύο διανομές BSD που αξίζει να αναφέρουμε είναι το NeXTStep, το λειτουργικό σύστημα που πρωτοστάτησε από το NeXT, το οποίο έγινε η βάση για macOS, μεταξύ άλλων προϊόντων, και το MINIX, ένα εκπαιδευτικό λειτουργικό σύστημα που αποτέλεσε την βάση για τον Linus Torvalds καθώς ανέπτυσσε το Linux.

Το Unix προσανατολίζεται στις αρχές της σαφήνειας, της φορητότητας και της ταυτότητας:

- *Σαφήνεια*: Η αρθρωτή σχεδίαση του Unix επιτρέπει στις διεργασίες να εκτελούνται με περιορισμένο και καθορισμένο τρόπο. Το σύστημα αρχείων του είναι ενοποιημένο και ιεραρχικό, το οποίο απλοποιεί τον χειρισμό των δεδομένων. Σε αντίθεση με ορισμένους από τους προκατόχους του, το Unix υλοποιεί εκατοντάδες (και όχι χιλιάδες) κλήσεις συστήματος, καθεμία από τις οποίες έχει σχεδιαστεί για να είναι απλή και σαφής στο στόχο.
- *Φορητότητα*: Γράφοντας το Unix σε C, η ομάδα στο Bell Labs τοποθέτησε το Unix για ευρεία χρήση. Η C σχεδιάστηκε για να έχει πρόσβαση χαμηλού επιπέδου στη μνήμη, ελάχιστη υποστήριξη χρόνου εκτέλεσης και αποτελεσματική σχέση μεταξύ της γλώσσας και των οδηγιών του μηχανήματος. Επειδή λοιπόν η βάση είναι η C σημαίνει ότι το Unix είναι προσαρμόσιμο και εύκολο στη χρήση σε μια ποικιλία υλικού.
- *Ταυτότητα*: Ο πυρήνας του Unix είναι προσαρμοσμένος στον στόχο (που μοιράζεται το έργο Multics) της διατήρησης πολλαπλών χρηστών και ροών εργασίας. Ο χώρος του πυρήνα παραμένει ξεχωριστός από τον χώρο χρήστη στο Unix, το οποίο επιτρέπει την ταυτόχρονη εκτέλεση πολλαπλών εφαρμογών.

4.1.1. Η Εξέλιξη του Linux

Το Unix έθεσε σημαντικά ερωτήματα για προγραμματιστές, αλλά παρέμεινε επίσης ιδιόκτητο στις πρώτες εκδόσεις του. Το επόμενο κεφάλαιο της ιστορίας του είναι η ιστορία του πώς εργάστηκαν οι προγραμματιστές για να δημιουργήσουν εναλλακτικές λύσεις ανοιχτού κώδικα.

Πειράματα ανοιχτού κώδικα

Ο Richard Stallman ήταν μια κεντρική προσωπικότητα μεταξύ των προγραμματιστών που εμπνεύστηκαν να δημιουργήσουν μη ιδιόκτητες εναλλακτικές λύσεις στο Unix. Ενώ εργαζόταν στο Εργαστήριο Τεχνητής Νοημοσύνης του MIT, ξεκίνησε εργασίες για το έργο GNU (αναδρομικό για το "GNU's not Unix!"). Αποχώρησε τελικά από το εργαστήριο το 1984 ώστε να μπορούσε να διανείμει στοιχεία GNU ως δωρεάν λογισμικό. Ο πυρήνας GNU, γνωστός ως GNU HURD, έγινε το επίκεντρο του Ιδρύματος Ελεύθερου Λογισμικού (FSF), που ιδρύθηκε το 1985 με επικεφαλής τον Stallman.

Ένας άλλος προγραμματιστής εργάστηκε για μια δωρεάν εναλλακτική λύση για το Unix: Ο Φιλανδός προπτυχιακός Linus Torvalds. Αφού απογοητεύτηκε με την άδεια χρήσης του MINIX, ο Torvalds ανακοίνωσε σε μια ομάδα χρηστών του MINIX στις 25 Αυγούστου 1991 ότι ανέπτυξε το δικό του λειτουργικό σύστημα, το οποίο έμοιαζε με το MINIX. Αν και αρχικά αναπτύχθηκε στο MINIX χρησιμοποιώντας τον μεταγλωττιστή GNU C, ο πυρήνας Linux έγινε γρήγορα ένα μοναδικό έργο με μια ομάδα προγραμματιστών που κυκλοφόρησαν την έκδοση 1.0 του πυρήνα με τον Torvalds το 1994. Ο Torvalds είχε χρησιμοποιήσει τον κώδικα του GNU, συμπεριλαμβανομένου του GNU C Compiler, με τον πυρήνα του, και παραμένει αλήθεια ότι πολλές διανομές Linux βασίζονται σε στοιχεία GNU. Ο Stallman έχει πιέσει να επεκτείνει τον όρο «Linux» σε «GNU / Linux», τον οποίο υποστήριζε ότι θα συμπεριλαμβάνει τόσο τον ρόλο του έργου GNU στην ανάπτυξη του Linux όσο και τα υποκείμενα ιδανικά που προώθησαν το έργο GNU και τον πυρήνα Linux. Σήμερα, ο όρος "Linux" χρησιμοποιείται συχνά για να δείξει τόσο την παρουσία του πυρήνα του Linux όσο και τα στοιχεία GNU. Ταυτόχρονα, τα ενσωματωμένα συστήματα σε πολλές φορητές συσκευές και smartphone χρησιμοποιούν συχνά τον πυρήνα Linux με λίγα έως καθόλου στοιχεία GNU.

4.1.2. Βασικά χαρακτηριστικά του Linux

Αν και ο πυρήνας Linux κληρονόμησε πολλούς στόχους και ιδιότητες από το Unix, διαφέρει από το προηγούμενο σύστημα με τους ακόλουθους τρόπους:

- Το βασικό του στοιχείο είναι ο πυρήνας, ο οποίος αναπτύσσεται ανεξάρτητα από άλλα στοιχεία του λειτουργικού συστήματος. Αυτό σημαίνει ότι το Linux δανείζεται στοιχεία από διάφορες πηγές (όπως το GNU) για να περιλαμβάνει ένα ολόκληρο λειτουργικό σύστημα.
- Είναι δωρεάν και ανοιχτού κώδικα. Συντηρημένος από μια κοινότητα προγραμματιστών, ο πυρήνας διαθέτει άδεια βάσει της άδειας GNU General Public License (ένα απόσπασμα των εργασιών του FSF στο έργο GNU) και διατίθεται για λήψη και τροποποίηση. Η GPL ορίζει ότι η παράγωγη εργασία πρέπει να διατηρεί τους όρους αδειοδότησης του αρχικού λογισμικού.

- ❖ Έχει μονολιθικό πυρήνα, παρόμοιο με το Unix, αλλά μπορεί δυναμικά να κάνει load και unload κώδικα του πυρήνα κατά παραγγελία.
- ❖ Διαθέτει συμμετρική υποστήριξη πολλαπλών επεξεργαστών (SMP), σε αντίθεση με τις παραδοσιακές εφαρμογές του Unix. Αυτό σημαίνει ότι ένα μόνο λειτουργικό σύστημα μπορεί να έχει πρόσβαση σε πολλούς επεξεργαστές, οι οποίοι μοιράζονται μια κύρια μνήμη και πρόσβαση σε όλες τις συσκευές I / O.
- ❖ Ο πυρήνας του είναι προληπτικός, μια άλλη διαφορά από το Unix. Αυτό σημαίνει ότι ο προγραμματιστής μπορεί να θέσει μία διακοπή σε ένα πρόγραμμα οδήγησης ή σε άλλο μέρος του πυρήνα ενώ εκτελείται.
- ❖ Ο πυρήνας του δεν κάνει διάκριση μεταξύ νημάτων και κανονικών διεργασιών.
- ❖ Περιλαμβάνει μια διεπαφή γραμμής εντολών (CLI) και μπορεί επίσης να περιλαμβάνει ένα γραφικό περιβάλλον εργασίας χρήστη (GUI).

4.1.3. Η εξέλιξη των διανομών του Linux

Στην αρχή, υπήρχε το Unix. Δημιουργήθηκε από τους Ken Thompson και Dennis Ritchie, το 1969. Κατά τη διάρκεια της δεκαετίας του '80 πολλά έργα ξεκίνησαν τη ζωή τους, όλα βασισμένα στο συνολικό όραμα που είναι το Unix. Το GNU, του Richard Stallman, το Berkley Software Distribution (BSD) καθώς και το MINIX (Mini-Unix) που κυκλοφόρησε στον ακαδημαϊκό κόσμο σε συνδυασμό με τα προαναφερθέντα. Το 1991 ένας νεαρός Φινλανδός μαθητής, που ονομάζεται Linus Torvalds, συνδύασε όλα τα συστατικά που αποτελούσαν αυτά τα συστήματα σε έναν πυρήνα που θα άλλαζε τον κόσμο.

Υπάρχουν πολλοί μύθοι που μιλάνε για την έναρξη του Linux, κάποιοι από τους οποίους είναι:

- Ο Linus, ενώ έπαιζε στο MINIX, έστειλε δεδομένα στον σκληρό του δίσκο αντί για το μόντεμ του και κατέστρεψε τα διαμερίσματα MINIX που είχε δημιουργήσει, οδηγώντας τον έτσι στην απογοήτευσή του για τους περιορισμούς του λειτουργικού συστήματος και αποφάσισε να δημιουργήσει το δικό του .
- Ο Linus, έγραψε τον πυρήνα για να αποκτήσει καλύτερη λειτουργικότητα του νέου μηχανήματος Intel 386 που χρησιμοποιούσε.
- Του απαγορεύτηκε να βελτιώσει περαιτέρω το MINIX, και έτσι συνέχισε να αναπτύσσει το δικό του λειτουργικό.

Όποια και αν είναι η πραγματική ιστορία, δημιούργησε με επιτυχία έναν δωρεάν εξομοιωτή τερματικού που βασίστηκε στο MINIX, το οποίο βασίστηκε στο Unix, το οποίο τελικά θα μπορούσε να λειτουργήσει για έναν πυρήνα λειτουργικού συστήματος και στις 25 Αυγούστου 1991, ο Linus δημοσίευσε αυτό το διάσημο μήνυμα στην ομάδα συζητήσεων MINIX:

From torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)

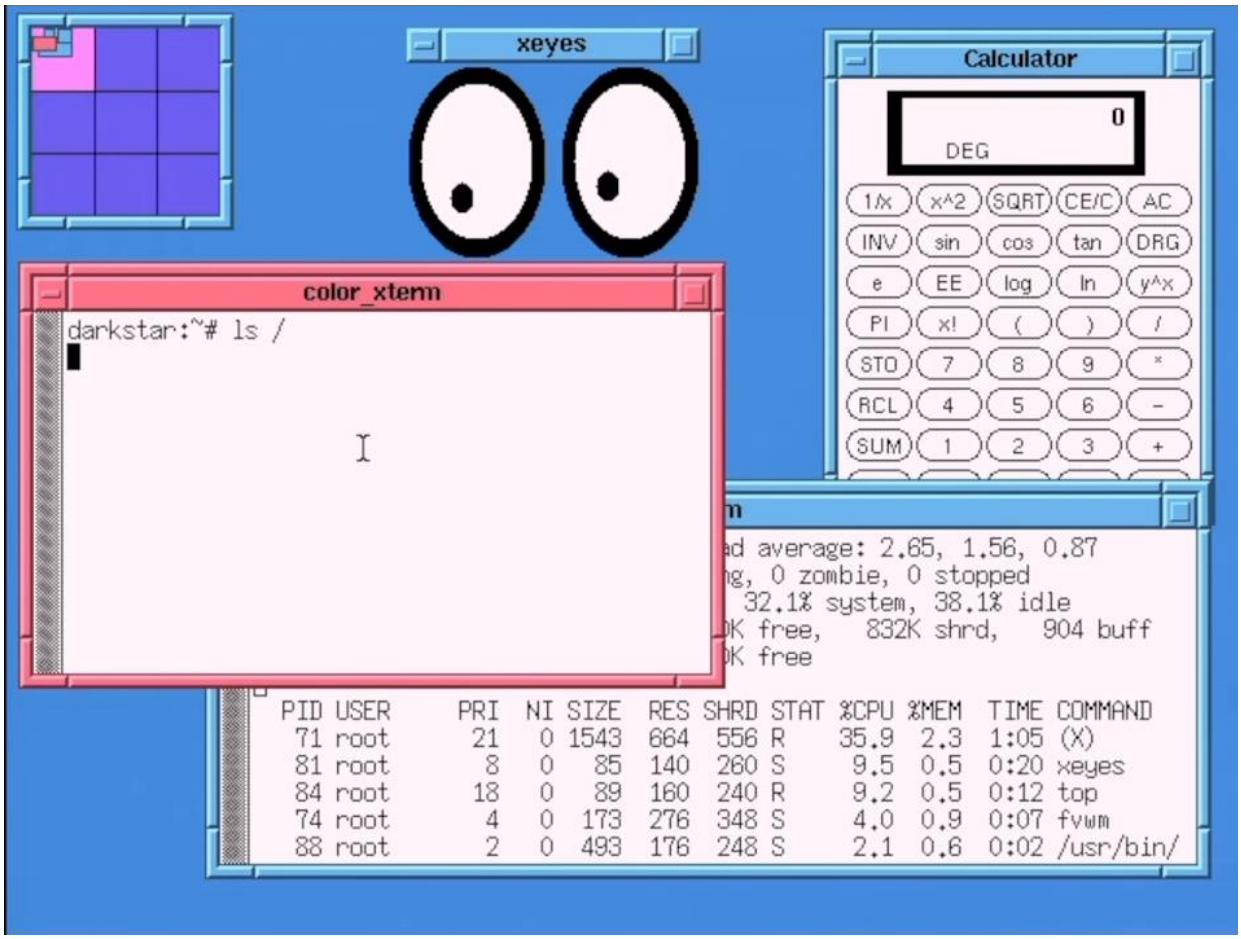
Newsgroups: comp.os.minix
Subject: What would you like to see most in minix?
Summary: small poll for my new operating system
Message-ID:
Date: 25 Aug 91 20:57:08 GMT
Organization: University of Helsinki

Hello everybody out there using minix –
I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) among other things).

I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want. Any suggestions are welcome, but I won't promise I'll implement them:-)

Μετά από αυτό, οι διακομιστές FTP σε όλο τον κόσμο έγιναν αρένες με εκδόσεις Linux (αρχικά ονομάστηκαν «Freax»), οι οποίοι αυξήθηκαν με εκπληκτικό ρυθμό λόγω του αριθμού των συμμετεχόντων. Αυτή την χρονιά λοιπόν η έκδοση 0.01 του Linux ήταν γεγονός. Μεταξύ 1992 και 1994 είδαμε την άνοδο των πιο ισχυρών ιδρυτών της σύγχρονης επιφάνειας εργασίας των Linux: Slackware, Red Hat και Debian, μαζί με τον Linux Kernel να αυξάνεται σε version 0.95, ο πρώτος Kernel που μπορεί να τρέχει το σύστημα X Window.

Το 1992 το SLS (Softlanding Linux System) του Peter MacDonald ήταν ένα από τα πρώτα συστήματα που υιοθέτησαν τον «νέο» πυρήνα Linux εκείνη την εποχή. Το SLS ήταν πολύ μπροστά από την εποχή του, καθώς ήταν η πρώτη διανομή Linux που περιείχε όχι μόνο τον πυρήνα Linux 0.99, αλλά και τη στοίβα TCP / IP και το σύστημα X Windows. Το 1993 λόγω των απογοητεύσεων της διεπαφής του SLS με λάθη, δύο νέες διανομές που βασίστηκαν στο SLS βγήκαν στο προσκήνιο. Το Slackware του Patrick Volkerding όπως φαίνεται στην εικόνα 4.1, το οποίο στέφθηκε ως η μακρύτερη τρέχουσα διανομή Linux και το Debian του Ian Murdock το οποίο πήρε το όνομά του συνδυάζοντας το όνομα της τότε φιλενάδας του Ian, Ντέμπρα (Debra), με το δικό του.



Εικόνα 4.1

Το 1994 καθώς εξελίχθηκε το Slackware, άρχισαν να σχηματίζονται άλλες διανομές, χρησιμοποιώντας το Slackware ως βάση κώδικα. Μια τέτοια διανομή που εμφανίστηκε στη σκηνή το 1994 ήταν το «Software und System-Entwicklung», ή όπως ήταν πιο γνωστό, «S.u.S.E Linux».

Μια τελευταία διανομή που είδε το φως της ημέρας στις 3 Νοεμβρίου 1994 ονομάστηκε «Red Hat Commercial Linux», που δημιουργήθηκε από τον Marc Ewing και πήρε το όνομά του από το παρόμοιο χρωματιστό καπέλο που φορούσε ενώ ήταν στο Πανεπιστήμιο. Επίσης στις 14 Μαρτίου 1994, κυκλοφόρησε το Linux 1.0.0 με 176.250 γραμμές κώδικα.

Το 1995 το Jurix Linux ήταν μια ενδιαφέρουσα διανομή που ήταν αξιοσημείωτη για διάφορους λόγους. Φέρεται να ήταν η πρώτη διανομή που περιλάμβανε ένα πρόγραμμα εγκατάστασης με δυνατότητα δέσμης ενεργειών, επιτρέποντας σε μια εγκατάσταση που βασίζεται σε διαχειριστή να αντιγράφει τη διαδικασία εγκατάστασης σε παρόμοια μηχανήματα. Ήταν ένα από τα πρώτα Linux λειτουργικά που υποστήριζε πλήρως το bootp και το NFS, και ένα από τα πρώτα συστήματα Linux που προορίζονταν να χρησιμοποιήσουν το EXT2. Αλλά αυτό που πραγματικά έκανε το Jurix ένα σημαντικό ορόσημο στην ιστορία του Linux ήταν το γεγονός ότι ήταν το βασικό σύστημα που χρησιμοποιήθηκε για τη δημιουργία του openSUSE Linux που γνωρίζουμε και χρησιμοποιούμε σήμερα.

Οι εκδόσεις Linux με βάση το Red Hat γνώρισαν μεγάλη επιτυχία κατά τη διάρκεια αυτής της πενταετούς περιόδου. Αξιοσημείωτες εκδόσεις όπως Caldera, Mandrake, TurboLinux, Yellow Dog και Red Flag ξεκίνησαν όλες από την ξαφνική μεγάλη και συνεχής εξελιξη του πυρήνα Linux, που εξελίχθηκε , από το 1995 έως το 2000, στις εκδόσεις 1.2.0 έως 2.2. Στην πραγματικότητα, η έκδοση 2.0, που κυκλοφόρησε το 1996, είχε περίπου 41 εκδόσεις στη σειρά. Ήταν αυτή η γρήγορη ανατροπή του πυρήνα και η προσθήκη ορισμένων πολύ σημαντικών χαρακτηριστικών που εγκαθίδρυσαν το λειτουργικό σύστημα Linux ως το λειτουργικό σύστημα διακομιστή της επιλογής για επαγγελματίες πληροφορικής σε όλο τον κόσμο. Η έκδοση 2.0, για παράδειγμα, είχε χαρακτηριστικά όπως υποστήριξη SMP, καλύτερη διαχείριση μνήμης και μπορούσε να τρέξει σε περισσότερους τύπους επεξεργαστών. Η έκδοση 2.2 περιελάμβανε βελτίωση του SMP, υποστήριξη για την αρχιτεκτονική PowerPC και δυνατότητα μόνο για ανάγνωση για το NTFS.

Το 1996 τα συστήματα που βασίζονται στο Debian, αν και δεν είναι τόσο ενεργά όσο τα αντίστοιχα του Red Hat, άρχισαν να αναπτύσσονται και ευνόησαν μια πολύ λιγότερο τεχνική προσέγγιση διακομιστή για τις διανομές τους. Όντας περισσότερο λειτουργικό σύστημα με προσανατολισμό στην επιφάνεια εργασίας, μια διανομή με βάση το Debian εμφανιζόταν συχνά στο μπροστινό μέρος των δημοφιλών περιοδικών εκείνη την εποχή, παρουσιάζοντας αξιοσημείωτες καταχωρήσεις όπως: Libranet, Storm, Finnix και Corel Linux.

Φυσικά, τα πιο αξιοσημείωτα συμβάντα κατά τη διάρκεια αυτών των πέντε ετών, ήταν η γέννηση του KDE και του Gnome. Το KDE (Kool Desktop Environment) ιδρύθηκε το 1996 από τον Matthias Ettrich, φοιτητή στο Πανεπιστήμιο του Tübingen, ο οποίος πρότεινε όχι μόνο ένα σύνολο εφαρμογών εργασίας, αλλά και ένα ολόκληρο περιβάλλον επιφάνειας εργασίας. Μέχρι το 1998, η έκδοση 1.0 του KDE ήταν ανοιχτή στον κόσμο και η πρώτη διανομή που το χρησιμοποίησε ήταν το Mandrake. Το 2000 κυκλοφόρησε, η έκδοση 2.0 και παρουσίασε ένα πολύ βελτιωμένο σύστημα.

Το 1997 οι Miguel de Icaza και Federico Mena ανακοίνωσαν την ανάπτυξη ενός νέου περιβάλλοντος επιφάνειας εργασίας και συνοδευτικών εφαρμογών. Με βάση το GTK +, αυτό το νέο περιβάλλον επιφάνειας εργασίας ονομάστηκε Gnome. Το Gnome γρήγορα έγινε ένα αποδεκτό περιβάλλον για επιτραπέζιους υπολογιστές, το οποίο ήταν γρήγορο, εύκαμπτο και πολύ φιλικό για τον μέσο χρήστη και μέχρι τον Μάιο του 2000 κυκλοφόρησε το Gnome 1.2 "Bongo".

Το 1998 η Oracle και η Sun ανακοίνωσαν επίσημη υποστήριξη για Linux, καθώς το λειτουργικό σύστημα γίνεται όλο και πιο δημοφιλές και περισσότεροι διαχειριστές συστήματος αρχίζουν να το υιοθετούν στους διακομιστές τους.

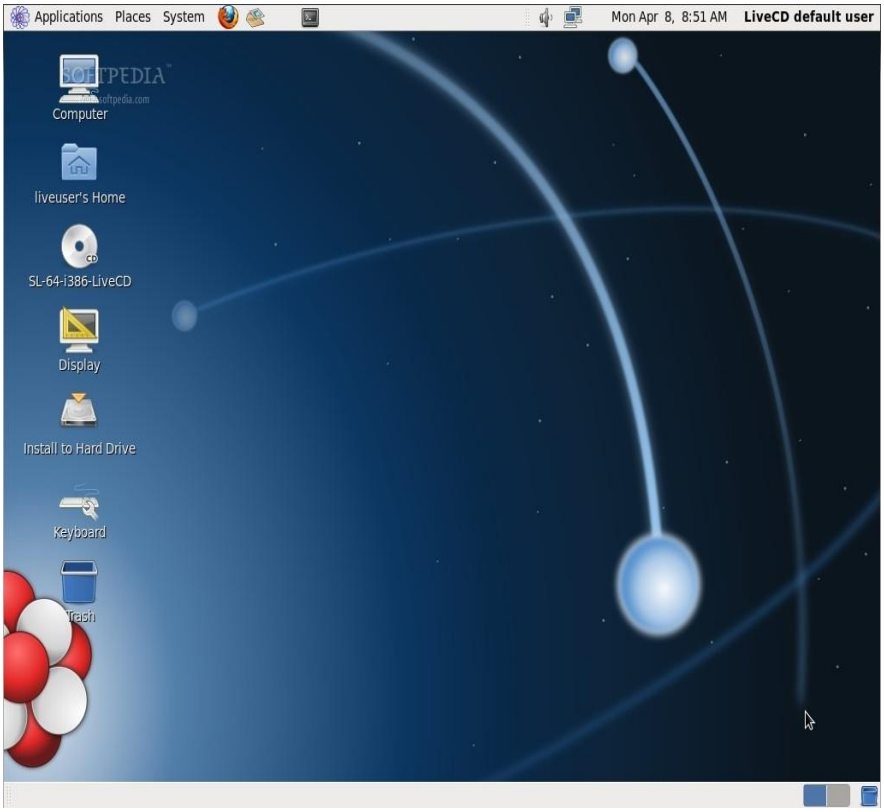
Το 1999 η Red Hat μπαίνει στο χρηματιστήριο και επιτυγχάνει το όγδοο μεγαλύτερο κέρδος την πρώτη ημέρα στη Wall Street, τροφοδοτώντας περαιτέρω την άνοδο του Linux.

Το 2000 το Knoppix, μία φιλική διανομή με βάση το Debian που αναπτύχθηκε από τον Klaus Knopper, ήταν επίσης ένα από τα πιο δημοφιλή της εποχής του. Αξίζει να σημειωθεί για πολλούς λόγους, αλλά ο κύριος ήταν το γεγονός ότι μπορούσε να ξεκινήσει απευθείας από το CD. Αυτό ίσως είναι κάτι που θεωρούμε δεδομένο αυτές τις μέρες, αλλά το Knoppix 1.4, όπως κυκλοφόρησε στις 30 Σεπτεμβρίου 2000, θα μπορούσε να εισαχθεί σε οποιονδήποτε υπολογιστή και να εκκινήσει σε ένα πλήρως λειτουργικό Linux, με

πρόσβαση σε μια τεράστια γκάμα υλικού και δυνατότητα επικοινωνίας και αυτόματης σύνδεσης σε σχεδόν οποιοδήποτε δίκτυο διαθέσιμο εκείνη τη στιγμή.
Το Linux είναι open source και πρέπει να αναπτυχθεί. Αλλά για να διασφαλιστεί η προστασία και η πρόοδος του Linux πρέπει να δημιουργηθεί μια ομάδα για να διατηρήσει το Linux ανεξάρτητο. Έτσι, το 2000 ιδρύθηκε το Ίδρυμα Linux, για να υποστηρίξει το έργο του Linus και της αναπτυσσόμενης κοινότητας, στη δημιουργία και τη βελτίωση του Linux, αλλά και να το υπερασπιστεί και να το διατηρήσει εντός των βασικών αξιών της ελευθερίας, της συνεργασίας και της εκπαίδευσης.

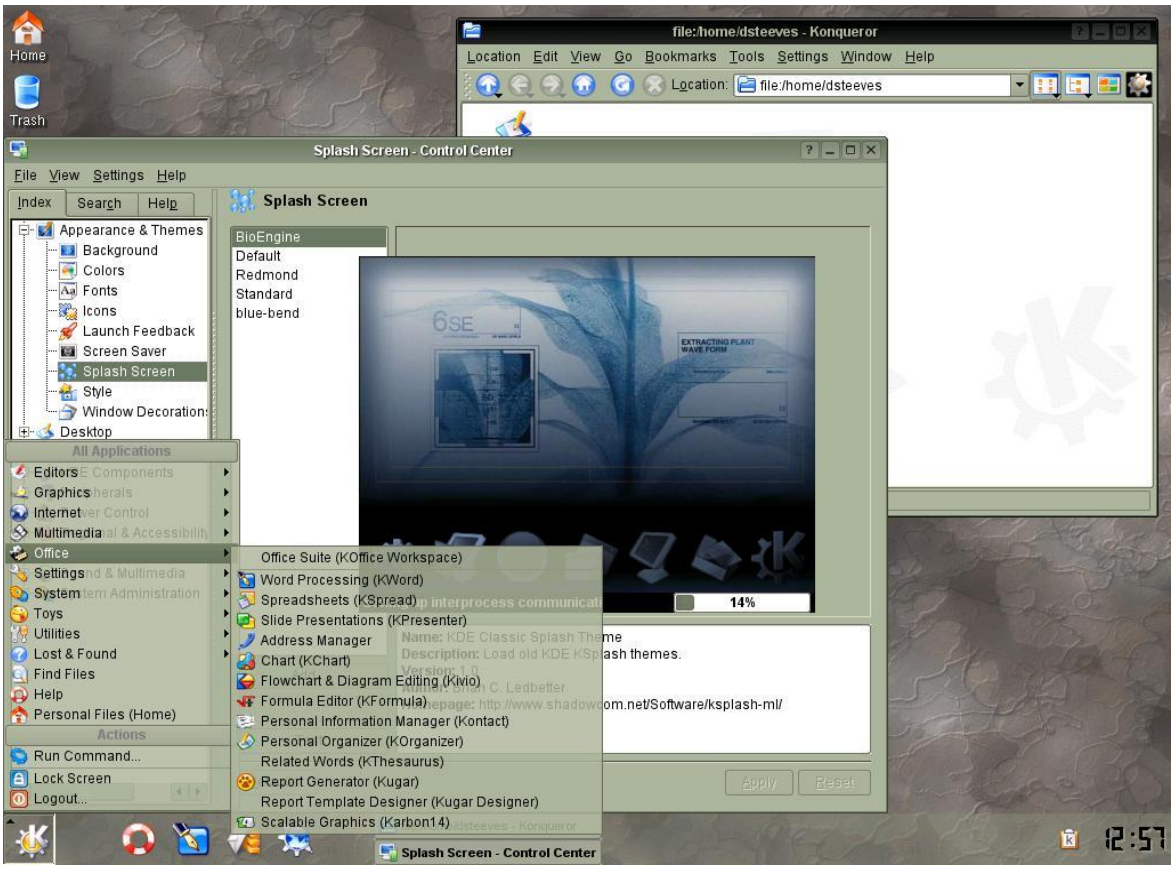
Το 2001 μια σημαντική στιγμή στον πυρήνα του Linux ήρθε με την έκδοση 2.4, που κυκλοφόρησε στις 4 Ιανουαρίου. Η έκδοση 2.4 περιείχε υποστήριξη για USB, κάρτες PC, ISA Plug and Play ,Bluetooth, RAID και EXT3. Στην πραγματικότητα, το 2.4.x ήταν ο μακρύτερος υποστηριζόμενος πυρήνας, που έληξε με το 2.4.37.11 το 2011 και έδειξε πόσο ευέλικτο και ισχυρός ήταν ο πυρήνας Linux από τις πρώτες μέρες του 1.0.

Το 2002 η Red Hat, έχοντας τώρα απολαύσει λίγο χρόνο στο χρηματιστήριο, αποφάσισε ότι παρόλο που κέρδισαν χρήματα μέσω της υποστήριξης του δωρεάν Red Hat Linux OS τους, ήρθε η ώρα να υιοθετήσουν μια πιο επιχειρηματική και εμπορική προσέγγιση. Από αυτό προέκυψε μια αμφίδρομη διάσπαση, γεννήθηκε το Red Hat Enterprise Linux 2.1, με πυρήνα 2.4.9, μεγαλύτερη σταθερότητα και μακροπρόθεσμη υποστήριξη για τον εταιρικό χρήστη και το Fedora Core για τη διανομή της κοινότητας. Με το RHEL να είναι ανοιχτού κώδικα, η Red Hat καθιστά τον πηγαίο κώδικα ελεύθερα διαθέσιμο στους διακομιστές FTP της, τον οποίο πολλές ομάδες κατέβασαν και μεταγλώττισαν στις δικές τους διανομές (κυρίως για την αφαίρεση των αναφορών και των αποθετηρίων του Red Hat). Τα CentOS, Oracle Linux, CERN και Scientific Linux είναι παραδείγματα τέτοιων διανομών με όλα τα θετικά μιας καλά χτισμένης διανομής, αλλά χωρίς πρόσβαση στις εξειδικευμένες γνώσεις και λογισμικό της Red Hat.



Εικόνα 4.2

Τον Δεκέμβριο του 2002 κυκλοφόρησε μια αξιοσημείωτη διανομή, το CRUX. Με ιδιαίτερη έμφαση στο θέμα «κρατήστε το απλό» που είχε γίνει δημοφιλές κατά τη διάρκεια αυτής της περιόδου, το CRUX ήταν εξαιρετικά ελαφρύ και επικεντρώθηκε στον προγραμματιστή σε αντίθεση με τον τελικό χρήστη. Σε μια εποχή που οι διανομές Linux άρχισαν να αυξάνονται εκθετικά και να ανταγωνίζονται για τη θέση της αντικατάστασης των Windows, το CRUX, εικόνα 4.3, είχε μία διαφορετική οπτική, να γίνει μια ευπρόσδεκτη μινιμαλιστική διανομή, κάτι το οποίο δεν απέδωσε. Αυτό που είναι αξιοσημείωτο για το CRUX, ήταν το γεγονός ότι ήταν η έμπνευση και η βάση για το απίστευτα δημοφιλές, Arch Linux.



Εικόνα 4.3

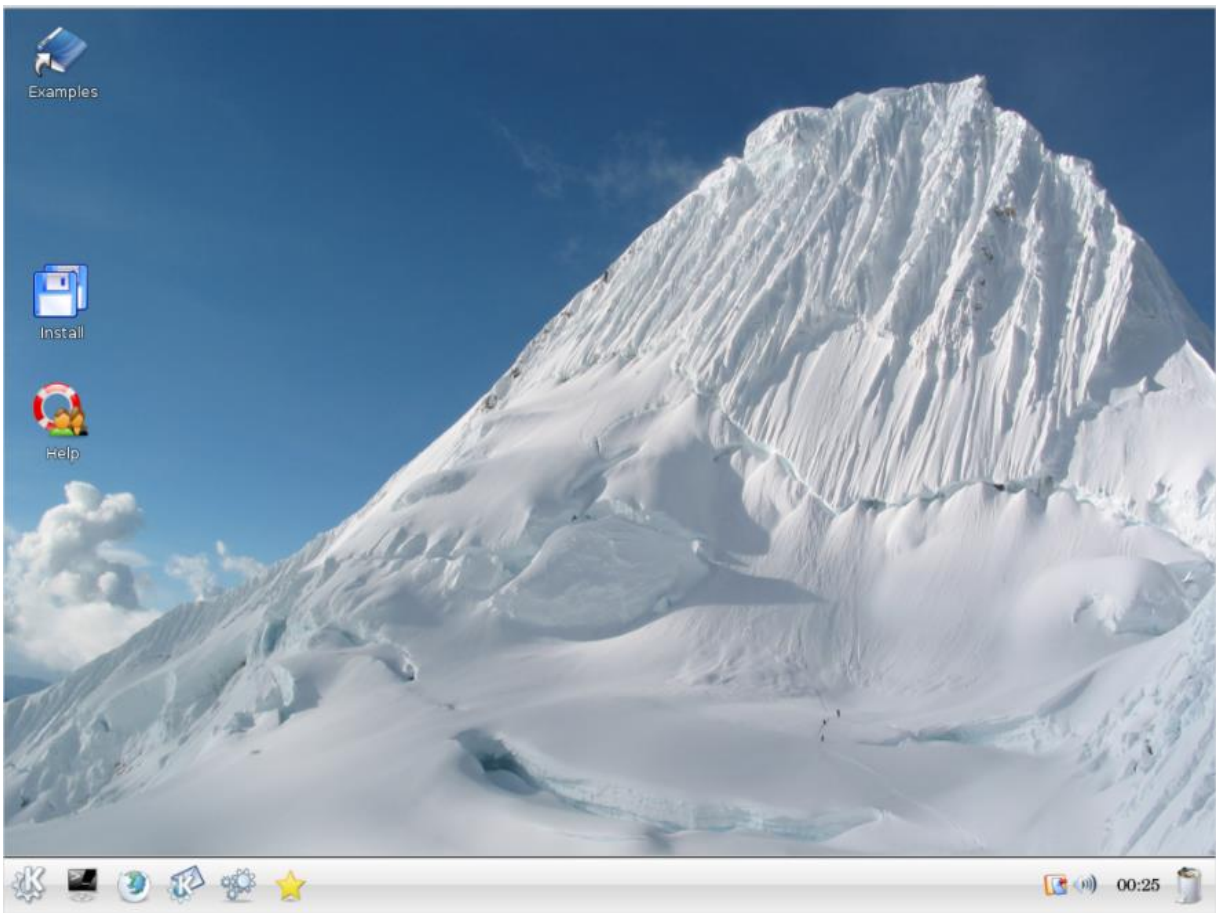
Στις 18 Δεκεμβρίου 2003 ανακοινώθηκε η έκδοση 2.6 του πυρήνα. Με την υποστήριξη που παρέχεται για PAE, νέους επεξεργαστές, βελτιωμένη υποστήριξη 64-bit, μεγέθη συστήματος αρχείων 16 TB, EXT4 και πολλά άλλα.

Το 2004 καθώς οι διανομές Linux εξακολουθούσαν να θεωρούνται απομακρυσμένες από εκείνους που προτιμούσαν τα Windows της Microsoft χρειαζόταν μια νέα φιλοσοφία για να γίνουν τα Linux ποιο προσιτά στον απλό χρήστη. Χρειαζόταν κάτι που θα έκανε το Linux πιο προσωπικό και πιο ανθρώπινο. Με βάση το Debian, ο στόχος του Ubuntu ήταν να δημιουργήσει μια εύχρηστη επιφάνεια εργασίας Linux που θα μπορούσε να ενημερωθεί ώστε να περιλαμβάνει τις τελευταίες εκδόσεις για τον τελικό χρήστη με πολύ μικρή εμπειρία στο Linux. Με την κυκλοφορία του Ubuntu 4.10, του Warty Warthog, στις 20 Οκτωβρίου 2004 πραγματοποιήθηκε αυτό το όνειρο. Υπάρχουν λίγα από αυτά που

μπορούν να ειπωθούν σχετικά με την άνοδο του Ubuntu, η δημοτικότητά του αυξήθηκε σε τέτοιο σημείο όπου μαζί με το υπόλοιπο οικογενειακό δέντρο του Ubuntu, έχουν γίνει μια από τις πιο γνωστές διανομές Linux στον κόσμο.

Εικόνα 4.4

Το 2006 κυκλοφόρησε το Linux Mint 1.0 Ada, εικόνα 4.5, με ένα μείγμα FOSS και ιδιόκτητου λογισμικού, αυτό το "work-out-the-box" Linux distro ακολούθησε για λίγο τη βάση του Ubuntu μέχρι το 2007, όταν και άρχισε να χρησιμοποιεί τη δική του βάση κώδικα . Το Linux Mint έχει προσαρμοστεί για να υποστηρίζει και να προσφέρει τις νεότερες τεχνολογίες, διατηρώντας παράλληλα μία σύνδεση με τις προτιμήσεις των χρηστών του. Εξ ου και η τεράστια υποστήριξη για αυτή τη μεγάλη διανομή.



Εικόνα 4.5

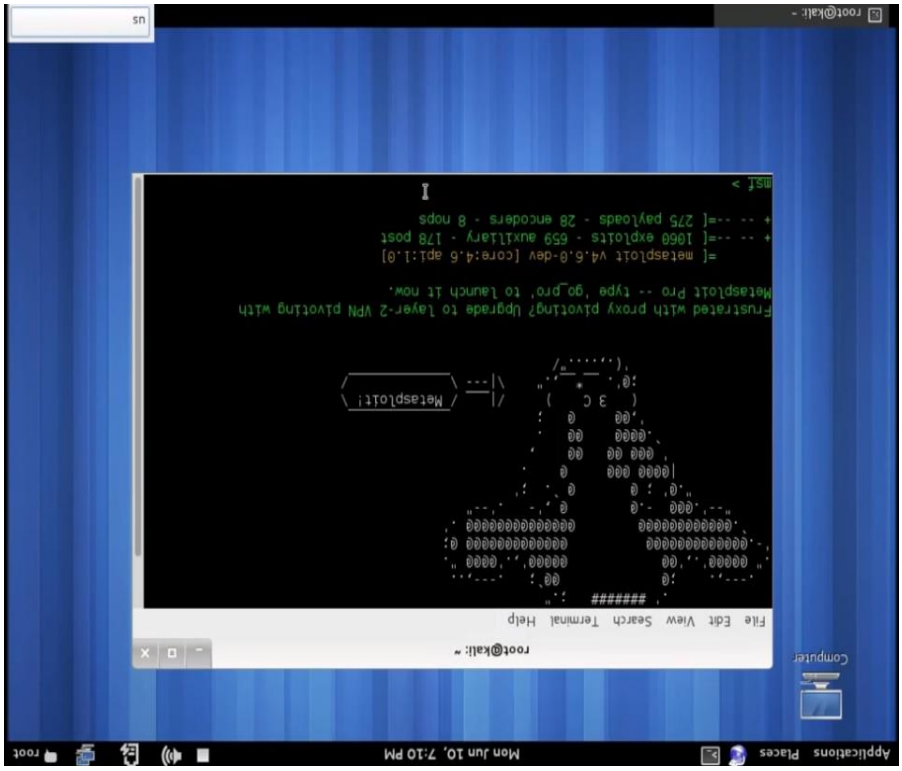
Το 2007 κυκλοφόρησε το KDE4 και δέχθηκε κριτική λόγω της έλλειψης σταθερότητας, με τον ίδιο τον Linus να δηλώνει ότι το KDE 4.0 ήταν μια «διακοπή για τα πάντα» και «ημιψημένη» κυκλοφορία. Ωστόσο, οι χρήστες άρχισαν να απολαμβάνουν την επιφάνεια εργασίας του Plasma, καθώς και την πρωτοποριακή εμφάνιση και αίσθηση, έτσι ώστε τη στιγμή που κυκλοφόρησε το KDE 4.2 το 2009, όλοι είχαν ξεχάσει την τρομερή εμπειρία που είχαν προηγουμένως.

Στις 23η Σεπτεμβρίου 2008 κυκλοφόρησε το πιο δημοφιλές λειτουργικό σύστημα που βασίζεται σε Linux . Αν και οι περισσότεροι χρήστες του δεν έχουν ιδέα ότι βασίζεται στο Linux! Αυτό το λειτουργικό σύστημα είναι το Android το οποίο φαίνεται στην εικόνα 4.6. Η έκδοση 1.0 κυκλοφόρησε με το HTC Dream και θα μπορούσε να επιτύχει ό, τι θα περίμενε κανείς από ένα σύγχρονο smartphone, αλλά ήταν με λάθη. Η έκδοση 1.1 διόρθωσε τα περισσότερα από τα σφάλματα. Η έκδοση 1.5 "Cupcake" του Android άρχισε πραγματικά να παρουσιάζει ενδιαφέρον και άνοιξε το δρόμο για τα smartphone που έχουν κατακλύσει τον κόσμο.

Εικόνα 4.6

Το 2011 το Ubuntu ήταν το ποιο γνωστό λειτουργικό της περιόδου. Ήταν σταθερά στην κορυφή των γραφημάτων χρηστών του Linux, είχε μια τεράστια βάση υποστηρικτών και ήταν εύκολο στη χρήση. Τον Απρίλιο, πραγματοποιήθηκε η δέκατη τέταρτη κυκλοφορία του Ubuntu, με μια ελαφρώς διαφορετική εμφάνιση το Unity. Μπορούμε να πούμε ότι σχεδόν όλοι την εποχή εκείνη το μισούσαν και πολλοί εξακολουθούν να το κάνουν (παρά τις τακτικές ενημερώσεις έως ότου η Canonical το εγκατέλειψε πρόσφατα). Μετά από μερικά χρόνια με τον πυρήνα 2.6.x, κυκλοφόρησε η έκδοση 3.0

Στις 13 Μαρτίου 2013 κυκλοφόρησε μία ακόμη πολύ γνωστή διανομή η οποία χρησιμοποιείτε ευρέως από ανθρώπους που ασχολούνται με την ασφάλεια, το Kali Linux, εικόνα 4.7. Έχει πάνω από 600 προεγκατεστημένα προγράμματα δοκιμής διείσδυσης, όπως το Armitage (ένα γραφικό εργαλείο διαχείρισης επιθέσεων στον κυβερνοχώρο), το Nmap (ένας σαρωτής θύρας), το Wireshark (ένας αναλυτής πακέτων), το John the Ripper (cracker κωδικού πρόσβασης), ng (μια σουίτα λογισμικού για δοκιμαστική διείσδυση ασύρματων LAN), Burp suite και σαρωτές ασφαλείας εφαρμογών ιστού OWASP ZAP. Αναπτύχθηκε από τους Mati Aharoni και Devon Kearns στην Offensive Security μέσω της επανεγγραφής του BackTrack, της προηγούμενης διανομής τους για δοκιμές ασφαλείας Knoppix. Αρχικά, σχεδιάστηκε με έμφαση στον έλεγχο του πυρήνα, από τον οποίο πήρε το όνομά του Kernel Auditing LInux. Το όνομα θεωρείται μερικές φορές λανθασμένο ότι προέρχεται από την Kali θεά των Ινδών. Ο τρίτος βασικός προγραμματιστής, ο Raphaël Hertzog, τους προσχώρησε ως ειδικός του Debian. Το Kali Linux βασίζεται στον κλάδο του Debian Testing. Τα περισσότερα πακέτα που χρησιμοποιεί το Kali εισάγονται από τα αποθετήρια του Debian. Με την έκδοση 2019.4 τον Νοέμβριο του 2019, η προεπιλεγμένη διεπαφή χρήστη άλλαξε από το GNOME σε Xfce, με την έκδοση GNOME να είναι ακόμα διαθέσιμη.



Εικόνα 4.7

4.2. Linux Server OS

Στα προηγούμενα μιλήσαμε για την ιστορική ανάπτυξη των Linux και για κάποιες από τις διανομές που υπήρχαν ή υπάρχουν ακόμη. Τα Linux ως ελεύθερο λογισμικό έχουν πάρα πολλές διαφορετικές διανομές, άλλες δωρεάν και άλλες επί πληρωμή. Ποια είναι όμως η διαφορά ανάμεσα στις διανομές που προορίζονται για χρήση σε έναν προσωπικό υπολογιστή και στις διανομές που προορίζονται για διακομιστές;

Στην πραγματικότητα όσον αφορά τον πυρήνα τους σε αρκετές περιπτώσεις δεν υπάρχουν διαφορές. Οι διαφορές είναι στις εφαρμογές και στις υπηρεσίες που έχουν προ εγκατεστημένες οι δύο εκδόσεις, αν πρόκειται για εκδόσεις που διαμοιράζουν desktop και server διανομές. Υπάρχουν φυσικά και εκδόσεις, κυρίως επί πληρωμή που προορίζονται αποκλειστικά για διακομιστές και workstation όπως είναι οι εκδόσεις της RedHat (να σημειώσουμε εδώ ότι η RedHat χρηματοδοτεί το Fendora το οποίο είναι μια δωρεάν διανομή Linux).

Για να γίνουμε λίγο ποιο κατανοητοί στις διαφορές ανάμεσα στις Desktop και Server διανομές θα μελετήσουμε κάποιες από τις ποιο σημαντικές διαφορές ενός από τα ποιο γνωστά λειτουργικά Linux, το Ubuntu, στις δύο διαφορετικές εκδόσεις του, Desktop και Server.

Οι ποιο σημαντικές διαφορές των δύο εκδόσεων συνοψίζονται σε:

Γραφικό περιβάλλον διεπαφής χρήστη

Η κύρια διαφορά στο Ubuntu Desktop και το Ubuntu Server είναι το περιβάλλον της επιφάνειας εργασίας. Ενώ το Ubuntu Desktop περιλαμβάνει γραφικό περιβάλλον εργασίας χρήστη, το Ubuntu Server δεν το κάνει.

Αυτό συμβαίνει επειδή οι περισσότεροι διακομιστές λειτουργούν headless. Αυτό σημαίνει ότι τρέχουν χωρίς ένα παραδοσιακό πληκτρολόγιο, ποντίκι και οθόνη για να αλληλοεπιδράσουν οι χρήστες με το μηχάνημα. Αντ' αυτού, οι διακομιστές συνήθως διαχειρίζονται απομακρυσμένα χρησιμοποιώντας SSH. Ενώ το SSH είναι ενσωματωμένο σε λειτουργικά συστήματα που βασίζονται σε Unix, είναι πολύ απλό να χρησιμοποιήσουμε SSH και στα Windows.

Παρόλο που ορισμένα λειτουργικά συστήματα διακομιστών Linux διαθέτουν γραφικά περιβάλλοντα επιφάνειας εργασίας (GUI), πολλά δεν διαθέτουν. Για παράδειγμα, το Container Linux από CoreOS βασίζεται εξ ολοκλήρου στη γραμμή εντολών. Το Ubuntu Server δεν διαθέτει GUI, ενώ το Ubuntu Desktop υποθέτει ότι ο υπολογιστής μας χρησιμοποιεί εξόδους βίντεο. Επομένως, το Ubuntu Desktop εγκαθιστά ένα GUI.

Εφαρμογές

Το Ubuntu Desktop περιέχει εφαρμογές κατάλληλες για γενική χρήση, δηλαδή υπάρχει προ εγκατεστημένη μια σουίτα εφαρμογών γραφείου, λογισμικό πολυμέσων και πρόγραμμα περιήγησης ιστού.

Από τη άλλη πλευρά το Ubuntu Server περιλαμβάνει τυπικά πακέτα. Αυτά επικεντρώνονται στις απαιτήσεις διακομιστή. Κατά συνέπεια, το Ubuntu Server μπορεί να λειτουργήσει ως διακομιστής email, διακομιστής αρχείων, διακομιστής ιστού και διακομιστής samba. Συγκεκριμένα πακέτα περιλαμβάνουν Bind9 και Apache2.

Ενώ οι εφαρμογές του Ubuntu Desktop επικεντρώνονται για χρήση στον κεντρικό υπολογιστή, τα πακέτα του Ubuntu Server επικεντρώνονται στο να επιτρέπουν τη σύνδεση με τους πελάτες καθώς και την ασφάλεια.

Εγκατάσταση

Επειδή το Ubuntu Server δεν διαθέτει GUI, η εγκατάσταση διαφέρει από αυτήν του Ubuntu Desktop. Η εγκατάσταση του Ubuntu Desktop είναι ουσιαστικά όπως κάθε άλλη εγκατάσταση λογισμικού, το Ubuntu Server όμως χρησιμοποιεί ένα process-driven μενού. Η χρήση του Ubuntu Server αντί του Ubuntu Desktop δεν είναι μια εντελώς νέα εμπειρία. Τουλάχιστον εάν έχουμε εμπειρία στη γραμμή εντολών και στο SSH, ο Ubuntu Server θα πρέπει να φαίνεται οικείος. Υπάρχουν και άλλες βασικές ομοιότητες από τις οποίες ξεχωρίζουμε τον πυρήνα (Kernel) και την υποστήριξη.

Πυρήνας

Μετά το Ubuntu 12.04, και οι δύο παραλλαγές Server και Desktop χρησιμοποιούν τον ίδιο πυρήνα. Προηγουμένως, το Desktop και ο Server χρησιμοποιούσαν διαφορετικούς πυρήνες Επειδή τόσο το Ubuntu Desktop όσο και το Ubuntu Server χρησιμοποιούν τον ίδιο πυρήνα, μπορούμε να προσθέσουμε τυχόν πακέτα και στις δύο παραλλαγές. Αυτό σημαίνει ότι ενώ η προεπιλεγμένη εγκατάσταση διαφέρει, μπορούμε να την προσαρμόσουμε ανάλογα τη χρήση για την οποία το χρειαζόμαστε.

Έτσι, μπορούμε να εγκαταστήσουμε με τον Ubuntu Server και να εγκαταστήσουμε ένα GUI εάν αποφασίσουμε ότι χρειαζόμαστε. Εναλλακτικά, μπορείτε να εγκαταστήσουμε το Ubuntu Desktop και να προσθέσουμε τα απαραίτητα πακέτα για να δημιουργήσουμε έναν διακομιστή. Δεδομένου ότι το Ubuntu Server και Desktop μοιράζονται τον ίδιο πυρήνα, οι προεπιλεγμένες διαφορές εγκατάστασης δεν αποκλείουν μελλοντικές εγκαταστάσεις πακέτων λογισμικού.

Υποστήριξη

Ομοίως, η υποστήριξη άλλαξε με την κυκλοφορία του 12.04. Πριν από το Ubuntu 12.04 LTS, οι εκδόσεις Desktop παρουσίασαν έναν τριετή κύκλο υποστήριξης. Οι αντίστοιχοι Server έναν πενταετή κύκλο υποστήριξης. Αλλά με το ντεμπούτο των 12.04 LTS, οι παραλλαγές του Ubuntu Desktop και Server μετακινήθηκαν και οι δύο σε έναν κύκλο υποστήριξης πέντε ετών.

Λαμβάνοντας υπόψη τις διαφορές και τις ομοιότητες, έρχεται τώρα το μεγάλο ερώτημα: Πρέπει να χρησιμοποιήσουμε το Ubuntu Server ή το Ubuntu Desktop;

Εφόσον χρησιμοποιούμε μια έκδοση LTS του Ubuntu, η έκδοση Server ή Desktop μπορούν να λειτουργούν σε περιβάλλον διακομιστή. Οι κύριοι παράγοντες που διαχωρίζουν τα δύο παραμένουν το GUI και τα προεπιλεγμένα πακέτα. Ωστόσο, επειδή ο πυρήνας του Ubuntu είναι ίδιος σημαίνει ότι μπορούμε να εγκαταστήσουμε τα ίδια πακέτα και στις δύο εκδόσεις. Συνεπώς η απάντηση στο ερώτημα μας εξαρτάτε από τις γνώσεις μας αλλά και κυρίως από τις ανάγκες μας.

4.3. Ιστορική εξέλιξη των Windows Server

Τα λειτουργικά συστήματα για Εξυπηρετητές προορίζονται για χρήση στα πλαίσια οργανισμών και επιχειρήσεων, έτσι ώστε να τους βοηθήσουν στην ανάπτυξη μιας ισχυρής και παράλληλα ευέλικτης υποδομής για την πραγματοποίηση των επιχειρησιακών τους λειτουργιών. Η Microsoft ασχολήθηκε με την ανάπτυξη λειτουργικών συστημάτων για Εξυπηρετητές από το 1988 με τη σειρά Windows NT. Το πρώτο λειτουργικό σύστημα της σειράς NT έγινε διαθέσιμο το 1993 και από τότε έως σήμερα η εταιρία έχει αναπτύξει άλλα 9 λειτουργικά συστήματα τα οποία εντάσσονται στην κατηγορία των Εξυπηρετητών. Παρακάτω παρουσιάζεται η εξέλιξη των λειτουργικών αυτών συστημάτων.

4.3.1. Microsoft Windows NT Advanced Server 3.1

Η ανάπτυξη των Windows NT ξεκίνησε τον Νοέμβριο του 1988, αφού η Microsoft προσέλαβε μια ομάδα προγραμματιστών από την Digital Equipment Corporation με επικεφαλής τον Dave Cutler. Πολλά στοιχεία του σχεδιασμού αντικατοπτρίζουν την προηγούμενη εμπειρία DEC με VMS και RSX-11. Το λειτουργικό σύστημα σχεδιάστηκε για να λειτουργεί σε πολλές αρχιτεκτονικές συνόλων εντολών και σε πολλές πλατφόρμες υλικού σε κάθε αρχιτεκτονική. Οι εξαρτήσεις της πλατφόρμας κρύβονται σε μεγάλο βαθμό από το υπόλοιπο σύστημα από μια μονάδα λειτουργίας πυρήνα που ονομάζεται HAL.

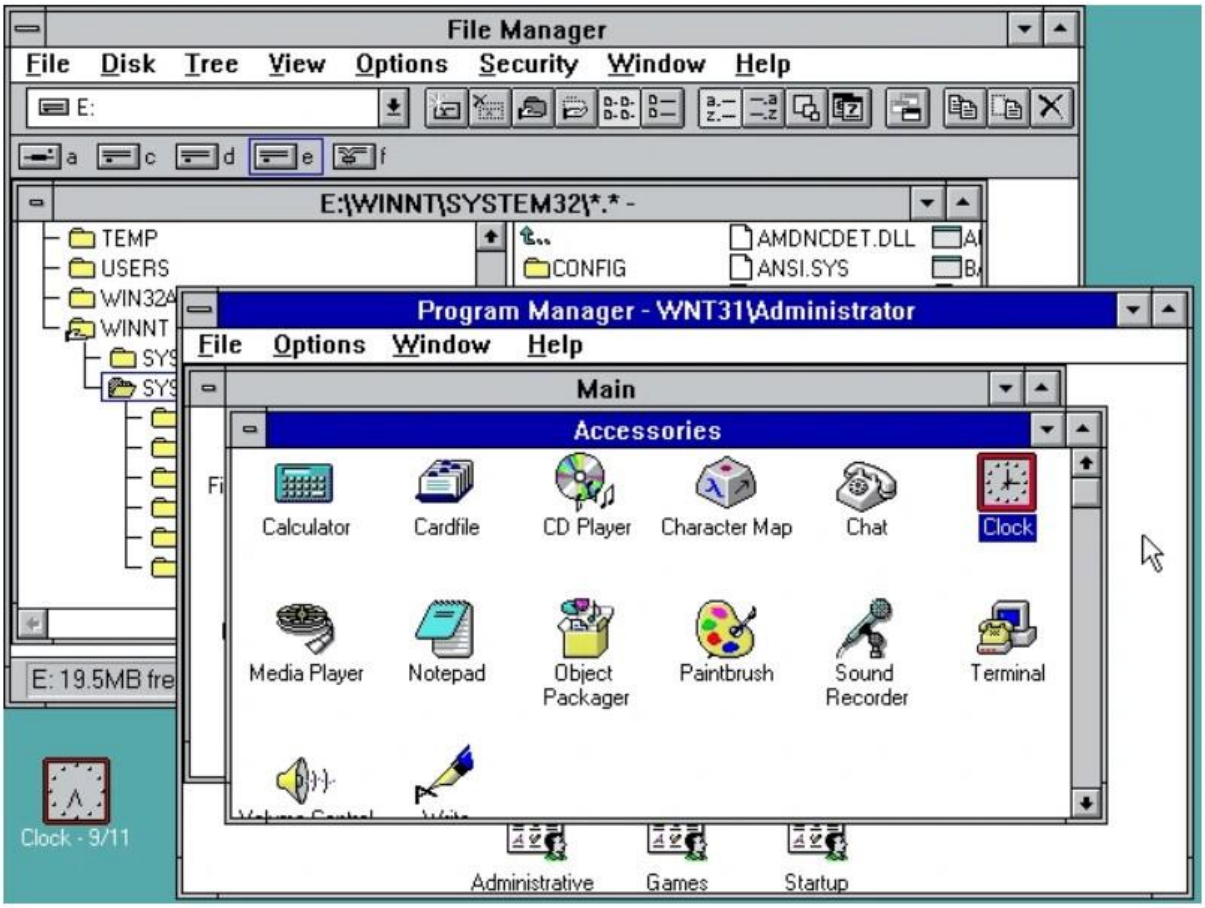
Εικόνα 4.8

Τα Windows NT προορίζονταν αρχικά να είναι OS / 2 3.0, η τρίτη έκδοση του λειτουργικού συστήματος που αναπτύχθηκε από κοινού από τη Microsoft και την IBM. Όταν τα Windows 3.0 κυκλοφόρησαν τον Μάιο του 1990, ήταν τόσο επιτυχημένα που η Microsoft αποφάσισε να αλλάξει την κύρια διεπαφή προγραμματισμού εφαρμογών για το NT OS / 2 που δεν κυκλοφόρησε ακόμα από ένα εκτεταμένο OS / 2 API σε εκτεταμένα Windows API. Αυτή η απόφαση προκάλεσε ένταση μεταξύ της Microsoft και της IBM και η συνεργασία τελικά κατέρρευσε. Η IBM συνέχισε μόνο την ανάπτυξη OS / 2, ενώ η Microsoft συνέχισε να εργάζεται για τα πρόσφατα μετονομαζόμενα Windows NT.

Η πρώτη δημόσια επίδειξη των Windows NT, την εποχή που ονομάζεται "Windows Advanced Server for LAN Manager", πραγματοποιήθηκε σε μια διάσκεψη

προγραμματιστών τον Αύγουστο του 1991 και το προϊόν ανακοινώθηκε επίσημα στο Spring 1993 COMDEX στην Ατλάντα της Γεωργίας.
Οι διεπαφές προγραμματισμού εφαρμογών στα Windows NT υλοποιούνται ως υποσυστήματα πάνω από το εγγενές API χωρίς έγγραφα. Αυτό επέτρεψε την καθυστερημένη υιοθέτηση του API των Windows. Τα Windows NT ήταν το πρώτο λειτουργικό σύστημα της Microsoft που χρησιμοποίησε το UCS-2 εσωτερικά. Τα Windows NT παρουσίασαν το Win32 API, μια εφαρμογή 32-bit του 16-bit Windows API. Οι περισσότερες εφαρμογές Windows 16-bit θα μπορούσαν να μεταφερθούν στο νέο σύστημα με ελάχιστες αλλαγές και επαναπροσδιορισμούς. Το Win32 παρείχε επίσης εγγενή υποστήριξη API για πολλές νέες δυνατότητες, όπως η δικτύωση και το multithreading.

Το όλο έργο είχε ένα κωδικό όνομα, "NTOS", το οποίο διατηρείται στο όνομα αρχείου του πυρήνα των Windows NT, ntoskrnl.exe. Δεδομένου ότι στόχευε να γίνει η επόμενη έκδοση του OS / 2, ένα πιο επίσημο όνομα του έργου ήταν "NT OS / 2". Αυτό το όνομα διατηρείται έως τώρα σε ορισμένα αρχεία του κιτ ανάπτυξης προγραμμάτων οδήγησης των Windows NT.
Στιγμιότυπο οθόνης της επιφάνειας εργασίας Microsoft Windows NT Advanced Server 3.1 φαίνεται στην εικόνα 4.9.



Εικόνα 4.9

Η διάθεση του Windows NT πραγματοποιήθηκε σε μια σειρά εκδόσεων για την καλύτερη ικανοποίηση των αναγκών των οργανισμών. Οι εκδόσεις αυτές ήταν:

- Windows NT 3.1 Workstation
- Windows NT 3.1 Advanced Server
- Windows NT 3.1J (Support for Japanese language)
- Windows NT for Workgroups 3.1

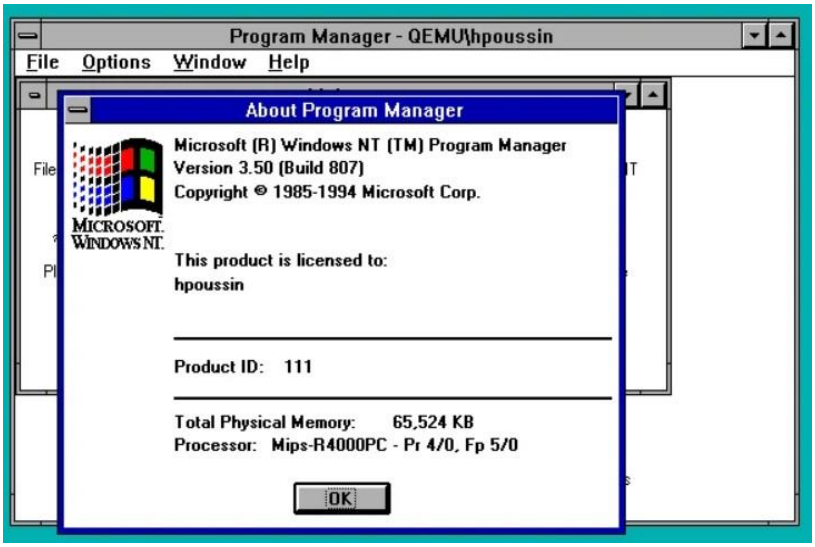
4.3.2. Microsoft Windows NT Server 3.5

Τα Windows NT 3.5 (με κωδικό όνομα "Daytona") είναι η δεύτερη έκδοση του λειτουργικού συστήματος Microsoft Windows NT. Κυκλοφόρησαν στις 21 Σεπτεμβρίου 1994.
Ένας από τους πρωταρχικούς στόχους κατά την ανάπτυξη των Windows NT 3.5 ήταν η αύξηση της ταχύτητας του λειτουργικού συστήματος. Ως αποτέλεσμα, στο έργο δόθηκε το κωδικό όνομα "Daytona" σε σχέση με το Daytona International Speedway στο Daytona Beach της Φλόριντα.
Το λογότυπο των Microsoft Windows NT Server 3.5 φαίνεται στην εικόνα 4.9.

Εικόνα 4.10

Αυτή είναι η πρώτη έκδοση των Windows NT που υιοθετεί τα ονόματα Windows NT Workstation και Windows NT Server για τις εκδόσεις του. Οι εκδόσεις της προηγούμενης έκδοσης των Windows NT, Windows NT 3.1, ονομάστηκαν Windows NT και Windows NT Advanced Server. Η έκδοση Workstation επέτρεψε μόνο 10 ταυτόχρονους πελάτες να έχουν πρόσβαση στο διακομιστή αρχείων και χωρίς πελάτες Mac. Η έκδοση διακομιστή περιελάμβανε όλες τις λειτουργίες και τις επιλογές δικτύου σε αυτό το σύστημα.
Τα Windows NT 3.5

περιελάμβαναν ενσωματωμένη υποστήριξη Winsock και TCP / IP. Η αρχική εμπορικά διαθέσιμη έκδοση των Windows NT, έκδοση 3.1, περιελάμβανε μόνο μια ιδιόκτητη και αρκετά ελλιπή εφαρμογή του TCP / IP που βασίζεται στο AT&T UNIX System V "Streams" API. Γράφονται ξανά οι στοίβες TCP / IP και IPX / SPX στα Windows NT 3.5. Η υποστήριξη NetBIOS μέσω TCP / IP (NetBT) ως επίπεδο συμβατότητας για TCP / IP εισήχθη όπως επίσης και οι πελάτες Microsoft DHCP και WINS και διακομιστές DHCP και WINS. Στιγμιότυπο οθόνης επιφάνειας εργασίας Microsoft Windows NT 3.5 φαίνεται στην εικόνα 4.11.



Εικόνα 4.11

Τα Windows NT 3.5 μπορούν να μοιράζονται αρχεία μέσω FTP και εκτυπωτών μέσω LPR και να ενεργούν ως διακομιστές Gopher, Web και WAIS. Το Windows NT 3.5 Resource Kit περιλάμβανε την πρώτη εφαρμογή του Microsoft DNS. Τα Windows NT 3.5 περιλάμβαναν Υπηρεσία Απομακρυσμένης Πρόσβασης για απομακρυσμένη πρόσβαση μόντεμ μέσω τηλεφώνου σε υπηρεσίες LAN χρησιμοποιώντας είτε πρωτόκολλα SLIP είτε PPP.

Άλλες νέες δυνατότητες στα Windows NT 3.5 περιλαμβάνουν το VFAT (δυνατότητα χρήσης μεγάλων ονομάτων αρχείων έως 255 χαρακτήρων) και υποστήριξη για θύρες ολοκλήρωσης εισόδου / εξόδου. Περιέχει μια νέα οθόνη εκκίνησης. Επίσης, αναβάθμισε την υποστήριξη Object Linking and Embedding (OLE) από την έκδοση 1.0 στην έκδοση 2.0 και είναι πιο αποτελεσματική - η απόδοση είναι υψηλότερη και απαιτεί λιγότερη μνήμη από τα Windows NT 3.1. Τα Windows NT 3.5 δεν υποστηρίζουν φορητούς υπολογιστές, καθώς δεν είχαν προγράμματα οδήγησης για κάρτες προσαρμογέα PCMCIA.

Τον Ιούλιο του 1995, τα Windows NT 3.5 με Service Pack 3 αξιολογήθηκαν από την Εθνική Υπηρεσία Ασφάλειας ως συμμόρφωση με τα κριτήρια TCSEC C2.

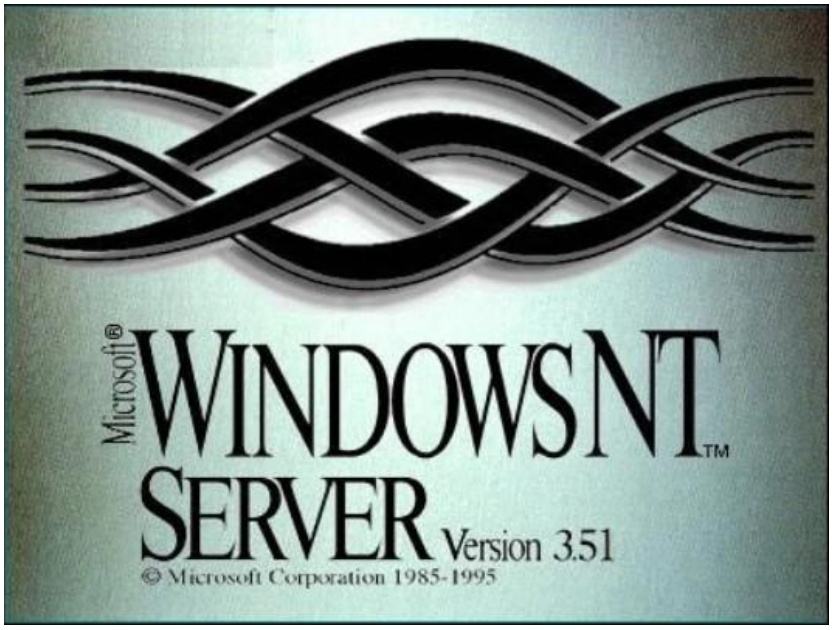
Στα Windows NT 3.5 δεν είναι δυνατή η εγκατάσταση σε επεξεργαστή νεότερο από τον αρχικό Pentium (πυρήνας P5). Ωστόσο στα Windows NT 3.51 το διόρθωσαν.

Η διάθεση του Windows NT 3.5 πραγματοποιήθηκε στις παρακάτω εκδόσεις για την καλύτερη ικανοποίηση των αναγκών των οργανισμών. Οι εκδόσεις αυτές ήταν:

- Windows NT 3.5 Workstation
- Windows NT 3.1 Server

4.3.3. Microsoft Windows NT Server 3.51

Η κυκλοφορία των Windows NT 3.51 ονομάστηκε "η έκδοση PowerPC" στη Microsoft. Η αρχική πρόθεση ήταν να κυκλοφορήσει μια έκδοση PowerPC του NT 3.5, αλλά σύμφωνα με τον David Thompson της Microsoft, ο οποίος δήλωσε "βασικά καθόμασταν περίπου 9 μήνες διορθώνοντας σφάλματα ενώ περιμέναμε την IBM να ολοκληρώσει το υλικό Power PC". Οι εκδόσεις του NT 3.51 κυκλοφόρησαν επίσης για τις αρχιτεκτονικές x86, MIPS και Alpha.

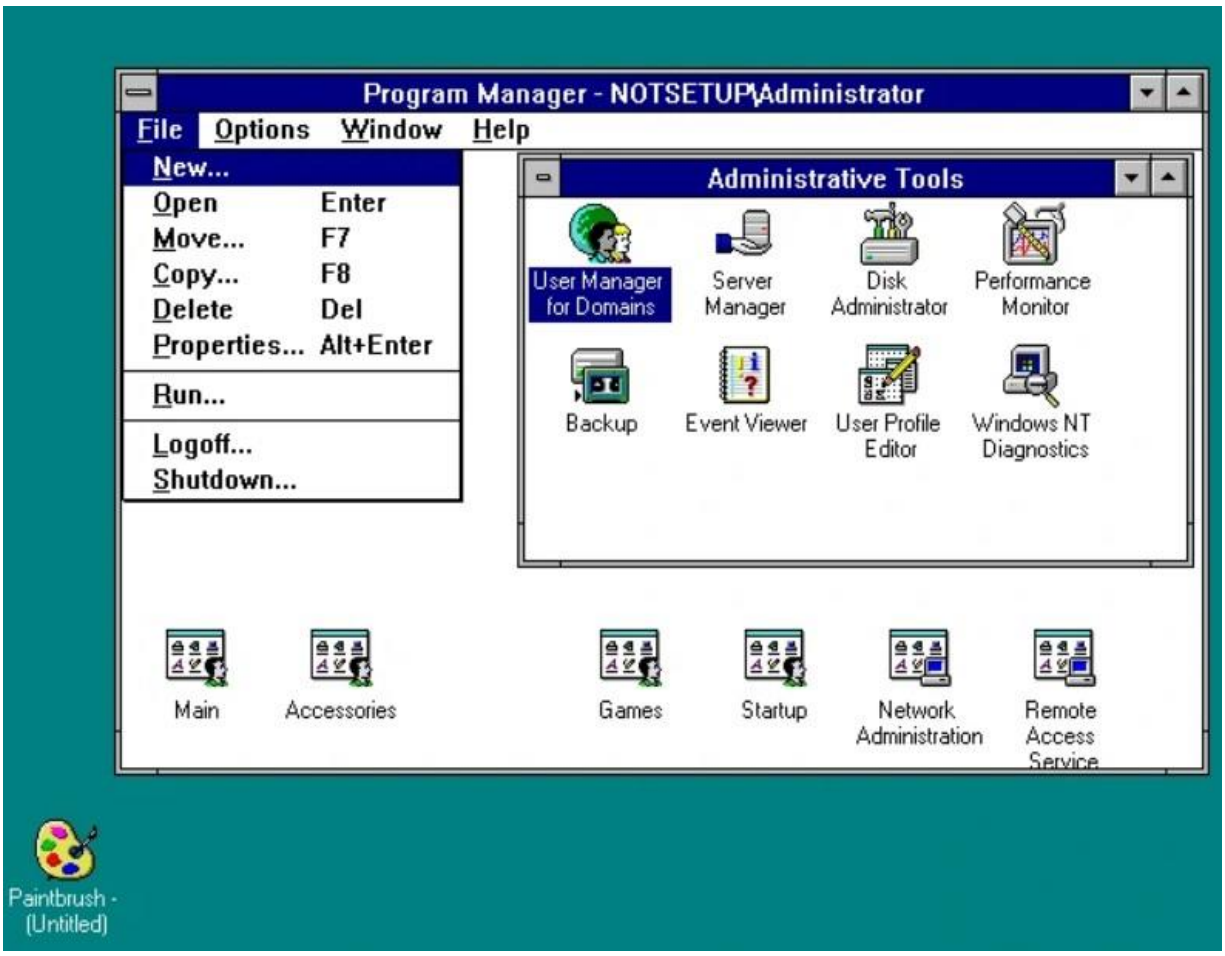


Εικόνα 4.12

Οι νέες δυνατότητες που εισήχθησαν στα Windows NT 3.51 περιλαμβάνουν υποστήριξη PCMCIA, συμπίεση αρχείων NTFS, αντικαταστάσιμη WinLogon (GINA), υποστήριξη 3D σε OpenGL, επίμονες διαδρομές IP κατά τη χρήση TCP / IP, αυτόματη εμφάνιση περιγραφικών κειμένων όταν ο δείκτης του ποντικιού τοποθετήθηκε στα κουμπιά της γραμμής εργαλείων ("συμβουλές εργαλείων") και υποστήριξη για τα κοινά στοιχεία ελέγχου των Windows 95.

Παρά τη σημαντική διαφορά στη βάση του πυρήνα, τα Windows NT 3.51 είναι εύκολα σε θέση να εκτελούν μεγάλο αριθμό εφαρμογών Win32 που έχουν σχεδιαστεί για τα Windows 95. Οι πιο πρόσφατες εφαρμογές 32-bit δεν θα λειτουργήσουν, καθώς οι προγραμματιστές δεν επέτρεψαν στην εφαρμογές τους να λειτουργούν με οποιαδήποτε έκδοση των Windows νωρίτερα από τα Windows 98. Επίσης, ορισμένες εφαρμογές δεν λειτουργούν σωστά με την παλαιότερη διεπαφή Windows NT 3.51. Παρ 'όλα αυτά, στις νέες εφαρμογές της η Microsoft κυκλοφόρησε το πρόβλημα, απελευθερώνοντας 32-bit εκδόσεις του Microsoft Office μέχρι το Office 97 SR2b, το οποίο βασίζεται σε εκδόσεις 16-bit της τεχνολογίας του Internet Explorer. Αυτό συμβαίνει πιθανώς επειδή οι εκδόσεις 32-bit του Internet Explorer 4.0 και αργότερα ενσωματώθηκαν στην επιφάνεια εργασίας των Windows 95 και ο NT 3.51 εξακολουθούσε να χρησιμοποιεί την επιφάνεια εργασίας των Windows 3.1. Αργότερα, προσφέρθηκαν έως και IE 5.0, αλλά όχι αργότερα εκδόσεις 5.x.

Στις 26 Μαΐου 1995, η Microsoft κυκλοφόρησε μια δοκιμαστική έκδοση ανανέωσης κελύφους, που ονομάστηκε Shell Technology Preview, και συχνά αναφέρεται ανεπίσημα ως "NewShell". Αυτή ήταν η πρώτη ενσάρκωση του σύγχρονου GUI των Windows με τη γραμμή εργασιών και το μενού Έναρξη. Σχεδιάστηκε για να αντικαταστήσει το κέλυφος που βασίζεται στη Διαχείριση προγραμμάτων / διαχειριστή αρχείων των Windows 3.x με το γραφικό περιβάλλον εργασίας χρήστη που βασίζεται στην Εξερεύνηση των Windows.



Εικόνα 4.13

Η κυκλοφορία παρείχε δυνατότητες πολύ παρόμοιες με εκείνες του κελύφους των Windows "Chicago" (κωδικός ονομασία για τα Windows 95) κατά τη διάρκεια των τελικών φάσεων beta. Ωστόσο, προοριζόταν να είναι τίποτα περισσότερο από μια δοκιμαστική κυκλοφορία. Υπήρξε μια δεύτερη δημόσια κυκλοφορία της Shell Technology Preview, που ονομάζεται Shell Technology Preview Update, η οποία διατέθηκε στους χρήστες MSDN και CompuServe στις 8 Αυγούστου 1995. Και οι δύο εκδόσεις πραγματοποιήθηκαν στις εκδόσεις του Windows Explorer 3.51.1053.1. Το πρόγραμμα Shell Technology Preview δεν είδε ποτέ τελική κυκλοφορία στο NT 3.51. Όλο το πρόγραμμα μεταφέρθηκε στην ομάδα ανάπτυξης του Καΐρου που τελικά ενσωμάτωσε τον νέο σχεδιασμό κελύφους στον κώδικα NT με την κυκλοφορία του NT 4.0 τον Ιούλιο του 1996.
Πέντε Service Pack κυκλοφόρησαν για το NT 3.51, το οποίο εισήγαγε τόσο διορθώσεις σφαλμάτων όσο και νέες δυνατότητες. Το Service Pack 5, για παράδειγμα, επιλύει ζητήματα που σχετίζονται με το πρόβλημα του έτους 2000.
Το NT 3.51 ήταν το τελευταίο της σειράς που εκτελέστηκε σε επεξεργαστή Intel 80386. Η ικανότητά του να χρησιμοποιεί διαμερίσματα HPFS (τα οποία δεν μπορούσαν τα Windows 2000 και νεότερα) και η ικανότητά του να εκτελεί τουλάχιστον μερικά από τα κοινά API ελέγχου, σημαίνει ότι εξακολουθεί να βρίσκει χώρο για περιστασιακή χρήση σε

παλαιότερα μηχανήματα. Τα Windows NT 3.51, όπως και άλλες εκδόσεις των Windows NT.3x, έχουν κάποια συμβατότητα με τις εφαρμογές OS / 2 1.x. Ωστόσο, οι εφαρμογές έπρεπε να είναι σε λειτουργία κειμένου.
Τα Windows NT 3.51 υποστηρίζουν σκληρούς δίσκους IDE, EIDE, SCSI και ESDI. Τα μόνα σχήματα διευθύνσεων EIDE που υποστηρίζονται είναι η λογική αντιμετώπιση μπλοκ, το ONTrack Disk Manager, το EZDrive και ο τομέας Extended cylinder-head.

4.3.4. Microsoft Windows NT Server 4.0

Ο διάδοχος των Windows 3.51, Windows NT 4.0 εισήγαγε τη σύγχρονη διεπαφή χρήστη των Windows 95 στη σειρά προϊόντων των Windows NT, συμπεριλαμβανομένων των Windows Shell, Windows Explorer (γνωστή ως Windows NT Explorer) και τη χρήση της ονοματολογίας "My". Περιλαμβάνει επίσης τις περισσότερες εφαρμογές που έχουν εισαχθεί με τα Windows 95. Εσωτερικά, τα Windows NT 4.0 ήταν γνωστά ως Shell Update Release (SUR). Διάφορα εργαλεία διαχείρισης, ιδίως Διαχείριση χρηστών για Τομείς, Διαχειριστής διακομιστή και Διαχείριση υπηρεσιών ονόματος τομέα έχουν βελτιώσει γραφικές διεπαφές χρήστη. Το μενού Έναρξη στα Windows NT 4.0 διαχωρίζει τις συντομεύσεις και τους φακέλους ανά χρήστη από τις συντομεύσεις και τους φακέλους όλων των χρηστών με μια διαχωριστική γραμμή. Τα Windows NT 4.0 περιλαμβάνουν ορισμένες βελτιώσεις από το Microsoft Plus για Windows 95 τέτοια όπως το παιχνίδι 3D Pinball, εξομάλυνση γραμματοσειράς, μεταφορά πλήρους παραθύρου, εικονίδια υψηλών χρωμάτων και τέντωμα της ταπετσαρίας για να ταιριάζει στην οθόνη. Το Windows Desktop Update θα μπορούσε επίσης να εγκατασταθεί στα Windows NT 4.0 προκειμένου να ενημερωθεί η έκδοση κελύφους και να εγκατασταθεί το Task Scheduler. Το Windows NT 4.0 Resource Kit περιλάμβανε το βοηθητικό πρόγραμμα Jungle, Musical, Utopia και Robotic Desktop.
Τα Windows NT 4.0 είναι η τελευταία μεγάλη έκδοση των Microsoft Windows που υποστηρίζει τις αρχιτεκτονικές CPU Alpha, MIPS ή PowerPC. Παρέμεινε σε χρήση από τις επιχειρήσεις για αρκετά χρόνια, παρά τις πολλές προσπάθειες της Microsoft να κάνει τους πελάτες να κάνουν αναβάθμιση σε Windows 2000 και νεότερες εκδόσεις. Ήταν επίσης η τελευταία κυκλοφορία στη γραμμή Windows NT που ονομάστηκε Windows NT.

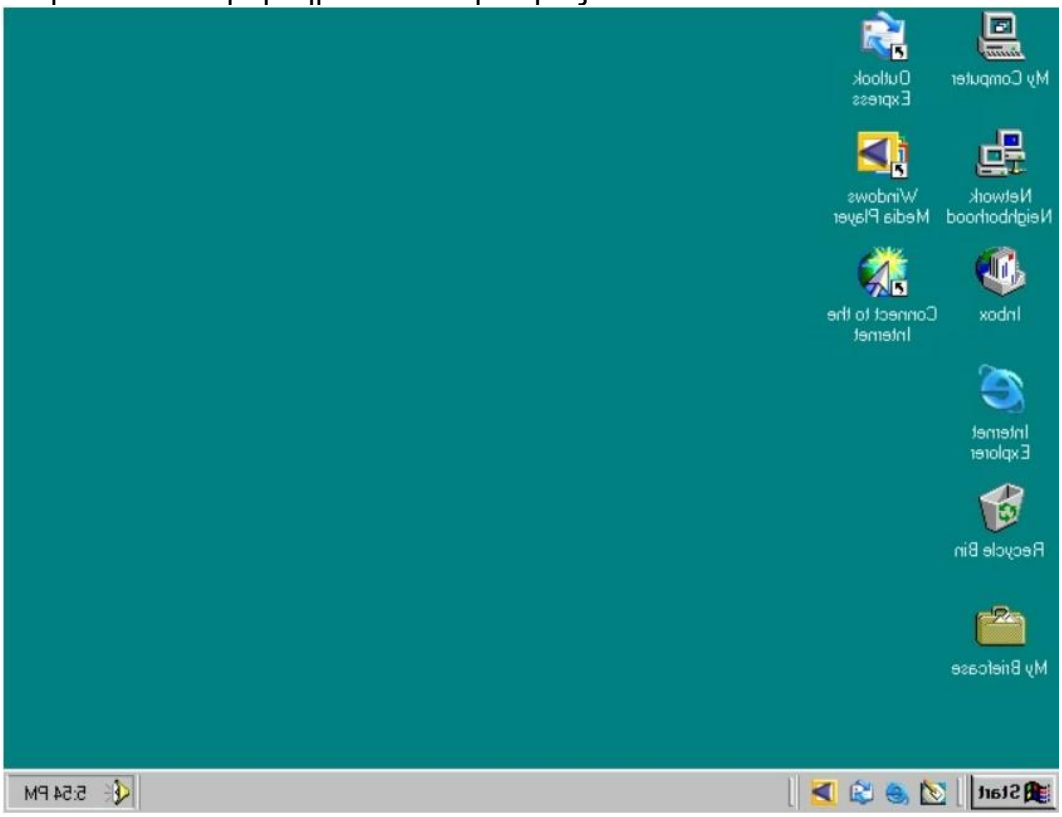
Εικόνα 4.14

Αν και η κύρια βελτίωση ήταν η προσθήκη του κελύφους των Windows 95, υπάρχουν αρκετές σημαντικές επιδόσεις, επεκτασιμότητα και βελτιώσεις χαρακτηριστικών στην αρχιτεκτονική πυρήνα, στον πυρήνα, USER32, COM και MSRPC. Τα Windows NT 4.0 παρουσίασαν επίσης την έννοια των πολιτικών συστήματος και του επεξεργαστή πολιτικής συστήματος.

Άλλες σημαντικές δυνατότητες που περιλαμβάνονται σε αυτήν την κυκλοφορία ήταν το Crypto API, το Telephony API 2.0 με περιορισμένη υποστήριξη Unimodem, η οποία ήταν η πρώτη έκδοση του TAPI σε Windows NT, DCOM και νέες δυνατότητες OLE και Microsoft Transaction Server για εφαρμογές δικτύου, Microsoft Message Queuing (MSMQ), η οποία βελτίωσε την επικοινωνία μεταξύ διεργασιών, το Winsock 2 και τις βελτιώσεις στοίβας TCP / IP και την υποστήριξη ανασυγκρότησης του συστήματος αρχείων.

Οι εκδόσεις διακομιστή των Windows NT 4.0 περιλαμβάνουν Internet Information Services 2.0, Microsoft FrontPage 1.1, NetShow Services, Remote Access Service (που περιλαμβάνει διακομιστή PPTP για λειτουργίες VPN) και υπηρεσία πολλαπλών πρωτοκόλλων Routing. Υπάρχουν νέοι οδηγοί διαχείρισης και μια ελαφριά έκδοση του βοηθητικού προγράμματος Network Monitor που αποστέλλεται με το System Management Server. Η έκδοση Enterprise παρουσίασε τον Microsoft Cluster Server.

Μια σημαντική διαφορά από τις προηγούμενες εκδόσεις των Windows NT είναι ότι η διεπαφή συσκευής γραφικών (GDI) μετακινείται σε λειτουργία πυρήνα και όχι σε λειτουργία χρήστη στη διαδικασία CSRSS. Αυτό εξάλειψε μια διαδικασία για να επεξεργαστεί η μεταγωγή περιβάλλοντος στις κλήσεις λειτουργιών GDI, με αποτέλεσμα μια σημαντική βελτίωση της απόδοσης σε σχέση με τα Windows NT 3.51, ιδιαίτερα στη γραφική διεπαφή χρήστη. Ωστόσο, αυτό επιβάλλει επίσης ότι τα προγράμματα οδήγησης γραφικών και εκτυπωτών έπρεπε να εκτελούνται και σε λειτουργία πυρήνα, με αποτέλεσμα πιθανά προβλήματα σταθερότητας.



Εικόνα 4.15

Τα Windows NT 4.0 ήταν η πρώτη έκδοση των Microsoft Windows που συμπεριέλαβε το DirectX ως στάνταρ - η έκδοση 2 εστάλη με την αρχική έκδοση των Windows NT 4.0

και η έκδοση 3 συμπεριλήφθηκε με την κυκλοφορία του Service Pack 3 στα μέσα του 1997. Σε αντίθεση με τα Windows 95 (τα οποία δεν περιελάμβαναν το DirectX μέχρι την κυκλοφορία του OSR2 τον Αύγουστο του 1996), τα Windows NT 4.0 δεν υποστηρίζουν Direct3D και USB. Οι νεότερες εκδόσεις του DirectX δεν κυκλοφόρησαν για τα Windows NT 4.0, αν και ήταν διαθέσιμο ένα ανεπίσημο πακέτο DirectX 5. Ωστόσο, τα γραφικά με επιτάχυνση υλικού OpenGL υποστηρίζονται σταθερά από την πρώτη στιγμή και χρησιμοποιήθηκαν επιτυχώς από πολλά βιντεοπαιχνίδια και εφαρμογές 3D (π.χ. Quake I, II και III, Unreal, 3D Studio MAX, SoftImage, Maya ...).

Στις πρώτες εκδόσεις του 4.0, παρουσιάστηκαν πολλά προβλήματα σταθερότητας, καθώς τα γραφικά και οι πωλητές εκτυπωτών έπρεπε να αλλάξουν τα προγράμματα οδήγησης τους ώστε να είναι συμβατά με τις διεπαφές λειτουργίας πυρήνα που εξήχθησαν σε αυτές από το GDI.

Τα Windows NT 4.0 περιελάμβαναν επίσης μια νέα εφαρμογή Windows Task Manager. Οι προηγούμενες εκδόσεις των Windows NT περιελάμβαναν την εφαρμογή Λίστα εργασιών, αλλά εμφάνιζε μόνο εφαρμογές που βρίσκονται αυτήν τη στιγμή στην επιφάνεια εργασίας. Για να παρακολουθούνται πόση CPU και πόσοι πόροι μνήμης χρησιμοποιούνται, οι χρήστες αναγκάστηκαν να χρησιμοποιήσουν Performance Monitor. Τα Windows NT 4.0 αναβάθμισαν την προσομοίωση x86 του NTVDM στις εκδόσεις RISC από 286 σε 486.

Ο διακομιστής Windows NT 4.0 συμπεριλήφθηκε στις εκδόσεις 4.0 και 4.5 της σουίτας BackOffice Small Business Server.

Η διάθεση των Windows Server NT 4.0 πραγματοποιήθηκε στις παρακάτω εκδόσεις για την καλύτερη ικανοποίηση των αναγκών των οργανισμών. Οι εκδόσεις αυτές ήταν:

- Windows Server NT 4.0, που κυκλοφόρησε το 1996, σχεδιάστηκε για συστήματα διακομιστών μικρής κλίμακας.

- Windows NT 4.0, Enterprise Edition, κυκλοφόρησε το 1997, είναι ο πρόδρομος της γραμμής Enterprise της οικογένειας διακομιστών των Windows (Advanced Server στα Windows 2000). Ο Enterprise Server σχεδιάστηκε για δίκτυα υψηλής ζήτησης και υψηλής κυκλοφορίας. Windows NT 4.0 Server, Enterprise Edition περιλαμβάνει Service Pack 1 και 3.

- Windows NT 4.0 Terminal Server Edition, κυκλοφόρησε το 1998, επιτρέπει στους χρήστες να συνδέονται εξ αποστάσεως. Η ίδια λειτουργικότητα ονομάστηκε Terminal Services στα Windows 2000 και μεταγενέστερες εκδόσεις διακομιστή και επίσης ενεργοποιεί τη δυνατότητα απομακρυσμένης επιφάνειας εργασίας που εμφανίστηκε για πρώτη φορά στα Windows XP.

4.3.5. Microsoft Windows Server 2000

Τα Windows 2000, επίσης γνωστά ως Windows NT 5.0, βασίζονται στην τεχνολογία NT ως μια σειρά λειτουργικών συστημάτων που παράγονται από τη Microsoft για χρήση σε προσωπικούς υπολογιστές, επιτραπέζιους υπολογιστές, φορητούς υπολογιστές και διακομιστές. Τα Windows 2000 κυκλοφόρησαν στις 15 Δεκεμβρίου 1999 και είναι ο διάδοχος των Windows NT 4.0 και είναι η τελική έκδοση των Microsoft Windows για την εμφάνιση της ονομασίας "Windows NT". Τα διαδέχθηκαν τα Windows XP για επιτραπέζια συστήματα τον Οκτώβριο του 2001 και τα Windows Server 2003 για διακομιστές τον Απρίλιο του 2003. Τα Windows Me κυκλοφόρησαν επτά μήνες μετά τα Windows 2000 και ένα χρόνο πριν από τα Windows XP. Τα Windows Me είχαν σχεδιαστεί για οικιακή χρήση, ενώ τα Windows 2000 είχαν σχεδιαστεί για επιχειρήσεις.

Εικόνα 4.16

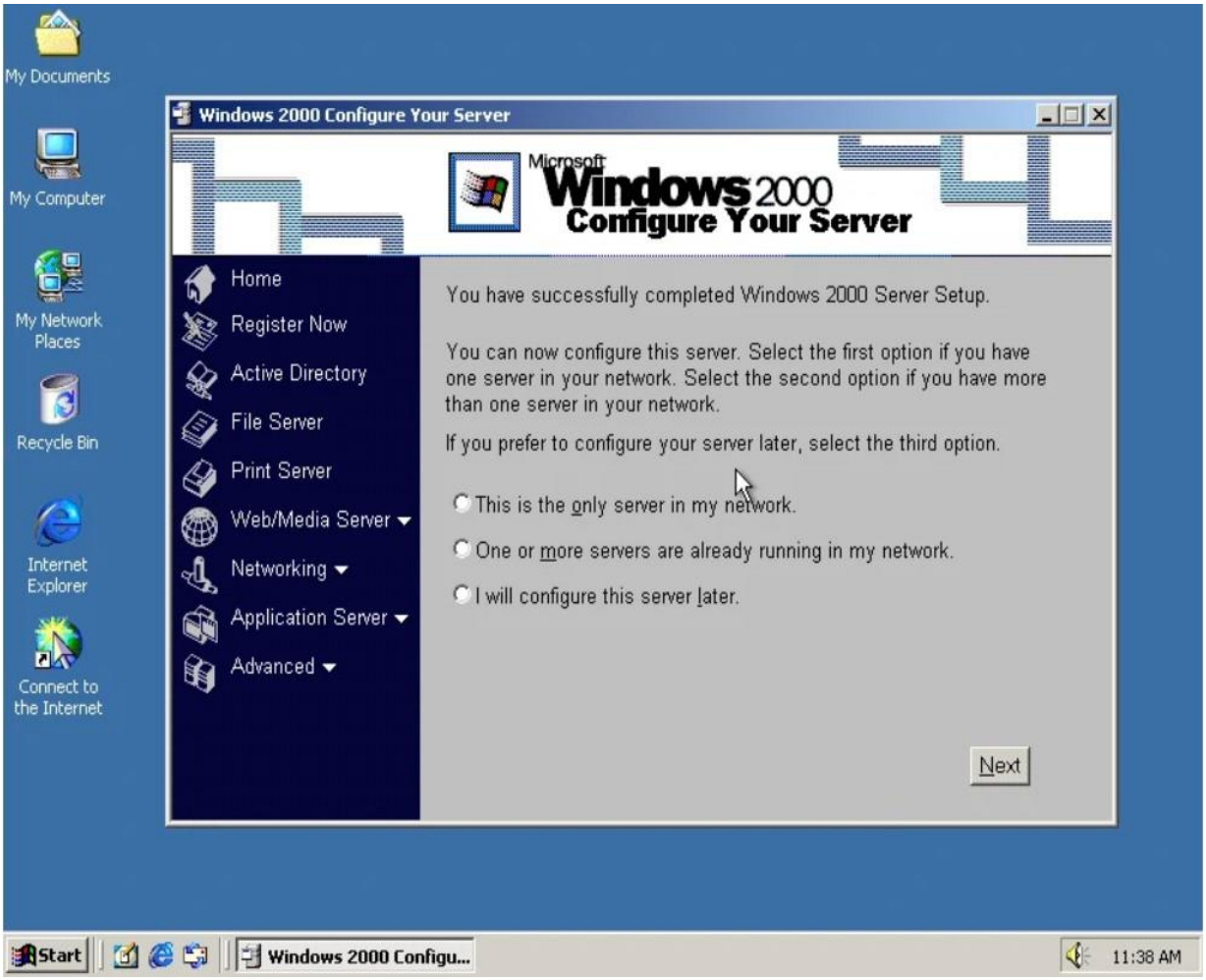
Από τον Σεπτέμβριο του 2011, το Windows Update v4 τερματίστηκε με αποτέλεσμα έναν ατελείωτο βρόχο από την προσπάθεια πρόσβασης στην τοποθεσία που επηρέασε όλες τις εκδόσεις της οικογένειας των Windows 9x και των Windows 2000 έως το Service Pack 3. Τα Windows 2000 Service Pack 4 δεν είναι πλέον συμβατά με Windows Update v6 χωρίς τον πιο πρόσφατο παράγοντα Windows Update.

Η Microsoft πούλησε τα Windows Advanced Server 2000 Limited Edition και Windows Datacenter Server 2000 Limited Edition, τα οποία λειτουργούσαν σε μικροεπεξεργαστές Intel Itanium 64-bit και κυκλοφόρησαν το 2001. Ενώ κάθε έκδοση των Windows 2000 στοχεύτηκε σε διαφορετική αγορά, μοιράστηκαν ένα βασικό σύνολο δυνατοτήτων, συμπεριλαμβανομένων πολλών βοηθητικών προγραμμάτων συστήματος, όπως η Microsoft Management Console και οι τυπικές εφαρμογές διαχείρισης συστήματος.

Η υποστήριξη για άτομα με ειδικές ανάγκες έχει βελτιωθεί σε σχέση με τα Windows NT 4.0 με αρκετές νέες υποστηρικτικές τεχνολογίες και η Microsoft αύξησε την υποστήριξη για διαφορετικές γλώσσες και πληροφορίες για τις τοπικές ρυθμίσεις.

Όλες οι εκδόσεις του λειτουργικού συστήματος υποστηρίζουν το σύστημα αρχείων Windows NT, NTFS 3.0, το σύστημα αρχείων κρυπτογράφησης, καθώς και βασική και δυναμική αποθήκευση δίσκου. Η οικογένεια διακομιστών των Windows 2000 διαθέτει πρόσθετες δυνατότητες, συμπεριλαμβανομένης της δυνατότητας παροχής υπηρεσιών Active Directory (ένα ιεραρχικό πλαίσιο πόρων), του κατανεμημένου συστήματος αρχείων (ένα σύστημα αρχείων που υποστηρίζει την κοινή χρήση αρχείων) και τους όγκους αποθήκευσης που είναι περιττοί. Τα Windows 2000 μπορούν να εγκατασταθούν είτε μέσω χειροκίνητης είτε χωρίς παρακολούθηση εγκατάστασης. Οι εγκαταστάσεις χωρίς επίβλεψη βασίζονται στη χρήση αρχείων απαντήσεων για τη συμπλήρωση των

πληροφοριών εγκατάστασης και μπορούν να εκτελεστούν μέσω ενός CD με δυνατότητα εκκίνησης χρησιμοποιώντας το Microsoft Systems Management Server, από το Εργαλείο προετοιμασίας συστήματος.



Εικόνα 4.17

Η Microsoft κυκλοφόρησε τα Windows 2000 ως την πιο ασφαλή έκδοση των Windows ποτέ. Ωστόσο, έγινε στόχος πολλών επιθέσεων ιών υψηλού προφίλ, όπως οι Code Red και Nimda.

Η Microsoft κυκλοφόρησε διάφορες εκδόσεις των Windows 2000 για διαφορετικές αγορές και επιχειρηματικές ανάγκες: Professional, Server, Advanced Server και Datacenter Server. Κάθε έκδοση περιλαμβάνονταν σε ξεχωριστό πακέτο. Οι εκδόσεις αυτές ήταν:

- Windows 2000 Professional τα οποία σχεδιάστηκαν ως λειτουργικό σύστημα επιτραπέζιων υπολογιστών για επιχειρήσεις και χρήστες ενέργειας. Είναι η έκδοση πελάτη των Windows 2000. Προσφέρει μεγαλύτερη ασφάλεια και σταθερότητα από πολλά από τα προηγούμενα λειτουργικά συστήματα των Windows. Υποστηρίζει έως και δύο επεξεργαστές και μπορεί να υποστηρίξει έως και 4 GB

μνήμης RAM. Οι απαιτήσεις συστήματος είναι επεξεργαστής Pentium (ή ισοδύναμος) 133 MHz ή μεγαλύτερος, τουλάχιστον 32 MB μνήμης RAM, 650 MB χώρου στο σκληρό δίσκο και μονάδα CD-ROM (συνιστάται: Pentium II, 128 MB RAM, 2 GB χώρου στο σκληρό δίσκο και μονάδα CD-ROM).

- Τα Windows Server 2000 τα οποία μοιράζονται την ίδια διεπαφή χρήστη με τα Windows 2000 Professional. Περιέχουν επιπλέον στοιχεία για τον υπολογιστή ο οποίος εκτελεί ρόλους διακομιστή, υποδομής καθώς και λογισμικού εφαρμογών. Ένα σημαντικό νέο στοιχείο που εισήχθη στις εκδόσεις του διακομιστή είναι το Active Directory, το οποίο είναι μια υπηρεσία καταλόγου για όλη την επιχείρηση που βασίζεται στο LDAP (Lightweight Directory Access Protocol). Επιπλέον, η Microsoft ενσωμάτωσε τον έλεγχο ταυτότητας δικτύου Kerberos, αντικαθιστώντας το σύστημα ελέγχου ταυτότητας NTLM (NT LAN Manager) που χρησιμοποιείται συχνά σε προηγούμενες εκδόσεις. Αυτό παρείχε επίσης μια αμιγώς μεταβατική σχέση εμπιστοσύνης μεταξύ των τομέων των Windows 2000 σε ένα σύμπλεγμα δομών (μια συλλογή από έναν ή περισσότερους τομείς των Windows 2000 που μοιράζονται ένα κοινό σχήμα, διαμόρφωση και καθολικό κατάλογο, που συνδέονται με αμφίδρομες μεταβατικές σχέσεις εμπιστοσύνης). Επιπλέον, τα Windows 2000 εισήγαγαν ένα Domain Name Server που επιτρέπει τη δυναμική καταχώριση των διευθύνσεων IP. Τα Windows Server 2000 υποστηρίζουν έως 4 επεξεργαστές, απαιτούν 128 MB μνήμης RAM και 1 GB χώρου στο σκληρό δίσκο. Ωστόσο οι απαιτήσεις ενδέχεται να είναι υψηλότερες ανάλογα με τα εγκατεστημένα στοιχεία.

- Τα Windows Advanced Server 2000 είναι μια παραλλαγή του λειτουργικού συστήματος Windows Server 2000 που έχει σχεδιαστεί για μεσαίες έως μεγάλες επιχειρήσεις. Προσφέρει υποδομή συμπλέγματος για υψηλή διαθεσιμότητα και επεκτασιμότητα εφαρμογών και υπηρεσιών, συμπεριλαμβανομένης της κύριας υποστήριξης μνήμης έως και 8 gigabyte (GB) σε συστήματα διεύθυνσης φυσικής διεύθυνσης (PAE) και την ικανότητα να κάνει SMP 8 κατευθύνσεων. Υποστηρίζει εξισορρόπηση φόρτου TCP / IP και βελτιωμένα συμπλέγματα διακομιστών δύο κόμβων με βάση τον Microsoft Cluster Server (MSCS) στον Windows NT Server 4.0 Enterprise Edition. Περιορισμένος αριθμός αντιγράφων μιας έκδοσης IA-64, που ονομάστηκε Windows Advanced Server 2000, Limited Edition διατέθηκε μέσω OEM. Οι απαιτήσεις συστήματος είναι παρόμοιες με εκείνες του Windows Server 2000, ωστόσο ενδέχεται να χρειαστεί να είναι υψηλότερες για κλίμακα σε μεγαλύτερη υποδομή.

- Τα Windows Datacenter Server 2000 είναι μια παραλλαγή των Windows Server 2000 που έχει σχεδιαστεί για μεγάλες επιχειρήσεις που μετακινούν συχνά μεγάλες ποσότητες εμπιστευτικών ή ευαίσθητων δεδομένων μέσω κεντρικού διακομιστή. Όπως και ο Advanced Server, υποστηρίζει συμπλέγματα, ανακατεύθυνση και εξισορρόπηση φορτίου. Οι ελάχιστες απαιτήσεις του συστήματος είναι φυσιολογικές, αλλά έχει σχεδιαστεί για να μπορεί να παρέχει προηγμένο, ανεκτικό σε σφάλματα και κλιμακωτό υλικό - για παράδειγμα υπολογιστές με έως 32 CPU και 64 GB RAM, με αυστηρές δοκιμές και πιστοποιήσεις συστήματος, διαμέριση

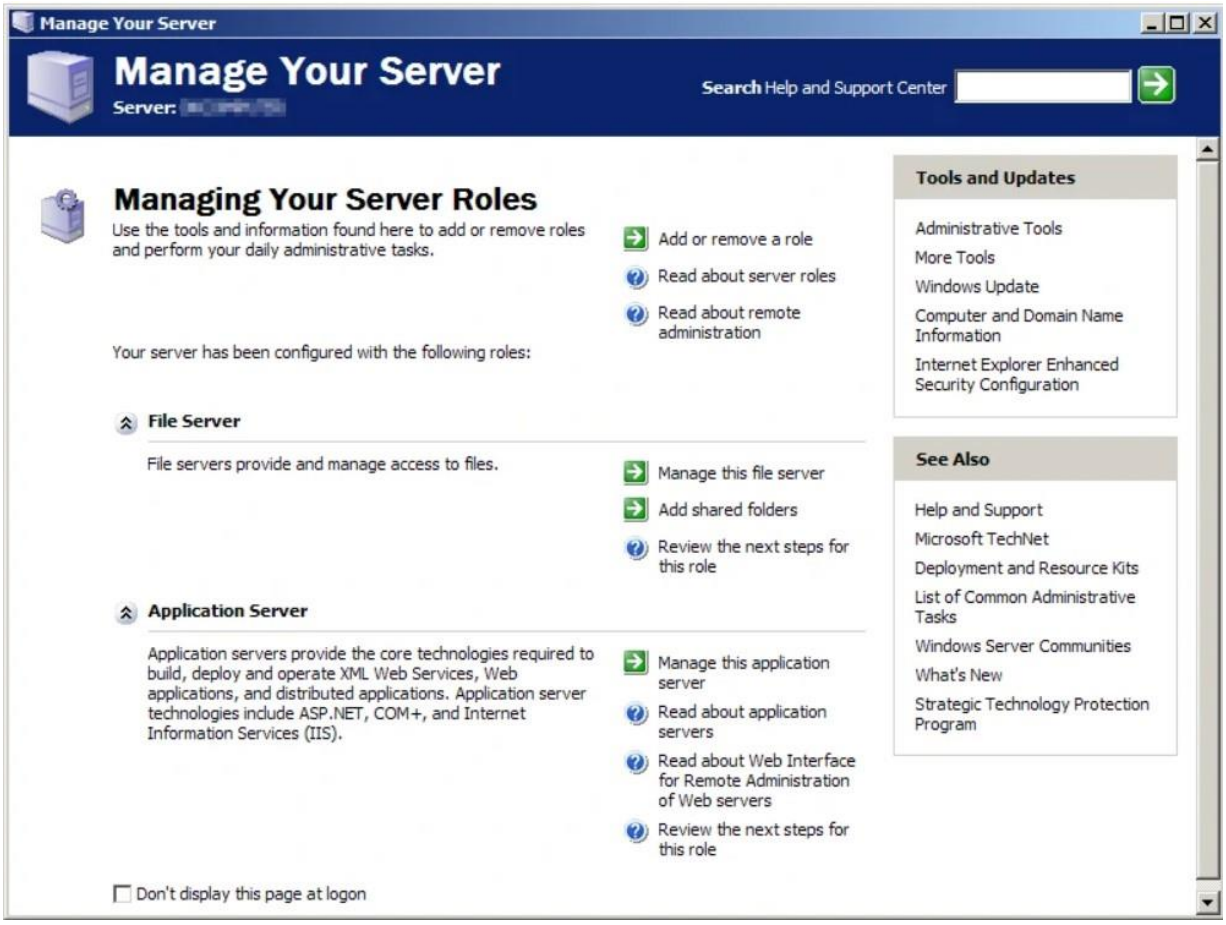
υλικού, συντονισμένη συντήρηση και αλλαγή ελέγχου. Περιορισμένος αριθμός αντιγράφων μιας έκδοσης IA-64, που ονομάστηκε Windows Datacenter Server 2000, Limited Edition διατέθηκε μέσω OEM. Οι απαιτήσεις συστήματος είναι παρόμοιες με εκείνες του Windows Advanced Server 2000, ωστόσο μπορεί να χρειαστεί να είναι υψηλότερες για κλίμακα σε μεγαλύτερη υποδομή.

4.3.6. Microsoft Windows Server 2003

Τα Windows Server 2003 (τα οποία φέρουν τον αριθμό έκδοσης 5.2) κυκλοφόρησαν στις 24 Απριλίου 2003, είναι η συνέχεια του Windows Server 2000, που περιλαμβάνει συμβατότητα και άλλες δυνατότητες από τα Windows XP. Σε αντίθεση με τα Windows Server 2000, η προεπιλεγμένη εγκατάσταση του Windows Server 2003 δεν έχει ενεργοποιήσει κανένα από τα στοιχεία του διακομιστή, για να μειώσει την επιφάνεια επίθεσης των νέων μηχανών. Τα Windows Server 2003 περιλαμβάνουν λειτουργίες συμβατότητας που επιτρέπουν την εκτέλεση παλαιότερων εφαρμογών με μεγαλύτερη σταθερότητα. Κατασκευάστηκαν πιο συμβατά με τη δικτύωση βάσει τομέα των Windows NT 4.0. Η ενσωμάτωση και αναβάθμιση ενός τομέα Windows NT 4.0 σε Windows 2000 θεωρήθηκε δύσκολη και χρονοβόρα και γενικά θεωρήθηκε αναβάθμιση όλων ή τίποτα, κυρίως όταν πρόκειται για την υπηρεσία καταλόγου Active Directory. Ο Windows Server 2003 έφερε βελτιωμένη συμβατότητα Active Directory και καλύτερη υποστήριξη ανάπτυξης, για να διευκολύνει τη μετάβαση από τα Windows NT 4.0 σε Windows Server 2003 και Windows XP Professional.

Εικόνα 4.18

Έχουν γίνει σημαντικές βελτιώσεις σε διάφορες υπηρεσίες, όπως ο διακομιστής Ιστού IIS (ο οποίος σχεδόν ξαναγράφηκε για τη βελτίωση της απόδοσης και της ασφάλειας), κατανεμημένο σύστημα αρχείων (το οποίο υποστηρίζει τώρα τη φιλοξενία πολλών ριζών DFS σε έναν μόνο διακομιστή), Terminal Server, Active Directory, διακομιστής εκτύπωσης και μια σειρά από άλλες αναβαθμίσεις. Τα Windows Server 2003 ήταν επίσης το πρώτο λειτουργικό σύστημα που κυκλοφόρησε η Microsoft μετά την ανακοίνωση της πρωτοβουλίας Trustworthy Computing, και ως εκ τούτου, περιέχει μια σειρά βελτιώσεων στις προεπιλογές και τις πρακτικές ασφαλείας.



Εικόνα 4.19

Το προϊόν υπέστη πολλές αλλαγές ονόματος κατά τη διάρκεια της ανάπτυξης. Όταν πρωτοεμφανίστηκε σε τεχνικούς δοκιμαστές beta στα μέσα του 2000, ήταν γνωστά με το κωδικό όνομα, "Whistler Server". Στη συνέχεια άλλαξε σε "Windows Server 2002" για σύντομο χρονικό διάστημα στα μέσα του 2001, προτού μετονομαστεί σε "Windows .NET Server" ως μέρος της προσπάθειας της Microsoft να προωθήσει το νέο ολοκληρωμένο πλαίσιο εταιρικής και ανάπτυξης, Microsoft .NET. Ωστόσο, λόγω φόβων σύγχυσης της αγοράς σχετικά με το τι αντιπροσωπεύει το ".NET" και απαντώντας σε κριτική, η Microsoft κατάργησε το .NET από το όνομα κατά τη διάρκεια του σταδίου Release Candidate στα τέλη του 2002. Αυτό επέτρεψε στο όνομα .NET να ισχύει αποκλειστικά για το .NET Framework, όπως προηγουμένως είχε φανεί ότι το .NET ήταν απλώς μια ετικέτα για μια γενιά προϊόντων της Microsoft.
Βελτιώσεις σε σχέση με τα Windows Server 2000 φαίνονται παρακάτω:

- ✓ Βελτιώσεις στην υπηρεσία καταλόγου Active Directory (όπως η δυνατότητα απενεργοποίησης κλάσεων από το σχήμα ή η εκτέλεση πολλαπλών παρουσιών του διακομιστή καταλόγου (ADAM))

- ✓ Βελτιώσεις στο χειρισμό και τη διαχείριση πολιτικής ομάδας

- ✓ Βελτιωμένη διαχείριση δίσκων, συμπεριλαμβανομένης της δυνατότητας δημιουργίας αντιγράφων ασφαλείας από σκιές αρχείων, επιτρέποντας τη δημιουργία αντιγράφων ασφαλείας ανοιχτών αρχείων.

- ✓ Βελτιωμένα εργαλεία δέσμης ενεργειών και γραμμής εντολών, τα οποία αποτελούν μέρος της πρωτοβουλίας της Microsoft να φέρει ένα πλήρες κέλυφος εντολών στην επόμενη έκδοση των Windows.

- ✓ Υποστήριξη για ένα "χρονόμετρο παρακολούθησης" που βασίζεται σε υλικό, το οποίο μπορεί να επανεκκινήσει τον διακομιστή εάν το λειτουργικό σύστημα δεν ανταποκρίνεται εντός συγκεκριμένου χρονικού διαστήματος.

Windows Server 2003 R2

Μια σημαντική ενημέρωση του Windows Server 2003, που ονομάζεται επίσημα R2, επίσης γνωστή ως Windows 2003 R2 (Windows XP Server R2) (με κωδικό όνομα Whistler Server R2), κυκλοφόρησε στην κατασκευή στις 6 Δεκεμβρίου 2005. Διανέμεται ως δεύτερο CD, με το πρώτο CD να είναι το Windows Server SP1. Πρόκειται για μια νέα έκδοση του λειτουργικού συστήματος διακομιστή εισάγοντας νέες αναβαθμίσεις:

- Διαχείριση διακομιστή υποκαταστημάτων (**Branch Office Server Management**)
  - ❖ Εργαλεία κεντρικής διαχείρισης για αρχεία και εκτυπωτές
  - ❖ Διεπαφή διαχείρισης χώρου ονομάτων ενισχυμένου κατανεμημένου συστήματος αρχείων (DFS)
  - ❖ Πιο αποτελεσματική αναπαραγωγή δεδομένων WAN με απομακρυσμένη διαφορική συμπίεση
- Διαχείριση ταυτότητας και πρόσβασης (**Identity and Access Management**)
  - ❖ Extranet Single Sign-On and identity federation
  - ❖ Κεντρική διαχείριση πρόσβασης σε εφαρμογές extranet
  - ❖ Αυτόματη απενεργοποίηση πρόσβασης στο extranet με βάση τις πληροφορίες λογαριασμού Active Directory
  - ❖ Καταγραφή πρόσβασης χρήστη
  - ❖ Ιστός πολλαπλής πλατφόρμας με ενιαία σύνδεση και συγχρονισμός κωδικού πρόσβασης χρησιμοποιώντας την υπηρεσία πληροφοριών δικτύου (NIS)
- Διαχείριση αποθήκευσης (**Storage Management**)
  - ❖ Διαχείριση πόρων διακομιστή αρχείων (αναφορές χρήσης αποθηκευτικού χώρου)
  - ❖ Βελτιωμένη διαχείριση ποσοστώσεων
  - ❖ Ο έλεγχος αρχείων περιορίζει τους επιτρεπόμενους τύπους αρχείων
  - ❖ Διαχείριση αποθήκευσης για Storage Area Networks (SAN) (διαμόρφωση πίνακα αποθήκευσης)
- Τεχνολογίες 64-bit και .NET για απόδοση στο διαδίκτυο
  - ❖ Υπηρεσίες Windows SharePoint
  - ❖ ASP.NET
  - ❖ IIS 6.0
  - ❖ Υποστήριξη x64

- Εικονικοποίηση διακομιστή (**Server Virtualization**)
  - ❖ Μια νέα πολιτική αδειοδότησης επιτρέπει έως και 4 εικονικά στιγμιότυπα
- Βοηθητικά προγράμματα και SDK για πρόσθετες εφαρμογές που βασίζονται σε UNIX, προσφέροντας ένα σχετικά πλήρες περιβάλλον ανάπτυξης Unix.
  - ❖ Βασικά βοηθητικά προγράμματα
  - ❖ Βοηθητικά προγράμματα SVR-5
  - ❖ Βασικό SDK
  - ❖ SDK GNU
  - ❖ Βοηθητικά προγράμματα GNU
  - ❖ UNIX Perl
  - ❖ Πρόσθετο Visual Studio Debugger

4.3.7. Microsoft Windows Server 2008

Τα Windows Server 2008 (με κωδικό όνομα Windows Longhorn Server) είναι μία από τις σειρές λειτουργικών συστημάτων διακομιστή των Microsoft Windows. Κυκλοφόρησε στις 4 Φεβρουαρίου 2008 και είναι ο διάδοχος των Windows Server 2003 R2. Τα Windows Server 2008 είναι ο αντίστοιχος διακομιστής των Windows Vista.

Εικόνα 4.20

Όπως τα Windows Vista, τα Windows 7 και τα Windows Server 2008 είναι ενσωματωμένα στα Windows NT 6.x.

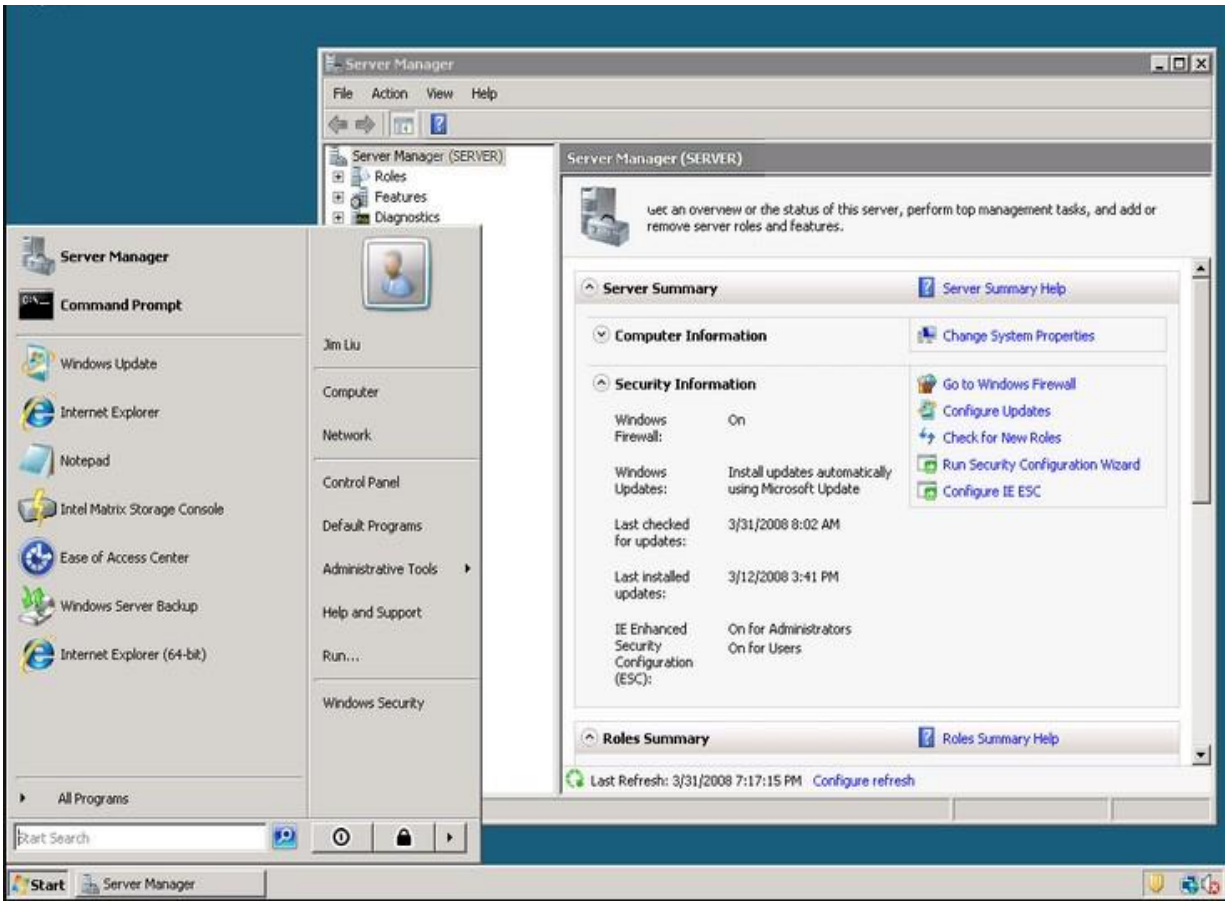
Τα Windows Server 2008 είναι κατασκευασμένα από την ίδια βάση κώδικα με τα Windows Vista. Επομένως, μοιράζονται την ίδια αρχιτεκτονική και λειτουργικότητα. Δεδομένου ότι η βάση κώδικα είναι κοινή, έρχεται αυτόματα με τις περισσότερες από τις τεχνικές δυνατότητες, την ασφάλεια, τη διαχείριση και τις διοικητικές δυνατότητες που είναι καινούργιες για τα Windows Vista.

Βελτιώσεις όπως:

- επανασχεδιασμένη στοίβα δικτύου (εγγενές IPv6, εγγενές ασύρματο, βελτιώσεις ταχύτητας και ασφάλειας)
- βελτιωμένη εγκατάσταση
- ανάπτυξη και ανάκτηση με βάση την εικόνα
- βελτιωμένα εργαλεία διάγνωσης, παρακολούθησης, καταγραφής συμβάντων και αναφορών
- νέα χαρακτηριστικά ασφαλείας όπως το BitLocker και το ASLR (τυχαιοποίηση διάταξης χώρου διευθύνσεων)
- βελτιωμένο τείχος προστασίας των Windows με ασφαλή προεπιλεγμένη διαμόρφωση

- .NET Framework 3.0 τεχνολογίες,
- συγκεκριμένα Windows Communication Foundation
- Microsoft Message Queuing και Windows Workflow Foundation
- βελτιώσεις στον πυρήνα του kernel, τη μνήμη και του συστήματος αρχείων.

Οι επεξεργαστές και οι συσκευές μνήμης είναι μοντελοποιημένες ως Plug and Play devices, για να επιτρέπεται η άμεση σύνδεση αυτών των συσκευών. Αυτό επιτρέπει στους πόρους του συστήματος να χωρίζονται δυναμικά χρησιμοποιώντας το Dynamic Hardware Partitioning. Κάθε διαμέρισμα έχει τη δική του μνήμη, τον επεξεργαστή και τις συσκευές γέφυρας υποδοχής εισόδου / εξόδου ανεξάρτητα από άλλα διαμερίσματα.



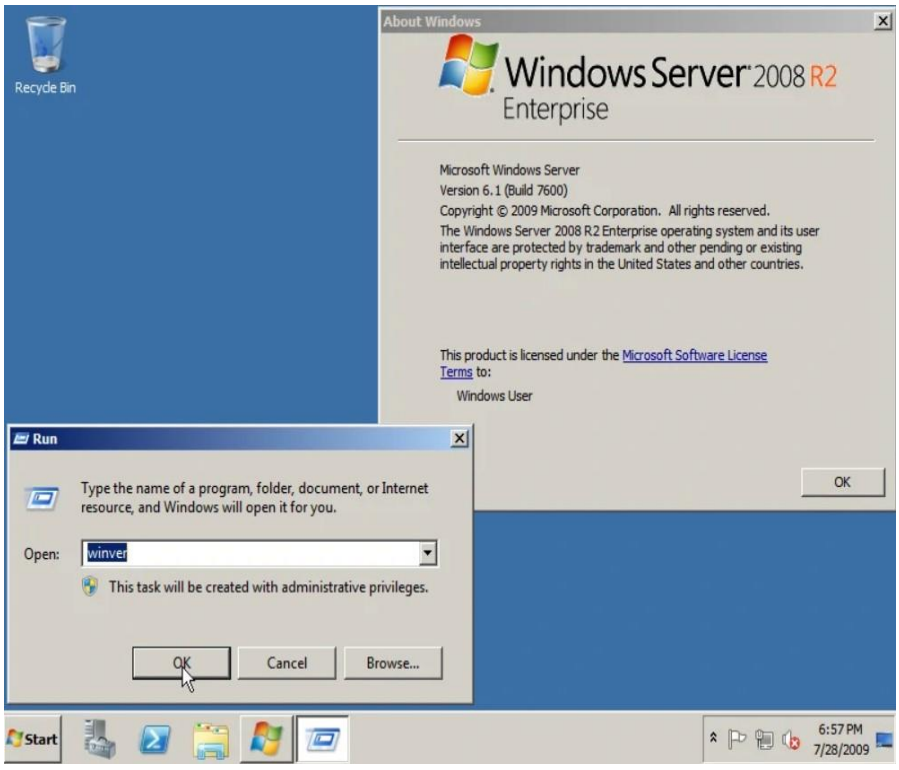
Εικόνα 4.21

Οι περισσότερες εκδόσεις του Windows Server 2008 είναι διαθέσιμες σε εκδόσεις x86-64 και IA-32. Αυτές οι εκδόσεις διατίθενται σε δύο DVD: Ένα για την εγκατάσταση της παραλλαγής IA-32 και το άλλο για x64. Τα Windows Server 2008 για συστήματα που βασίζονται σε Itanium υποστηρίζει επεξεργαστές IA-64. Η έκδοση IA-64 είναι βελτιστοποιημένα σενάρια υψηλού φόρτου εργασίας, όπως διακομιστές βάσεων δεδομένων και εφαρμογές Line of Business (LOB). Ως εκ τούτου, δεν έχει βελτιστοποιηθεί για χρήση ως διακομιστής αρχείων ή διακομιστής πολυμέσων. Ο Windows Server 2008 είναι το τελευταίο λειτουργικό σύστημα διακομιστή Windows 32-bit. Οι εκδόσεις των Windows Server 2008 περιλαμβάνουν:

- Windows Server 2008 Standard (IA-32 and x86-64)
- Windows Server 2008 Enterprise (IA-32 and x86-64)
- Windows Server 2008 Datacenter (IA-32 and x86-64)
- Windows HPC Server 2008 (Codenamed "Socrates") (replacing Windows Compute Cluster Server)
- Windows Web Server 2008 (IA-32 and x86-64)
- Windows Storage Server 2008 (Codenamed "Magni") (IA-32 and x86-64)
- Windows Small Business Server 2008 (Codenamed "Cougar") (x86-64) for small businesses
- Windows Essential Business Server 2008 (Codenamed "Centro") (x86-64) for medium-sized businesses (Discontinued)
- Windows Server 2008 for Itanium-based Systems
- Windows Server 2008 Foundation (Codenamed "Lima") (x86-64) for OEMs only

Windows Server 2008 R2

Windows Server 2008 R2 κυκλοφόρησαν στις 22 Ιουλίου 2009 και έγινε γενικά διαθέσιμο στις 22 Οκτωβρίου 2009.



Εικόνα 4.22

Οι βελτιώσεις περιλαμβάνουν νέα λειτουργικότητα για την υπηρεσία καταλόγου Active Directory, νέες δυνατότητες εικονικοποίησης και διαχείρισης, έκδοση 7.5 του διακομιστή Web Information Services και υποστήριξη για έως και 256 λογικούς επεξεργαστές. Είναι χτισμένο στον ίδιο πυρήνα που χρησιμοποιείται με τα Windows 7 που είναι προσανατολισμένα στον πελάτη και είναι το πρώτο λειτουργικό σύστημα 64 bit που κυκλοφόρησε από τη Microsoft.

Κυκλοφόρησαν επτά εκδόσεις του Windows Server 2008 R2: Foundation, Standard, Enterprise, Datacenter, Web, HPC Server και Itanium, καθώς και Windows Storage

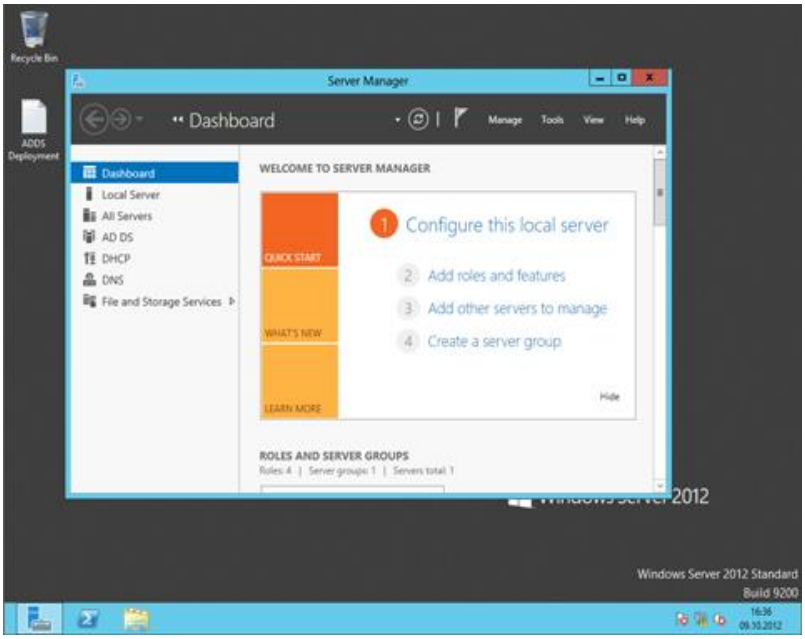
Server 2008 R2. Κυκλοφόρησε επίσης μια παραλλαγή οικιακού διακομιστή που ονομάζεται Windows Home Server 2011. Τα διαδέχτηκαν τα Windows Server 2012.

4.3.8. Microsoft Windows Server 2012

Τα Windows Server 2012 (με κωδικό όνομα Windows Server 8) είναι η έκτη έκδοση της σειράς λειτουργικών συστημάτων Windows Server. Είναι η έκδοση διακομιστή των Windows 8 και είναι ο διάδοχος των Windows Server 2008 R2 και ο προκάτοχος του Windows Server 2016. Ξεκίνησε την υλοποίηση την 1η Αυγούστου 2012 και κυκλοφόρησε στο κοινό στις 4 Σεπτεμβρίου 2012.

Εικόνα 4.23

Τα Windows Server 2012 είναι πιθανώς η πιο σημαντική έκδοση των Windows Server. Με ένα καινοτόμο νέο περιβάλλον εργασίας χρήστη, νέα ισχυρά εργαλεία διαχείρισης, βελτιωμένη υποστήριξη του Windows PowerShell και εκατοντάδες νέες δυνατοτήτες στους τομείς δικτύωσης, αποθήκευσης και εικονικοποίησης, Τα Windows Server 2012 μπορούν να βοηθήσουν το τμήμα IT να προσφέρει περισσότερα, μειώνοντας παράλληλα το κόστος. Σχεδιάστηκαν επίσης για το cloud ξεκινώντας από κάτω και παρέχει ένα θεμέλιο για δημόσια κτίρια και ιδιωτικές λύσεις cloud για να επιτρέψουν στις επιχειρήσεις να έχουν τα οφέλη των πολλών πλεονεκτημάτων του cloud computing.



Εικόνα 4.24

Αξιοσημείωτες νέες δυνατότητες και βελτιώσεις περιλαμβάνουν:

- Η νέα διεπαφή χρήστη από τα Windows 8 (αρχικά από το Windows Phone 7)
- Δυνατότητα εναλλαγής μεταξύ των επιλογών διεπαφής διακομιστή GUI και διακομιστή πυρήνα χωρίς επανεγκατάσταση
- Ένας επανασχεδιασμένος Task Manager
- Βελτιώσεις σε Active Directory, Hyper-V και το νέο IIS 8
- Ένα νέο μοντέλο αδειοδότησης

Τα Windows Server 2012 είναι διαθέσιμα μόνο σε 4 εκδόσεις:

- Foundation - Περιορίζεται σε μια CPU και περιορισμένες συνδέσεις, το AD πρέπει να είναι σε δενδροειδή μορφή. Διατίθεται μόνο μέσω OEM.
- Essentials - Περιορίζεται σε 2 CPU, υψηλότερα όρια από το Foundation. Διαθέσιμο μέσω Retail, VL και OEM.
- Standard - Προσθέτει Hyper-V, Server Core, ADFS και χρησιμοποιεί CAL. Διαθέσιμο μέσω Retail, VL και OEM.
- Datacenter - Απεριόριστα δικαιώματα εικονικοποίησης. Διατίθεται μόνο μέσω VL ή OEM

Η Microsoft είχε δηλώσει ότι τα Windows Server 2012 δεν θα υποστηρίζουν επεξεργαστές 32-bit (IA-32) ή Itanium (IA-64), αλλά δεν έχουν κυκλοφορήσει επίσημα άλλες απαιτήσεις συστήματος, εκτός από το Release Candidate.
Κάθε άδεια χρήσης των Windows Server 2012 Standard ή του Datacenter επιτρέπει έως και δύο chip επεξεργαστή. Κάθε άδεια χρήσης των Windows Server 2012 Standard επιτρέπει έως και δύο εικονικές παρουσίες των Windows Server 2012 Standard σε αυτόν τον φυσικό διακομιστή. Εάν απαιτούνται περισσότερες εικονικές παρουσίες των Windows Server 2012 Standard, κάθε πρόσθετη άδεια χρήσης των Windows Server 2012 επιτρέπει έως και δύο ακόμη εικονικές παρουσίες των Windows Server 2012 Standard, παρόλο που ο ίδιος ο φυσικός διακομιστής μπορεί να έχει επαρκείς άδειες για τον αριθμό των επεξεργαστών του. Επειδή τα Windows Server 2012 Datacenter δεν έχουν όριο στον αριθμό των εικονικών παρουσιών ανά διακομιστή με άδεια χρήσης, χρειάζονται μόνο αρκετές άδειες για τον φυσικό διακομιστή για οποιονδήποτε αριθμό εικονικών παρουσιών των Windows Server 2012 Datacenter. Αν ο αριθμός των επεξεργαστών ή των εικονικών παρουσιών είναι μονός αριθμός, ο αριθμός των αδειών που απαιτείται είναι ο ίδιος με τον επόμενο ζυγό αριθμό. Για παράδειγμα, ένας διακομιστής με έναν επεξεργαστή-chip θα εξακολουθούσε να απαιτεί 1 άδεια, όπως εάν ο διακομιστής ήταν δύο επεξεργαστές-τσιπ και ένας διακομιστής πέντε επεξεργαστών-τσιπ θα απαιτούσε 3 άδειες, το ίδιο σαν εάν ο διακομιστής ήταν έξι επεξεργαστής-chip και εάν απαιτούνται 15 εικονικές παρουσίες του Windows Server 2012 Standard σε έναν διακομιστή, απαιτούνται 8 άδειες χρήσης των Windows Server 2012, οι οποίες μπορούν να καλύψουν έως και 16 εικονικές παρουσίες.

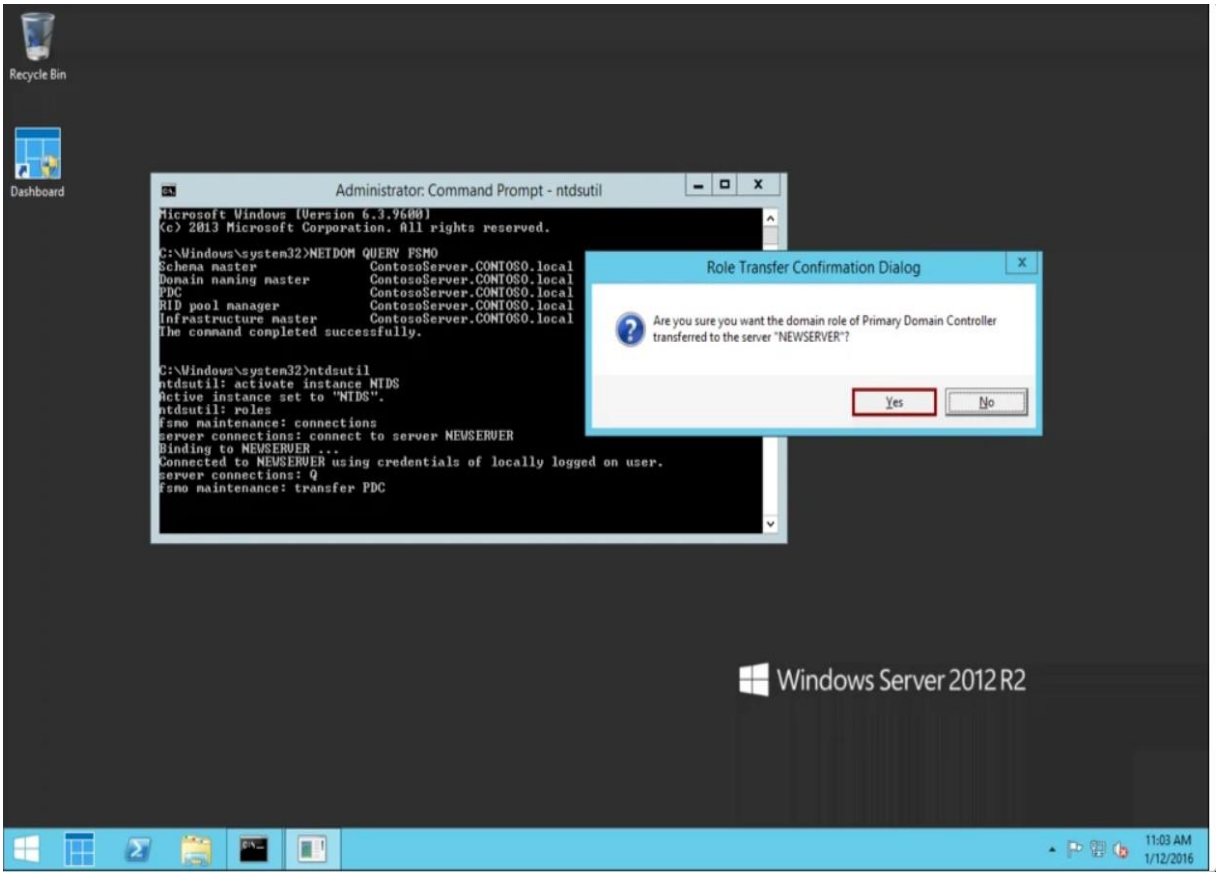
Windows Server 2012 R2

Οι ακόλουθες δυνατότητες εισάγονται στον Windows Server 2012 R2:

- **Automated Tiering**: Ο αποθηκευτικός χώρος αποθηκεύει τα αρχεία με τα πιο συχνά προσβάσιμα αρχεία με ταχύτερα φυσικά μέσα
- **Deduplication for VHD**: Μειώνει τον αποθηκευτικό χώρο για αρχεία VHD με πολύ παρόμοιο περιεχόμενο αποθηκεύοντας τα παρόμοια περιεχόμενα μόνο μία φορά
- **Windows PowerShell v4**, το οποίο περιλαμβάνει μια δυνατότητα επιθυμητής ρύθμισης παραμέτρων
- **Ενσωματωμένη υποστήριξη του Office 365** (έκδοση Essentials)
- **Οι διεπαφές χρήστη** αλλάζουν από τα Windows 8.1, συμπεριλαμβανομένου του ορατού κουμπιού "Έναρξη"
- **Εικονικές μηχανές** με βάση το UEFI
- **Αναβαθμίσεις** από εξομοιωτές προγραμμάτων οδήγησης σε προγράμματα οδήγησης συνθετικού υλικού για ελαχιστοποίηση της υποστήριξης παλαιού τύπου
- **Ταχύτερη ανάπτυξη VM** (περίπου στο μισό χρόνο)
- **Υπηρεσίες πληροφοριών Διαδικτύου 8.5**: Υποστήριξη για καταγραφή παρακολούθησης συμβάντων για Windows και δυνατότητα καταγραφής κεφαλίδων αιτήματος / απόκρισης. Για βελτίωση της επεκτασιμότητα, εάν το IIS έχει διαμορφωθεί με 100 ή περισσότερους ιστότοπους, από προεπιλογή δεν θα ξεκινήσει αυτόματα καμία από αυτές. Παράλληλα, έχει προστεθεί μια νέα επιλογή διαμόρφωσης "Idle Worker Process Page-Out" στα σύνολα εφαρμογών για να δώσει εντολή στα Windows να καταργήσουν τη διαδικασία εάν ήταν αδρανής για την περίοδο αδράνειας (από προεπιλογή, 20 λεπτά).
- **Αποκλεισμός μηνυμάτων διακομιστή**: Βελτιώσεις ποιότητας απόδοσης και καταγραφής συμβάντων, υποστήριξη για Hyper-V Live Migration μέσω SMB, διαχείριση προτεραιότητας εύρους ζώνης και δυνατότητα κατάργησης υποστήριξης SMB 1.012
- **Υπηρεσίες ανάπτυξης των Windows**: Υποστήριξη για τη διαχείριση του WDS μέσω του PowerShell
- **Το Windows Defender** είναι διαθέσιμο σε μια εγκατάσταση Core Server και είναι εγκατεστημένο και ενεργοποιημένο από προεπιλογή
- **Διαχείριση διευθύνσεων IP (IPAM)**: Επέκταση για την υποστήριξη ελέγχου πρόσβασης βάσει ρόλου, επιτρέποντας τον λεπτομερή έλεγχο επί των οποίων οι χρήστες μπορούν να προβάλλουν ή να αλλάζουν διαμορφώσεις για κρατήσεις DHCP, εύρη, μπλοκ διευθύνσεων IP, εγγραφές πόρων DNS κ.λπ. ενοποίηση με το System Center Virtual Machine Manager 2012 R2 για συντονισμένη πολιτική IP σε φυσικά και εικονικά περιβάλλοντα. Η βάση δεδομένων IPAM μπορεί να αποθηκευτεί σε μια παρουσία SQL Server αντί για την εσωτερική βάση δεδομένων των Windows
- **Η Πολιτική ομάδας (Group Policy)** έχει μια νέα ρύθμιση "Policy cache" η οποία επιτρέπει σε μηχανήματα που συνδέονται με τομέα να αποθηκεύουν ένα αντίγραφο των ρυθμίσεων πολιτικής ομάδας στον υπολογιστή-πελάτη και,

ανάλογα με την ταχύτητα πρόσβασης στον ελεγκτή τομέα, χρησιμοποιούνται απευθείας κατά την εκκίνηση αντί να περιμένει για λήψη των ρυθμίσεων πολιτικής. Αυτό μπορεί να βελτιώσει τους χρόνους εκκίνησης σε μηχανήματα που είναι αποσυνδεδεμένα από το δίκτυο της εταιρείας. Προστέθηκαν νέες ρυθμίσεις πολιτικής ομάδας για να καλύψουν νέες δυνατότητες στα Windows 8.1 και στον Internet Explorer 11, όπως ενεργοποίηση / απενεργοποίηση της υποστήριξης SPDY/3, διαμόρφωση διατάξεων οθόνης έναρξης, και ανίχνευση αριθμών τηλεφώνου σε ιστοσελίδες

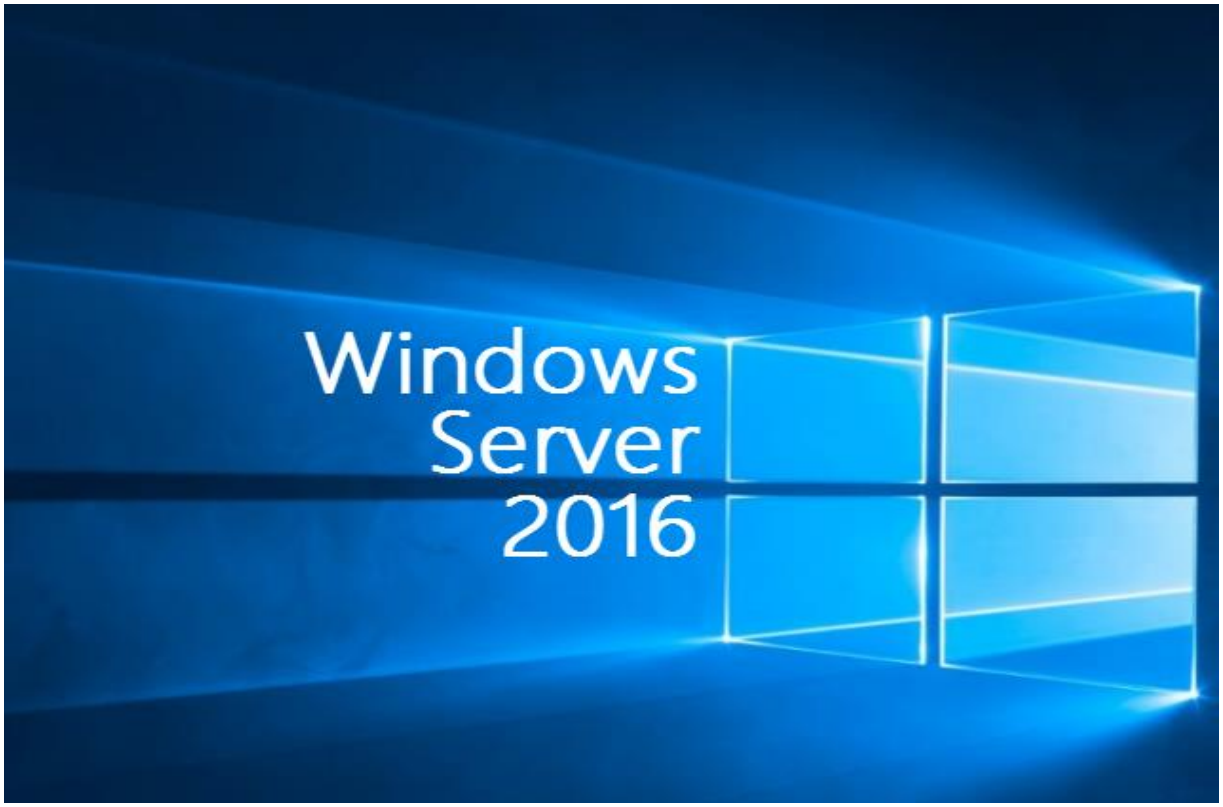
- Η υποστήριξη TLS επεκτείνεται για την υποστήριξη RFC 5077, "Transport Layer Security (TLS) Session Resumeption χωρίς Server-Side State", η οποία βελτιώνει την απόδοση μακροχρόνιων TLS-ασφαλών συνδέσεων που πρέπει να επανασυνδεθούν λόγω λήξης περιόδου λειτουργίας
- Ο ρόλος Hyper-V και η κονσόλα διαχείρισης Hyper-V προστίθενται στην έκδοση Essentials
- Οι υπηρεσίες ενημέρωσης διακομιστή των Windows διατέθηκαν για την έκδοση Windows Server 2012 R2 Essentials
- Το ReFS απέκτησε υποστήριξη για εναλλακτικές ροές δεδομένων και αυτόματη διόρθωση σφαλμάτων σε χώρους ισοτιμίας



Εικόνα 4.25

4.3.9. Microsoft Windows Server 2016

Τα Windows Server 2016 είναι ένα λειτουργικό σύστημα διακομιστή που αναπτύχθηκε από τη Microsoft ως μέρος της οικογένειας λειτουργικών συστημάτων Windows NT, που αναπτύχθηκε ταυτόχρονα με τα Windows 10. Η πρώτη έκδοση πρώιμης προεπισκόπησης (Technical Preview) έγινε διαθέσιμη την 1η Οκτωβρίου 2014, μαζί με την πρώτη τεχνική προεπισκόπηση του System Center.
Σε αντίθεση με τις προηγούμενες εκδόσεις των Windows Server, οι οποίες κυκλοφόρησαν ταυτόχρονα με το λειτουργικό σύστημα πελάτη, τα Windows Server 2016 κυκλοφόρησαν στις 18 Ιουλίου 2016, στο συνέδριο Ignite της Microsoft και έγινε γενικά διαθέσιμα στις 2 Αυγούστου 2016.



Εικόνα 4.26

Τα Windows Server 2016 διαθέτουν μια ποικιλία νέων δυνατοτήτων, όπως:

- ✓ **Active Directory Federation Services**: Είναι δυνατή η ρύθμιση παραμέτρων του AD FS για έλεγχο ταυτότητας χρηστών που είναι αποθηκευμένοι σε καταλόγους που δεν ανήκουν σε AD, όπως συμβατές με τους X.500 Lightweight Directory Access Protocol (LDAP) καταλόγους και βάσεις δεδομένων SQL
- ✓ **Windows Defender**: Το Windows Server Antimalware είναι εγκατεστημένο και ενεργοποιημένο από προεπιλογή χωρίς το GUI, το οποίο είναι μια δυνατότητα εγκατάστασης των Windows.

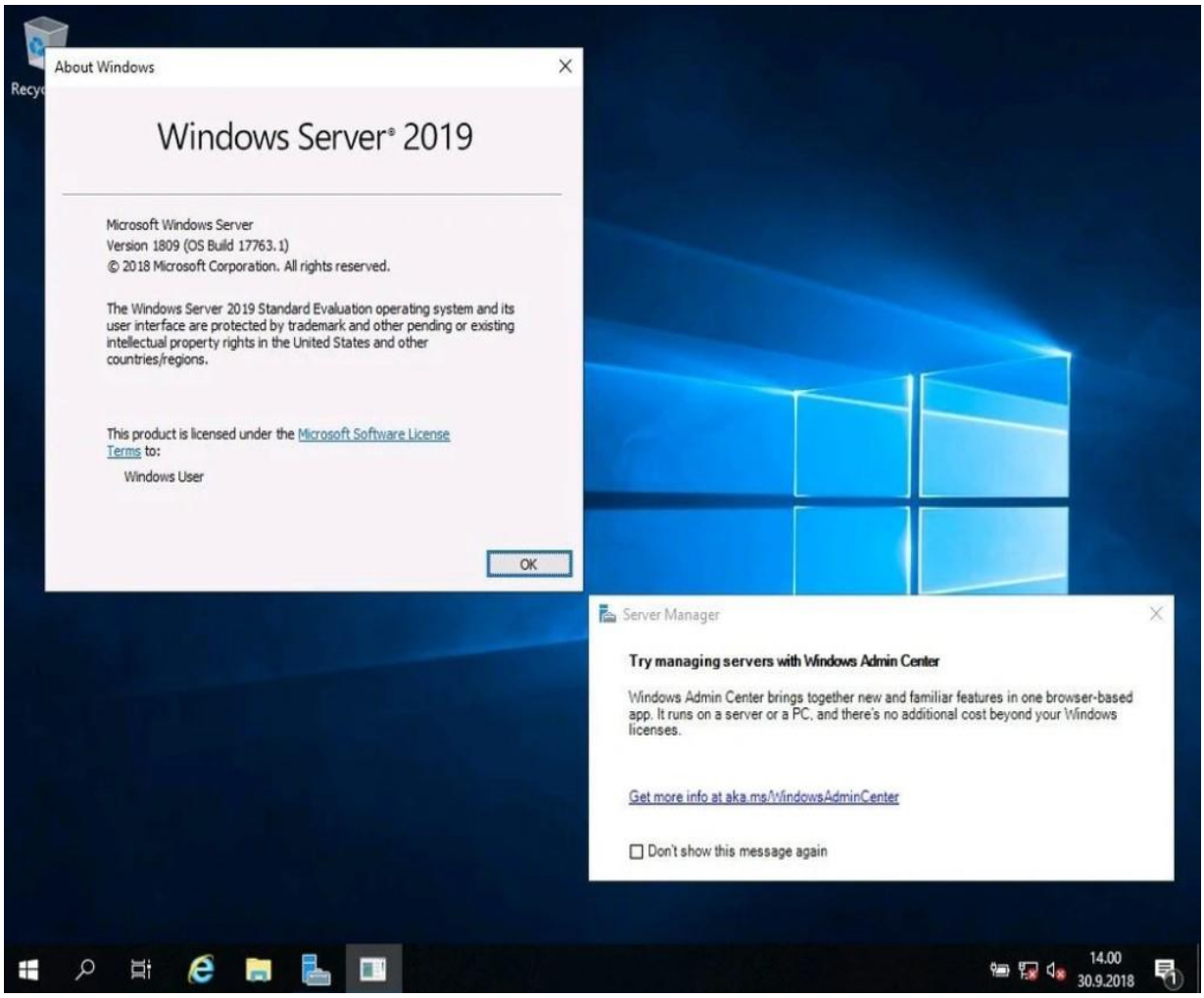
- ✓ **Υπηρεσίες απομακρυσμένης επιφάνειας εργασίας**: Υποστήριξη για OpenGL 4.4 και OpenCL 1.1, βελτιώσεις απόδοσης και σταθερότητας. Ρόλος MultiPoint Services
- ✓ **Υπηρεσίες αποθήκευσης**: κεντρικές πολιτικές αποθήκευσης QoS. Αποθήκευση αντιγράφων (storage-agnostic, επίπεδο μπλοκ με βάση τον όγκο, σύγχρονη και ασύγχρονη αναπαραγωγή χρησιμοποιώντας SMB3 μεταξύ διακομιστών για ανάκτηση καταστροφών). Το Replica Storage αντιγράφει μπλοκ αντί για αρχεία. Αρχεία τα οποία μπορεί να χρησιμοποιούνται ήδη . Δεν είναι multi-master, όχι one-to-many και δεν είναι μεταβατικό. Αναπαράγει περιοδικά στιγμιότυπα και η κατεύθυνση αναπαραγωγής μπορεί να αλλάξει
- ✓ **Failover Clustering**: Αναβάθμιση κυλιόμενου λειτουργικού συστήματος συμπλέγματος, αντίγραφα αποθήκευσης
- ✓ **Διαδικτυακός διακομιστής μεσολάβησης**: Προληπτικός έλεγχος για τη βασική δημοσίευση εφαρμογών HTTP, δημοσίευση τομέων μπαλαντέρ με εφαρμογές, ανακατεύθυνση HTTP σε HTTPS. Διάδοση διεύθυνσης IP πελάτη για εφαρμογές backend
- ✓ **IIS 10**: Υποστήριξη για HTTP/2
- ✓ **Windows PowerShell 5.1**
- ✓ **Κοντέινερ διακομιστή των Windows**

Δυνατότητες δικτύωσης

- ➢ **DHCP**: Καθώς η προστασία πρόσβασης δικτύου καταργήθηκε στα Windows Server 2012 R2, στον Windows Server 2016 ο ρόλος DHCP δεν υποστηρίζει πλέον το NAP
- ➢ **DNS client**: Σύνδεση υπηρεσίας - βελτιωμένη υποστήριξη για υπολογιστές με περισσότερες από μία διεπαφές δικτύου
- ➢ **DNS Server**: Πολιτικές DNS, νέοι τύποι εγγραφών DDS (TLSA, SPF και άγνωστες εγγραφές), νέα cmdlet PowerShell και παράμετροι
- ➢ Το Windows Server Gateway υποστηρίζει Generic Routing Encapsulation (GRE) tunnel
- ➢ **Διαχείριση διευθύνσεων IP (IPAM)**: Υποστήριξη για /31, /32 και /128 υποδίκτυα. ανακάλυψη διακομιστών DNS που βασίζονται σε αρχεία και συνδέονται με τομέα · νέες λειτουργίες DNS. καλύτερη ενοποίηση της διαχείρισης DNS, DHCP και IP Address (DDI)
- ➢ **Network Controller**: Ένας νέος ρόλος διακομιστή για τη διαμόρφωση, διαχείριση, παρακολούθηση και αντιμετώπιση προβλημάτων εικονικών και φυσικών συσκευών δικτύου και υπηρεσιών στο κέντρο δεδομένων
- ➢ **Εικονικοποίηση δικτύου Hyper-V**: Προγραμματιζόμενος διακόπτης Hyper-V (ένα νέο δομικό στοιχείο της λύσης δικτύωσης που καθορίζεται από λογισμικό της Microsoft). Υποστήριξη ενθυλάκωσης VXLAN. Διαλειτουργικότητα του Microsoft Software Load Balancer. Καλύτερη συμβατότητα IEEE Ethernet

4.3.10. Microsoft Windows Server 2019

Τα Windows Server 2019 είναι η τελευταία έκδοση του λειτουργικού συστήματος διακομιστή από τη Microsoft, ως μέρος της οικογένειας λειτουργικών συστημάτων Windows NT. Τα Windows Server 2019 ανακοινώθηκαν στις 20 Μαρτίου 2018 και η πρώτη έκδοση προεπισκόπησης των Windows Insider κυκλοφόρησε την ίδια ημέρα. Κυκλοφόρησε για γενική διαθεσιμότητα στις 2 Οκτωβρίου 2018.



Εικόνα 4.27

Στις 6 Οκτωβρίου 2018, η διανομή της έκδοσης 1809 των Windows (Build 17763) τέθηκε σε παύση ενώ η Microsoft διερεύνησε ένα ζήτημα με τη διαγραφή δεδομένων χρήστη κατά τη διάρκεια μιας επιτόπιας αναβάθμισης. Η συγκεκριμένη έκδοση επηρέαζε συστήματα όπου ένας φάκελος προφίλ χρήστη (π.χ. Έγγραφα, Μουσική ή Εικόνες) είχε μετακινηθεί σε άλλη τοποθεσία, αλλά τα δεδομένα παρέμειναν στην αρχική θέση. Ο κύκλος ζωής του προϊόντος λογισμικού για τον διακομιστή 2019 επαναφέρθηκε σύμφωνα με τη νέα έκδοση στις 13 Νοεμβρίου 2018.

Τα Windows Server 2019 διαθέτουν τις ακόλουθες νέες δυνατότητες:

- Υποστήριξη για Kubernetes (Beta)
- Άλλες νέες δυνατότητες GUI από τα Windows 10 έκδοση 1809
  - Απευθείας χώροι αποθήκευσης
  - Υπηρεσία μετεγκατάστασης αποθήκευσης
  - Αντίγραφο αποθήκευσης
  - Πληροφορίες συστήματος
- Βελτιωμένο Windows Defender
- Κέντρο διαχείρισης των Windows

4.4. Σύγκριση των Windows Server και Linux

Κατά την επιλογή ενός λειτουργικού συστήματος διακομιστή, τα Windows διαθέτουν πολλές δυνατότητες για τις οποίες φυσικά και πληρώνονται. Το Linux είναι ανοιχτού κώδικα και ως εκ τούτου δεν διαθέτει την προσωποποιημένη υποστήριξη που έχει ένα πληρωμένο λειτουργικό.

Ας θεωρήσουμε τον διακομιστή ως λογισμικό για τον χειρισμό των εργασιών του υλικού. Το υλικό μπορεί να κυμαίνεται από έναν μόνο κεντρικό υπολογιστή συνδεδεμένο σε ένα εσωτερικό δίκτυο, έως μια σειρά υψηλής τεχνολογίας εξωτερικών υπηρεσιών υλικού στο cloud. Το αν θα χρησιμοποιήσετε Windows ή Linux ως λειτουργικό σύστημα του διακομιστή σας, εξαρτάται από τις επιχειρηματικές σας ανάγκες, την τεχνογνωσία σας και το λογισμικό που θέλετε να φορτώσετε. Ένας ακόμη παράγοντας επιλογής θα μπορούσε να είναι ο πάροχος με τον οποίο θέλετε να συνεργαστείτε.

Πλεονεκτήματα των Windows Server OS

Το πακέτο διακομιστή των Windows έχει σχεδιαστεί επαγγελματικά από τη Microsoft για να αποκομίσει κέρδος και ως εκ' τούτου έχει ορισμένα επιτακτικά πλεονεκτήματα. Πληρώνετε για το λειτουργικό και συνεπώς θα λαμβάνετε καλύτερη υποστήριξη από το ανοιχτό λογισμικό Linux, το οποίο είναι λίγο πολύ αναπτυγμένο και υποστηριζόμενο από την κοινότητα. Η υποστήριξη πελατών των Windows γίνεται μέσω της Microsoft και των μεταπωλητών της.

Οι εφαρμογές Windows (Outlook, Office, κ.λπ.) θα ενσωματωθούν αμέσως σε διακομιστές Windows. Εάν χρησιμοποιείτε λογισμικό και υπηρεσίες Windows, είναι λογικό να τα εκτελείτε σε μια εγγενή πλατφόρμα.

Εάν χρησιμοποιείτε backend βάσης δεδομένων που βασίζεται σε Microsoft SQL, δεν θα εκτελείται σε διακομιστή Linux, εκτός εάν εγκαταστήσετε έναν εξομοιωτή Windows. Για να το κάνετε αυτό, πρέπει να αγοράσετε ένα αντίγραφο των Windows και του λογισμικού της βάσης δεδομένων ξεχωριστά.

Ο διακομιστής των Windows θεωρείται συχνά μια ολοκληρωμένη λύση που είναι γρήγορη και εύκολη στην εγκατάσταση. Εάν θέλετε πρόσβαση σε απομακρυσμένη επιφάνεια εργασίας με ένα διαισθητικό γραφικό περιβάλλον εργασίας χρήστη, τα Windows το προσφέρουν χωρίς να χρειάζεται να εκτελείτε εντολές στο terminal που απαιτείται από το Linux.

Τα Windows Server παρέχουν ένα ASP (Active Server Page), είναι μια ιστοσελίδα που περιλαμβάνει μικρά ενσωματωμένα προγράμματα, δηλαδή σενάρια. Τα σενάρια και οι ιστοσελίδες που δημιουργείτε με αυτά τα προγράμματα θα εκτελούνται μόνο σε διακομιστή Windows. Ο διακομιστής Microsoft επεξεργάζεται αυτά τα σενάρια πριν από τη φόρτωση της σελίδας για έναν χρήστη. Αυτό δεν είναι δυνατό με το Linux.

Οφέλη των διακομιστών Linux έναντι των Windows

Το Linux είναι ένα λειτουργικό σύστημα ανοιχτού κώδικα (OS) και μια πλατφόρμα υποδομής πληροφορικής που επιτρέπει διανομές όπως το Ubuntu, το Fedora και το CentOS. Ο πηγαίος κώδικας του είναι διαθέσιμος για τους προγραμματιστές ώστε να τον αλλάξουν και να ενημερώσουν τον τρόπο λειτουργίας του λογισμικού. Οι χρήστες μπορούν να επεξεργαστούν χαρακτηριστικά ή να διορθώσουν σφάλματα.
Το Linux, επειδή είναι ανοιχτού κώδικα, είναι δωρεάν. Οι πάροχοι Business Server δεν χρειάζεται να μεταφέρουν επιπλέον έξοδα στον πελάτη. Από την άλλη πλευρά, με διακομιστές Windows, η εταιρεία συνήθως πρέπει να πληρώσει για το λειτουργικό σύστημα και μια άδεια περιοδικής χρήσης.
Το Linux έχει άμεση συμβατότητα με άλλα προϊόντα λογισμικού ανοιχτού κώδικα και παρέχει μια γρήγορη διεπαφή με απρόσκοπτη συμβατότητα. Οι χρήστες Linux μπορούν να εκτελέσουν προγράμματα Windows, αλλά πρέπει να αγοράσουν λογισμικό διεπαφής και να πληρώσουν για άδεια χρήσης των Windows. Αυτό είναι βολικό όταν έχετε εφαρμογές παλαιού τύπου που πρέπει να εκτελούνται σε εξομοιωτή Windows.
Οι διακομιστές Linux και οι εφαρμογές που εκτελούν χρησιμοποιούν γενικά λιγότερους πόρους υπολογιστών, καθώς έχουν σχεδιαστεί για να λειτουργούν έτσι. Ένα πλεονέκτημα είναι ότι οι προγραμματιστές μπορούν να τροποποιήσουν τους διακομιστές και το λογισμικό Linux κατά τη λειτουργία και χωρίς επανεκκίνηση, κάτι που δεν είναι δυνατό σε περιβάλλον Windows. Οι διακομιστές των Microsoft Windows τείνουν να επιβραδύνονται με εργασίες πολλαπλών βάσεων δεδομένων, με υψηλότερο κίνδυνο διακοπής λειτουργίας.
Παρόλο που κανένα σύστημα δεν είναι απρόσβλητο από επιθέσεις σε hacking και malware, το Linux τείνει να είναι ένας στόχος χαμηλού προφίλ. Επειδή τα Windows χρησιμοποιούν την πλειονότητα του λογισμικού στον κόσμο, οι hacker προτιμούν τα Windows για τις επιθέσεις τους.

Σύγκριση των δύο λειτουργικών

Τώρα που έχουμε περιγράψει με λίγα λόγια τόσο τα Windows όσο και το Linux, ας κάνουμε μερικές τελικές συγκρίσεις:

- ✓ Η καμπύλη μάθησης για την εγκατάσταση και διαχείριση ενός διακομιστή Linux είναι μεγάλη. Οι χρήστες των Windows δεν χρειάζεται να είναι ειδικοί προγραμματισμού για την προσαρμογή του διακομιστή.
- ✓ Το Linux είναι μια καλύτερη επιλογή για προγραμματιστές ιστού που μπορούν να διαμορφώσουν έναν διακομιστή Apache ή NGINX ανοιχτού κώδικα. Ομοίως, οι προγραμματιστές που εργάζονται με βάση δεδομένων MySQL γνωρίζουν ότι τα εργαλεία

ανάπτυξης Perl, PHP ή Python είναι μακροχρόνια αγαπημένα, με ευρύτερη διαδικτυακή υποστήριξη της κοινότητας.

- ✓ Ένα πακέτο διακομιστή Windows περιλαμβάνει τεχνική υποστήριξη, μαζί με τακτικές αναβαθμίσεις συστήματος και διορθώσεις ασφαλείας. Η τεχνολογία Linux προχώρησε με πιο αργό ρυθμό αλλαγής. Δεν χρειάζεται να κάνετε αναβάθμιση για δυνατότητες που μπορεί να μην χρειάζεστε συνεχώς. Μπορείτε να προσθέσετε μόνοι σας αυτές τις δυνατότητες στο Linux.
- ✓ Η υποστήριξη των Windows συνοδεύεται από το προϊόν, συνεπώς θα έχετε 24ωρη υποστήριξη. Το Linux δεν παρέχει τέτοιου είδους υποστήριξη καθώς είναι δωρεάν και οι απαντήσεις στην κοινότητα του Linux μπορεί να μην είναι τόσο γρήγορες.

5. Εγκατάσταση Windows Server 2008

5.1. Απαιτήσεις συστήματος

Όπως σε οποιαδήποτε άλλη έκδοση των Windows, έτσι και τα Windows Server 2008 απαιτούν ένα ελάχιστο επίπεδο υλικού. Τα Windows Server 2008 διατίθενται σε πολλές εκδόσεις για την υποστήριξη των διαφορετικών αναγκών διακομιστών και φόρτου εργασίας των οργανισμών. Οι τέσσερις κύριες εκδόσεις περιλαμβάνουν Windows Server 2008 Standard, Windows Server 2008 Enterprise, Windows Server Datacenter 2008 και Windows Web Server 2008.

Στον πίνακα 5.1 συνοψίζουμε τις απαιτήσεις για την κάθε έκδοση.

Requirements	Minimum	Recommended	Optimal (Sever Core)	Optimal (Full Install)	Datacenter and Itanium Editions	Web and Standard Editions	Enterprise Edition
CPU Speed	1 GHz (x86) 1.4 GHz (x64)	2 GHz or faster	3 GHz or more	3 GHz or more			
RAM	512 MB	2 GB or more	1 GB or more	2 GB or more			
Disk Space for Setup	10 GB	40 GB or more	40 GB or more	40 GB or more			
Minimum Number of CPUs	1	2	2	2	8	1	1
Maximum Number of CPUs					64	4	8
Additional Drives	DVD-ROM	DVD-ROM	DVD-ROM	DVD-ROM	DVD-ROM	DVD-ROM	DVD-ROM
Video Mode: Minimum	SVGA (800 x 600) or higher	SVGA (800 x 600) or higher	SVGA (800 x 600) or higher	SVGA (800 x 600) or higher	SVGA (800 x 600) or higher	SVGA (800 x 600) or higher	SVGA (800 x 600) or higher

Πίνακας 5.1

Επειδή το μέγιστο υποστηριζόμενο μέγεθος της μνήμης RAM εξαρτάται, εκτός από την έκδοση, από την αρχιτεκτονική του συστήματος (32-bit ή 64-bit) στον πίνακα 5.2 παρουσιάζεται το μέγιστο υποστηριζόμενο μέγεθος για κάθε έκδοση των Windows Server.

Requirements	32-bit Web and Standard Editions	32-bit Enterprise and Datacenter Editions	64-bit Web and Standard Editions	64-bit Enterprise, Datacenter, and Itanium Editions
Maximum RAM	4 GB	64 GB	32 GB	2 TB

Πίνακας 5.2

Επίσης να σημειωθεί ότι υπολογιστές με RAM μεγαλύτερη από 16 GB χρειάζονται περισσότερο χώρο στον δίσκο για λειτουργίες του λειτουργικού, όπως paging, hibernation και dump files.

Συνήθως δεν εγκαθιστούμε έναν server με τις ελάχιστες απαιτήσεις. Κάνουμε έναν σχεδιασμό ανάλογα με τις ανάγκες μας και διαλέγουμε το υλικό που θα χρησιμοποιήσουμε. Παρακάτω παρουσιάζουμε κάποια βασικά πράγματα που λαμβάνουμε υπόψιν βάση των αναγκών μας.

- **Φυσικός ή εικονικός:** Γενικά όλοι οι φυσικοί διακομιστές είναι κεντρικοί διακομιστές και όλες οι υπηρεσίες είναι εικονικές.
- **Φυσικοί hosts:** Είναι σημαντικό να προσδιορίσουμε ένα μέγιστο αριθμό hosts ανά διακομιστή κεντρικού υπολογιστή για να διασφαλίσουμε ότι παρέχεται ένα δεδομένο επίπεδο των υπηρεσιών. Θα πρέπει να έχουμε υπόψιν ότι για να μπορέσουμε να εκτελέσουμε το Hyper-V οι φυσικοί διακομιστές θα πρέπει να είναι 64-bit. Εάν είναι 32-bit τότε θα πρέπει να χρησιμοποιήσουμε άλλο virtualization πρόγραμμα.
- **Επισκέπτες, αριθμός χρηστών ανά server:** πρέπει να προσδιοριστεί ένας μέγιστος αριθμός χρηστών ανά διακομιστή. Για να παρέχεται ένα δεδομένο επίπεδο υπηρεσίας, πρέπει να διασφαλιστεί ότι δεν υπάρχουν ποτέ περισσότεροι από έναν συγκεκριμένο αριθμό χρηστών
- **Μέγιστο αποδεκτό φορτίο διακομιστή:** Προσδιορίστε την ταχύτητα απόκρισης που θέλετε από έναν διακομιστή κατά την παροχή μιας δεδομένης υπηρεσίας. Για διακομιστές κεντρικού υπολογιστή, αυτό το φορτίο εξαρτάται κυρίως από την CPU και την RAM, είναι τα σημεία συμφόρησης. Για λειτουργικά συστήματα επισκεπτών, πρέπει να ληφθεί υπόψη ο αριθμός των χρηστών. Ένας καλός τρόπος για να γίνει αυτό είναι η παρακολούθηση της CPU και απόδοση εισόδου και εξόδου (I / O) στο διακομιστή.
- **Ελάχιστη χωρητικότητα διακομιστή:** Πρέπει να καθοριστεί η ελάχιστη χωρητικότητα υλικού για τους κεντρικούς διακομιστές με δεδομένο ότι δεν θα αλλαχθούν για κάποιο χρονικό διάστημα. Ο σχεδιασμός χωρητικότητας πρέπει να προσδιορίζει στοιχεία όπως ο αριθμός και το μέγεθος των επεξεργαστών, το μέγεθος της μνήμης RAM και το μέγεθος δίσκου.
- **Πολυεπεξεργασία και πολλαπλοί πυρήνες:** Εδώ θα πρέπει να δοθεί προσοχή και στο λειτουργικό σύστημα καθώς υπάρχει σαφής οριοθέτηση μεταξύ των

απαιτήσεων του λειτουργικού συστήματος. Στον πίνακα 5.1 γίνεται μία παρουσίαση των απαιτούμενων αριθμών πυρήνων.

- **Μέγεθος RAM:** Ο κανόνας είναι απλός: Όσο περισσότερη RAM τόσο καλύτερη απόδοση θα έχει διακομιστής. Όλα εξαρτώνται από το λειτουργία οποιουδήποτε δεδομένου διακομιστή, αλλά είναι καλός κανόνας να διπλασιάσουμε τις ελάχιστες απαιτήσεις της Microsoft και να ξεκινήσουμε με τουλάχιστον 4 GB μνήμης RAM. Ορισμένες λειτουργίες του διακομιστή χρειάζονται αρκετή RAM, όπως διακομιστές Terminal Services, εικονικοί κεντρικοί υπολογιστές ή διακομιστές εφαρμογών. Επιπλέον, το μέγεθος RAM επηρεάζει το αρχείο σελιδοποίησης. Ο καλύτερος κανόνας εδώ είναι για να ξεκινήσουμε το αρχείο σελιδοποίησης σε διπλάσιο μέγεθος της μνήμης RAM και να ορίσουμε το μέγιστο μέγεθος σε τέσσερις φορές το μέγεθος της μνήμης RAM.
- **Μέγεθος δίσκου:** Το μέγεθος και ο αριθμός των δίσκων που τοποθετούνται σε κάθε διακομιστή εξαρτάτε από διάφορους παράγοντες, όπως πόσα διαμερίσματα θα δημιουργήσουμε, πόσος χώρο θα κρατήσουμε για το λειτουργικό σύστημα, τα προγράμματα και τα ειδικά στοιχεία όπως το αρχείο σελιδοποίησης, πόσο χώρο θέλουμε για αποθήκευση δεδομένων κτλ. Μπορούμε να λάβουμε υπόψη ότι ο Windows Server 2008 προσφέρει καλύτερη απόδοση όταν διαβάζει και γράφει σε πολλούς δίσκους.

5.2. Διαδικασία εγκατάστασης

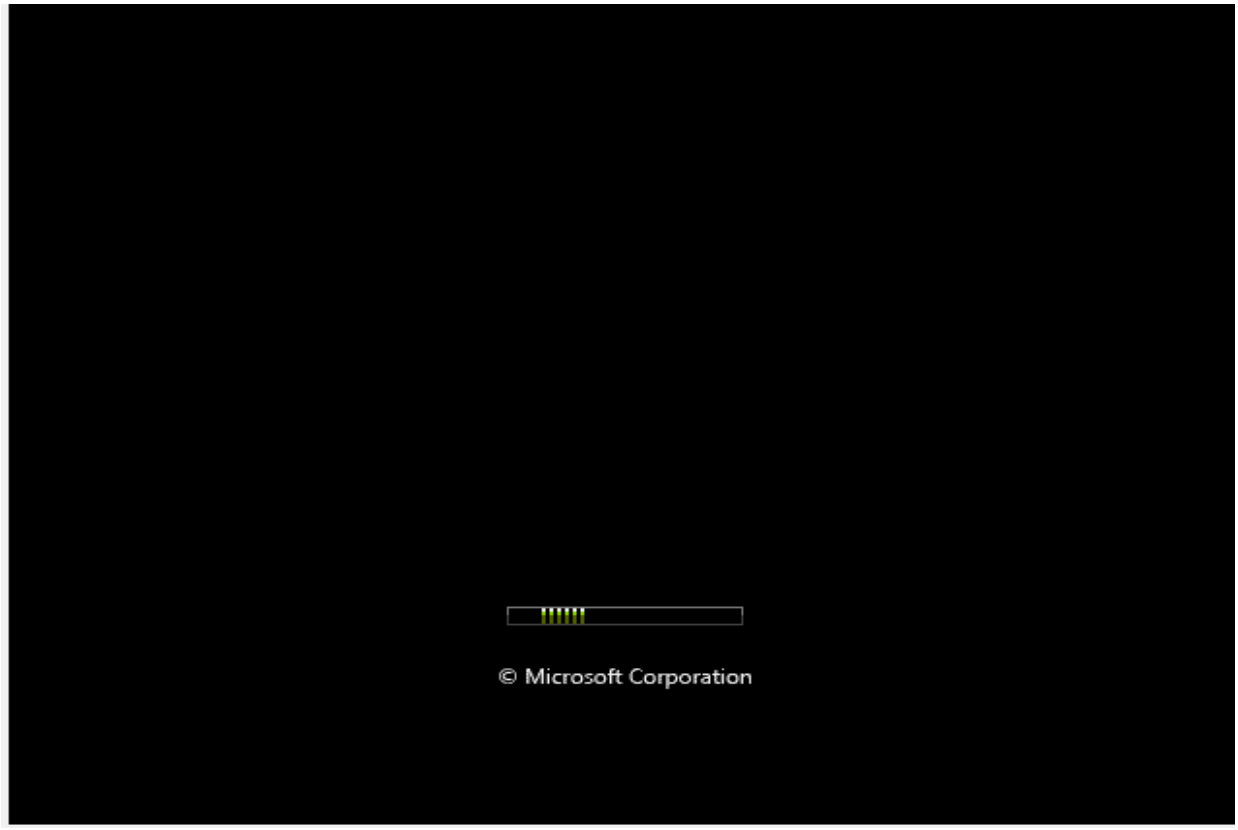
Τα παρακάτω βήματα περιγράφουν λεπτομερώς τη διαδικασία εγκατάστασης των Windows Server 2008. Η εν λόγω εγκατάσταση πραγματοποιήθηκε σε εικονικό μηχάνημα με χαρακτηριστικά:

- CPU: 4
- Memory: 4096 MB
- Hard drive: 40 GB

Μετά από την ολοκλήρωση download ενός αρχείου .iso με δυνατότητα εκκίνησης (bootable), το προσθέτουμε στον εικονικό δίσκο (virtual drive) του VM μας. Σε όλη αυτή την εγκατάσταση, δεχόμαστε τις προεπιλεγμένες επιλογές. Το σύστημά μας θα πρέπει να διαμορφωθεί για εκκίνηση από το virtual drive. Σε πραγματικό μηχάνημα θα πρέπει να ρυθμίσουμε το bios έτσι ώστε να ξεκινήσει ο υπολογιστής μας φορτώνοντας από το DVD-ROM.
Μετά την τοποθέτηση του αρχείου iso (αντίστοιχα DVD-ROM σε πραγματικό μηχάνημα) των Windows Server 2008 στη μονάδα virtual drive του Virtual Machine (DVD-ROM αντίστοιχα για το πραγματικό) γίνεται εκκίνηση του υπολογιστή μας. Εάν σας ζητηθεί να πατήσετε ένα πλήκτρο για εκκίνηση από το DVD, κάντε το. Μόλις ξεκινήσει η εγκατάσταση φορτώνονται τα απαραίτητα αρχεία των Windows Server 2008 όπως παρατηρούμε στις παρακάτω εικόνα.

Εικόνα 5.1

Μόλις φορτωθούν τα απαραίτητα αρχεία των windows προετοιμάζεται το αντίστοιχο GUI (Graphic User Interface) για τις επιλογές εγκατάστασης όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 5.2

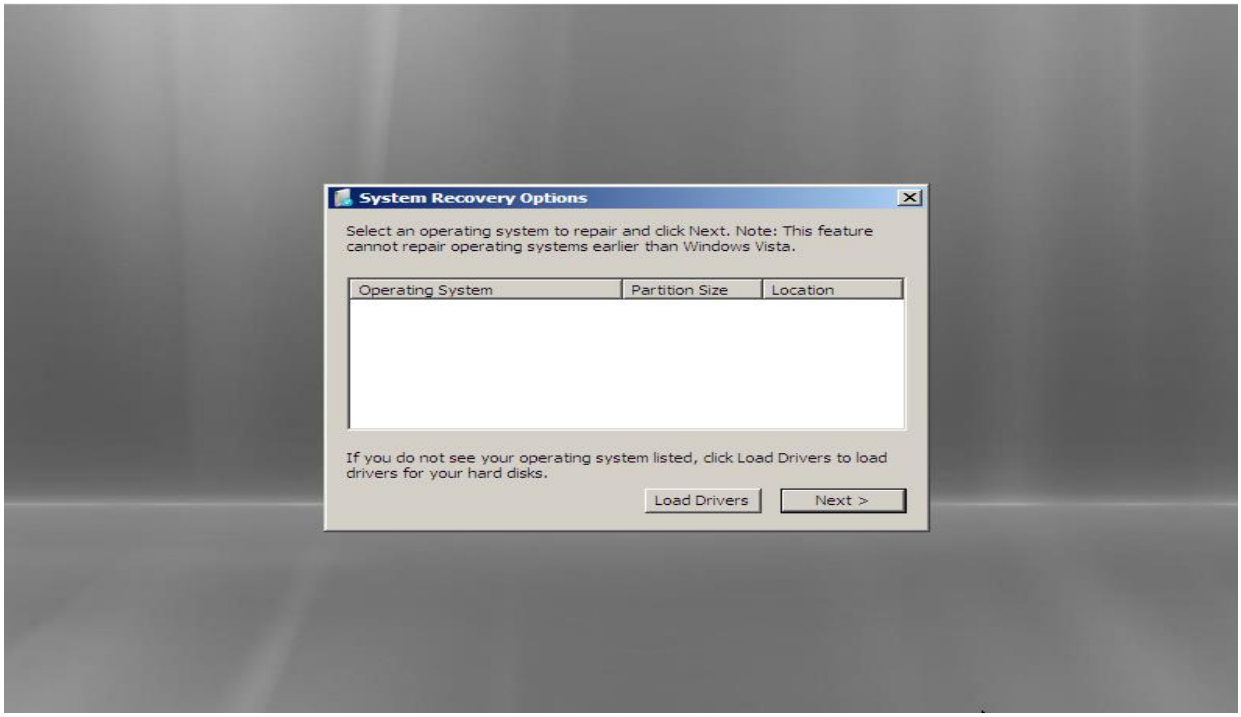
Αφού ολοκληρωθεί η φόρτωση του GUI εμφανίζεται μια γκρι οθόνη με τρεις άλλες επιλογές:

- ✓ Επιλογή γλώσσας εγκατάστασης
- ✓ Ώρα και μορφή νομίσματος
- ✓ Πληκτρολόγιο και μέθοδοι εισαγωγής πληκτρολογίου.

Επιλέγουμε την γλώσσα που επιθυμούμε για το λειτουργικό μας. Στη συνέχεια επιλέγουμε το format της ώρας και το νόμισμα, επιλέγουμε κατά την είσοδο μας στο λειτουργικό τη γλώσσα πληκτρολογίου που επιθυμούμε και τέλος πατάμε επόμενο βήμα (Next). Παρακάτω φαίνεται η εικόνα με τις παραπάνω επιλογές που μπορούμε να έχουμε.

Εικόνα 5.3

Στο επόμενο βήμα ο οδηγός εγκατάστασης έχει επιλογή για το τι πρέπει να γνωρίζουμε πριν από την εγκατάσταση των Windows αλλά και για επισκευή των Windows σε περιπτώσεις fail boot μίας ήδη υπάρχουσας εγκατάστασης των Windows. Η επισκευή φαίνεται στην παρακάτω εικόνα που εδώ δεν βρίσκει κάποια προϋπάρχουσα έκδοση επειδή πρόκειται για αρχική εγκατάσταση.

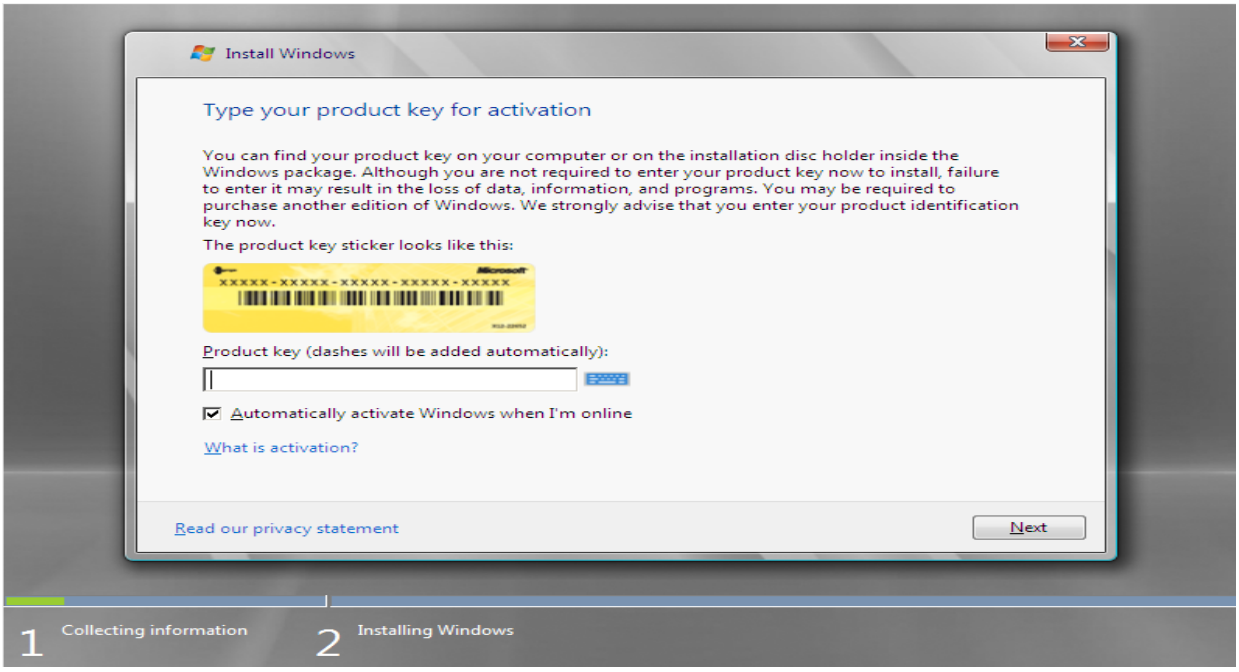


Εικόνα 5.4

Εφόσον πρόκειται για αρχική εγκατάσταση επιλέγουμε Εγκατάσταση Τώρα (Install Now). Οι επιλογές φαίνονται στην παρακάτω εικόνα.

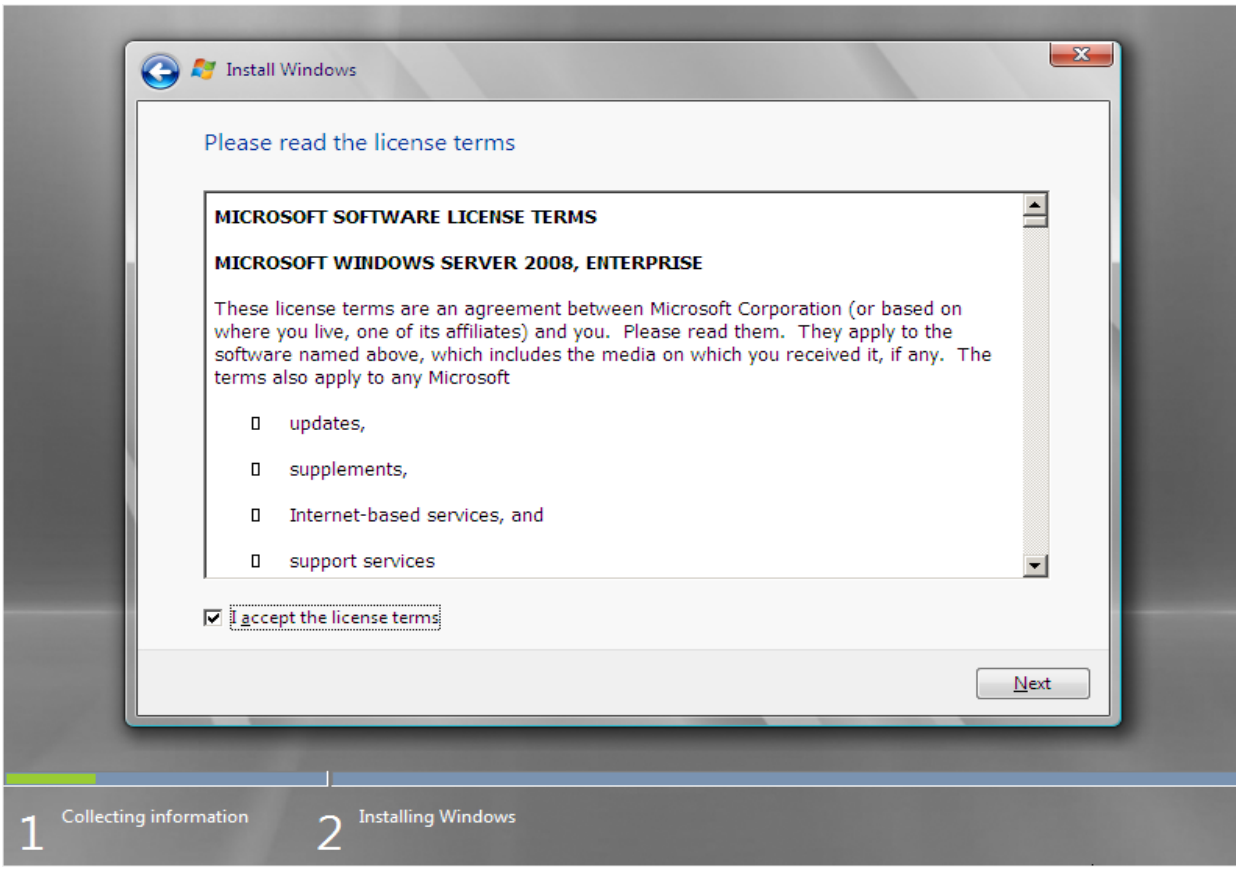
Εικόνα 5.5

Στη παρακάτω εικόνα ζητείται το product key του προϊόντος της Microsoft προκειμένου να ενεργοποιηθεί. Το τοποθετούμε και κάνουμε check την επιλογή εάν επιθυμούμε ενεργοποίηση του προϊόντος όταν θα έχουμε πρόσβαση στο internet. Μπορούμε επίσης να διαβάσουμε και τη δήλωση απορρήτου. Στην παρακάτω εικόνα φαίνονται οι επιλογές μας.



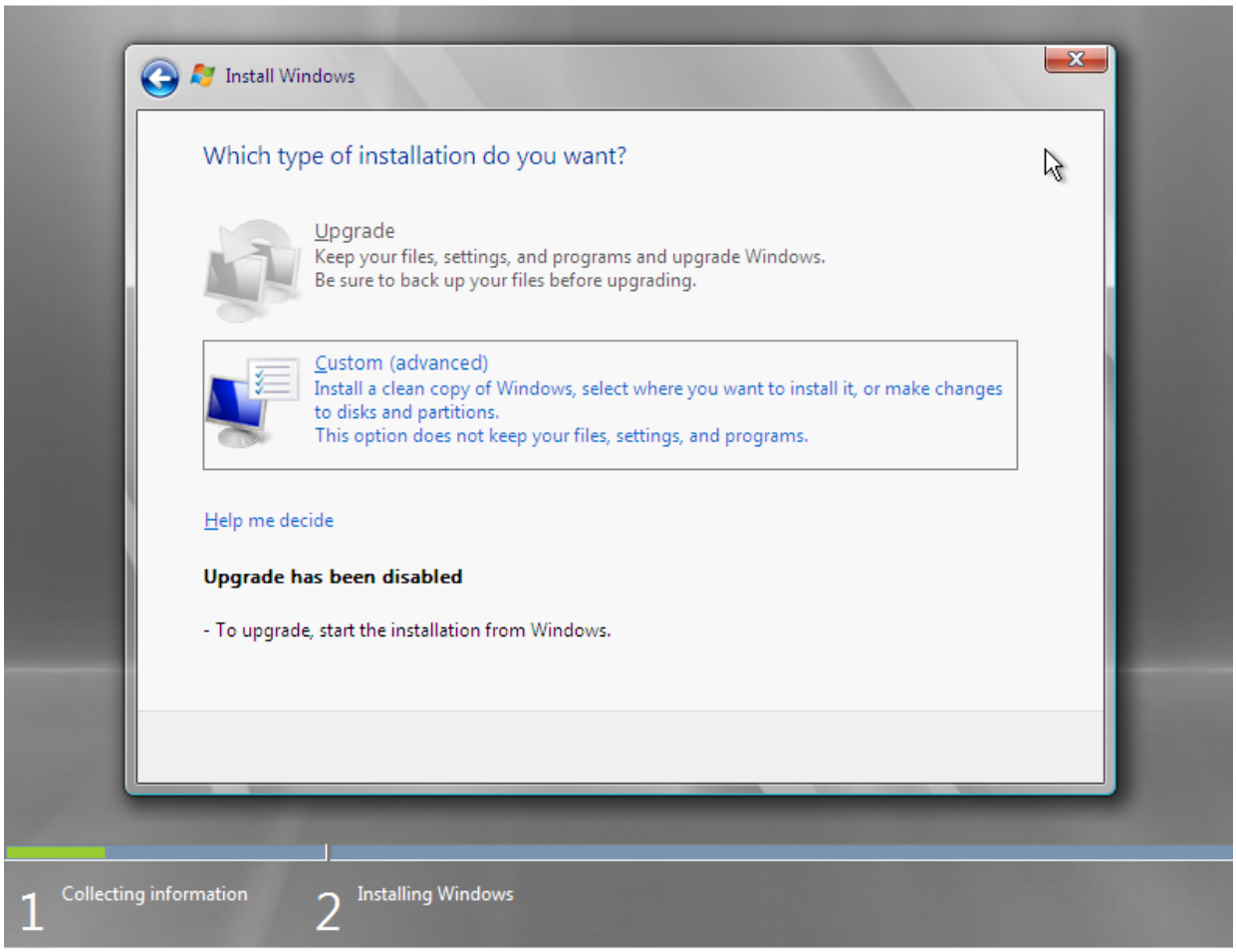
Εικόνα 5.6

Αποδεχόμαστε τους όρους χρήσης και στη συνέχεια πατάμε επόμενο (Εικόνα 5.6)



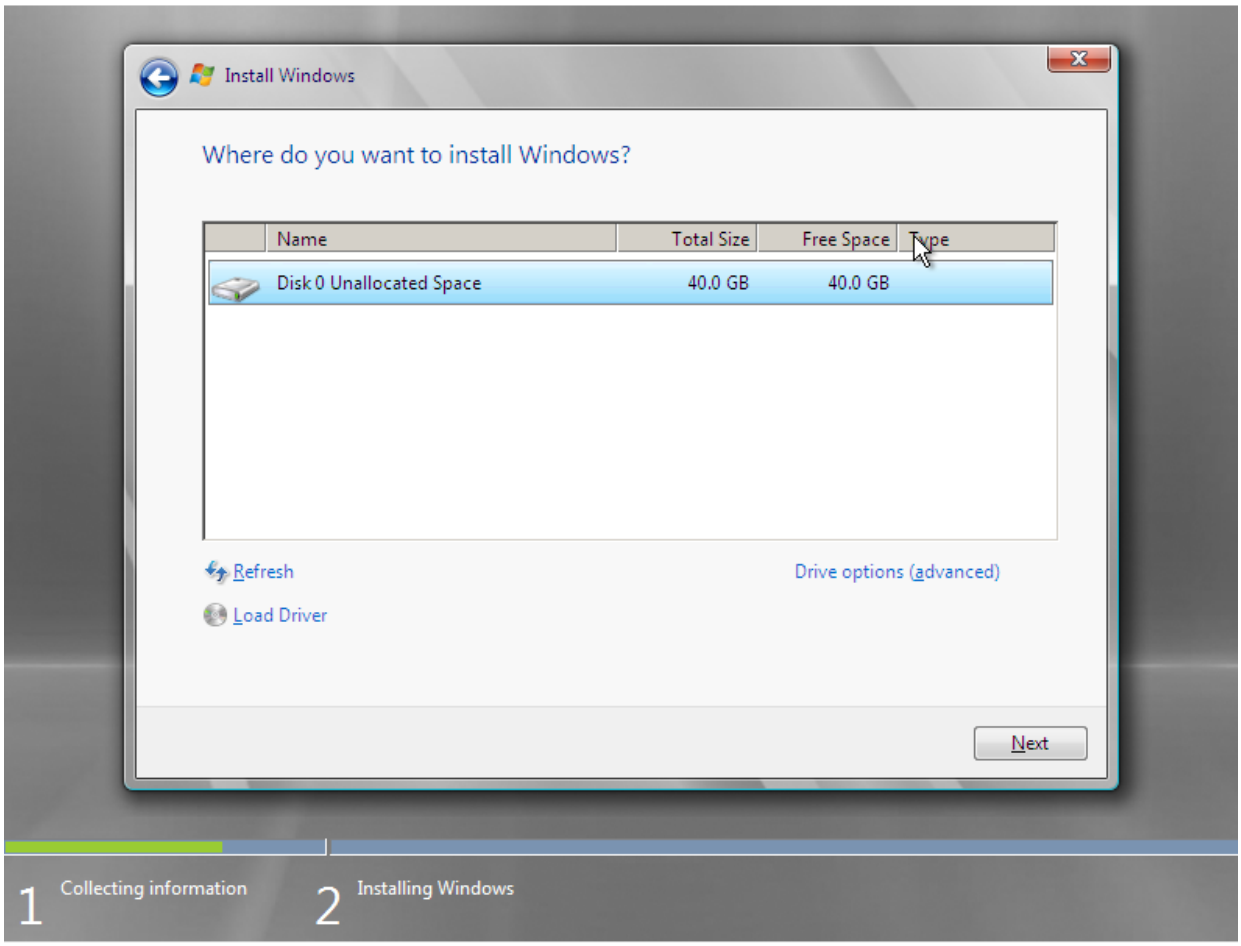
Εικόνα 5.7

Στη συνέχεια εμφανίζονται δύο επιλογές, Αναβάθμιση (Upgrade) και Προσαρμογή (Custom) σε αυτό το παράθυρο διαλόγου. Ο τύπος άδειας που έχουμε (αναβάθμιση ή πλήρης εγκατάσταση) καθορίζει ποια από τις επιλογές θα είναι διαθέσιμες. Επίσης εάν έχουμε μία πιο παλιά έκδοση των Windows Server θα μπορούσαμε να επιλέξουμε και πάλι Upgrade για να μην χάσουμε τις ρυθμίσεις και τα προγράμματα που ήδη έχουν εγκατασταθεί στην πιο παλιά έκδοση ή να ξεκινήσουμε το λειτουργικό μας κανονικά και αφού ήδη έχουμε εισαχθεί στην επιφάνεια εργασίας μέσω του DVD-ROM εγκατάστασης να υλοποιήσουμε την αναβάθμιση.
Στην εν λόγω εγκατάσταση που υλοποιούμε επειδή δεν υπάρχει καμία προηγούμενη έκδοση λειτουργικού συστήματος των Windows Server μας έχει απενεργοποιημένη την επιλογή Upgrade. Οπότε όπως φαίνεται και στην παρακάτω εικόνα επιλέγουμε Custom install.



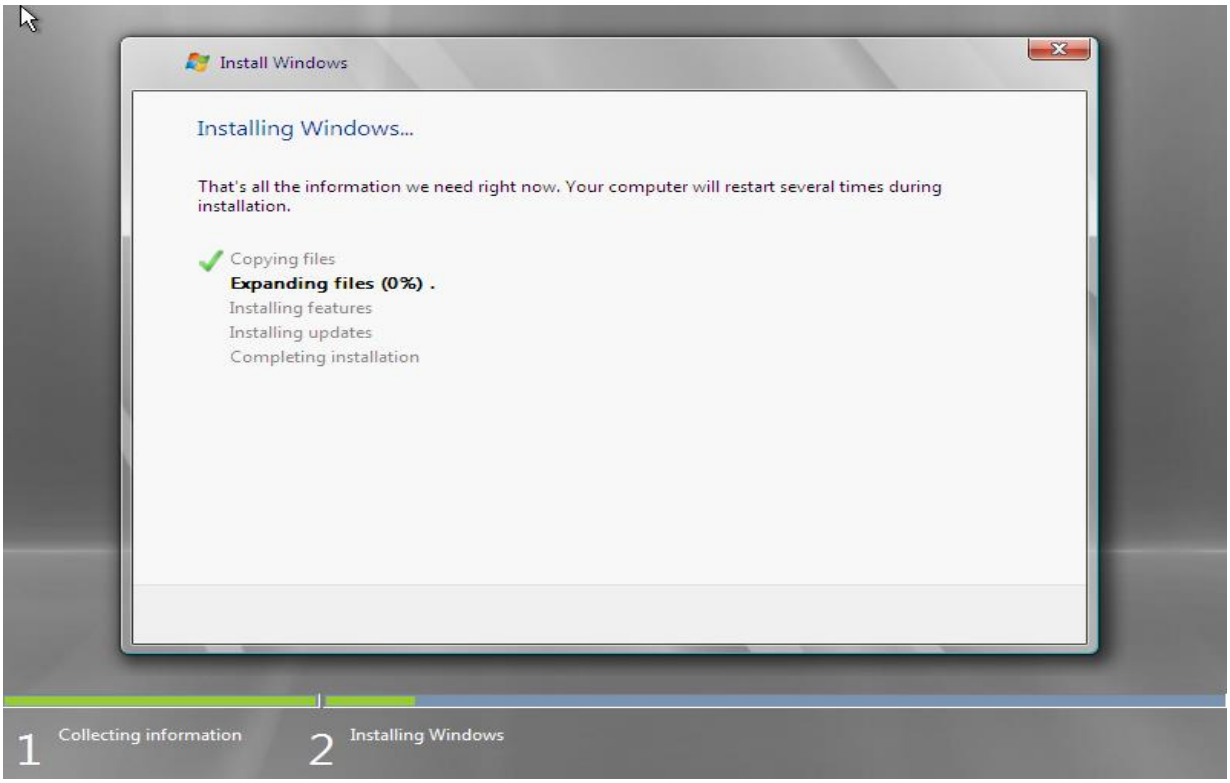
Εικόνα 5.8

Στη συνέχεια επιλέγουμε τη μονάδα δίσκου στην οποία θέλουμε να εγκαταστήσουμε τα Windows Server 2008. Εάν έχουμε μόνο ένα partition ενός δίσκου, δεν χρειάζεται να προσέξουμε κάτι κατά την εγκατάσταση γιατί θα εγκατασταθούν στο ένα και μοναδικό partition του δίσκου μας. Σε διαφορετική περίπτωση, εάν έχουμε περισσότερα του ενός partition θα πρέπει να γνωρίζουμε σε ποιο partition θα γίνει η εγκατάσταση γιατί διαφορετικά όλα τα δεδομένα που υπάρχουν σε αυτό το διαμέρισμα του δίσκου θα χαθούν. Οπότε χρειάζεται ιδιαίτερη προσοχή εάν έχουμε περισσότερα του ενός διαμερίσματα και φρόνιμο είναι να γνωρίζουμε εκ των προτέρων το μέγεθος του δίσκου που θα πραγματοποιήσουμε την εγκατάσταση.
Μπορούμε επίσης να κάνουμε κλικ στην επιλογή Ανανέωση για να ενημερωθεί η λίστα με τα διαθέσιμα διαμερίσματα ή να κάνουμε φόρτωση προγράμματος οδήγησης για να προστεθούν οποιαδήποτε υποστηρικτικά αρχεία που χρειάζονται για τη διαδικασία εγκατάστασης.
Χρησιμοποιώντας τα πλήκτρα βέλους για να επιλέξουμε το διαμέρισμα που επιθυμούμε επιλέγουμε το διαμέρισμα και στη συνέχεια κάνουμε κλικ στο Επόμενο. Στην παρακάτω εικόνα φαίνονται οι παραπάνω επιλογές.

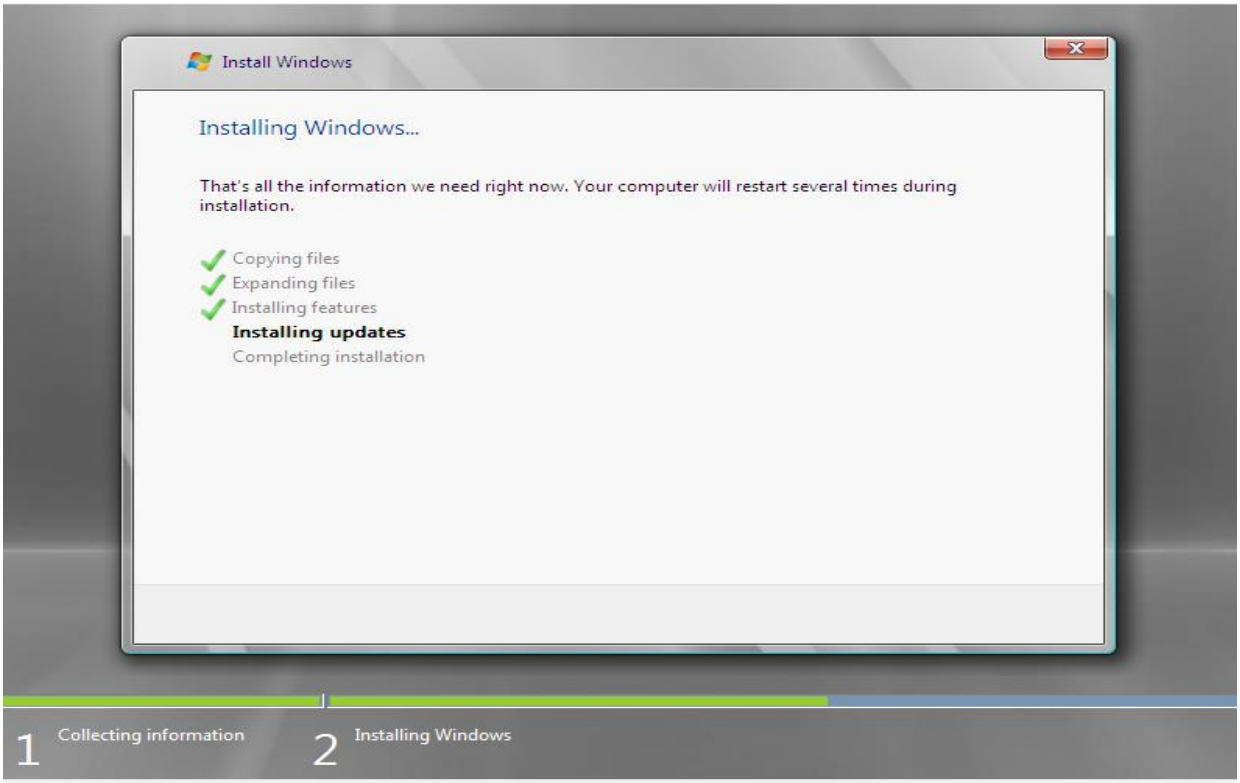


Εικόνα 5.9

Αφού κάνουμε κλικ στο Επόμενο, εμφανίζεται το παράθυρο διαλόγου Εγκατάσταση των Windows χωρίς επιλογές για να διαλέξουμε. Η εγκατάσταση ξεκινά την επεξεργασία της εγκατάστασης των Windows Server 2008 όπου το παράθυρο διαλόγου υποδεικνύει κάθε βήμα (από την αντιγραφή και την επέκταση αρχείων μέχρι την εγκατάσταση ενημερώσεων και ολοκλήρωση της εγκατάστασης) στην πορεία.
Η εγκατάσταση αφιερώνει σημαντικό χρονικό διάστημα για τη διαμόρφωση της μονάδας δίσκου, ειδικά για μεγάλα partition. Αφού ολοκληρωθεί η μορφοποίηση, το Setup ελέγχει τους σκληρούς δίσκους μας, δημιουργεί μια λίστα αρχείων και, στη συνέχεια, αντιγράφει ένα μεγάλο όγκο αρχείων, από το αρχείο iso λόγω του VM ή το DVD σε πραγματικό μηχάνημα, στη νέα μορφή. Ρύθμιση αντιγράφων και επέκταση αρχείων, εγκατάσταση λειτουργιών και ενημερώσεων και στη συνέχεια ολοκλήρωση της εγκατάστασης. Στις παρακάτω εικόνες παρουσιάζονται τα βήματα εγκατάστασης αρχείων των Windows Server 2008.

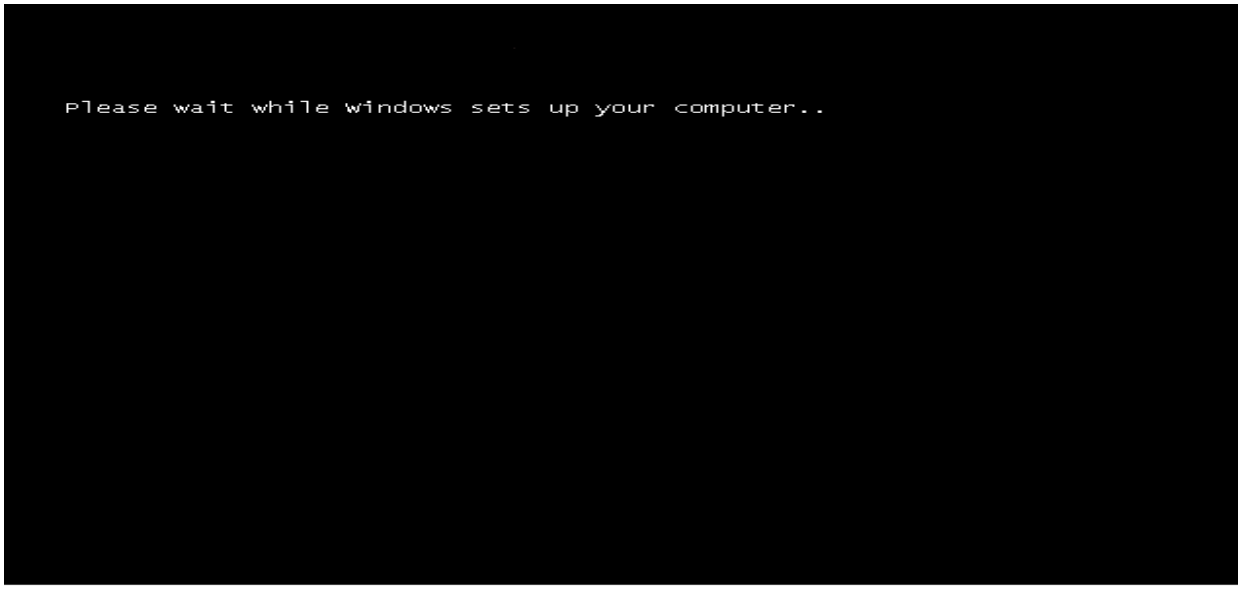


Εικόνα 5.10

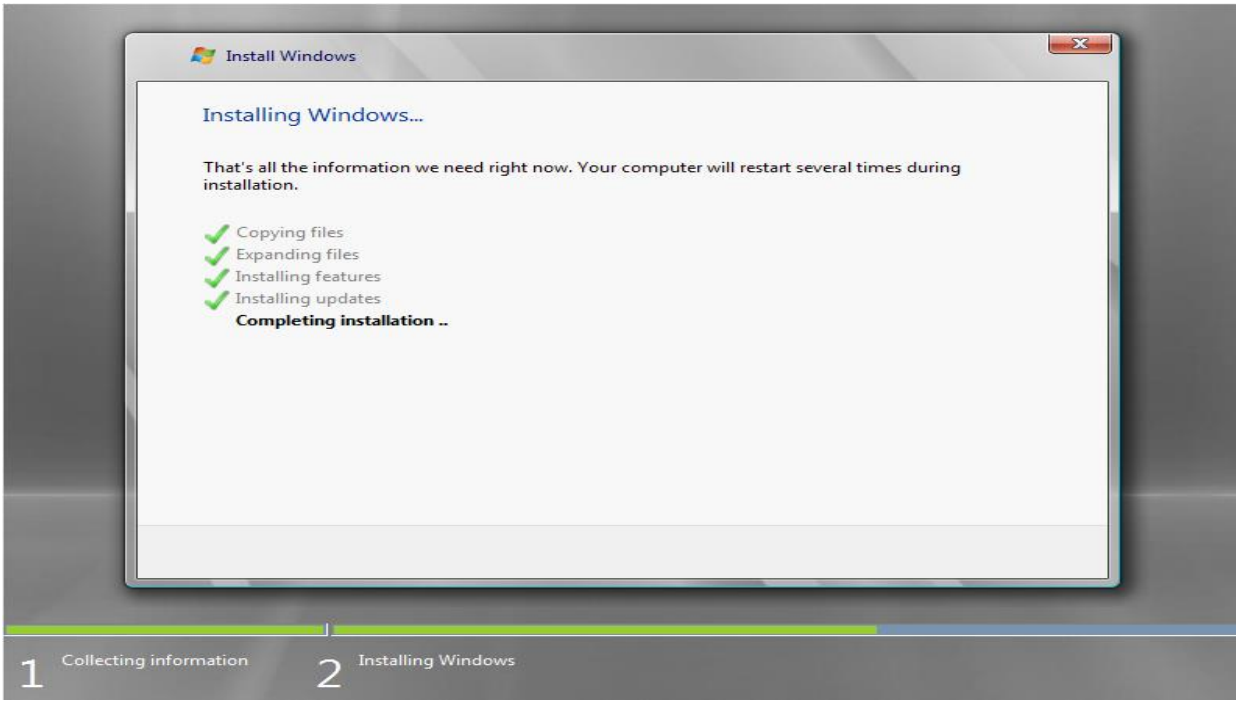


Εικόνα 5.11

Μετά την ολοκλήρωση της εγκατάστασης εμφανίζεται ένα μήνυμα που αναφέρει ότι το σύστημα θα επανεκκινήσει. Μπορούμε να πατήσουμε το πλήκτρο του Enter για άμεση επανεκκίνηση ή να περιμένουμε 15 δευτερόλεπτα για αυτόματη επανεκκίνηση.
Μετά την επανεκκίνηση του συστήματος δεν πατάμε κάποιο πλήκτρο για να φορτώσει πάλι το DVD εγκατάστασης των Windows Server 2008. Στη συνέχεια το πρόγραμμα εγκατάστασης των Windows Server 2008 σαρώνει τον υπολογιστή για συσκευές και εγκαθιστά κατάλληλα προγράμματα οδήγησης. Στις παρακάτω εικόνες παρουσιάζεται αυτή η λειτουργία.

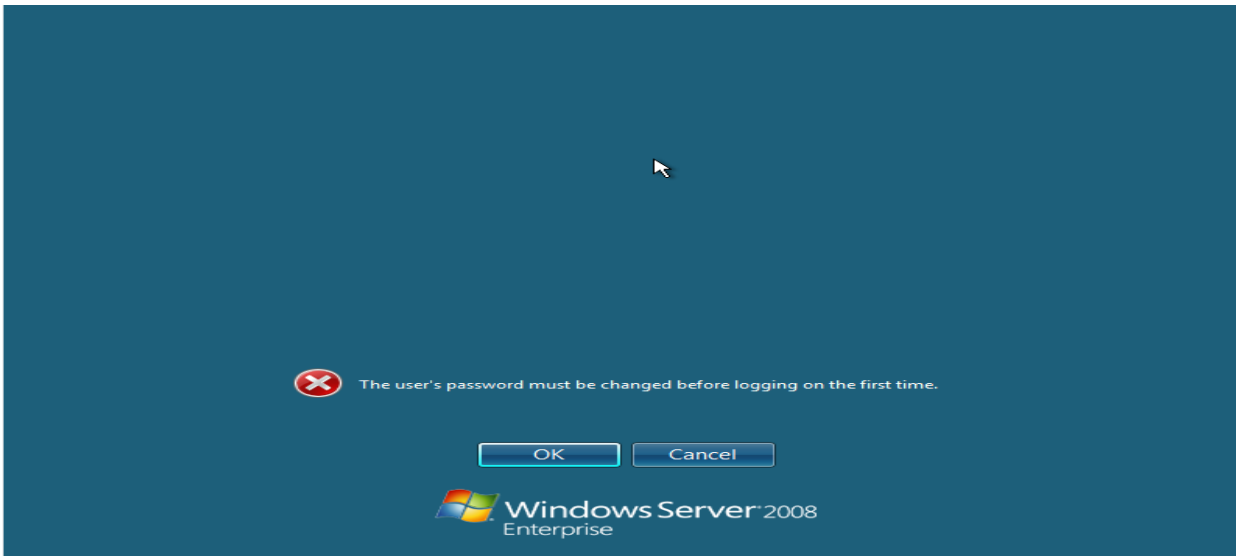


Εικόνα 5.12



Εικόνα 5.13

Εφόσον έχουν ολοκληρωθεί οι παραπάνω εργασίες το σύστημά μας εκτελεί πάλι επανεκκίνηση και μόλις επανέλθει, παρουσιάζεται το αρχικό παράθυρο διαλόγου όπου ζητείται εάν επιθυμούμε αλλαγή κωδικού πρόσβασης. Εάν επιλέξουμε ακύρωση ο κωδικός Administrator θα είναι κενός, κάτι το οποίο δεν προτείνεται. Στην παρακάτω εικόνα φαίνεται η εν λόγω λειτουργία.



Εικόνα 5.14

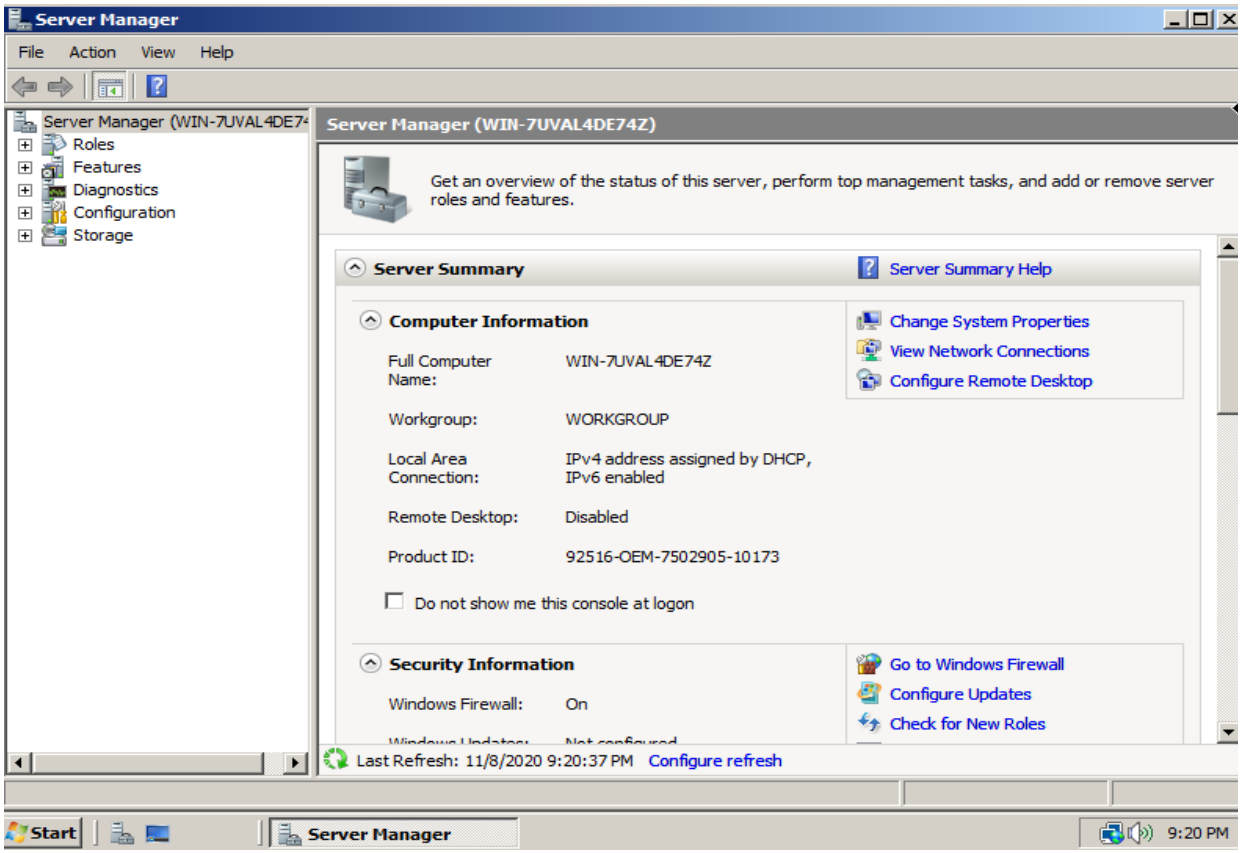
Κάνουμε κλικ στην επιλογή OK και στη συνέχεια μας παρουσιάζεται το παρακάτω παράθυρο διαλόγου όπου ορίζουμε τον κωδικό πρόσβασης διαχειριστή. Θεμιτό είναι να επιλέξουμε έναν ισχυρό κωδικό πρόσβασης.

Εικόνα 5.15

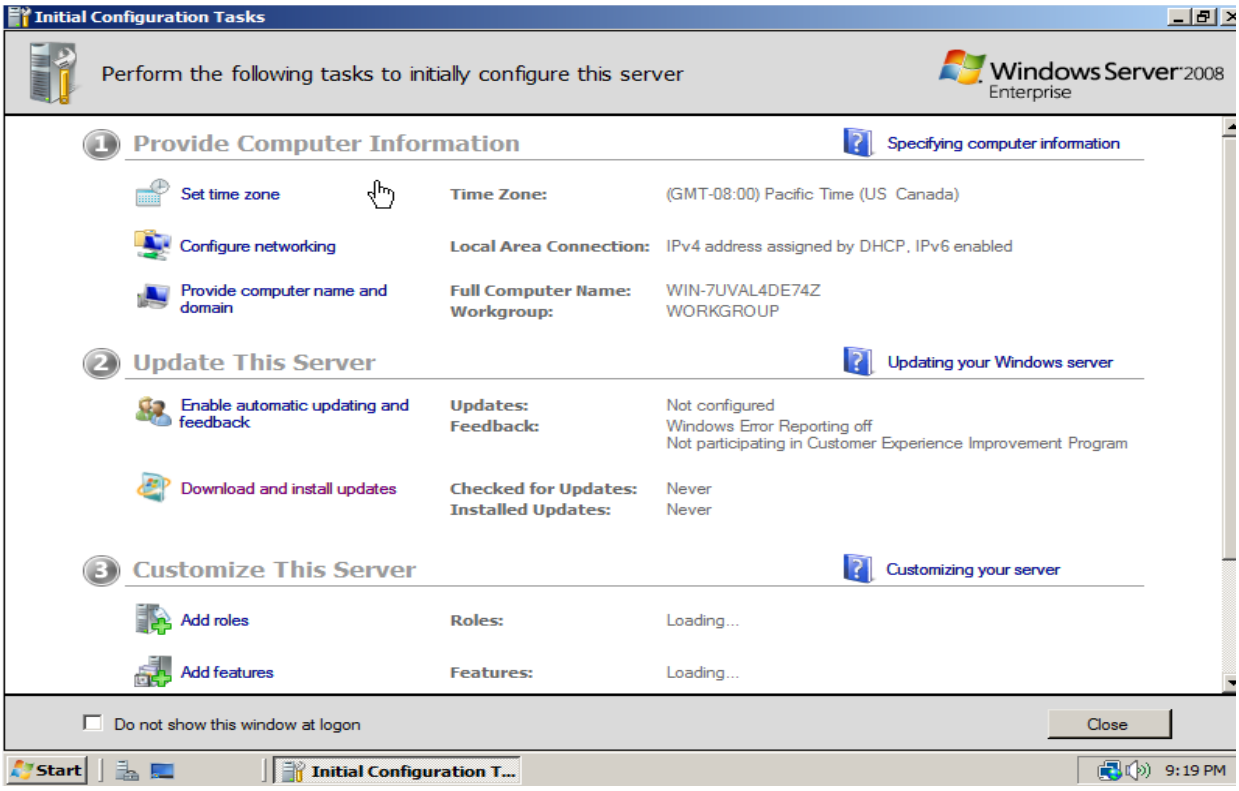
Αφού έχουμε επιλέξει έναν ισχυρό κωδικό διαχειριστή επιλέγουμε εισαγωγή και παρατηρούμε ότι ο κωδικός μας άλλαξε όπως φαίνεται στην παρακάτω εικόνα.

Εικόνα 5.16

Επιλέγουμε OK και στη συνέχεια μετά από λίγο διάστημα μας μεταφέρει στην επιφάνεια εργασίας των Windows Server 2008. Εφόσον γίνει αυτό θα παρατηρήσουμε ότι αυτόματα μας εμφανίζει τον Server Manager καθώς και τον οδηγό προσθήκης νέων υπηρεσιών. Στις επόμενες εικόνες παρουσιάζονται τα δύο παράθυρα διαλόγου υπηρεσιών.

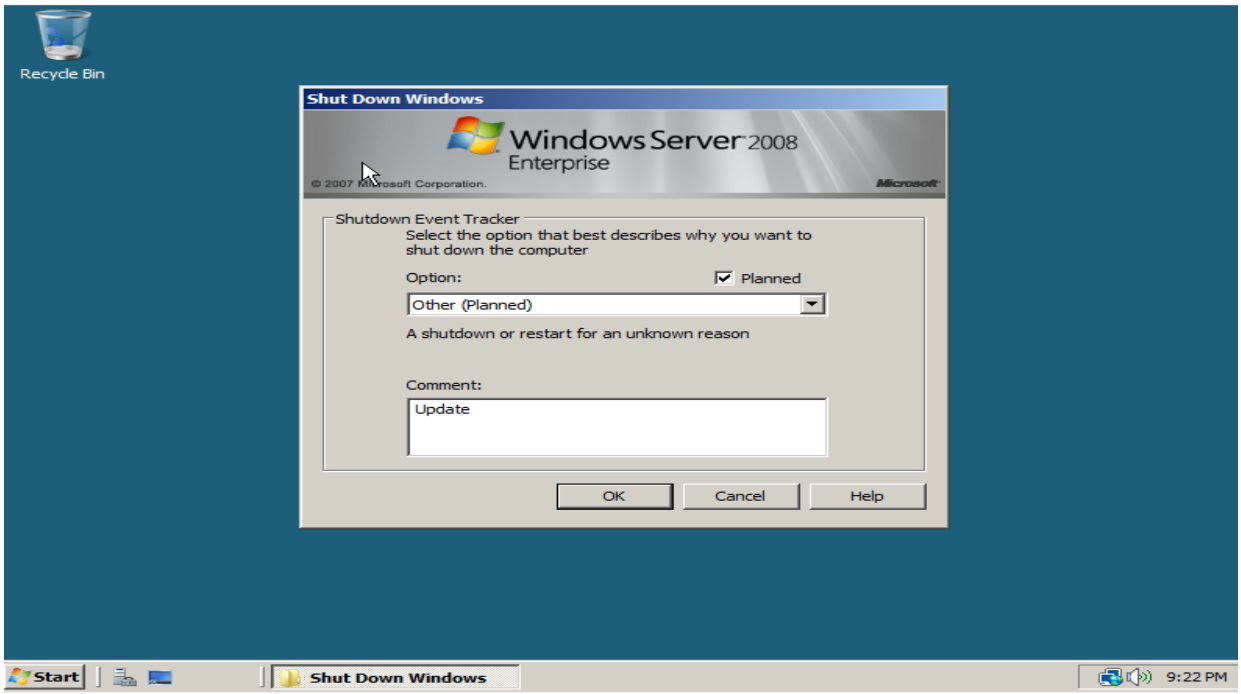


Εικόνα 5.17



Εικόνα 5.18

Προκειμένου να ελέγξουμε εάν εκτελέστηκαν όλα σωστά κάνουμε shutdown το σύστημά μας. Όταν επιλέγουμε shutdown μας εμφανίζεται ένα παράθυρο διαλόγου, όπως στην εικόνα παρακάτω, όπου ζητείται να αναφέρουμε τον λόγο τερματισμού των Windows Server.



Εικόνα 5.19

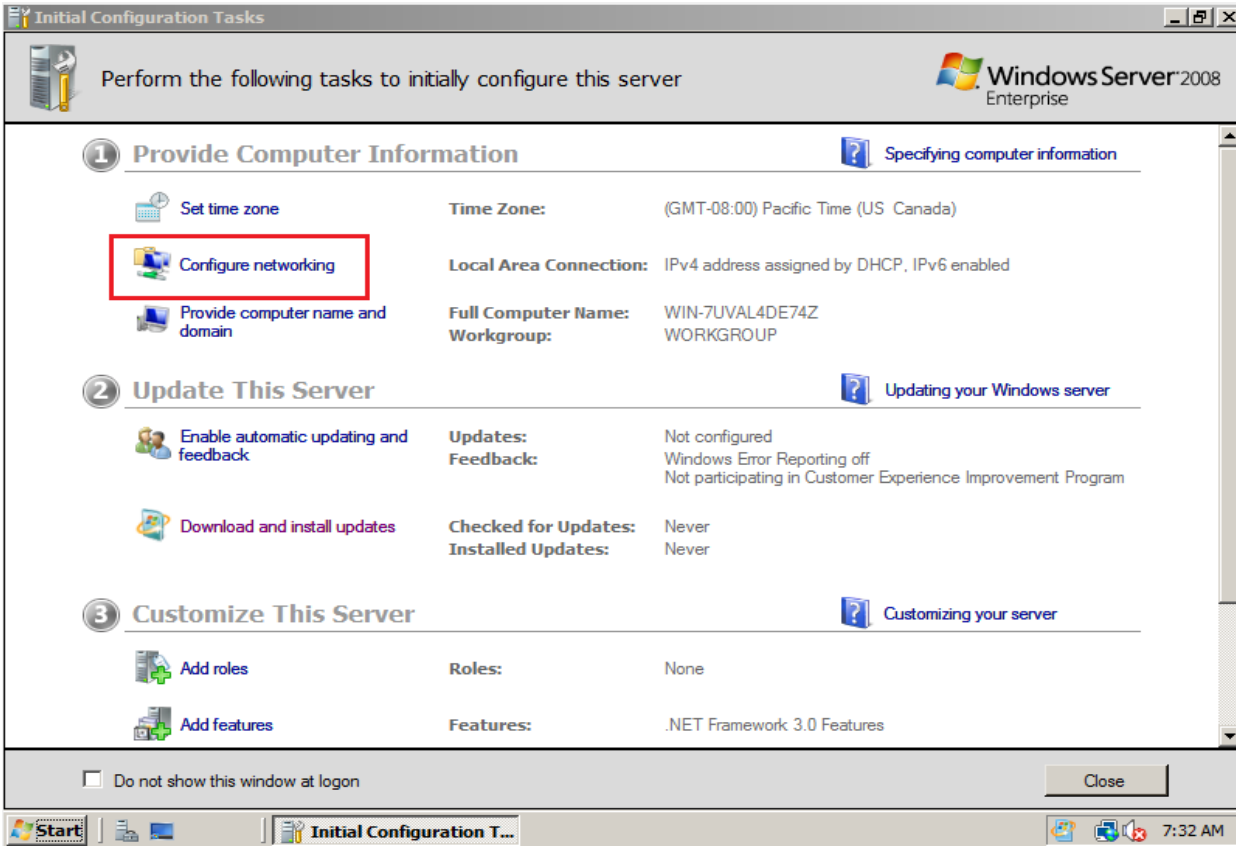
Εκτελούμε εκκίνηση του συστήματος και αφού πραγματοποιηθεί η εκκίνηση μας εμφανίζεται το παρακάτω παράθυρο διαλόγου.

Εικόνα 5.20

Προκειμένου να πραγματοποιηθεί η είσοδός μας στα Windows Server 2008 θα πρέπει να πατήσουμε τον συνδυασμό πλήκτρων Ctrl + Alt + Del για να εμφανιστεί το πλαίσιο διαλόγου Σύνδεση στα Windows. Πληκτρολογούμε τον κωδικό πρόσβασης διαχειριστή και επιλέγουμε είσοδος. Εφόσον τα στοιχεία σύνδεσής μας είναι σωστά εισερχόμαστε στην επιφάνεια εργασίας των Windows Server 2008.

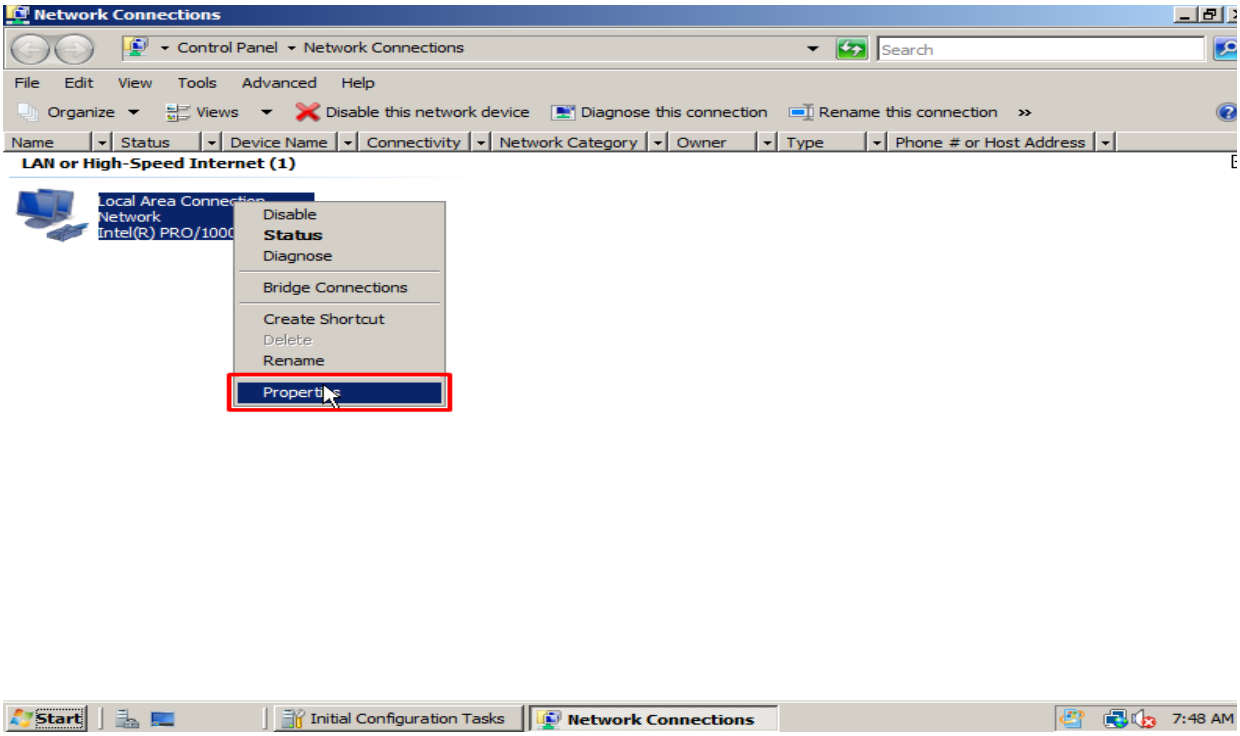
5.3. Αρχικές ρυθμίσεις

Μετά την αρχική εγκατάσταση θα πρέπει να κάνουμε τις αρχικές βασικές ρυθμίσεις του διακομιστή πριν από την εκχώρηση οποιονδήποτε ρόλων ή υπηρεσιών. Αρχικά μεταβαίνουμε στις ρυθμίσεις της κάρτας δικτύου προκειμένου να εγκαταστήσουμε static ip στο διακομιστή μας. Η διεύθυνση δικτύου που θα βάλουμε θα πρέπει να ανήκει στο υπάρχον δίκτυό μας. Κατά την είσοδό μας στην επιφάνεια εργασίας μας εμφανίζει το παράθυρο διαλόγου με τα Configuration Tasks. Επιλέγουμε Configure networking όπως φαίνεται στην εικόνα 5.21.



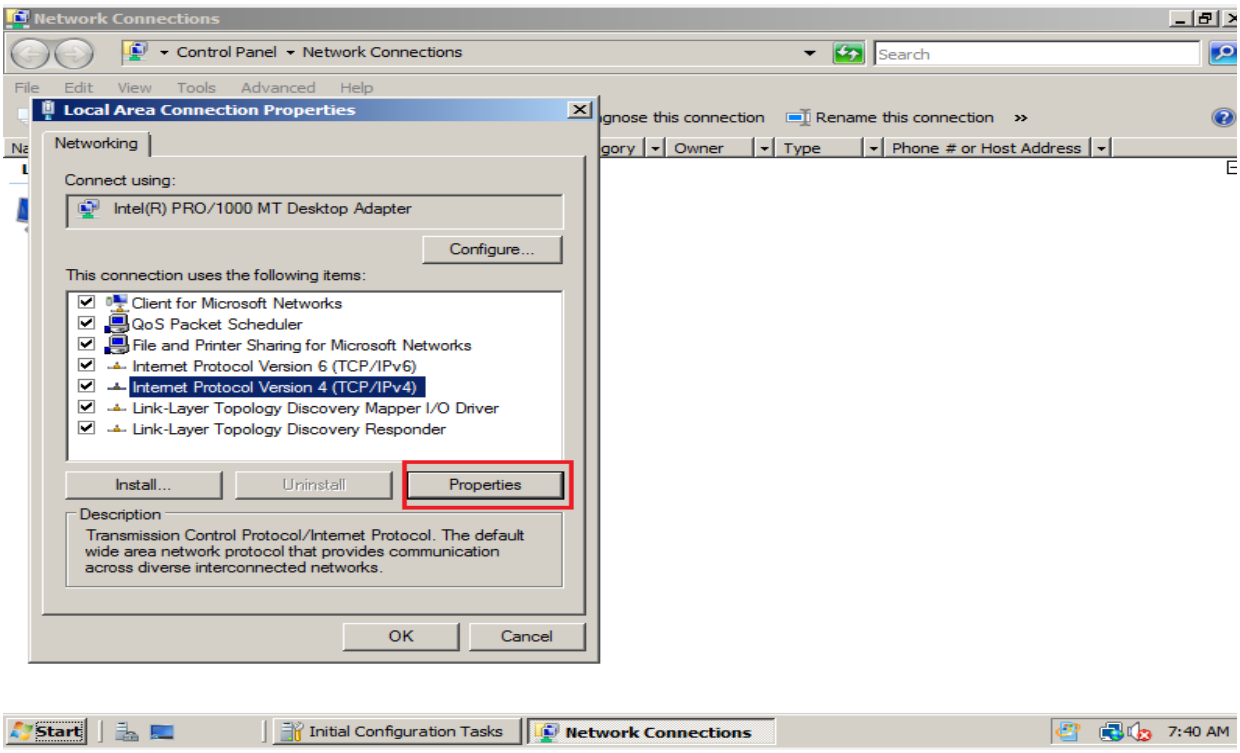
Εικόνα 5.21

Επιλέγοντας Configure networking θα μας εμφανίσει το επόμενο παράθυρο διαλόγου όπου εμφανίζονται οι διαθέσιμες συνδέσεις δικτύου. Ανάλογα με το hardware του διακομιστή μας θα μπορούσαμε να έχουμε παραπάνω από μία συνδέσεις δικτύου. Επιλέγουμε την σωστή και πατώντας δεξί κλικ επιλέγουμε ρυθμίσεις (Properties) όπως φαίνεται στην εικόνα 5.22.



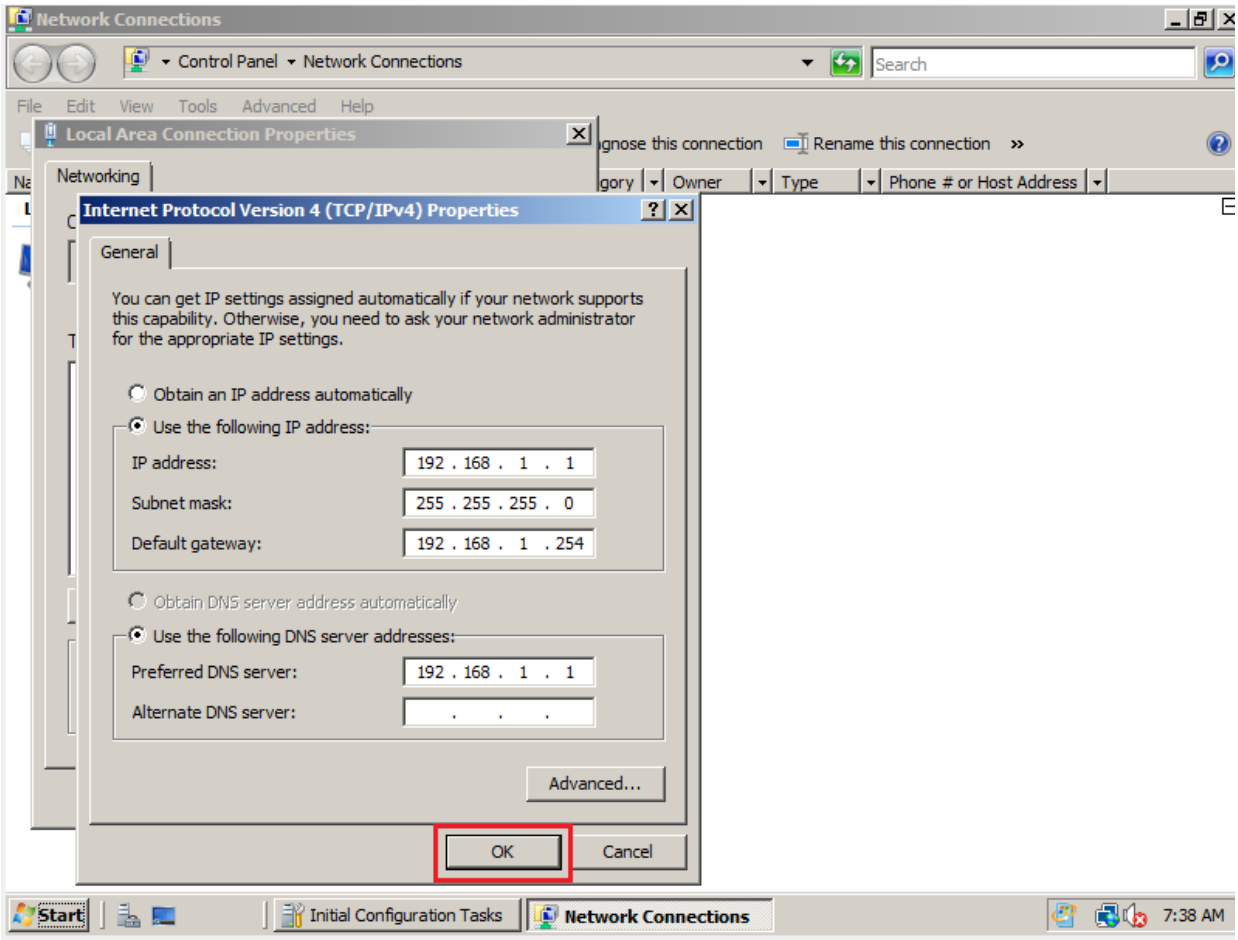
Εικόνα 5.22

Στην συνέχεια επιλέγουμε Internet Protocol TCP/IPv4 και πατάμε ρυθμίσεις όπως φαίνεται στην εικόνα 5.23



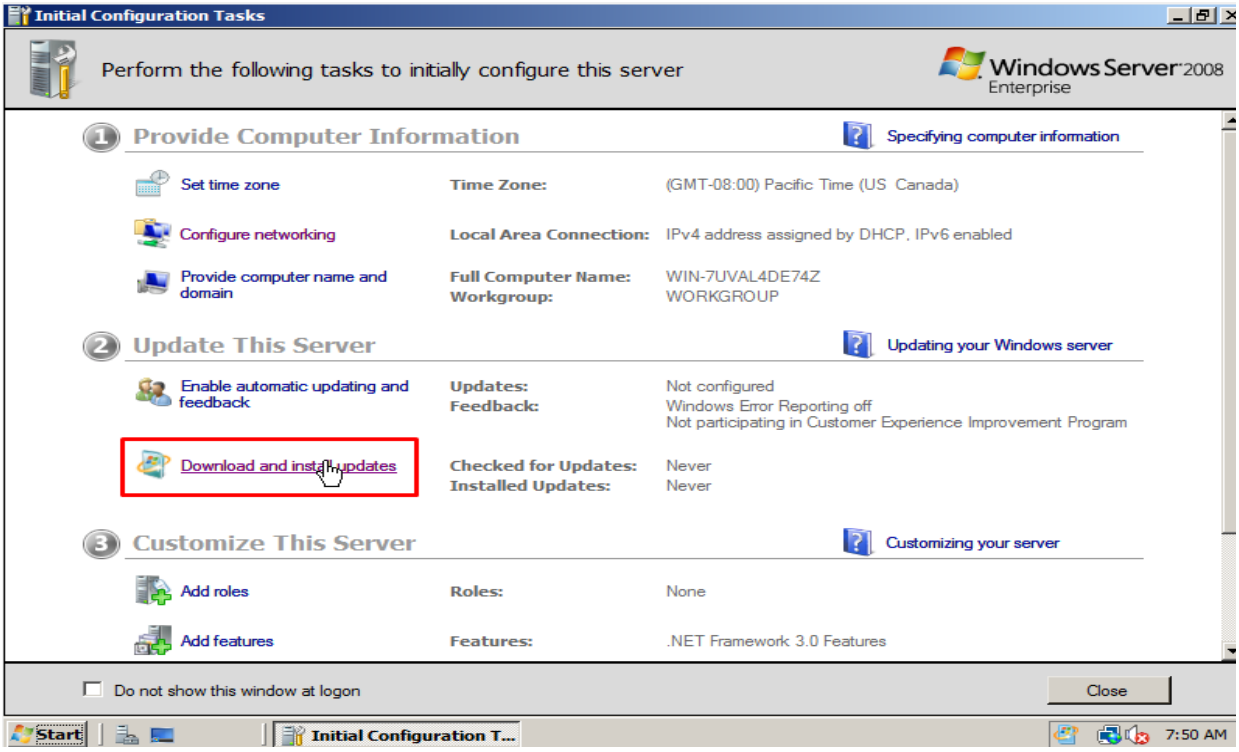
Εικόνα 5.23

Στο παράθυρο διαλόγου που θα εμφανιστεί μπορούμε να είτε να αφήσουμε να παίρνει αυτόματα ip ο διακομιστής μας είτε να του ορίσουμε εμείς μία στατική ip. Συστήνεται να ορίσουμε στατική ip γιατί όταν θα επιλέξουμε να του βάλουμε ρόλους θα πρέπει εξαρχής να γνωρίζουμε την ip του διακομιστή μας στο υπόλοιπο δίκτυο. Στην εικόνα 5.24 φαίνεται ένα ενδεικτικό παράδειγμα στατικής ip.



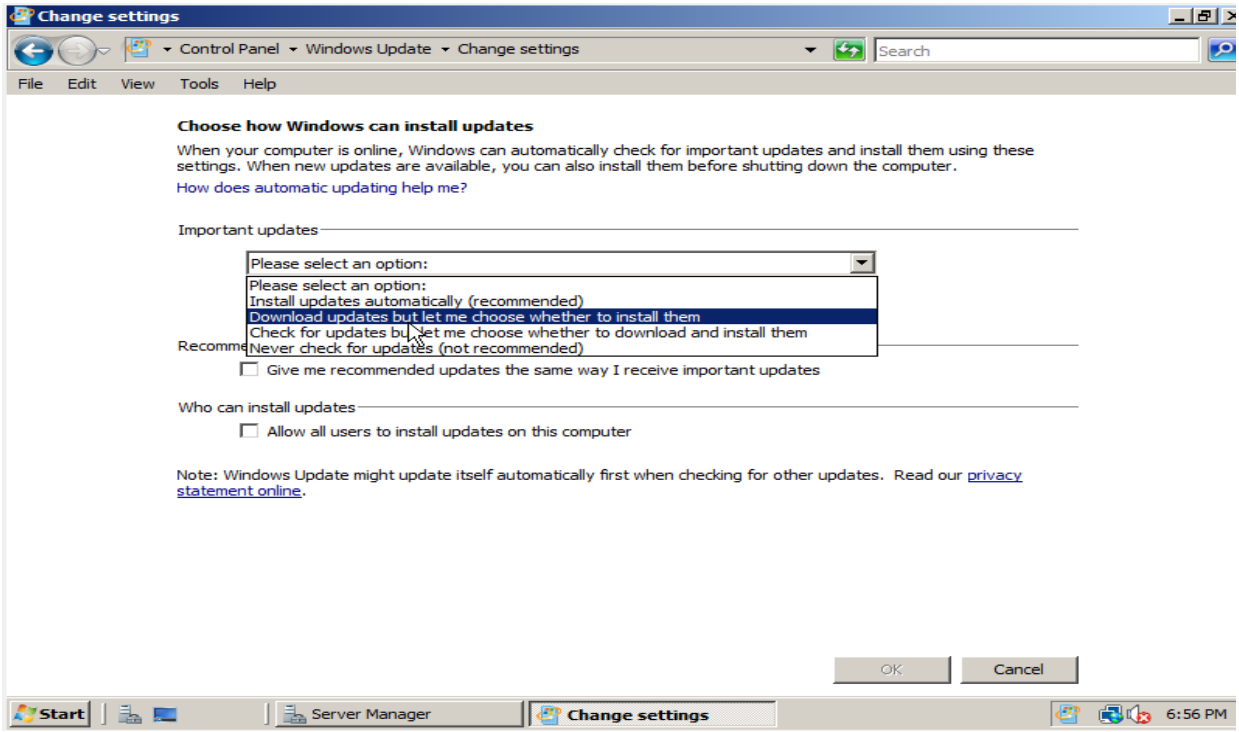
Εικόνα 5.24

Επόμενο σημαντικό βήμα είναι η ρύθμιση των Windows Update ώστε ο διακομιστής μας να είναι πάντα ενημερωμένος με τις τελευταίες σημαντικές ενημερώσεις, ειδικά σε θέματα ασφαλείας, που παρέχονται από τη Microsoft. Από το παράθυρο διαλόγου Configuration Tasks επιλέγουμε Download and Install updates όπως φαίνεται στην εικόνα 5.25.



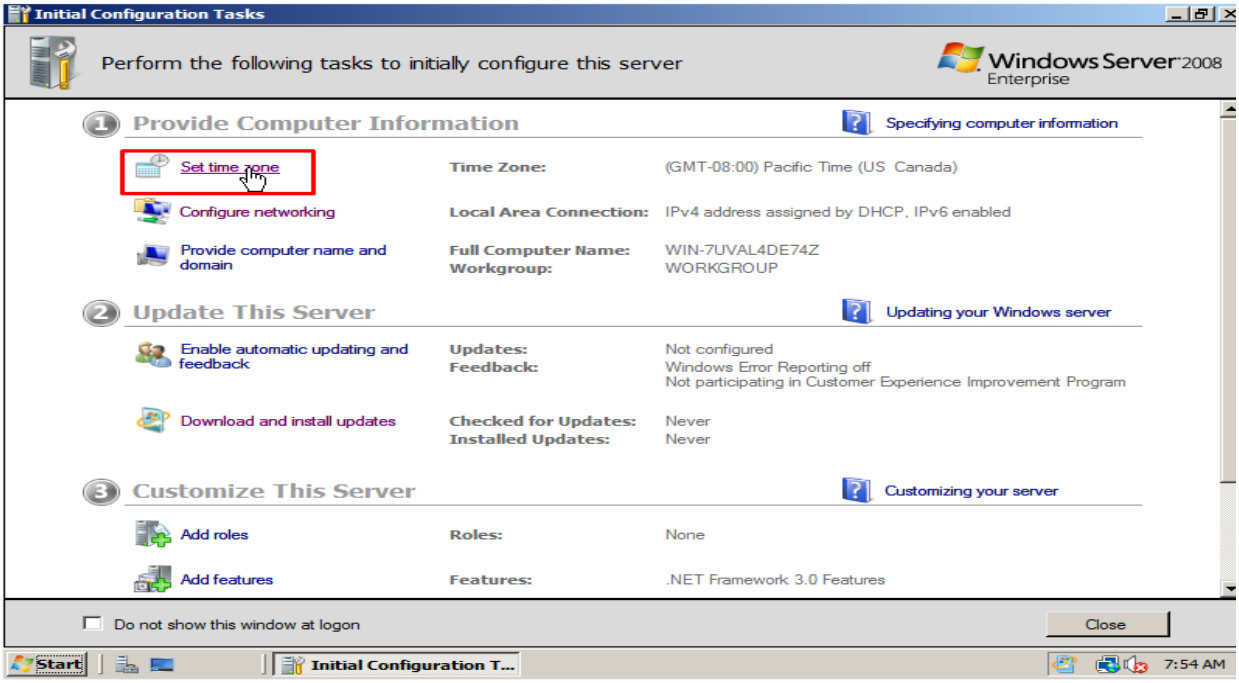
Εικόνα 5.25

Επειδή πρόκειται για διακομιστή προτείνεται να επιλέγουμε την δεύτερη επιλογή γιατί η Microsoft συνήθως μετά την εγκατάσταση νέων ενημερώσεων εκτελεί αυτόματα επανεκκίνηση στο λειτουργικό της. Η επιλογή μας φαίνεται στην εικόνα 5.26.



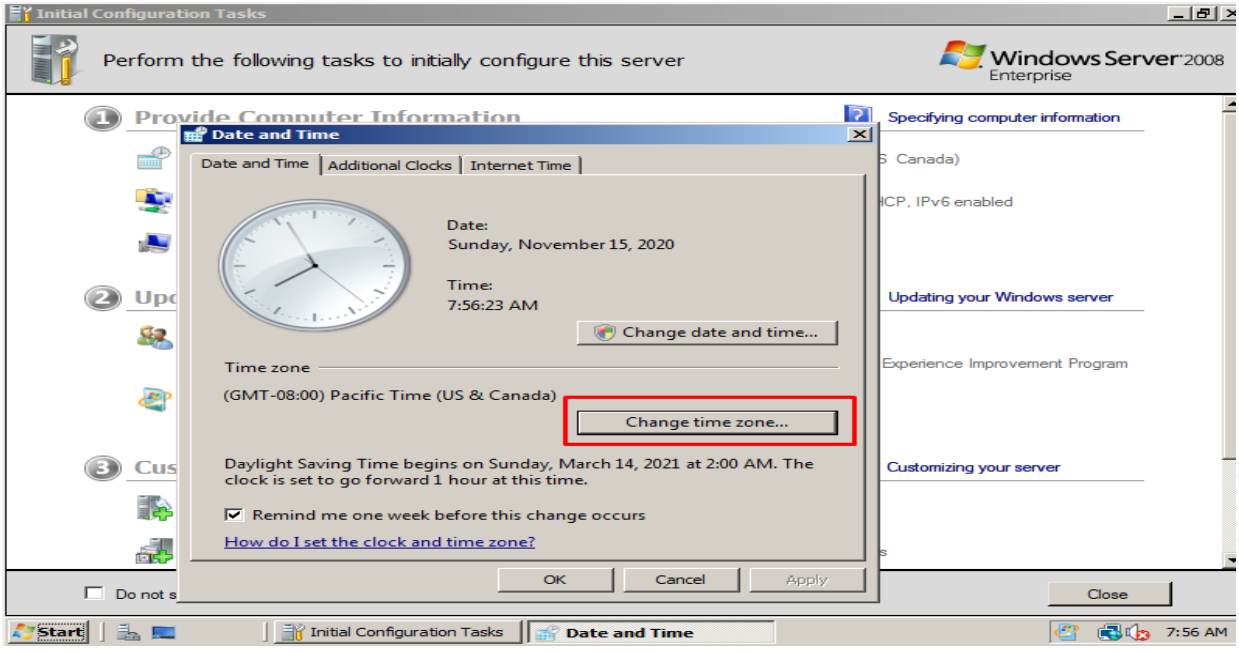
Εικόνα 5.26

Τέλος σημαντικό είναι να ρυθμίσουμε την ώρα, την ημερομηνία καθώς και το time zone του συστήματος δεδομένου ότι οι υπηρεσίες που θα εκτελούνται στο διακομιστή μας θα χρησιμοποιούν τις ανωτέρω ρυθμίσεις. Όπως φαίνεται στην εικόνα 5.27 επιλέγουμε Set time zone.



Εικόνα 5.27

Στο παράθυρο διαλόγου που μας εμφανίζεται, όπως στην εικόνα 5.28, επιλέγουμε Change time zone και βάζουμε την επιθυμητή.



Εικόνα 5.28

6. Ανάλυση των Windows Server 2008

6.1. Εισαγωγή

Τα Windows Server 2008 είναι ουσιαστικά η έκτη γενιά των λειτουργικών συστημάτων Windows Server. Όσον αφορά το περιβάλλον χρήσης μοιάζει αρκετά μεταξύ των Windows Server 2003 και Windows Vista. Κατά την αρχική εκκίνηση όπως φαίνεται και στην εικόνα 6.1 τα Windows 2008 μοιάζουν με Windows Vista σε σχέση με τα εικονίδια, γραμμές εργαλείων και μενού.

Εικόνα 6.1

Ωστόσο, επειδή τα Windows 2008 είναι περισσότερο λειτουργικό σύστημα επιχείρησης εργαλεία όπως η διεπαφή Windows Aero 3D δεν είναι προεγκατεστημένα και τις δυνατότητες πολυμέσων που βρίσκονται στις εκδόσεις Windows Vista Home ή Ultimate δεν περιλαμβάνονται στο λειτουργικό σύστημα από προεπιλογή.

6.1.1. Λειτουργίες στο παρασκήνιο των Windows Server 2008

Self-Healing NTFS (Αυτοθεραπεία NTFS)

Μία από τις νέες ενσωματωμένες τεχνολογίες στα Windows 2008 είναι η αυτοθεραπεία NTFS. Το λειτουργικό σύστημα έχει ένα νήμα που τρέχει στο παρασκήνιο, το οποίο κάνει διορθώσεις στο σύστημα αρχείων όταν το NTFS εντοπίζει κατεστραμμένο αρχείο ή κατάλογο. Στο παρελθόν όταν υπήρχε πρόβλημα συστήματος αρχείων, συνήθως έπρεπε να γίνει επανεκκίνηση του διακομιστή για να εκτελεστεί το chkdsk και να γίνει καθαρισμός των κατεστραμμένων από σφάλματα αρχείων και καταλόγων.

Είναι μία πρόσθετη δυνατότητα των Windows Server 2008 που διατηρεί το λειτουργικό σύστημα να τρέχει αξιόπιστα και με λιγότερα προβλήματα συστήματος.

Hot-Swappable Components (Εξαρτήματα με δυνατότητα εναλλαγής)

Στα Windows 2008 περιλαμβάνεται η δυνατότητα ανταλλαγής βασικών στοιχείων υλικού πυρήνα, όπως αντικατάσταση μνήμης, επεξεργαστών και καρτών προσαρμογέα PCI σε διακομιστή που υποστηρίζει αυτήν τη δυνατότητα.
Σε ένα περιβάλλον πληροφορικής όπου απαιτείται να υπάρχει μηδενικός χρόνος διακοπής σημαίνει ότι ένας διαχειριστής πληροφορικής δεν μπορεί καν τερματίσει ένα σύστημα για αντικατάσταση αποτυχημένων εξαρτημάτων. Με ενσωματωμένες δυνατότητες εναλλαγής στο λειτουργικό σύστημα η δυνατότητα αυτή βοηθά τους οργανισμούς να ελαχιστοποιήσουν τη διακοπή λειτουργίας του συστήματος
Στα Windows 2008, με σωστά υποστηριζόμενο υλικό, η αποτυχημένη μνήμη μπορεί να αλλάξει ενώ ο διακομιστής εκτελείται. Επιπλέον, οι πίνακες επεξεργαστών μπορούν να ανταλλάσσονται κατά την ώρα λειτουργίας και προσαρμογείς PCI όπως προσαρμογείς δικτύου ή προσαρμογείς επικοινωνίας μπορούν να προστεθούν ή να αφαιρεθούν από το σύστημα. Οι προμηθευτές υλικού διακομιστή παρείχαν προσθήκες στα Windows 2003 για την υποστήριξη αυτής της λειτουργικότητας. Ωστόσο, με αυτήν την ικανότητα ενσωματωμένη στα Windows 2008, οι επαγγελματίες πληροφορικής μπορούν να εκτελέσουν τα hot swaps και το λειτουργικό σύστημα και τις εφαρμογές κατά την διάρκεια λειτουργίας. Το λειτουργικό σύστημα θα αναγνωρίσει τις αλλαγές υλικού χωρίς τη χρήση ειδικά πρόσθετων στοιχείων λογισμικού.

Server Message Block 2.0 (Μπλοκ μηνυμάτων διακομιστή 2.0)

Το Server Message Block 2.0 αρχικά παρουσιάστηκε στα Windows Vista και τώρα βασίζεται στα Windows 2008 το οποίο είναι γνωστό ως SMB2. Το SMB2 είναι ένα πρωτόκολλο που χειρίζεται τη μεταφορά αρχείων μεταξύ συστημάτων. Το SMB2 συνδυάζει επικοινωνίες αρχείων και μέσω ενός μεγαλύτερου buffer επικοινωνιών μπορεί να μειώσει τον αριθμό των μετ' επιστροφής, που απαιτείται κατά τη μετάδοση, δεδομένων μεταξύ συστημάτων. Επειδή περισσότερες πληροφορίες διαβάζονται σε ένα buffer και μεταφέρονται χωρίς συγκεκριμένη δομή , οι πληροφορίες μεταδίδονται πολύ πιο γρήγορα. Οι περισσότεροι χρήστες σε δίκτυο τοπικής περιοχής υψηλής ταχύτητας (LAN) δεν θα παρατηρήσουν τις βελτιώσεις κατά το άνοιγμα και την αποθήκευση αρχείων όπως το Microsoft Office σε Windows Server 2008. Ωστόσο, για χρήστες που ενδέχεται να αντιγράφουν μεγάλα αρχεία εικόνας ή σύνολα δεδομένων μεταξύ των συστημάτων θα διαπιστώσουν ότι οι πληροφορίες αντιγράφονται από 10 έως 30 φορές πιο γρήγορα. Η βελτίωση είναι πολύ αισθητή σε καταστάσεις δικτύου ευρείας περιοχής (WAN) σε δίκτυα με υψηλή καθυστέρηση. Επειδή μια τυπική μεταφορά αρχείων απαιτεί σύντομα τμήματα ανάγνωσης και εγγραφής δεδομένων, ένα αρχείο μπορεί να διαρκέσει λεπτά για να μεταφερθεί σε ένα WAN. Το ίδιο αρχείο μπορεί να μεταφερθεί σε δευτερόλεπτα μεταξύ των συνδεδεμένων συστημάτων SMB2 επειδή η συνομιλία μετ' επιστροφής μειώνεται δραστικά.
Για να λειτουργεί αποτελεσματικά το SMB2, τα συστήματα και στα δύο άκρα πρέπει να είναι Windows 2008 συστήματα, συστήματα Windows Vista ή συνδυασμός των δύο.

Parallel Session Creation (Δημιουργία παράλληλης συνόδου)

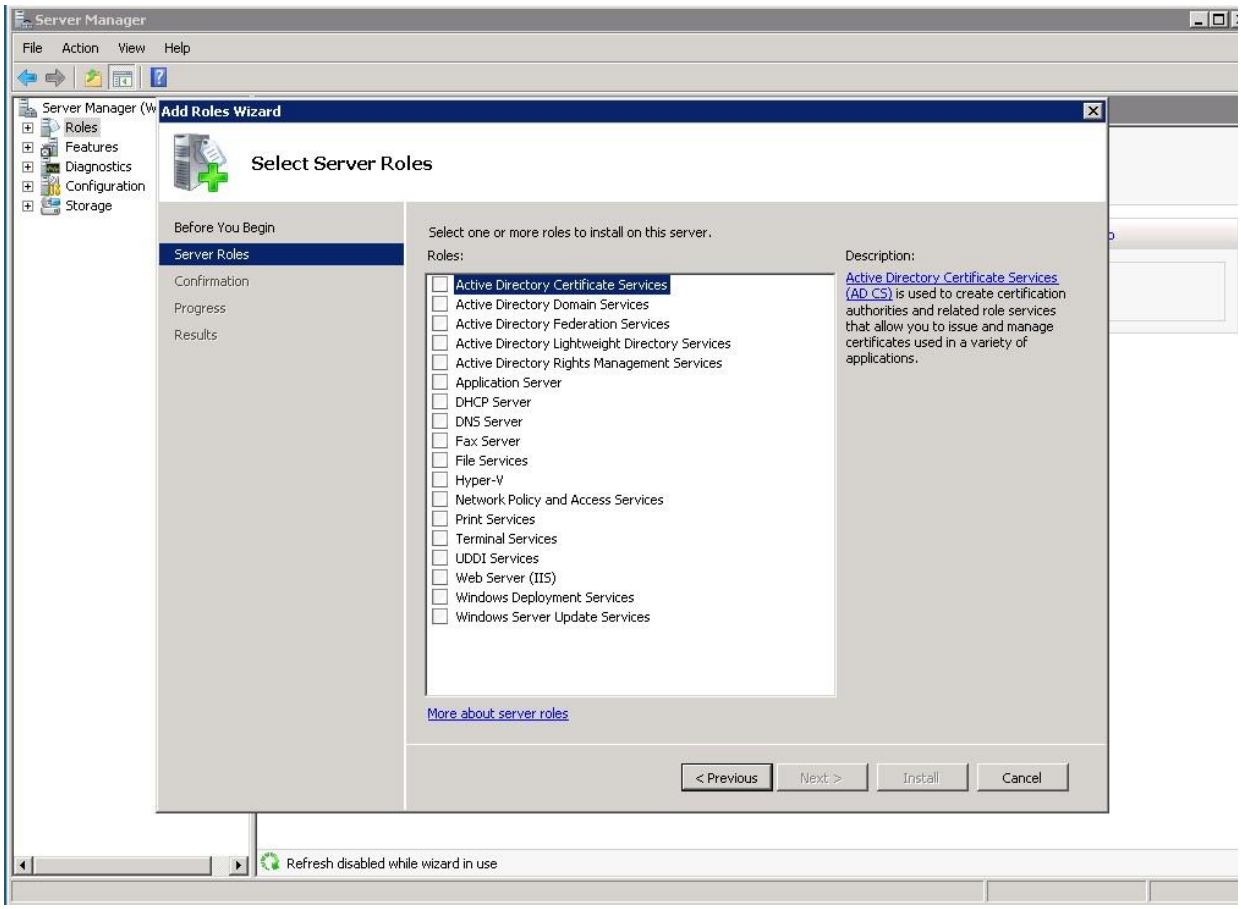
Στα Windows Server 2008, το υποσύστημα Session Manager (smss.exe) δημιουργεί μια παρουσία του για να προετοιμάσει κάθε συνεδρία σε αντιστοιχία με τον αριθμό των επεξεργαστών στο διακομιστή. Στο παρελθόν με τα Windows Server 2003 ή παλαιότερα, υπήρχε μόνο μία παρουσία smss.exe με αποτέλεσμα τα αιτήματα έπρεπε να διεκπεραιωθούν διαδοχικά. Με παράλληλη επεξεργασία συνεδριών, τεχνολογιών όπως οι υπηρεσίες Windows Terminal Services επωφελούνται σε μεγάλο βαθμό από αυτήν τη βελτίωση. Για παράδειγμα, έχοντας επτά clients Terminal Services στην ουρά για να συνδεθούν και να εκτελέσουν λεπτές συνεδρίες πελατών σε έναν διακομιστή με επεξεργαστή οκτώ πυρήνων, κάθε μία από τις επτά συνεδρίες πελατών μπορεί ταυτόχρονα να συνδεθεί να έτσι ώστε να γίνει ενεργοποίηση και εκτέλεση εφαρμογών με ταχύτητα επεξεργαστή.
Το σημαντικό είναι ότι αυτή είναι μια τεχνολογία που ο διαχειριστής δικτύου δεν εγκαθιστά, διαμορφώνει ή εκτελεί ξεχωριστά, αλλά είναι πλέον ενσωματωμένο στα Windows 2008, το οποίο τελικά βελτιώνει την πρώτη απόδοση των εφαρμογών και των εργασιών που χρησιμοποιούσαν σειριακές σειρές σε έναν διακομιστή που μπορεί τώρα χειριστεί παράλληλα με κάθε επεξεργαστή πυρήνα που χειρίζεται τις πρόσθετες εργασίες.

Υπηρεσία καθαρισμού κυψελών προφίλ χρήστη

Μια άλλη τεχνολογία ενσωματωμένη στα Windows Server 2008 είναι η Υπηρεσία καθαρισμού κυψελών προφίλ χρήστη. Αυτή η υπηρεσία βοηθά να διασφαλιστεί ότι οι περίοδοι σύνδεσης των χρηστών τερματίζονται πλήρως όταν αποσυνδέεται ένας χρήστης από ένα σύστημα. Καταργεί προσωρινό περιεχόμενο αρχείων, περιεχόμενο μνήμης cache και άλλες πληροφορίες που συνήθως δημιουργούνται κατά τη διάρκεια μιας περιόδου λειτουργίας χρήστη, αλλά θεωρείται περιττή για μακροπρόθεσμο αποθηκευτικό χώρο.
Αυτή η υπηρεσία είναι ιδιαίτερα χρήσιμη για οργανισμούς που χρησιμοποιούν Windows 2008 Terminal Services όπου οι συνεδρίες χρηστών δημιουργούνται συνήθως σε έναν διακομιστή και για λόγους ασφαλείας, τα δεδομένα από το προφίλ του χρήστη καταργούνται όταν ο χρήστης αποσυνδέεται από τη συνεδρία.

6.1.2. Windows Server 2008 ως διακομιστής εφαρμογών

Όσο έχουν σημειωθεί σημαντικές βελτιώσεις στα Windows 2008 που βελτιώνουν σημαντικά την απόδοση, την αξιοπιστία και την επεκτασιμότητα των Windows 2008 στις επιχειρήσεις, οι διακομιστές των Windows είναι εξαιρετικοί διακομιστές εφαρμογών που φιλοξενούν κρίσιμες επιχειρηματικές εφαρμογές για οργανισμούς.
Κατά την εγκατάσταση των Windows 2008, η κονσόλα διαχείρισης διακομιστή παρέχει μια λίστα ρόλων διακομιστή που μπορούν να προστεθούν σε ένα σύστημα, όπως φαίνεται στην εικόνα 6.2.



Εικόνα 6.2

Οι διάφοροι ρόλοι διακομιστή στα Windows Serer 2008 εμπίπτουν συνήθως σε τρεις βασικές κατηγορίες, ως εξής:

- *File and Print Services (Υπηρεσίες αρχείων και εκτύπωσης)*: Ως διακομιστής αρχείων και εκτύπωσης, τα Windows 2008 παρέχουν τις βασικές υπηρεσίες που αξιοποιούνται από χρήστες κατά την αποθήκευση δεδομένων και την εκτύπωση πληροφοριών στο δίκτυο. Έχουν γίνει αρκετές βελτιώσεις στα Windows 2008 για την ασφάλεια αρχείων και ανοχή σφαλμάτων διακομιστή αρχείων.
- *Domain Services (Υπηρεσίες τομέα)*: Σε εταιρικά περιβάλλοντα που εκτελούν τη δικτύωση των Windows, συνήθως ο οργανισμός εκτελεί την υπηρεσία καταλόγου Active Directory για να παρέχει κεντρικοποιημένη σύνδεση με αυθεντικοποίηση. Η υπηρεσία καταλόγου Active Directory εξακολουθεί να αποτελεί βασικό στοιχείο στα Windows 2008 με πολλές επεκτάσεις στη βασική εσωτερική έννοια του δάσους ενός οργανισμού καθώς και διευρυμένα ομοσπονδιακά δάση που επιτρέπουν στους Active Directory να διασυνδέονται με ένα άλλο.
- *Application Services (Υπηρεσίες εφαρμογών)*: Τα Windows 2008 παρέχουν τη βάση για την εγκατάσταση στις επιχειρήσεις εφαρμογές όπως το Microsoft Exchange, το Microsoft Office SharePoint Services, SQL Server και ούτω καθεξής. Αυτές οι εφαρμογές αρχικά κατασκευάζονται για να είναι συμβατές με τα Windows 2008 και αργότερα ενημερώνονται για να αξιοποιήσουν και να εκμεταλλευτούν πλήρως το νέες

τεχνολογίες ενσωματωμένες στο λειτουργικό σύστημα Windows 2008. Μερικές από τις εφαρμογές που συνοδεύουν τα Windows 2008 περιλαμβάνουν τις υπηρεσίες Windows Terminal Services για πρόσβαση υπολογιστών πελατών, Windows Διακομιστής πολυμέσων για φιλοξενία και μετάδοση βίντεο και ήχου, υπηρεσίες διακομιστή χρησιμότητας όπως DNS και DHCP, κοινή χρήση εγγράφων SharePoint και τεχνολογίες συνεργασίας και φιλοξενίας εικονικού διακομιστή.

6.1.3. Εκδόσεις των Windows Server 2008

Οι κύριες εκδόσεις των Windows Server 2008 περιλαμβάνουν τα Windows Server 2008 Standard Edition, όπου είναι η τυπική έκδοση, Windows Server 2008 Enterprise Edition, Windows Server 2008, Datacenter Edition, Windows Web Server 2008 και Windows 2008 Server Core.

Windows Server 2008 Standard Edition

Τα Windows Server 2008, Standard Edition είναι η πιο κοινή έκδοση διακομιστή του εν λόγω λειτουργικού συστήματος. Σε αντίθεση με προηγούμενες εκδόσεις των Windows Server όπου βασικές λειτουργίες και η επεκτασιμότητα για υποστήριξη μνήμης και επεξεργαστή περιορίστηκε μόνο στην Enterprise ή Datacenter Edition του λειτουργικού συστήματος, τα Windows Server 2008 Standard Edition είναι τώρα η προεπιλεγμένη έκδοση που αναπτύχθηκε από οργανισμούς.
Με τις διαθέσιμες εκδόσεις 32-bit και x64-bit, ένα βασικό σύστημα με Windows Server 2008 x64-bit Standard Edition υποστηρίζει έως τέσσερις βασικούς επεξεργαστές και 32 GB μνήμης (Το σύστημα 32-bit Standard Edition υποστηρίζει έως τέσσερις βασικούς επεξεργαστές και 4 GB μνήμης). Υποστηρίζει όλους τους ρόλους διακομιστών που είναι διαθέσιμοι στα Windows Server 2008, με εξαίρεση την ομαδοποίηση και το Active Directory Federation Services.
Η τυπική έκδοση είναι μια καλή έκδοση του λειτουργικού συστήματος που υποστηρίζει ελεγκτές τομέα, διακομιστές βοηθητικών προγραμμάτων (όπως DNS ή DHCP), διακομιστές αρχείων, διακομιστές εκτύπωσης, διακομιστές πολυμέσων, διακομιστές SharePoint και ούτω καθεξής. Οι περισσότεροι οργανισμοί, μεγάλοι και μικροί, βρίσκουν τις δυνατότητες της τυπικής έκδοσης επαρκής για τις περισσότερες υπηρεσίες δικτύου.

Windows Server 2008 Enterprise Edition

Με τα Windows Server 2008 Standard Edition που αναλαμβάνει το μεγαλύτερο μέρος των υπηρεσιών δικτύου, ο Windows Server 2008, Enterprise Edition επικεντρώνεται πραγματικά σε συστήματα διακομιστών που απαιτούν εξαιρετικά μεγάλης κλίμακας δυνατότητες επεξεργασίας και μνήμης καθώς και ομαδοποίηση ή Υπηρεσίες Active Directory Federation. Από τη βάση της επεκτασιμότητας της επεξεργασίας και χωρητικότητα μνήμης, εφαρμογές όπως η εικονικοποίηση των Windows ή η εταιρική ανταλλαγή σε διακομιστές 2007 ή SQL 2008 θα επωφεληθούν από τις δυνατότητες του Enterprise Edition των Windows Server 2008.

Κάθε φορά που ένας οργανισμός χρειάζεται να προσθέσει ομαδοποίηση στο περιβάλλον του, απαιτείται η έκδοση Enterprise ή Datacenter Edition. Η Enterprise Edition είναι η

κατάλληλη έκδοση του λειτουργικού συστήματος για υψηλή διαθεσιμότητα και απαιτήσεις υψηλής επεξεργασίας του πυρήνα σε διακομιστές εφαρμογών όπως διακομιστές SQL ή μεγάλα συστήματα συναλλαγών back-end ηλεκτρονικού εμπορίου. Η έκδοση Enterprise μπορεί να χειριστεί εκατοντάδες χρήστες σε έναν μόνο διακομιστή για οργανισμούς που αξιοποιούν τις δυνατότητες των Windows 2008 για Thin Client Terminal Υπηρεσίες που απαιτούν πρόσβαση σε μεγάλα σύνολα RAM και πολλούς επεξεργαστές. Η Enterprise Edition, με υποστήριξη για ομαδοποίηση διακομιστών, μπορεί να παρέχει στους οργανισμούς τις ασταμάτητες απαιτήσεις δικτύωσης πραγματικών δυνατοτήτων συνεχούς λειτουργίας σε ποσοστό 99,999% που απαιτούνται σε περιβάλλοντα υψηλής διαθεσιμότητας.

Windows Server 2008, Datacenter Edition

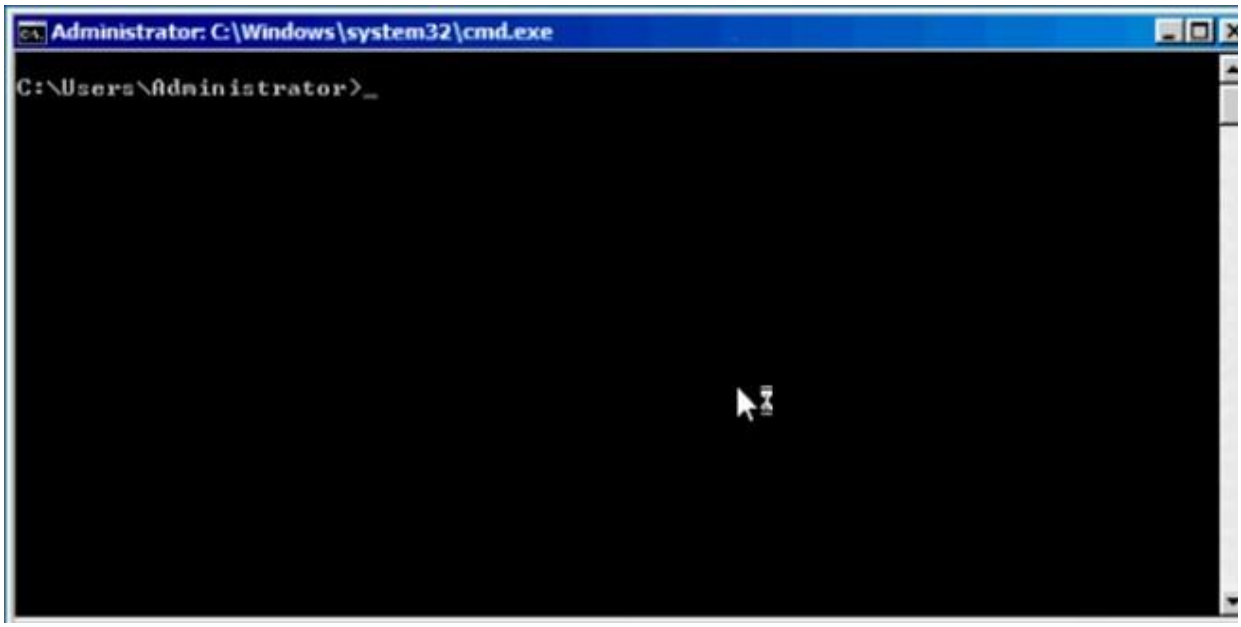
Τα Windows Server 2008 Datacenter Edition είναι μια έκδοση υλικολογισμικού που υποστηρίζει πολύ μεγάλης κλίμακας λειτουργίες κέντρων δεδομένων. Το Datacenter Edition υποστηρίζει οργανισμούς που χρειάζονται περισσότερους από οκτώ βασικούς επεξεργαστές. Το Datacenter Edition επικεντρώνεται σε οργανισμούς που χρειάζονται αναβαθμισμένη τεχνολογία διακομιστή για την υποστήριξη ενός μεγάλου συγκεντρωτικού χώρου αποθήκευσης δεδομένων σε έναν ή περιορισμένο αριθμό συστάδων διακομιστών. Ένας οργανισμός μπορεί να κλιμακώσει ή να αναβαθμίσει τις εφαρμογές διακομιστή του. Το Scale-out αναφέρεται σε μια εφαρμογή που εκτελείται καλύτερα όταν διανέμεται σε πολλούς διακομιστές, ενώ το Scale-up αναφέρεται σε μια εφαρμογή που αποδίδει καλύτερα όταν προστίθενται περισσότεροι επεξεργαστές σε ένα μόνο σύστημα. Οι τυπικές εφαρμογές κλίμακας περιλαμβάνουν υπηρεσίες διακομιστή ιστού, συστήματα ηλεκτρονικών μηνυμάτων και αρχεία και διακομιστές εκτύπωσης. Σε αυτές τις περιπτώσεις, οι οργανισμοί είναι καλύτερα να διανέμουν τις λειτουργικές εφαρμογές διακομιστή σε πολλά συστήματα Windows Server 2008 Standard Edition ή Enterprise Edition συστήματα ή ακόμα και συστήματα Windows Web Server 2008. Ωστόσο, οι εφαρμογές που αυξάνονται, όπως το ηλεκτρονικό εμπόριο ή οι εφαρμογές αποθήκευσης δεδομένων, επωφελούνται από την κατοχή όλων των δεδομένων και επεξεργασία σε ένα σύμπλεγμα διακομιστή. Για αυτές τις εφαρμογές, Windows Server 2008 η Datacenter Edition παρέχει καλύτερη συγκεντρωτική απόδοση κλιμάκωσης καθώς και το προστιθέμενο όφελος της ανοχής σφαλμάτων και των δυνατοτήτων ανακατεύθυνσης.
Αξίζει να σημειωθεί ότι τα Windows Server 2008 Datacenter Edition πωλούνται μόνο σε συστήματα με ιδιόκτητο υλικό. Επομένως ένας οργανισμός δεν μπορεί να αγοράσει το λογισμικό Datacenter Edition και να δημιουργήσει ή διαμορφώσει το δικό του σύστημα πολλαπλών επεξεργαστών 32 κατευθύνσεων. Το Datacenter Edition έχει αναπτυχθεί και δοκιμαστεί από μια κοινοπραξία προμηθευτών υλικού σε αυστηρά πρότυπα απόδοσης, αξιοπιστίας και υποστήριξης.

Windows Web Server 2008

Η έκδοση των Windows Web Server 2008 είναι μια έκδοση διακομιστή front-end του λειτουργικού με ένα σύστημα επικεντρωμένο σε ανάγκες διακομιστή εφαρμογών που είναι αφιερωμένες στις απαιτήσεις υπηρεσιών διαδικτύου.
Πολλοί οργανισμοί δημιουργούν απλούς διακομιστές ιστού ως διεπαφές στη βάση δεδομένων διακομιστών, διακομιστές ανταλλαγής μηνυμάτων ή συστήματα διακομιστών εφαρμογών δεδομένων. Η έκδοση Windows Web Server 2008 μπορεί να χρησιμοποιηθεί ως ένας απλός διακομιστής ιστού για να φιλοξενήσει περιβάλλοντα ανάπτυξης εφαρμογών ή μπορεί να ενσωματωθεί ως μέρος ενός πιο εξελιγμένου περιβάλλοντος web farm και web services που κλιμακώνεται σε πολλαπλά load-balanced συστήματα. Το σύστημα έχει σημαντικές βελτιώσεις στην επεκτασιμότητα σε σχέση με προηγούμενες εκδόσεις των Windows λειτουργικών συστημάτων και ένας οργανισμός μπορεί να εκχωρήσει άδεια πολλαπλών συστημάτων διαδικτυακών υπηρεσιών σε χαμηλότερο επίπεδο και κόστος ανά διακομιστή για την παροχή του scalability και redundancy που είναι επιθυμητά σε μεγάλα περιβάλλοντα διαδικτύου.

Windows Server 2008 Server Core

Μία νέα επιπρόσθετη έκδοση στα Windows Server 2008 είναι μια έκδοση διακομιστή Core του λειτουργικού συστήματος. Ο διακομιστής Windows Server 2008 Core, που φαίνεται στη εικόνα 6.3, είναι μια έκδοση χωρίς λειτουργικό περιβάλλον GUI των λειτουργιών συστήματος των Windows Server 2008.



Εικόνα 6.3

Όταν εκκινείται ένα σύστημα με εγκατεστημένο τον Core Server, το σύστημα δεν φορτώνεται μέχρι το κανονικό περιβάλλον εργασίας χρήστη με γραφικά των Windows. Αντ' αυτού, το σύστημα Server Core ξεκινά μια προτροπή σύνδεσης και από την

προτροπή σύνδεσης το σύστημα φορτώνει ένα περιβάλλον DOS. Δεν υπάρχει κουμπί Έναρξη, κανένα μενού, κανένα GUI καθόλου. Ο διακομιστής Core δεν πωλείται ως ξεχωριστή έκδοση, αλλά ως επιλογή εγκατάστασης που έρχεται με τις εκδόσεις Standard, Enterprise, Datacenter και Web Server του λειτουργικού συστήματος. Έτσι, όταν αγοράζετε μια άδεια χρήσης των Windows Server 2008, Standard Edition, το DVD έχει κοινό κωδικό με την τυπική έκδοσης συν μια τυπική έκδοση των Windows Server 2008 Core.

Οι δυνατότητες του λειτουργικού συστήματος περιορίζονται στην έκδοση του Server Core που εγκαθίσταται. Ο διακομιστής Windows Server 2008, Enterprise Edition Server Core έχει την ίδια μνήμη και τα όρια του επεξεργαστή ως τακτική Enterprise Edition των Windows 2008. Ο διακομιστής Core χρησιμοποιείται κυρίως σε διακομιστές κοινής ωφέλειας όπως ο ελεγκτές τομέα, διακομιστές DHCP, διακομιστές DNS, διακομιστές web IIS ή εικονικοποιημένα περιβάλλοντα Windows Servers.

Με την περιορισμένη επιβάρυνση παρέχονται περισσότεροι πόροι στις εφαρμογές που εκτελούνται στον διακομιστή λόγω και της κατάργησης του GUI και των σχετικών εφαρμογών. Ωστόσο υπάρχει λιγότερη ασφάλεια όσον αφορά το επιθετικό αποτύπωμα στο σύστημα Core Server. Επειδή οι περισσότεροι διαχειριστές δεν παίζουν Πασιέντζα ή χρησιμοποιούν το Media Player σε έναν ελεγκτή τομέα, οι εφαρμογές που τρέχουν είναι εφαρμογές που δεν χρειάζεται να διορθωθούν, να ενημερωθούν ή να διατηρηθούν στην έκδοση των Windows χωρίς GUI. Με λιγότερες εφαρμογές για επιδιόρθωση, το σύστημα απαιτεί λιγότερη συντήρηση και διαχείριση για να συνεχίσει να λειτουργεί.

6.2. Domain Name System (DNS)

Κατά την εφαρμογή της υπηρεσίας καταλόγου Active Directory στο περιβάλλον των Windows Server 2008, απαιτείται να έχουμε υλοποιήσει το DNS. Ενεργό αρχείο δεν μπορεί να υπάρξει χωρίς αυτό. Οι δύο οντότητες (Active Directory και DNS) είναι σαν τρένα και σιδηροδρομικές γραμμές. Οι κινητήρες του τρένου είναι πανίσχυρα μηχανήματα που μπορούν να τραβήξουν χιλιάδες τόνους εξοπλισμού, αλλά χωρίς τις γραμμές, δεν μπορούν να κινηθούν. Εάν οι γραμμές δεν ευθυγραμμίζονται σωστά, η αμαξοστοιχία μπορεί να εκτροχιάσει.
Κοιτάζοντας τη συσχέτιση μεταξύ της υπηρεσίας καταλόγου Active Directory και DNS, θα βρεθούν κοινά στοιχεία όπως οι συμβάσεις ονομασίας ζώνης. Εάν το όνομα τομέα της υπηρεσίας καταλόγου Active Directory είναι zygort.lcl , το DNS θα είναι επίσης zygort.lcl. Παρατηρούμε ότι το όνομα τομέα ανώτατου επιπέδου (TLD) για DNS, σε αυτήν την υπόθεση, δεν έχει ισοδύναμο τομέα εντός της υπηρεσίας καταλόγου Active Directory. Αυτό συμβαίνει επειδή, για τους περισσότερες εταιρείες, ο τομέας ανωτάτου επιπέδου δεν είναι μοναδικός και δεν ανήκει στην εταιρεία. Για παράδειγμα μια εταιρεία που χρησιμοποιεί widgets.com ως χώρος ονομάτων Active Directory. Το TLD που χρησιμοποιείται σε αυτήν την περίπτωση (com) ανήκει στην Internet Corporation για εκχωρημένα ονόματα και αριθμούς (ICANN) και είναι κοινή χρήση από εκατοντάδες χιλιάδες ιστότοπους που βασίζονται στο Διαδίκτυο. Κατά το σχεδιασμό της υπηρεσίας καταλόγου Active Directory, οι σχεδιαστές αποφάσισαν να διασφαλίσουν ότι η ρίζα του δάσους Active Directory θα μπορούσε να είναι μοναδική. Αυτό θα απαιτούσε τα ονόματα τομέα να λάβουν δύο στοιχεία τομέα: τον τομέα DNS της εταιρείας και το TLD στο οποίο κατοικεί.
Όταν ένας ελεγκτής τομέα είναι συνδεδεμένος στο διαδίκτυο, μέρος της ρουτίνας εκκίνησης είναι η απόπειρα εγγραφής του στις εγγραφές SRV που προσδιορίζουν τις υπηρεσίες που εκτελούνται στον ελεγκτή τομέα. Η μόνη απαίτηση για να λειτουργεί ένας διακομιστής DNS με την υπηρεσία καταλόγου Active Directory είναι ότι ο διακομιστής DNS υποστηρίζει εγγραφές SRV. Δεν έχει σημασία για τους πελάτες της υπηρεσίας καταλόγου Active Directory εάν οι εγγραφές εισάγονται χειροκίνητα από έναν διαχειριστή ή αυτόματα από τον ίδιο τον ελεγκτή τομέα. Το μόνο που έχει σημασία είναι ότι οι εγγραφές πρέπει να είναι σωστές. Εάν οι εγγραφές SRV δεν αναφέρονται στη ζώνη ή δεν έχουν εισαχθεί σωστά, ο πελάτης δεν θα μπορεί να εντοπίσει τον ελεγκτή τομέα. Εάν οι εγγραφές SRV παρατίθενται σωστά στη ζώνη DNS, ο κεντρικός υπολογιστής που παρέχει την υπηρεσία επιστρέφει στον πελάτη το όνομα του διακομιστή. Στη συνέχεια, ο πελάτης θα υποβάλει ερώτημα στο διακομιστή DNS για την εγγραφή A (εγγραφή ονόματος κεντρικού υπολογιστή) του ελεγκτή τομέα για την επίλυση της διεύθυνσης IP.

6.2.1. Επίλυση της διεύθυνσης IP

Οι πιο βασικές από όλες τις υπηρεσίες DNS παρέχουν τη δυνατότητα για ένα σύστημα πελάτη να στείλει ένα ερώτημα στο DNS διακομιστή, ζητώντας του να επιστρέψει τη διεύθυνση IP ενός συστήματος κεντρικού υπολογιστή. Αυτός ο τύπος ανάλυσης αναφέρεται ως προς τα εμπρός ανάλυση ονόματος.
Το DNS παρέχει αυτή τη λειτουργικότητα φιλοξενώντας εγγραφές πόρων που καθορίζουν τη διεύθυνση IP για καθένα από τα συστήματα κεντρικού υπολογιστή στο χώρο ονομάτων

DNS. Ο χώρος ονομάτων αναφέρεται στο DNS διακομιστή ως η ζώνη. Για παράδειγμα, εάν ο χώρος ονομάτων DNS είναι zygort.lcl και υπάρχει ένα όνομα διακομιστή APFS01 με διεύθυνση IP 192.168.2.75, το όνομα της ζώνης θα είναι zygort.lcl και ο διακομιστής θα έχει μια εγγραφή πόρων που συνδέει το όνομα APFS01 με τη διεύθυνση IP 192.168.2.75. Όταν ένας πελάτης στείλει ένα ερώτημα στον διακομιστή DNS που αναζητά APFS01.zygort.lcl , ο διακομιστής DNS θα απαντήσει στο ερώτημα με μια απάντηση που περιέχει τη διεύθυνση IP. Αυτός είναι ο πιο θεμελιώδης σκοπός του DNS, και ίσως η πιο χρησιμοποιούμενη συνάρτηση – εύρεση μιας διεύθυνσης IP όταν ένας πελάτης στέλνει ένα ερώτημα.

Υπάρχει ένας άλλος τύπος ανάλυσης γνωστός ως αντίστροφη ανάλυση ονόματος. Η αντίστροφη ανάλυση ονόματος επιτρέπει σε έναν πελάτη να υποβάλει ερώτημα για ένα όνομα κεντρικού υπολογιστή όταν γνωρίζει την IP διεύθυνση του εν λόγω συστήματος. Αυτό λειτουργεί με τον ίδιο τρόπο όπως το σύστημα αναγνώρισης κλήσης στο τηλέφωνο. Όταν λαμβάνουμε μια τηλεφωνική κλήση, ο αριθμός τηλεφώνου αντιστοιχεί σε ένα «φιλικό» όνομα που μπορεί να έχουμε ήδη καταχωρίσει. Δεδομένου ότι είναι πολύ πιο εύκολο να θυμόμαστε ονόματα από μεγάλους αριθμούς, αυτό το κάνει πολύ πιο εύκολο να προσδιορίσουμε ακριβώς ποιος καλεί. Εάν ένα όνομα δεν σχετίζεται με έναν τηλεφωνικό αριθμό, τότε θα εμφανιστεί μόνο ο αριθμός τηλεφώνου. Υπάρχουν πολλά προγράμματα και βοηθητικά προγράμματα που χρησιμοποιούν αντίστροφη ανάλυση ονόματος και ίσως φανεί χρήσιμο να είμαστε πιο σίγουροι ότι έχουμε τις σωστές πληροφορίες που περιλαμβάνονται στη ζώνη.

Οι διακομιστές DNS θα επιλύσουν ερωτήματα εντός των ζωνών που έχουν διαμορφωθεί σε αυτούς. Μπορούμε να έχουμε περισσότερες από μία ζώνες σε έναν διακομιστή και ο διακομιστής θα αποδεχτεί και θα απαντήσει σε ερωτήματα για εγγραφές στις ζώνες αυτές. Όταν ένας πελάτης στέλνει ένα ερώτημα για μια ζώνη που δεν φιλοξενείται στον διακομιστή DNS, ο διακομιστής DNS πρέπει να εκτελέσει πρόσθετες εργασίες για να ανταποκριθεί σωστά στον πελάτη. Ο διακομιστής DNS θα πραγματοποιήσει αναζήτηση μέχρι την κορυφή της ιεραρχίας DNS, γνωστή ως η ρίζα , για βοήθεια. Αυτοί οι ριζικοί διακομιστές DNS παρατίθενται στην καρτέλα Root Hints της σελίδας ιδιοτήτων του διακομιστή DNS. Ο διακομιστής DNS θα στείλει ένα δικό του ερώτημα σε έναν από αυτούς τους διακομιστές ρίζας, ζητώντας επίλυση. Οι ριζικοί διακομιστές θα αναφέρουν στον κατάλληλο διακομιστή TLD DNS. Στη συνέχεια, ο διακομιστής DNS θα υποβάλει ερώτημα στον διακομιστή DNS TLD για βοήθεια. Ο διακομιστής TLD θα παραπέμψει τον διακομιστή DNS στο κατάλληλο διακομιστή DNS τομέα δεύτερου επιπέδου. Αυτή η διαδικασία θα συνεχιστεί έως ότου ένας διακομιστής DNS με την εγγραφή πόρων επιλύσει το αίτημα, είτε με επιτυχημένη αναζήτηση είτε με αποτυχημένη.

Υπάρχουν προβλήματα που μπορούν να αντιμετωπιστούν με τις τυπικές μεθόδους ανάλυσης DNS. Δεν είναι πάντα προσβάσιμος κάθε χώρος ονομάτων από το Διαδίκτυο. Το όνομα zygort.lcl είναι ένα πρωταρχικό παράδειγμα αυτού. Αν επρόκειτο να πραγματοποιήσετε μια αναζήτηση σε ένα όνομα διακομιστή εντός αυτού του χώρου ονομάτων χρησιμοποιώντας συμβατικές μεθόδους DNS, η αναζήτηση θα αποτύχει. Πρέπει να υπάρχει μια άλλη μέθοδος επίλυσης των ερωτημάτων DNS για αυτές τις ζώνες. Το άλλο πρόβλημα έγκειται σε εταιρείες που δεν θέλουν να κάνουν ερωτήσεις στους διακομιστές DNS τους εκτός του οργανισμού τους. Επειδή οι διακομιστές DNS κοιτάζουν τη ρίζα του Διαδικτύου ως το αρχικό σημείο εκκίνησης για την επίλυση ονομάτων, σε αυτήν την περίπτωση πρέπει να υπάρχει ένας τρόπος για να μπορούμε να αποτρέπουμε

την εν λόγω λειτουργία. Έχουν εισαχθεί νέες επιλογές για την αντιμετώπιση αυτών των ζητημάτων.
Αυτή η συμπεριφορά "ρίζας ζώνης" δεν εμφανίζεται σε διακομιστή DNS των Windows Server 2008 όταν ρυθμίσουμε τον πρώτο ελεγκτή τομέα. Αυτό δεν σημαίνει ότι χρειαζόμαστε άδεια Dcpromo για να εγκαταστήσετε την υπηρεσία DNS. θα μπορούσαμε πρώτα να διαμορφώσουμε τη ζώνη DNS και, στη συνέχεια, να προωθήσουμε τον ελεγκτή τομέα. Αυτό θα μας επιτρέψει να διαμορφώσουμε τη ζώνη με τον τρόπο που θέλουμε και, στη συνέχεια, να επιτρέψουμε την εγγραφή του ελεγκτή τομέα. Εάν δημιουργήσουμε τη ζώνη με μη αυτόματο τρόπο, πρέπει να βεβαιωθούμε ότι έχουμε ρυθμίσει τη ζώνη για δυναμικές ενημερώσεις. Διαφορετικά, θα λάβουμε ένα μήνυμα σφάλματος που δηλώνει ότι ο τομέας δεν έχει ρυθμιστεί.

6.2.2. Επιλογή τύπου ζώνης

Για κάθε ζώνη που χρησιμοποιούμε, θα πρέπει να καθορίσουμε πώς θα ρυθμίσουμε τις παραμέτρους των διακομιστών DNS για να τις χρησιμοποιήσουμε. Υπάρχουν τρεις τύποι κύριων ζωνών στους Windows Server 2003 και Windows Server 2008:

- Πρωτοβάθμια (primary),
- Δευτεροβάθμια (secondary)
- Στέλεχος (stub)

Τα δεδομένα για τη ζώνη μπορούν να περιέχονται σε ένα αρχείο της μονάδας δίσκου του συστήματος του διακομιστή DNS και να διαβάζεται από τη μνήμη κατά την εκκίνηση ή μπορεί να διατηρηθεί στην υπηρεσία καταλόγου Active Directory. Η επιλογή αυτή είναι γνωστή ως τυπικός τύπος ζώνης, ο οποίος χρησιμοποιεί μεταφορές ζώνης ως μέσο αποστολής των δεδομένων σε άλλους διακομιστές DNS που φιλοξενούν τη ζώνη. Το τελευταίο είναι γνωστό ως ολοκληρωμένη υπηρεσία καταλόγου Active Directory και χρησιμοποιεί την αντιγραφή Active Directory για την αποστολή των δεδομένων. Από τους τρεις τύπους ζώνης, υπάρχει η επιλογή δημιουργίας πρωτογενούς και στελεχών ζώνης Active Directory – ολοκληρωμένη. Ωστόσο, οι δευτερεύουσες ζώνες δεν μπορούν
να είναι ενσωματωμένες στην υπηρεσία καταλόγου Active Directory. Κάθε ένα από αυτά έχει τη θέση του στην υποδομή που υλοποιούμε, αλλά θα πρέπει να γνωρίζουμε πότε να επιλέξουμε το ένα από το άλλο γιατί μπορεί να προκληθεί σύγχυση.

Πρωτεύουσες ζώνες (Primary Zones)

Οι πρωτεύουσες ζώνες διατηρούνται παραδοσιακά σε ένα μόνο σύστημα και είναι γνωστές ως τυπικές πρωτεύουσες ζώνες . Οι κύριες ζώνες είναι τα σημεία ενημέρωσης στο DNS. Ο περιορισμός σε αυτές οι ζώνες είναι το εγγενές σημείο αποτυχίας τους. Αν και τα δεδομένα ζώνης μπορούν να μεταφερθούν σε άλλον διακομιστή που λειτουργεί ως δευτερεύουσα ζώνη, εάν ο διακομιστής που κατέχει την κύρια ζώνη δεν είναι διαθέσιμος, δεν μπορούμε να κάνουμε αλλαγές στη πρωτεύουσα ζώνη. Σε αυτήν την περίπτωση, πρέπει να προωθηθεί μια δευτερεύουσα ζώνη σε πρωτογενή εάν πρέπει να κάνουμε ενημερώσεις στη ζώνη.
Ένας άλλος περιορισμός στις τυπικές πρωτεύουσες ζώνες προέρχεται από το ενιαίο σημείο ενημέρωσης. Όταν χρησιμοποιούμε πελάτες που υποστηρίζουν δυναμικές ενημερώσεις DNS, ο μόνος διακομιστής στη ζώνη που μπορεί να λάβει τις ενημερώσεις

είναι αυτός που κρατά την πρωτεύουσα ζώνη. Κάθε φορά που ένας δυναμικός πελάτης DNS έρχεται στο διαδίκτυο, ερωτά τον προτιμώμενο διακομιστή DNS για την εγγραφή έναρξης εξουσιοδότησης (Start of Authority – SOA) για τη ζώνη στην οποία ετοιμάζεται για να εγγραφεί. Η εγγραφή SOA ενημερώνει τον πελάτη του διακομιστή που είναι έγκυρος για τη ζώνη. Ο πελάτης στη συνέχεια στέλνει τις δυναμικές πληροφορίες εγγραφής DNS στον διακομιστή που κρατά την κύρια ζώνη. Αυτό δεν είναι πρόβλημα εκτός εάν ο διακομιστής στον οποίο εγγράφεται ο πελάτης βρίσκεται σε αργή ή υπερβολική χρήση WAN συνδέσμου. Η πρόσθετη κυκλοφορία εγγραφής DNS μπορεί να γίνει πολύ δυσκίνητη. Επιπλέον, τα ίδια δεδομένα πρέπει στη συνέχεια να επιστρέψουν μέσω του συνδέσμου WAN εάν ένας διακομιστής κατέχει τη δευτερεύουσα
ζώνη όπου απαιτείται μεταφορά ζώνης.
Αυτή η κατάσταση οδήγησε τους διαχειριστές να δημιουργήσουν υποτομείς εντός της ιεραρχίας DNS για υποστήριξη των απομακρυσμένων τοποθεσιών. Με αυτόν τον τρόπο, οι απομακρυσμένες τοποθεσίες έχουν τους δικούς τους διακομιστές DNS για να κρατήσουν τις πρωτεύουσες ζώνες, με τον γονικό τομέα να διατηρεί εγγραφές ανάθεσης στον υποτομέα. Οι πελάτες καταχωρούνται εντός της ζώνης τοπικά και τα μόνα δεδομένα που πρέπει να σταλούν μέσω του συνδέσμου WAN είναι τα ερωτήματα για πληροφορίες ζώνης και μεταφορές ζώνης εάν μια δευτερεύουσα ζώνη έχει ρυθμιστεί σε άλλον διακομιστή.
Ωστόσο, αυτό το σενάριο έχει δύο προβλήματα:

- ενδέχεται να μην έχουμε στη διάθεσή μας διαχειριστές για τις απομακρυσμένες τοποθεσίες και
- η επισκεψιμότητα ερωτημάτων θα μπορούσε να καταναλώσει περισσότερο εύρος ζώνης στο σύνδεσμο WAN από ότι θα απαιτούσε απλά μια διαδικασία εγγραφής.

Τι πρέπει λοιπόν να κάνει ένας διαχειριστής; Εκτός από την αξιολόγηση της επισκεψιμότητας που θα δημιουργηθεί από οποιοδήποτε από τα δύο σενάρια για προσδιορισμό που θα είναι το μικρότερο από τα δύο προβλήματα, θα μπορούσε να χρησιμοποιήσει τις νέες και βελτιωμένες τεχνολογίες Microsoft DNS. Χρήση της υπηρεσίας καταλόγου Active Directory στις ζώνες βελτιώνουν σημαντικά την υποδομή DNS. Οι ενσωματωμένες πρωτεύουσες ζώνες Active Directory αποθηκεύουν τις εγγραφές ζώνης στον κατάλογο Active Directory. Οποιοσδήποτε διακομιστής DNS με ενσωματωμένες πρωτεύουσες ζώνες Active Directory μπορεί στη συνέχεια να χρησιμοποιήσει αυτές τις εγγραφές. Οι ελεγκτές τομέα που κρατούν τα δεδομένα αυτά θα αναπαράγουν τις αλλαγές μεταξύ τους. Αυτό επιτρέπει εκτός από την ενημέρωση σε οποιονδήποτε από τους Active Directory ενσωματωμένους διακομιστές DNS αλλά και την αναπαραγωγή αυτών των ενημερώσεων σε κάθε άλλον Active Directory– ενσωματωμένο διακομιστή DNS.

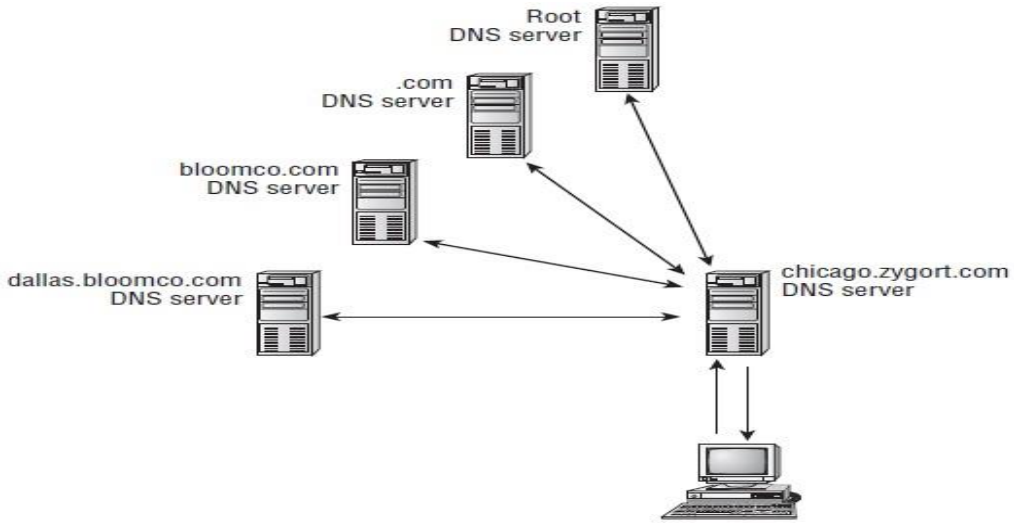
Δευτερεύουσες ζώνες (Secondary Zones)

Οι δευτερεύουσες ζώνες υπήρχαν όσο και οι πρωτεύουσες. Όταν ένας διαχειριστής ήθελε έναν άλλο διακομιστή DNS για να φιλοξενήσει τις ίδιες πληροφορίες ζώνης με την κύρια ζώνη, θα δημιουργήσει μια δευτερεύουσα ζώνη, η οποία θα φιλοξενήσει πανομοιότυπες πληροφορίες όπως στην πρωτογενή ζώνη. Τα δεδομένα ζώνης μέσα σε μία δευτερεύουσα ζώνη είναι ένα αντίγραφο μόνο για ανάγνωση της βάσης δεδομένων της κύριας ζώνης.

Οι δευτερεύουσες ζώνες εξακολουθούν να έχουν τη θέση τους σε έναν οργανισμό. Εάν έχουμε μια απομακρυσμένη τοποθεσία όπου δεν θέλουμε να υποστηρίξουμε έναν ελεγκτή τομέα, αλλά θέλουμε να παρέχουμε τοπική ανάλυση στους πελάτες, μπορούμε να δημιουργήσουμε μια δευτερεύουσα ζώνη σε έναν διακομιστή εντός αυτής της τοποθεσίας. Αυτό θα μειώσει το ποσό της επισκεψιμότητας ερωτημάτων που πρέπει να περάσουν μέσα από τον σύνδεσμο WAN, αλλά θα ζητηθεί η αποστολή της μεταφοράς ζώνης από έναν κύριο διακομιστή κατά μήκος του συνδέσμου WAN στη δευτερεύουσα ζώνη. Συνήθως, θα υπάρχουν περισσότερα ερωτήματα που αποστέλλονται από πελάτες από ότι θα υπάρξουν δυναμικές ενημερώσεις από πελάτες. Ωστόσο, θα πρέπει να παρακολουθείται η κίνηση που διέρχεται μέσω του συνδέσμου WAN προκειμένου να προσδιοριστεί εάν χρησιμοποιείται ο σύνδεσμος κατάλληλα.

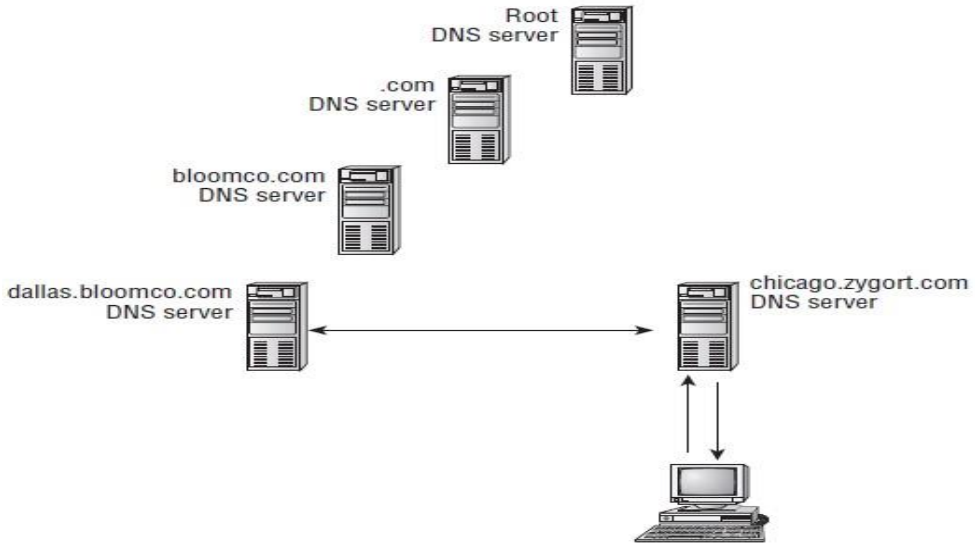
Ζώνες στέλεχος (Stub Zones)

Οι ζώνες στέλεχος δεν περιέχουν όλες τις εγγραφές από τη ζώνη όπως οι τύποι πρωτογενούς και δευτερεύουσας ζώνης. Αντιθέτως μόνο ένα υποσύνολο εγγραφών από τη ζώνη, αρκετά ώστε να παρέχει στον πελάτη τις πληροφορίες που είναι απαραίτητες για τον εντοπισμό ενός διακομιστή DNS που μπορεί να ανταποκριθεί σε ένα ερώτημα για εγγραφές από τη ζώνη. Όταν δημιουργείται η ζώνη stub, συμπληρώνεται με την εγγραφή SOA μαζί με τις εγγραφές NS και εγγραφές A που αντιστοιχούν στους διακομιστές DNS που προσδιορίζονται στην εγγραφή SOA. Όλα αυτά γίνονται αυτόματα. Ο διαχειριστής της ζώνης δεν χρειάζεται να δημιουργήσει το SOA, όνομα διακομιστή (Name Server – NS), ή A εγγραφές. Αντ' αυτού, καθώς δημιουργείται η ζώνη, ο διακομιστής DNS θα επικοινωνήσει με έναν διακομιστή που είναι έγκυρος για τη ζώνη αυτή και θα ζητήσει τη μεταφορά αυτών των εγγραφών. Μόλις ολοκληρωθεί, ο διακομιστής DNS κρατάει τη ζώνη stub και στη συνέχεια θα επικοινωνεί περιοδικά με τον εξουσιοδοτημένο διακομιστή για να διαπιστώσει εάν υπάρχουν αλλαγές στις εγγραφές SOA, NS και A. Μπορούμε να ελέγξουμε πόσο συχνά ο διακομιστής DNS μπορεί να ζητά ενημερώσεις ρυθμίζοντας τις παραμέτρους του διαστήματος ανανέωσης στην εγγραφή SOA για τη ζώνη.
Όταν ένας πελάτης κάνει ερώτηση στον διακομιστή DNS για να επιλύσει τη διεύθυνση IP ενός κεντρικού υπολογιστή, ο διακομιστής DNS θα κάνει προσπάθεια εντοπισμού της εγγραφής A για το όνομα κεντρικού υπολογιστή. Εάν ο διακομιστής DNS έχει ρυθμιστεί με ζώνη stub για το όνομα τομέα που περιέχεται στο ερώτημα, ο διακομιστής DNS θα στείλει ένα επαναληπτικό ερώτημα απευθείας σε έναν έγκυρο διακομιστής DNS για τη ζώνη. Στην εικόνα 6.4 , φαίνεται η κοινή διαδρομή ερωτήματος που πραγματοποιείται όταν ένας πελάτης προσπαθεί να επιλύσει μια διεύθυνση. Σε αυτήν την περίπτωση, ο πελάτης προσπαθεί να εντοπίσει τον server1.dallas.bloomco.com. Όταν ο πελάτης chicago.zygort.com στέλνει το αναδρομικό ερώτημα στον διακομιστή DNS, ο διακομιστής DNS θα "περπατήσει το δέντρο" στέλνοντας επαναληπτικά ερωτήματα στους διακομιστές DNS εκτελώντας τη διαδρομή έτσι ώστε να φτάσει τελικά σε έναν διακομιστή DNS που είναι έγκυρος για το dallas.bloomco.com.



Εικόνα 6.4

Στην εικόνα 6.5, έχουμε διαμορφώσει τον ίδιο διακομιστή με μια ζώνη stub για το dallas.bloomco.com.



Εικόνα 6.5

Όταν ο πελάτης στέλνει το αναδρομικό ερώτημα στον διακομιστή DNS του, ο διακομιστής DNS έχει μια ζώνη που αναφέρεται στη βάση δεδομένων της που της επιτρέπει να γνωρίζει ποιοι διακομιστές πρέπει να επικοινωνήσουν κατά την προσπάθεια εντοπισμού του dallas.bloomco.com. Ο διακομιστής DNS μπορεί στη συνέχεια να στείλει ένα μόνο επαναληπτικό ερώτημα στον εξουσιοδοτημένο διακομιστή και στη συνέχεια να στείλει το αποτέλεσμα πίσω στον πελάτη, καθιστώντας έτσι τη διαδικασία ανάλυσης πολύ πιο αποτελεσματική.
Όμως τίθεται το ερώτημα, "Γιατί να μην χρησιμοποιήσουμε μία υπό όρους προώθηση αντί για τη ζώνη στέλεχος;" Υπάρχουν δύο λόγοι για τους οποίους θέλουμε να χρησιμοποιήσουμε μια ζώνη stub αντί για μια προώθηση υπό όρους. Πρώτον, το stub

zone έχει αυτόματες δυνατότητες ενημέρωσης. Όταν επιτευχθεί το διάστημα ανανέωσης στην εγγραφή SOA, ο διακομιστής που διατηρεί τη ζώνη stub θα επικοινωνήσει με έναν εξουσιοδοτημένο διακομιστή για τη ζώνη και θα ενημερώσει τη λίστα διακομιστών ονομάτων και τις σχετικές διευθύνσεις τους. Οι υπό όρους προωθήσεις βασίζονται στο διαχειριστικό προσωπικό οι οποίοι κάνουν την ενημέρωση. Δεύτερον, η υπό όρους προώθηση θα απαιτήσει περισσότερη ισχύ επεξεργασίας προκειμένου να εκτελεστεί η λογική της αξιολόγησης των συνθηκών και να προσδιοριστεί ποια αντιστοιχεί. Οι πληροφορίες για τη stub zone διατηρούνται στη βάση δεδομένων DNS και μπορούν να αναλυθούν πολύ πιο γρήγορα.

6.2.3. Προστασία DNS

Το DNS είναι μια υπηρεσία που είναι πολύ επιρρεπείς για επιθέσεις, επειδή υπάρχουν πάρα πολλοί clients (πελάτες) που βασίζονται σε αυτό προκειμένου να εντοπίσουν τα συστήματα κεντρικού υπολογιστή που προσπαθούν να επικοινωνήσουν. Θα μπορούσαμε να καλούμε απευθείας τον διακομιστή ιστού με τη διεύθυνση IP του, αλλά είναι πολύ δύσκολο για τους περισσότερους από εμάς να θυμόμαστε τις διευθύνσεις IP των διακομιστών που επιθυμούμε να επικοινωνήσουμε.
Συνήθως υπάρχουν δύο μέθοδοι επίθεσης εναντίον διακομιστών DNS:

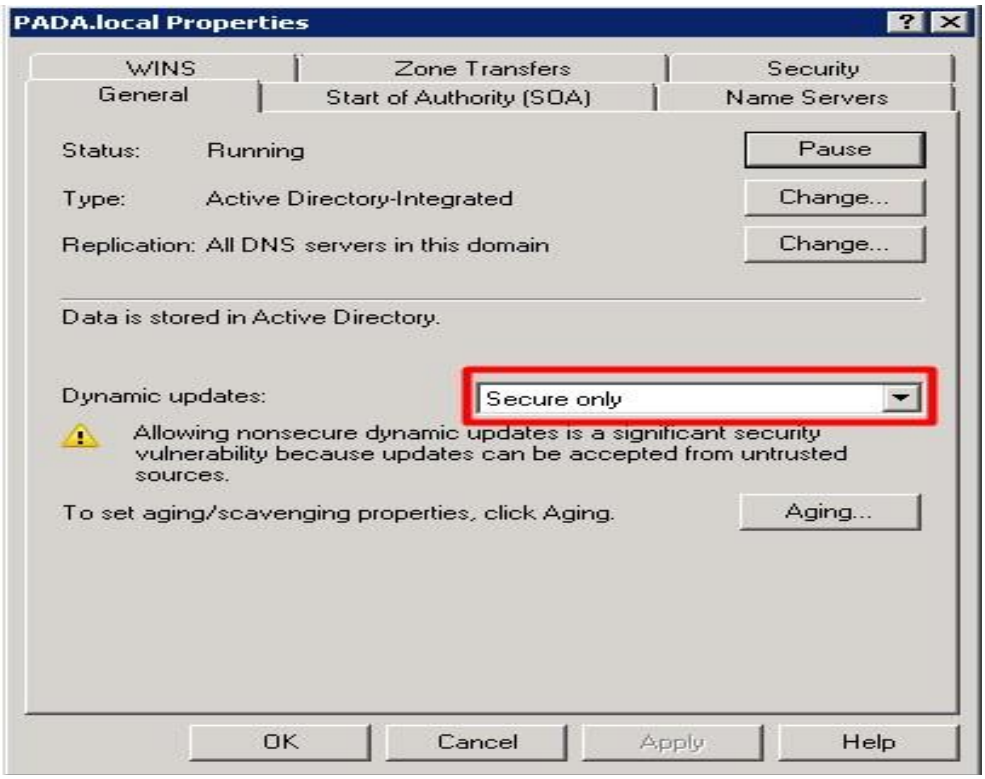
- επιθέσεις άρνησης υπηρεσίας (DoS)
- και κατάχρηση της ανάλυσης ονόματος.

Όταν κάποιος επιτίθεται στον διακομιστή DNS, ουσιαστικά προσπαθεί να αποτρέψει ή να παραπλανήσει επηρεάζοντας αρνητικά όλες τις υπηρεσίες του. Με επιθέσεις άρνησης υπηρεσίας, ο εισβολέας προσπαθεί να αποκλείσει τον διακομιστή DNS να απαντά σε ερωτήματα πελατών, αποκλείοντας έτσι τους πελάτες. Κατά την κατάχρηση της ανάλυσης ονόματος που παρέχει ένας διακομιστής DNS, ο εισβολέας είτε θα προκαλέσει λάθος αποτελέσματα στα στοιχεία που επιστρέφει ο διακομιστής DNS στον πελάτη ή θα συλλέξει πληροφορίες σχετικά με μια εταιρεία από τα δεδομένα που ο διακομιστής DNS επιστρέφει. Αυτή η μέθοδος δεν εμποδίζει την υπηρεσία DNS να ανταποκρίνεται στους πελάτες αλλά απλά τους παρερμηνεύει, στέλνοντάς τους σε λάθος προορισμό.
Κατανοώντας πόσο σημαντικό είναι το DNS για την υποδομή μιας εταιρείας, οι σχεδιαστές του DNS δημιούργησαν την υπηρεσία με τέτοιο τρόπο ώστε να είναι αρκετά ασφαλής και ικανή να αντέξει επιθέσεις που προσπαθούν να καταργήσουν τους διακομιστές DNS που υποστηρίζουν μια εταιρεία. Ωστόσο, ορισμένοι επιτιθέμενοι θα προσπαθήσουν να καταστρέψουν τον διακομιστή DNS έτσι ώστε να μπορέσουν να μειώσουν την αποτελεσματικότητα της οποιαδήποτε εφαρμογής που τρέχει και να παρενοχλήσουν τους πελάτες καθώς προσπαθούν να εκτελέσουν οποιεσδήποτε από τις εργασίες τους. Οι επιθέσεις άρνησης υπηρεσίας μπορεί να είναι καταστροφικές, αλλά μπορούν να ληφθούν μέτρα για την αποτροπή τους.

Περιορισμός των δυναμικών ενημερώσεων

Ένας ενσωματωμένος διακομιστής DNS Active Directory μπορεί να ρυθμιστεί έτσι ώστε να δέχεται αιτήματα δυναμικής ενημέρωσης μόνο από εξουσιοδοτημένα συστήματα. Μόλις πραγματοποιηθεί η διαμόρφωση μιας ζώνης ως ενεργός κατάλογος - ενσωματωμένος, θα πρέπει να γίνει αλλαγή των ρυθμίσεων στις δυναμικές ενημερώσεις, έτσι ώστε να επιτρέπονται μόνο οι ασφαλείς ενημερώσεις. Εφόσον είναι ενεργοποιημένη

αυτή η επιλογή, μόνο τα μέλη της υπηρεσίας καταλόγου Active Directory μπορούν να ενημερώσουν τις εγγραφές ζώνης. Έτσι μόλις ενεργοποιηθούν οι ασφαλείς ενημερώσεις, ένας εισβολέας δεν μπορεί εύκολα να προσθέσει στη βάση δεδομένων ψευδές εγγραφές που θα μπορούσαν να προκαλέσουν υπερφόρτωση του ελεγκτή τομέα καθώς προσπαθεί να αναπαραγάγει τις οποιεσδήποτε αλλαγές. Στην εικόνα 6.6 φαίνονται οι ιδιότητες της ζώνης για το PADA.local. Όπως θα παρατηρήσουμε οι δυναμικές ενημερώσεις έχουν οριστεί σε Secure Only.



Εικόνα 6.6

Σε έναν τομέα που βασίζεται σε Windows Server 2003 ή 2008, μπορούμε να βεβαιωθούμε ότι τα δεδομένα DNS αναπαράγονται μόνο σε ελεγκτές τομέα που είναι διακομιστές DNS ή να καθορίσουμε ότι οι εγγραφές αναπαράγονται μόνο στους διακομιστές DNS που περιλαμβάνονται στο πεδίο εφαρμογής σε ένα διαμέρισμα της εφαρμογής.

Παρακολούθηση κυκλοφορίας

Εάν ο διακομιστής DNS φαίνεται να είναι υπερφορτωμένος και πιστεύουμε ότι η επιβάρυνση πόρων οφείλεται σε επίθεση, μπορούμε να χρησιμοποιήσουμε εργαλεία παρακολούθησης, όπως το Network Monitor της Microsoft ή ένα εργαλείο όπως το Sniffer, για να μπορέσουμε να εντοπίσουμε από πού προέρχεται η κίνηση. Εάν η κίνηση φαίνεται να είναι εκτός της εταιρείας, τότε το πιο πιθανό είναι να δεχόμαστε επίθεση. Εάν διαπιστώσουμε κάτι τέτοιο, μπορούμε να επιχειρήσουμε να μειώσουμε την κυκλοφορία διαμορφώνοντας το τείχος προστασίας να εφαρμόζει κανόνες που θα απορρίπτουν

πακέτα που προέρχονται από τις διευθύνσεις που είδαμε ότι πιθανόν να γίνονται οι επιθέσεις. Τα περισσότερα τείχη προστασίας μπορούν να διαμορφωθούν ώστε να απορρίπτουν τα πλαστά πακέτα.
Η εφαρμογή κανόνων δεν σημαίνει ότι θα μπορέσουμε να σταματήσουμε την επίθεση. Πιθανόν ο εισβολέας να πλαστογράφησε πρώτα τη διεύθυνσή του, για να μπορέσει να ξανακάνει επίθεση μέσω άλλης διεύθυνσης. Ορισμένα τείχη προστασίας έχουν δυνατότητες ανίχνευσης εισβολής και μπορούν να διαμορφώνουν δυναμικά το τείχος προστασίας και να απορρίπτουν πακέτα εάν θεωρούν ότι είναι επίθεση. Επομένως θα πρέπει να έχουμε υλοποιήσει σχέδια αποφυγής για την παρακολούθηση της κυκλοφορίας που εισέρχεται στο δίκτυό μας, ανεξάρτητα από το αν είναι δεσμευμένο για DNS. Αυτά τα σχέδια θα πρέπει να λαμβάνουν υπόψη τους την ανάγκη παρακολούθησης για τύπους επίθεσης καθώς και να ελέγχουν την υπερβολική παρακολούθηση των πακέτων που εκτελούν έτσι ώστε να μην επηρεάζει αρνητικά την απόδοση του δικτύου. Η πολιτική παρακολούθησης DNS πρέπει να περιλαμβάνει αναφορές για το ποιος θα είναι υπεύθυνος για το σχεδιασμό, τη λύση παρακολούθησης, ποιος θα εφαρμόσει την πολιτική, πού θα εφαρμοστούν οι ρυθμίσεις και ποιος θα είναι υπεύθυνος για τον έλεγχο των δεδομένων που συλλέγονται. Σε παραδοσιακούς οργανισμούς, ένας διαχειριστής μπορεί να έχει πολλά άτομα που είναι υπεύθυνα για κάθε μέρος της παρακολούθησης DNS. Υπάρχουν νέα διαθέσιμα εργαλεία παρακολούθησης, όπως το Microsoft Operations Manager, που θα ενοποιήσουν την παρακολούθηση πολλών συστημάτων σε μια συνεκτική λύση.

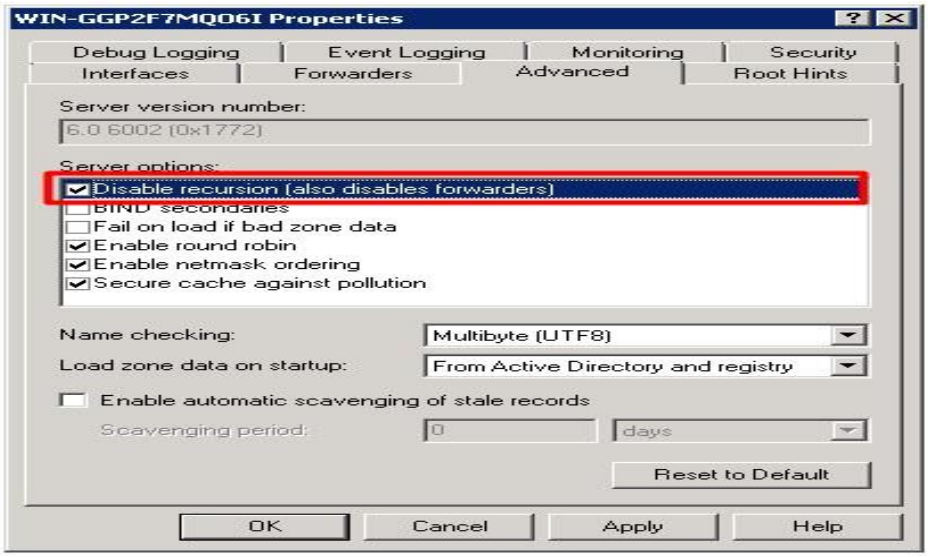
Ορισμός ποσοστώσεων

Σε τομείς Active Directory που βασίζονται σε Windows Server 2003 και 2008, υπάρχει η δυνατότητα να ορίσουμε ποσοστώσεις σχετικά με τον αριθμό αντικειμένων που επιτρέπεται να δημιουργεί ένας χρήστης στα διαμερίσματα της υπηρεσίας καταλόγου Active Directory. Μπορούμε να ορίσουμε διαφορετικές ποσοστώσεις σε κάθε διαμέρισμα της υπηρεσίας καταλόγου Active Directory, επειδή κάθε διαμέρισμα αξιολογείται χωριστά. Με τη χρήση ποσοστώσεων μπορούμε να ελέγχουμε αποτελεσματικά τον αριθμό των αντικειμένων που μπορούν να δημιουργηθούν από έναν λογαριασμό, καταργώντας έτσι κάθε προσπάθεια να γεμίσει μια ζώνη ολοκληρωμένης υπηρεσίας καταλόγου Active Directory πάρα πολλά ψεύτικα αντικείμενα. Μπορούμε να ορίσουμε ένα όριο ποσοστώσεων είτε σε λογαριασμούς χρηστών είτε σε λογαριασμούς ομάδας. Ένας λογαριασμός που έχει προστεθεί ρητά στη λίστα ποσοστώσεων και είναι μέλος μιας ομάδας που έχει εφαρμόσει ποσοστώσεις σε αυτήν θα είναι σε θέση να δημιουργήσει όσα αντικείμενα του έχουν αποδοθεί από τον περιορισμό της πολιτικής ποσοστώσεων. Όταν ένας χρήστης προσπαθεί να δημιουργήσει ένα αντικείμενο μέσα στο κοντέινερ όπου έχει οριστεί ένα όριο ποσοστώσεων, συγκρίνονται τα υπάρχοντα αντικείμενα στο όριο των ποσοστώσεων. Εάν ο χρήστης δεν έχει εκπληρώσει το όριο, το αντικείμενο μπορεί να δημιουργηθεί, αλλά εάν έχει φτάσει στα όρια που του αναλογούν τότε δεν έχει τη δυνατότητα δημιουργίας του αντικειμένου.
Η εντολή dsadd χρησιμοποιείται για τη δημιουργία ορίου για ένα διαμέρισμα Active Directory. Μπορείτε να ορίσουμε ποσοστώσεις σε οποιοδήποτε από τα διαμερίσματα, το σχήμα, τις διαμορφώσεις, τους τομείς ή τυχόν διαμερίσματα εφαρμογών. Στην πιο βασική της μορφή, μπορούμε να τη χρησιμοποιήσουμε για να ορίσετε απλώς ένα όριο σε ένα

διαμέρισμα. Για παράδειγμα, η εντολή dsadd quota -part zygort.lcl -acct zygort \ jprice -qlimit 10 θα περιόριζε τον λογαριασμό jprice έτσι ώστε να είναι σε θέση να δημιουργήσει μόνο 10 αντικείμενα εντός του διαμερίσματος τομέα zygort.lcl. Εάν αργότερα θέλουμε να τροποποιήσουμε τον αριθμό των αντικειμένων που θα μπορούσε να δημιουργήσει το jprice, θα μπορούσαμε να χρησιμοποιήσουμε την εντολή dsmod quota. Θα πρέπει βέβαια να γνωρίζουμε το πλήρως διακεκριμένο όνομα για την καταχώριση ποσοστώσεων προτού μπορέσουμε να αλλάξουμε το όριο των ποσοστώσεων. Με την εντολή quota dsquery μπορούμε να δούμε τα όρια που έχουν οριστεί.

Απενεργοποίηση αναδρομής

Η τυπική συμπεριφορά για έναν διακομιστή DNS είναι να αναλάβει τη διαδικασία ανάλυσης ονόματος όποτε ένας πελάτης προσπαθεί να επιλύσει ένα όνομα κεντρικού υπολογιστή. Οι πελάτες συνήθως στέλνουν ένα επαναληπτικό ερώτημα στον διακομιστή DNS τους και ο διακομιστής DNS ξεκινά τη διαδικασία αναδρομής για να εντοπίσει έναν διακομιστή DNS που μπορεί να προσδιορίσει τη διεύθυνση IP για το εν λόγω όνομα κεντρικού υπολογιστή. Ένας εισβολέας μπορεί να εκμεταλλευτεί αυτό το σενάριο και να αρχίσει να επιτίθεται στον διακομιστή DNS με πολλά ερωτήματα σε μια προσπάθεια να περιορίσει την ικανότητά του να ανταποκρίνεται σε έγκυρα ερωτήματα.
Όταν απενεργοποιούμε την αναδρομή σε έναν διακομιστή DNS, ουσιαστικά ο διακομιστής DNS δεν θα δεσμεύεται στον πελάτη και θα πρέπει να επιστρέφει μόνο παραπομπή στον πελάτη. Σε αυτό το σενάριο, ο διακομιστής DNS παίρνει ένα πολύ μικρότερο φορτίο, αλλά ο πελάτης θα αναλάβει μεγαλύτερο μέρος της εργασίας. Όσο οι πελάτες στέλνουν ερωτήματα στους διακομιστές DNS τους, οι διακομιστές DNS θα ελέγχουν τα δεδομένα ζώνης τους. Εάν ο διακομιστής DNS δεν είναι έγκυρος για τη ζώνη και δεν έχει αποθηκεύσει προσωρινά την καταχώριση, ο διακομιστής DNS θα παραπέμψει τον πελάτη σε άλλο διακομιστή DNS για επικοινωνία.
Για να απενεργοποιήσουμε την αναδρομή, ανοίγουμε τις ιδιότητες του διακομιστή DNS και επιλέγουμε απενεργοποίηση αναδρομής όπως φαίνεται στην εικόνα 6.7. Αυτό αφαιρεί το μεγαλύτερο μέρος της ευθύνης επίλυσης από τον διακομιστή DNS.



Εικόνα 6.7

6.2.4. Εγκατάσταση DNS

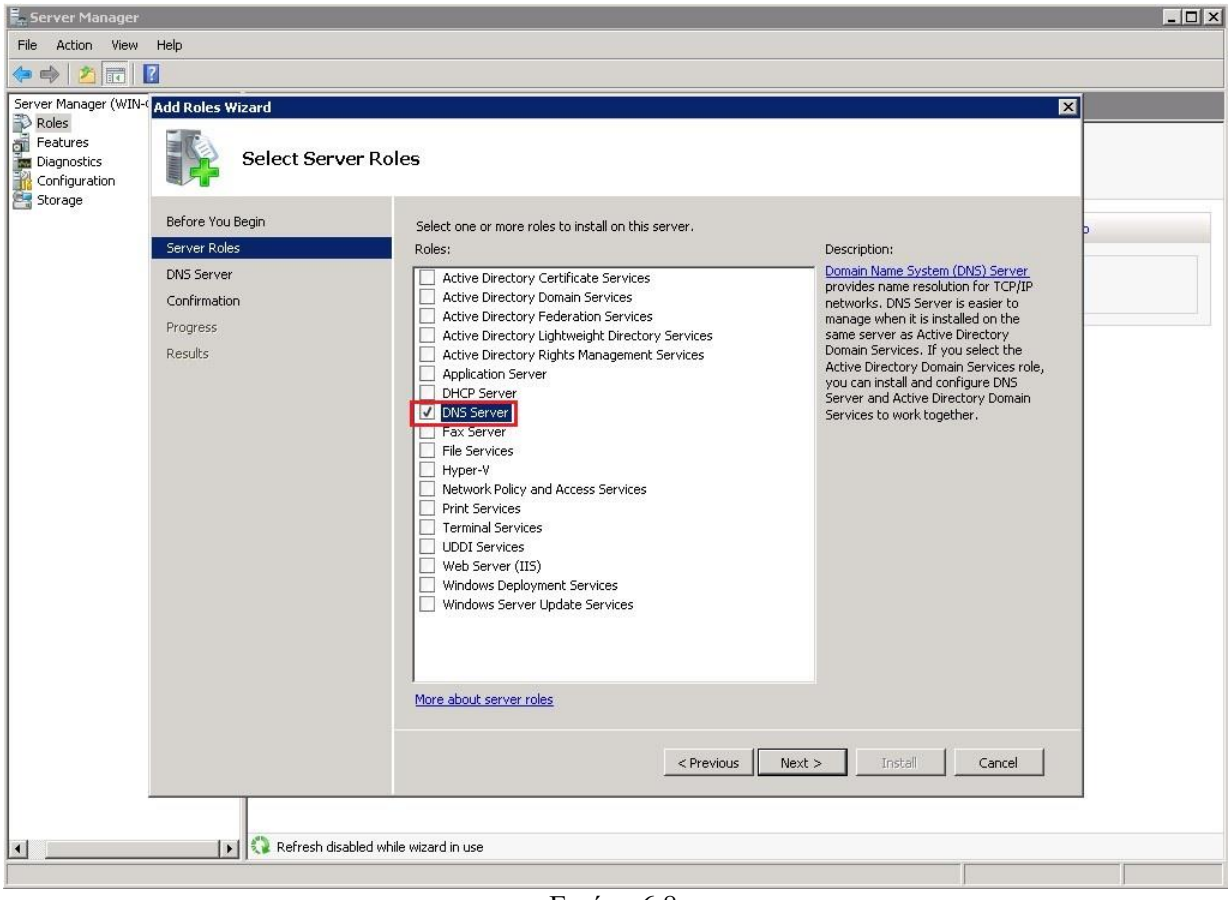
Η εγκατάσταση του Domain Name Services μπορεί να πραγματοποιηθεί με δύο τρόπους:

- Είτε με προσθήκη ρόλου – υπηρεσίας μέσα από τον Role Manager χωρίς να εγκαταστήσουμε κάποιο νέο Domain.

- Είτε με προσθήκη ρόλου – υπηρεσίας του Active Directory Domain Services όπου επειδή το DNS και το ADDS είναι δύο υπηρεσίες που πρέπει να λειτουργούν παράλληλα. Εδώ εγκαθιστούμε το νέο Domain το οποίο θα το συνδυάσει μαζί με όλες τις υπηρεσίες του ADDS

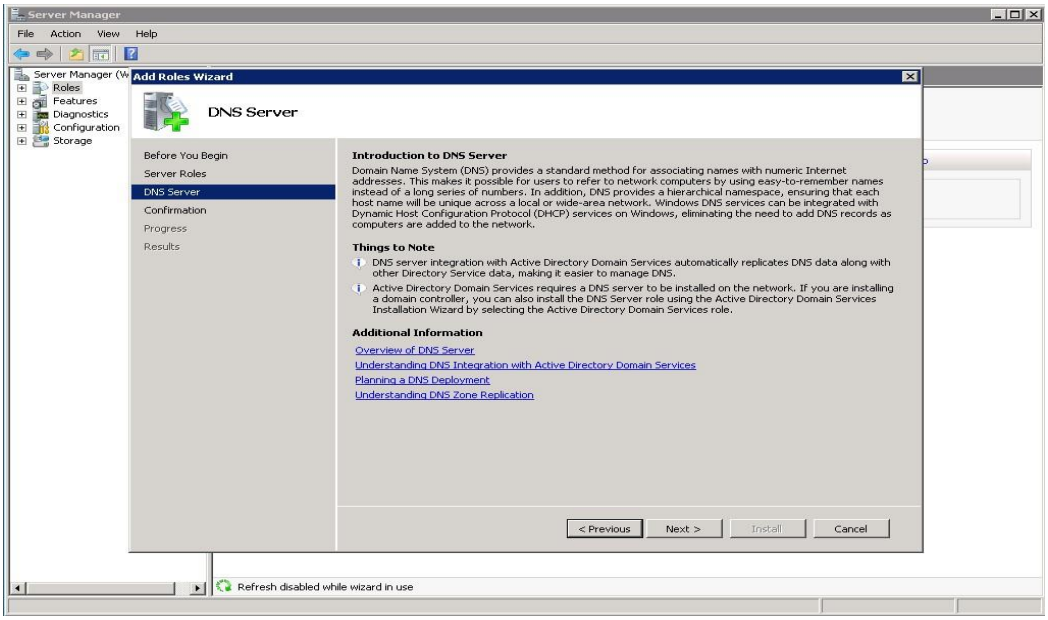
Εγκατάσταση υπηρεσίας DNS χωρίς το ADDS

Ανοίγουμε το παράθυρο διαλόγου του Server Manager. Στη συνέχεια επιλέγουμε τους ρόλους και πατάμε κλικ στην επιλογή Add Roles. Θα μας εμφανιστεί το παράθυρο διαλόγου όπως φαίνεται στην εικόνα 6.8. Επιλέγουμε την υπηρεσία DNS και στη συνέχεια πατάμε επόμενο (Next).



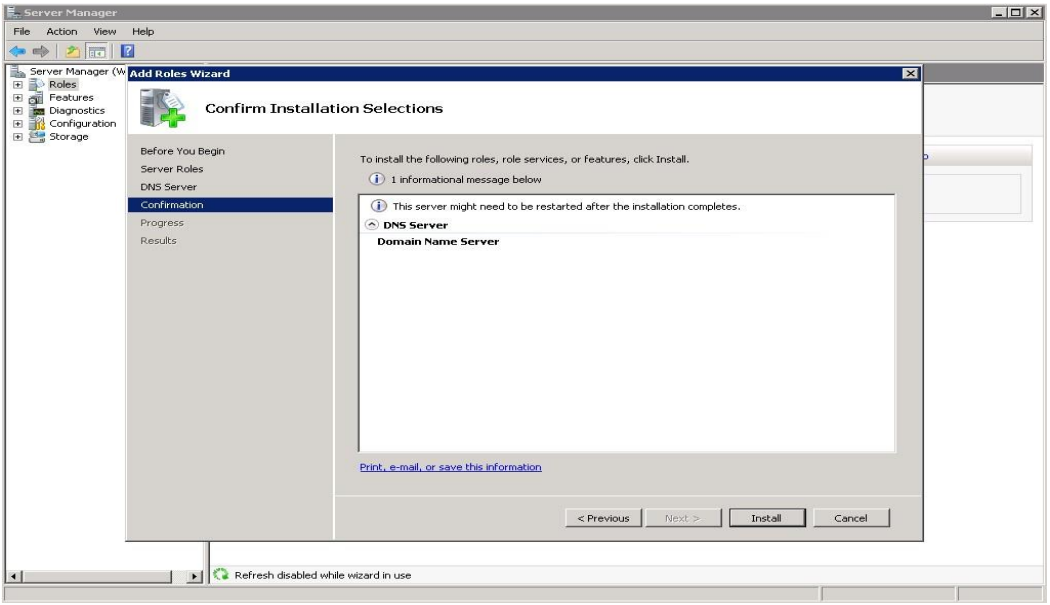
Εικόνα 6.8

Στη συνέχεια μας κάνει ένα overview της υπηρεσίας με τις δυνατότητες και τις επιλογές που μας παρέχει. Επιπρόσθετα παρέχονται και κάποια βοηθητικά link για να καταλάβουμε και να μας λυθούν οποιεσδήποτε απορίες τυχόν μπορεί να έχουμε για την υπηρεσία DNS. Στην εικόνα 6.9 φαίνονται οι παρακάτω δυνατότητες. Στη συνέχεια πατάμε επόμενο.



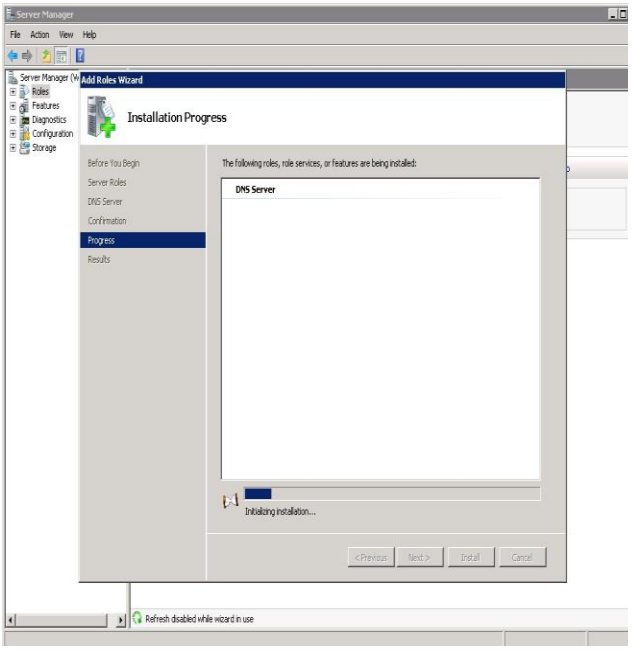
Εικόνα 6.9

Στο επόμενο παράθυρο διαλόγου το σύστημα μας ζητά να επιβεβαιώσουμε την επιλογή μας και αφού έχουμε ελέγξει ότι όλες τις επιλογές μας επιβεβαιώνουμε την επιλογή μας πατώντας στην επιλογή εγκατάστασης (Install) όπως φαίνεται στην εικόνα 6.10.

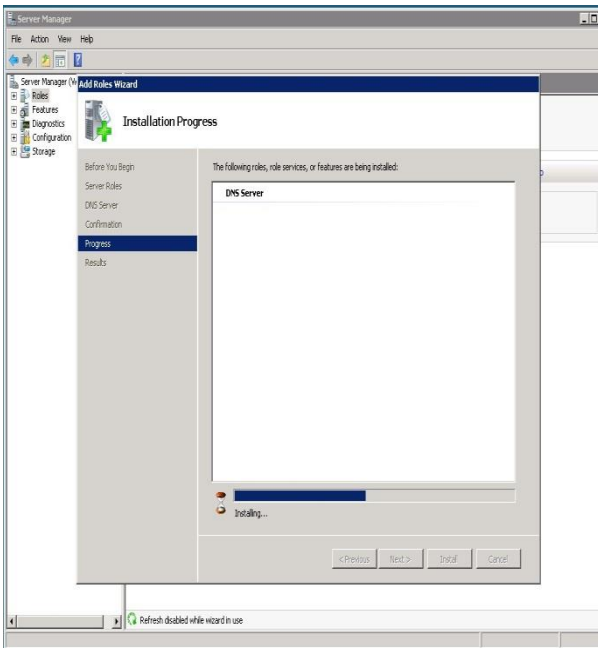


Εικόνα 6.10

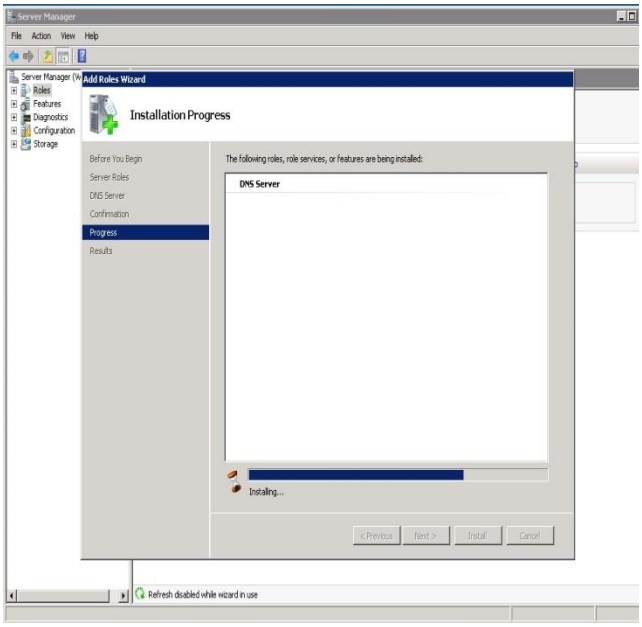
Στη συνέχεια το σύστημα ξεκινάει την εγκατάσταση της υπηρεσίας DNS. Η πρόοδος φαίνεται στις παρακάτω εικόνες.



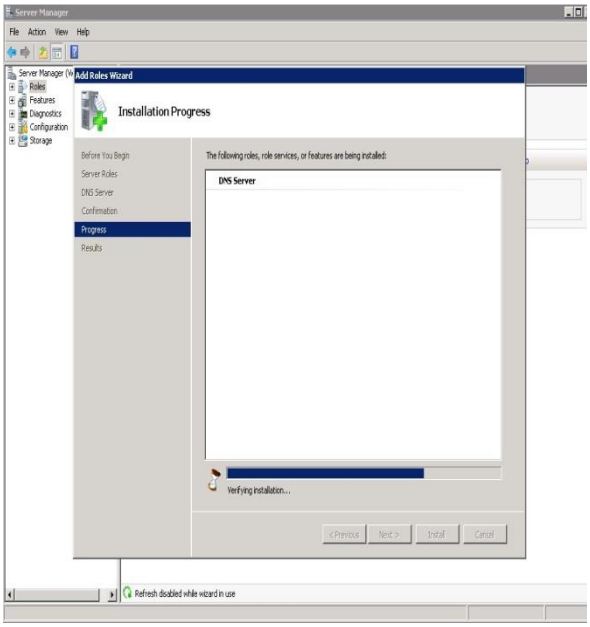
Εικόνα 6.11



Εικόνα 6.12

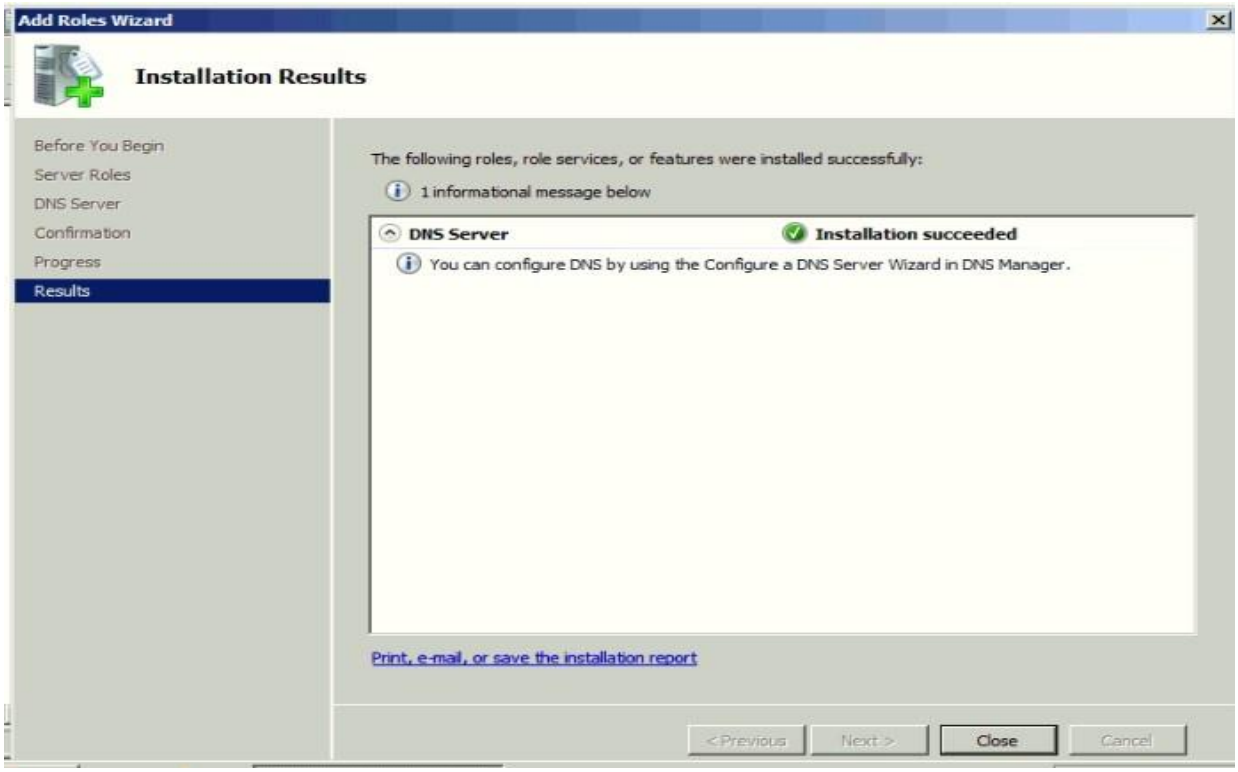


Εικόνα 6.13



Εικόνα 6.14

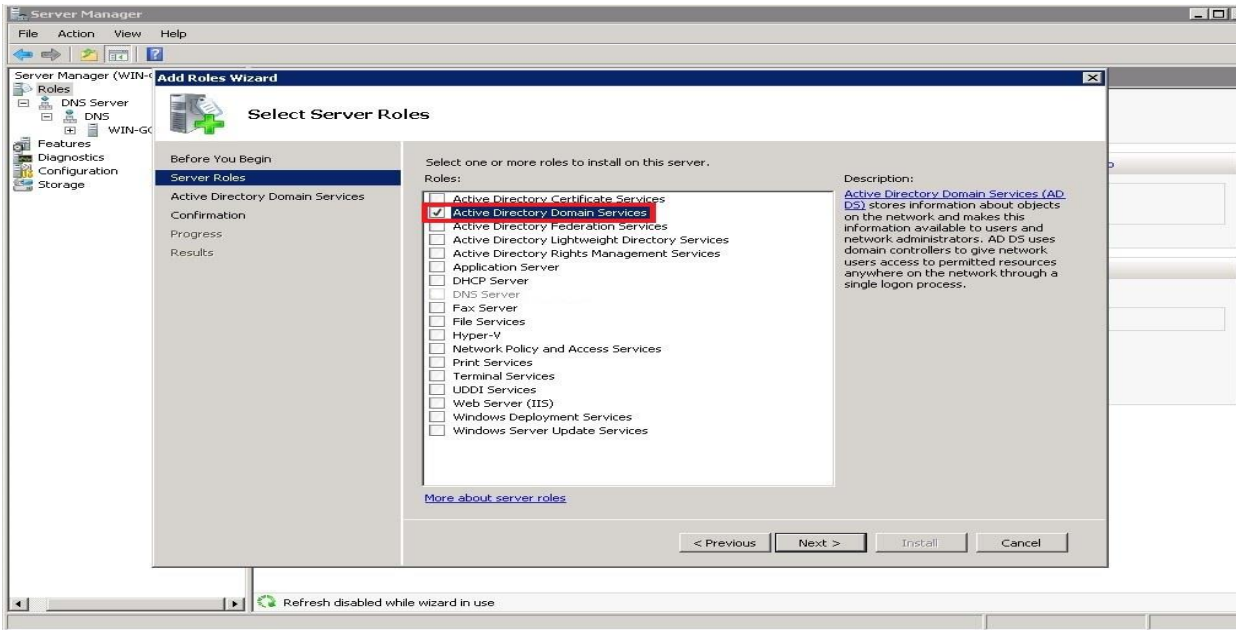
Τέλος το σύστημα μας ενημερώνει ότι η εγκατάσταση της νέας υπηρεσίας ολοκληρώθηκε και ότι μπορούμε να παραμετροποιήσουμε το νέο DNS με την βοήθεια του οδηγού DNS. Στην συνέχεια πατάμε στην επιλογή κλείσιμο (Close) για να ολοκληρώσουμε την εγκατάσταση. Οι επιλογές μας φαίνονται στην εικόνα 6.15.



Εικόνα 6.15

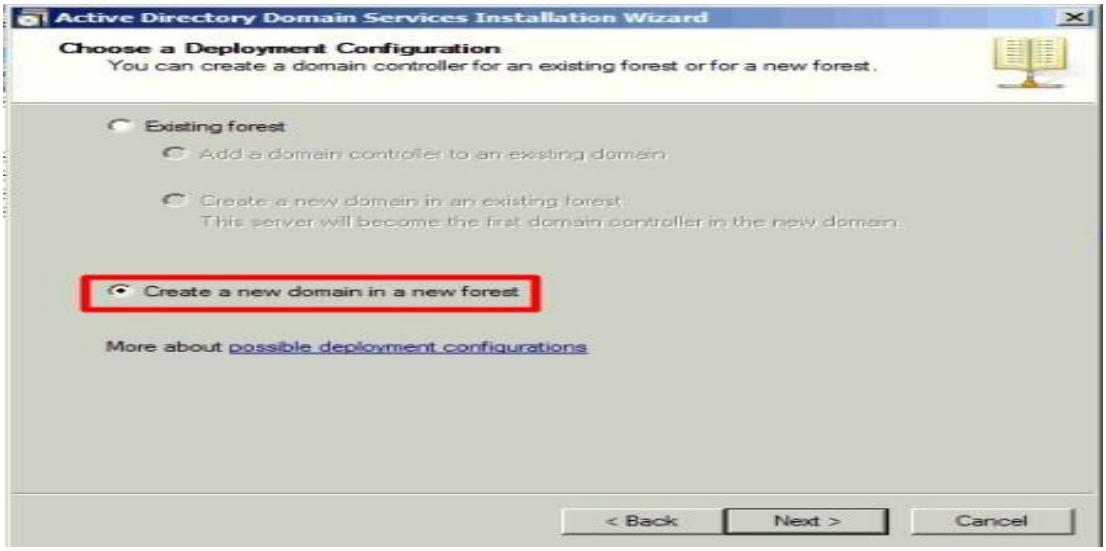
Εγκατάσταση υπηρεσίας DNS με το ADDS

Επιλέγουμε την υπηρεσία ADDS και στη συνέχεια επιλέγουμε Επόμενο (Next). Όπως παρατηρούμε στην εικόνα 6.16 δεν χρειάζεται να επιλέξουμε την υπηρεσία DNS γιατί θα μας υποχρεώσει το σύστημα από μόνο του σε επόμενο βήμα.



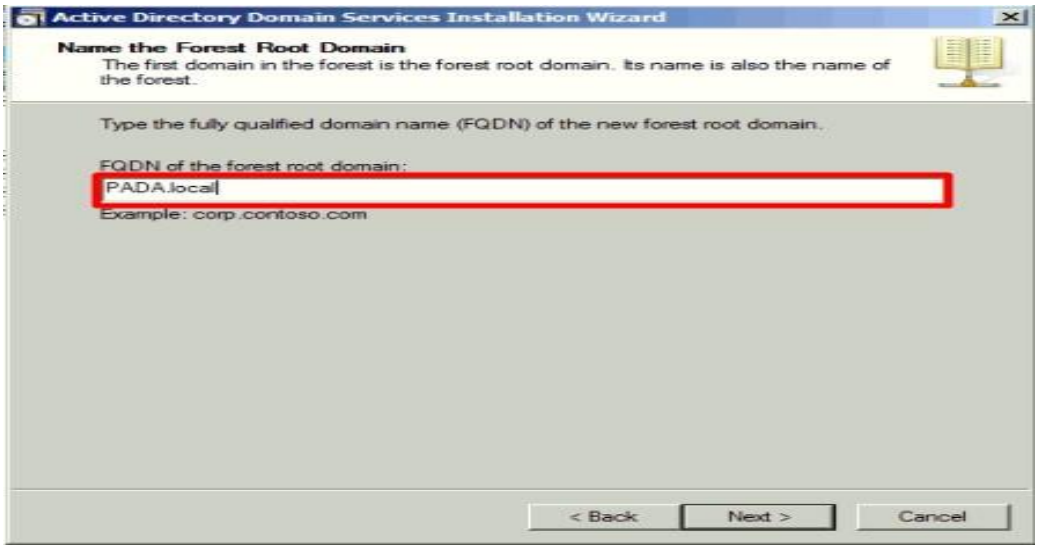
Εικόνα 6.16

Στο επόμενο βήμα στο παράθυρο διαλόγου που φαίνεται στην εικόνα 6.17 που ρωτάει εάν επιθυμούμε το ADDS ή εάν θέλουμε την δημιουργία ενός νέου Domain. Επιλέγουμε νέο Domain σε νέο Forest και στη συνέχεια πατάμε Επόμενο (Next).



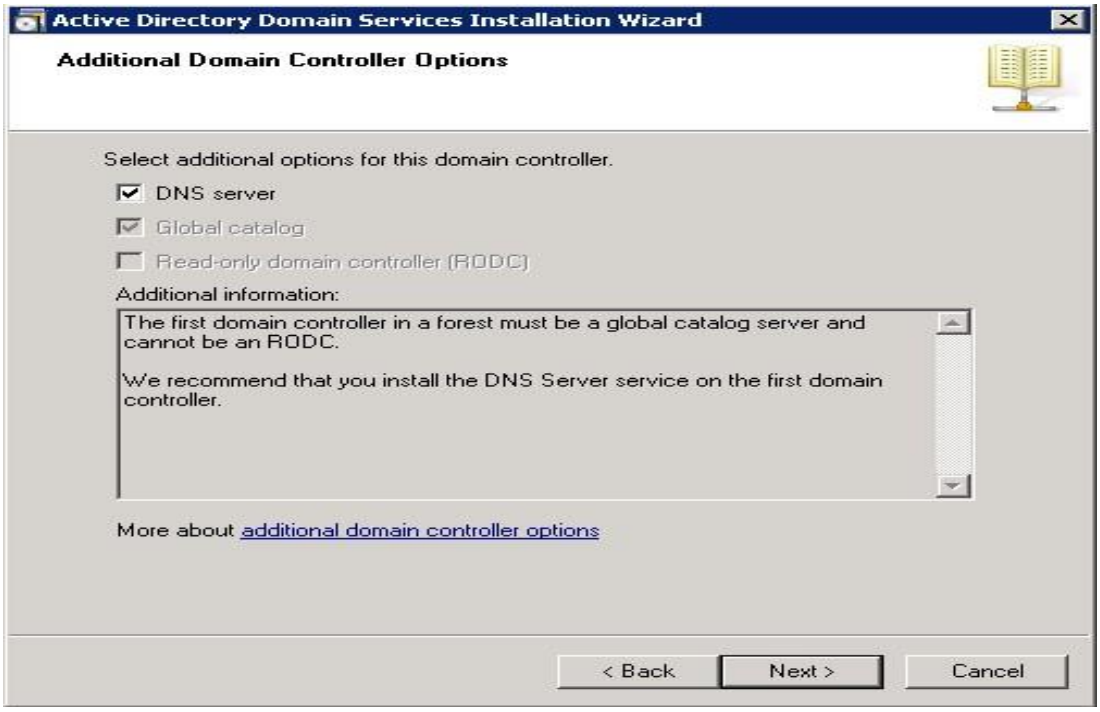
Εικόνα 6.17

Στην εικόνα 6.18 γράφουμε το όνομα του νέου Domain και στη συνέχεια πατάμε Επόμενο (Next).



Εικόνα 6.18

Στην εικόνα 6.19 όπως θα παρατηρήσουμε μας προτείνει το σύστημα να εγκαταστήσουμε την υπηρεσία DNS. Οπότε μαζί με την υπηρεσία ADDS εγκαθιστούμε ταυτόχρονα και την υπηρεσία DNS.



Εικόνα 6.19

6.3. Active Directory

Το Active Directory (AD) χρησιμοποιείται συχνά με τον ίδιο τρόπο όπως χρησιμοποιούνται οι λογαριασμοί διαχείρισης ασφαλείας (Security Accounts Manager – SAM) στους τομείς διαχείρισης (Domains) για την πραγματοποίηση ελέγχου ταυτότητας σε χρήστες και εξουσιοδότηση για πρόσβαση σε πόρους. Πολλά από τα χαρακτηριστικά από τα οποία το AD έχει ως πλήρη υπηρεσία καταλόγου δεν χρησιμοποιούνται.
Η υπηρεσία καταλόγου (Active Directory) μπορούμε να πούμε ότι είναι ένας τύπος βάσης δεδομένων που δημιουργείται ως "κατάλογος". Η διαφορά μεταξύ μιας σχεσιακής βάσης δεδομένων και ενός καταλόγου είναι ότι η βάση δεδομένων έχει βελτιστοποιηθεί για ενημέρωση, ενώ ο κατάλογος έχει βελτιστοποιηθεί για ανάγνωση. Με αυτόν τον τρόπο, το Active Directory αναπτύχθηκε με στόχο τα αντικείμενα που περιέχονται στον κατάλογο δεν θα αλλάζουν συχνά, αλλά θα χρησιμοποιηθούν για χρήστες, υπολογιστές και διαχειριστές για τον έλεγχο, τη διαχείριση και την παροχή πόρων σε έναν οργανισμό.
Μία από τις πιο βασικές λειτουργίες της υπηρεσίας καταλόγου είναι ότι παρέχει ένα κεντρικό αποθετήριο για πληροφορίες λογαριασμών χρηστών. Όταν ένας διαχειριστής δημιουργεί έναν λογαριασμό χρήστη, οι πληροφορίες του λογαριασμού διατηρούνται σε έναν ελεγκτή τομέα (Domain Controller) εντός του τομέα στον οποίο βρίσκεται ο χρήστης. Όλοι οι ελεγκτές τομέα εντός του τομέα θα λάβουν ένα πανομοιότυπο αντίγραφο του λογαριασμού χρήστη έτσι ώστε να γίνεται έλεγχος ταυτότητας του χρήστη χρησιμοποιώντας οποιονδήποτε ελεγκτή τομέα στον τομέα. Τυχόν αλλαγές που γίνονται στον λογαριασμό ενός χρήστη και πραγματοποιούνται σε έναν από τους ελεγκτές τομέα, αυτές οι αλλαγές αποστέλλονται σε όλους τους άλλους ελεγκτές τομέα εντός του τομέα. Αυτή η μεταφορά δεδομένων ονομάζεται αντιγραφή (Replication). Η αντιγραφή των πληροφοριών αυτών αποτελεί επιβάρυνση για το δίκτυο, ειδικά σε περιβάλλοντα με αρκετές χιλιάδες χρήστες, ομάδες, υπολογιστές και άλλα αντικείμενα. Προκειμένου να μετριαστεί το φορτίο αναπαραγωγής στο δίκτυο, το Active Directory αναπαράγει μόνο τα χαρακτηριστικά που έχουν αλλάξει και όχι ολόκληρο το αντικείμενο.

Τα κύρια στοιχεία που είναι σημαντικά για τη λειτουργικότητα του Active Directory Domain Services (AD DS) και προκειμένου να υπάρχει και συμβατότητα με το Διαδίκτυο αναλύονται στους παρακάτω τομείς:

- ✓ **Συμβατότητα TCP / IP:** Σε αντίθεση με ορισμένα από τα πρωτότυπα ιδιόκτητα πρωτόκολλα όπως IPX / SPX και NetBEUI, το πρωτόκολλο ελέγχου μετάδοσης (Transmission Control Protocol) / πρωτόκολλο Διαδικτύου (Internet Protocol) σχεδιάστηκε για cross-platform. Η επακόλουθη υιοθέτηση του TCP / IP ως πρότυπο Διαδικτύου για επικοινωνίες υπολογιστών το έχει ανεβάσει στην πρώτη γραμμή πρωτοκόλλων στο κόσμο και ουσιαστικά έγινε απαίτηση για τη λειτουργία των επιχειρησιακών συστημάτων. Τα AD DS και Windows 2008 χρησιμοποιούν τη στοίβα πρωτοκόλλων TCP / IP ως κύρια μέθοδος επικοινωνίας.
- ✓ **Υποστήριξη Lightweight Directory Access Protocol:** Το Lightweight Directory Access Protocol (LDAP) έχει αναδειχθεί ως το τυπικό πρωτόκολλο καταλόγου Διαδικτύου και χρησιμοποιείται για ενημέρωση και αναζήτηση δεδομένων στον κατάλογο. Το AD DS υποστηρίζει άμεσα το LDAP.
- ✓ **Υποστήριξη Domain Name System (DNS)** - Το DNS δημιουργήθηκε λόγω της ανάγκης μετάφρασης απλουστευμένων ονομάτων που μπορούν να κατανοηθούν από τον άνθρωπο (όπως το www.cco.com) σε μία Διεύθυνση IP που γίνεται κατανοητή από

έναν υπολογιστή (όπως 192.168.1.151). Η δομή του AD DS υποστηρίζει και απαιτεί αποτελεσματικά το DNS να λειτουργεί σωστά.

- ✓ **Υποστήριξη ασφάλειας:** Η υποστήριξη ασφαλείας βάσει προτύπων Διαδικτύου είναι ζωτικής σημασίας για την ομαλή λειτουργία ενός περιβάλλοντος που είναι ουσιαστικά συνδεδεμένο με εκατομμύρια υπολογιστές σε όλο τον κόσμο. Η έλλειψη ισχυρής ασφάλειας είναι μια προτροπή για παραβίαση και τα Windows 2008 και AD DS έχουν αυξήσει την ασφάλεια σε υψηλότερα επίπεδα. Υποστήριξη για IP Ασφάλεια (IPSec), Kerberos, Αρχές έκδοσης πιστοποιητικών και Secure Sockets Layer (SSL) κρυπτογράφηση είναι ενσωματωμένη στα Windows 2008 και AD DS.
- ✓ **Ευκολία διαχείρισης:** Αν και συχνά παραβλέπεται σε ισχυρές υλοποιήσεις υπηρεσιών καταλόγου, η ευκολία στην οποία το περιβάλλον διαχειρίζεται και διαμορφώνεται επηρεάζει άμεσα το συνολικό κόστος που σχετίζεται με τη χρήση του. Τα AD DS και Windows 2008 έχουν σχεδιαστεί ειδικά για ευκολία στη χρήση για να μειώσουν την καμπύλη μάθησης που σχετίζεται με τη χρήση ενός νέου περιβάλλοντος.

6.3.1. Active Directory Components

Το Active Directory (AD) είναι το όνομα που χρησιμοποιεί πλέον η Microsoft για την ομαδοποίηση όλων των λύσεων διαχείρισης ταυτότητας. Το AD περιλαμβάνει πέντε βασικά συστατικά όπου αυτοί οι ρόλοι αποτελούν την υποδομή διαχείρισης ταυτότητας που παρέχει η Microsoft σε οργανισμούς που υλοποιούνται πάνω σε υποδομές δικτύων. Καθένα παρέχει μια συγκεκριμένη υπηρεσία διαχείρισης ταυτότητας όπου κάθε υπηρεσία στοχεύει σε ένα συγκεκριμένο τμήμα του δικτύου:

- ➢ **AD Domain Services (ADDS)**, που αρχικά ονομαζόταν Active Directory, παρέχοντας υπηρεσίες ελέγχου ταυτότητας και εξουσιοδότησης σε δίκτυο. Το ADDS είναι ο πυρήνας του δικτύου Windows Server 2008. Είναι το κεντρικό συστατικό που δεν εξυπηρετεί μόνο την παροχή ελέγχου ταυτότητας και εξουσιοδότησης, αλλά και διαχείριση, ανταλλαγή πληροφοριών και διαθεσιμότητα πληροφοριών. Στην πραγματικότητα, το ADDS μπορεί να οριστεί ως εξής: «Ένα ασφαλές εικονικό περιβάλλον όπου οι χρήστες μπορούν να αλληλεπιδράσουν ο ένας με τον άλλον ή με στοιχεία δικτύου, όλα σύμφωνα με τους επιχειρηματικούς κανόνες μιας επιχείρησης. "

- ➢ **AD Lightweight Directory Services (ADLDS)**, που παλαιότερα ήταν γνωστό ως Active Directory Application Mode (ADAM) και στοχεύει στην παροχή μιας αποθήκευσης δεδομένων για περιβάλλοντα που δεν έχουν πρόσβαση σε πλήρες επίπεδο υπηρεσίας ADDS. Το ADLDS, από την άλλη πλευρά, έχει δύο κύριες χρήσεις:

1. Χρησιμοποιείται για την ενσωμάτωση εφαρμογών σε μια υπηρεσία καταλόγου χωρίς να χρειάζεται τροποποιήστε τη δομή του καταλόγου ADDS. Σε αυτήν την περίπτωση, το ADLDS σχηματίζει μια επέκταση του βασικού καταλόγου στο δίκτυο, μια επέκταση που μπορεί να δομηθεί σε μια βάση ανά εφαρμογή. Επιπλέον, αυτή η επέκταση γίνεται φορητή και μπορεί να εφαρμοστεί στην εκάστοτε εφαρμογή όπου και αν βρίσκεται.
2. Το ADLDS χρησιμοποιείται σε σενάρια αποστρατικοποιημένης ζώνης (DMZ). Λίγοι οργανισμοί θέλουν να εφαρμόσουν μια δομή ADDS σε DMZ, και ακόμη λιγότεροι θέλουν να συνδέσουν τους εσωτερικά ADDS σε εξωτερικές ζώνες. Εδώ μπαίνει το ADLDS. Μπορεί να χρησιμεύσει ως ο κατάλογος πηγής για δικαιώματα εφαρμογής χωρίς να τίθεται σε κίνδυνο κανένα στοιχείο που μπορεί να βρεθεί στην εσωτερική δομή ADDS.

- **AD Rights Management Services (ADRMS)**, οι οποίες βοηθούν στον κατάλληλο έλεγχο της χρήση εγγράφων και δεδομένων που δημιουργεί ο οργανισμός μιας επιχείρησης. Το ADRMS χρησιμοποιείται εσωτερικά για την προστασία της πνευματικής ιδιοκτησίας σας. Γίνεται μία επέκταση του ADDS και αποτελεί τον πυρήνα του συστήματος προστασίας δεδομένων σας.

- **AD Certificate Services (ADCS)**, η οποία ήταν παλαιότερα γνωστή ως δημόσια υποδομή κλειδιού (PKI) και χρησιμοποιείται για τη δημιουργία και διαχείριση αρχών πιστοποίησης. Χρησιμοποιείται κυρίως εσωτερικά, καθώς έχει σχεδιαστεί για να παρέχει υπηρεσίες PKI και στους δύο, χρήστες και υπολογιστές. Μπορεί να χρησιμοποιηθεί για την ψηφιακή υπογραφή προγραμμάτων οδήγησης συστήματος και λογισμικού, ενοποίηση με έλεγχο ταυτότητας έξυπνης κάρτας και γενικά παρέχει μη απορριφθέντες υπηρεσίες στην εσωτερική σας κοινότητα. Μπορεί επίσης να χρησιμοποιηθεί για την παροχή αυτών των υπηρεσιών σε εξωτερικές κοινότητες, αλλά για να γίνει αυτό, θα πρέπει να συνδέεται με μια εξωτερική, γνωστή αρχή πιστοποίησης που θα αποδείξει σε άλλους ότι είναι κάποιος πιστοποιημένος χρήστης.

- **AD Federation Services (ADFS)** που χρησιμοποιείται για την παροχή απλουστευμένων και ασφαλών οργανισμών ταυτοποίησης, καθώς και υπηρεσίες ενιαίας σύνδεσης για εφαρμογές Web. Το ADFS στοχεύει στην επέκταση της εσωτερικής δομής του ADDS στον εξωτερικό κόσμο μέσω κοινών θυρών πρωτοκόλλου ελέγχου μετάδοσης (TCP) / πρωτοκόλλου Διαδικτύου (IP), όπως η πόρτα 80 (Hypertext Transfer Protocol - HTTP) και η πόρτα 443 (Secure HTTP ή HTTPS). Συνήθως βρίσκεται στο DMZ και χρησιμοποιείται για τη δημιουργία συνεργασιών με άλλους οργανισμούς.

Όπως μπορούμε να δούμε και στην εικόνα 6.20, κάθε τεχνολογία AD παίζει σημαντικό ρόλο στην παροχή μιας πλήρως και ολοκληρωμένης υποδομής διαχείρισης ταυτότητας σε έναν οργανισμό.

Εικόνα 6.20

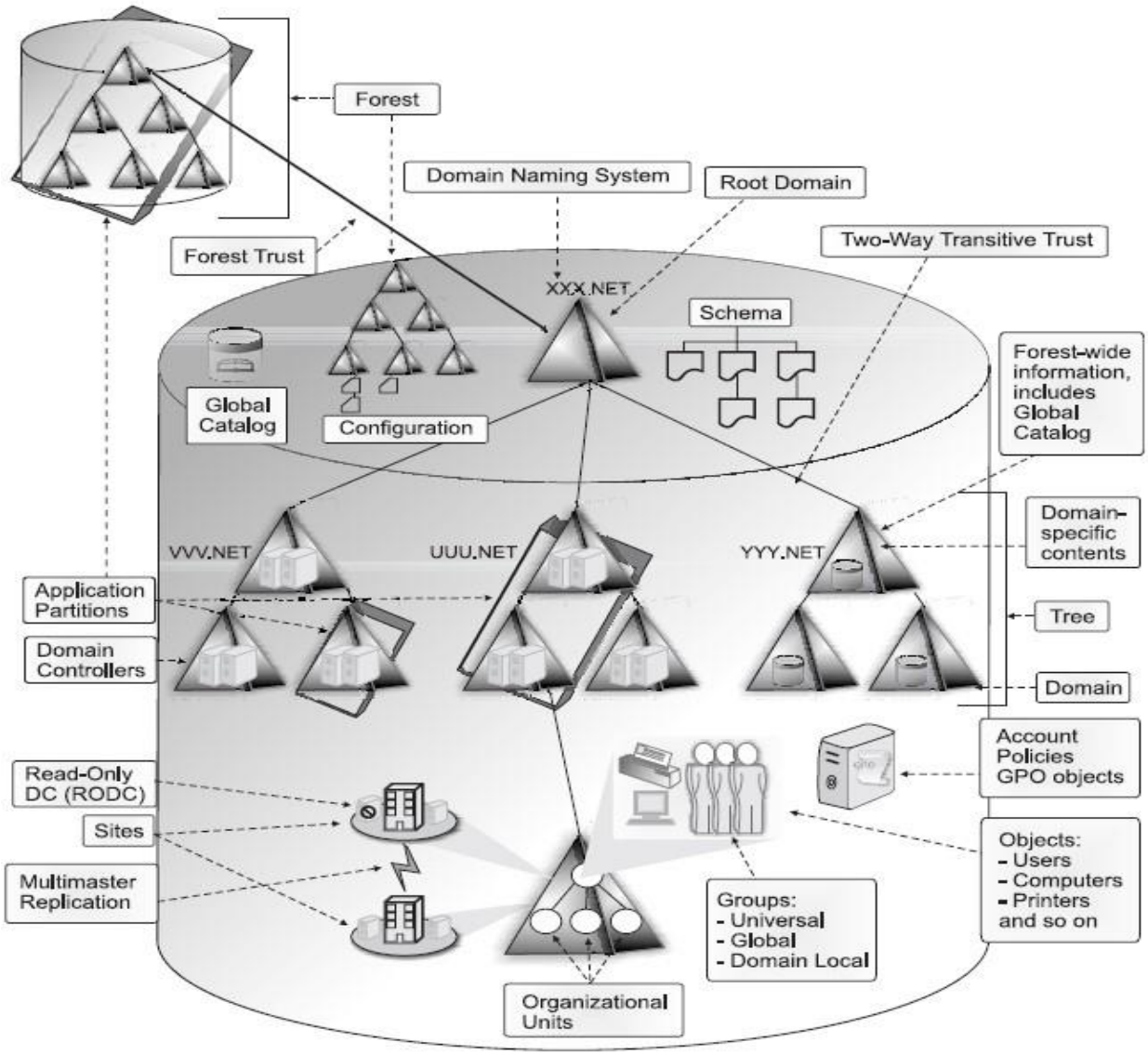
6.3.2. Active Directory Domain Services

Οι υπηρεσίες τομέα (Domain Services) Active Directory βασίζονται κυρίως σε μια ιεραρχική βάση δεδομένων όπως φαίνεται στην εικόνα 6.21. Ως εκ τούτου, εφόσον αναφερόμαστε σε βάση δεδομένων, η βάση δεδομένων καταλόγου περιέχει μια δομή βάσης δεδομένων. Αυτό το σχήμα ισχύει για κάθε μορφή Active Directory Domain Services (ADDS).

Ένα στιγμιότυπο της ε λόγω βάσης ορίζεται ως Ενεργό Δάσος καταλόγου (Active Directory forest). Το δάσος είναι το μεγαλύτερο ενιαίο διαμέρισμα για οποιαδήποτε δομή βάσης δεδομένων. Όλοι όσοι συμμετέχουν στο δάσος θα μοιράζονται ένα δεδομένο σύνολο χαρακτηριστικών και τύπων αντικειμένων. Αυτό δεν σημαίνει ότι το δάσος είναι το γενικό όριο της υπηρεσίας καταλόγου Active Directory. Τα δάση μπορούν να ομαδοποιηθούν μαζί για να μοιραστούν ορισμένες πληροφορίες. Τα Windows Server 2003 παρουσίασαν την έννοια του δάσους trusts, τα οποία επιτρέπουν στα δάση να μοιράζονται τμήματα ολόκληρης της βάσης δεδομένων Active Directory μαζί με άλλους και αντίστροφα. Αυτή η ιδέα παρουσιάζεται με τα Windows Server 2008 (WS08). Εάν γίνει σύγκριση του δάσους WS08 με τα Windows NT, τα NT περιελάμβαναν μια βάση δεδομένων διαχείρισης ταυτότητας, το Domain, το πεδίο εφαρμογής του ήταν σοβαρά περιορισμένο σε σύγκριση με το ADDS. Το NT θα μπορούσε να αποθηκεύσει το όνομα χρήστη ή υπολογιστή μαζί με κωδικούς πρόσβασης και μερικούς κανόνες που επηρεάζουν όλα τα αντικείμενα. Η βάση δεδομένων ADDS περιλαμβάνει περισσότερους από 200 τύπους αντικειμένων και πάνω από 1.000 χαρακτηριστικά προεπιλεγμένα. Φυσικά, μπορούν να προστεθούν περισσότεροι τύποι αντικειμένων ή χαρακτηριστικά στη βάση δεδομένων. Προϊόντα λογισμικού που εκμεταλλεύονται τις πληροφορίες που είναι αποθηκευμένες στο ADDS μπορούν επίσης να επεκτείνουν το σχήμα του. Το Microsoft Exchange, για παράδειγμα, διπλασιάζει σχεδόν το αριθμό αντικειμένων και χαρακτηριστικών στο δάσος λόγω της ενσωμάτωσής του στον κατάλογο.

Όπως κάθε βάση δεδομένων κατηγοριοποιεί αυτά τα αντικείμενα, σε αντίθεση όμως με τις σχεσιακές βάσεις δεδομένων, αυτή η βάση δεδομένων υλοποιεί μία ιεραρχική δομή επειδή βασίζεται στη δομή του Συστήματος Ονομάτων Χώρου (Domain Name System’s - DNS). Ακολουθεί δηλαδή μία ιεραρχική δομή όπως είναι και ο παγκόσμιος ιστός.

Τα δάση δρουν με τον ίδιο τρόπο. Σε ένα δάσος, το σημείο ρίζας (όπως και με την αρχική σελίδα σε μία ιστοσελίδα) είναι ο ριζικός τομέας. Κάθε δάσος ADDS πρέπει να έχει τουλάχιστον έναν τομέα. Οι τομείς ενεργούν ως χωριστά κοντέινερ αντικειμένων μέσα στο δάσος. Οι τομείς μπορούν να συγκεντρωθούν σε δέντρα. Τα δέντρα διαχωρίζονται μεταξύ τους μέσω του ονόματος DNS τους. Η Microsoft, για παράδειγμα, έχει ένα πολύφυτο δάσος. Το "namespace" του, το στοιχείο DNS που καθορίζει τα όρια του δάσους, είναι το microsoft.com. Ως εκ τούτου, όλοι οι τομείς σε αυτό το δέντρο έχουν ονόματα παρόμοια με αυτό domain.microsoft.com. Η Microsoft δημιούργησε ένα δεύτερο δέντρο όταν ενσωμάτωσε το MSN.com μέσα στο δάσος του. Ο χώρος ονομάτων MSN.com δημιούργησε αυτόματα ένα δέντρο και όλοι οι τομείς που βρίσκονται κάτω από αυτό ονομάζονται domain.MSN.com.



Εικόνα 6.21

Κάθε δάσος περιλαμβάνει τουλάχιστον ένα δέντρο και έναν τομέα. Ο τομέας είναι και η πολιτική ασφαλείας και το διοικητικό όριο μέσα στο δάσος. Απαιτείται να περιέχει αντικείμενα όπως χρήστες, υπολογιστές, διακομιστές, ελεγκτές τομέα (DC), εκτυπωτές, κοινόχρηστα αρχεία, εφαρμογές και πολλά περισσότερα. Εάν υπάρχουν περισσότεροι από έναν τομείς στο σύμπλεγμα, αυτοί θα συνδέονται αυτόματα με όλους τους άλλους μέσω μιας αυτόματης μεταβατικής αμφίδρομης εμπιστοσύνης. Ο τομέας ορίζεται ως όριο ασφαλείας επειδή περιέχει κανόνες που ισχύουν για τα αντικείμενα που περιέχει. Αυτοί οι κανόνες μπορούν να είναι υπό μορφή πολιτικών ασφαλείας ή αντικειμένων πολιτικής ομάδας (Group Policy Objects – GPOs). Οι πολιτικές ασφαλείας είναι κανόνες που εφαρμόζονται σε όλο τον τομέα. Τα GPO τείνουν να είναι πιο διακριτά και πρέπει να εφαρμόζονται σε συγκεκριμένα αντικείμενα κοντέινερ. Ενώ οι τομείς έχουν διακριτά όρια ασφαλείας, το δάσος θα παραμένει πάντα το απόλυτο όριο ασφάλειας εντός μιας δομής ADDS.

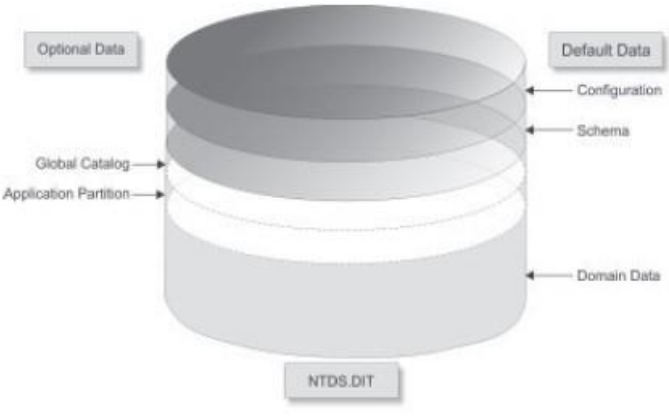
Ο τομέας ονομάζεται διοικητικό όριο επειδή, από προεπιλογή, οι πολιτικές που ισχύουν για τα αντικείμενά της δεν ξεπερνούν τα όρια του τομέα. Τα περιεχόμενα τομέα μπορούν να κατηγοριοποιηθούν περαιτέρω μέσω ομαδοποίησης τύπων αντικειμένων όπως οργανωτικές μονάδες (Organization Units – OU) ή ομάδες. Οι οργανωτικές μονάδες παρέχουν ομαδοποιήσεις που μπορούν να χρησιμοποιηθούν για διοικητικούς ή εξουσιοδοτημένους σκοπούς. Οι OUs χρησιμοποιούνται συνήθως για τον διαχωρισμό αντικειμένων κάθετα, επειδή αντικείμενα όπως χρήστες και υπολογιστές μπορούν να βρίσκονται μόνο σε μία OU. Τα group τείνουν να περιέχουν οριζόντιες συλλογές αντικειμένων. Ένα αντικείμενο όπως ένας χρήστης μπορεί να συμπεριληφθεί σε αρκετά group αλλά μόνο σε μία μόνο OU.
Δουλεύοντας σε ένα κατανεμημένο δάσος που αποτελείται από πολλά διαφορετικά δέντρα και δευτερεύοντες τομείς μπορεί να προκαλέσει σύγχυση στον χρήστη. Το ADDS υποστηρίζει την έννοια του καθολικού κύριου ονόματος (Universal Principal Name – UPN). Το UPN αποτελείται συνήθως από το όνομα χρήστη μαζί με το κοινόχρηστο ριζικό όνομα του δάσους. Αυτό το όνομα ρίζας μπορεί να είναι το όνομα του δάσους ή ένα ειδικό ψευδώνυμο που έχει εκχωρηθεί. Για παράδειγμα, σε ένα δάσος που ονομάζεται TandT.net, μπορεί να χρησιμοποιηθεί το name.surname@tandt.com ως UPN, διευκολύνοντας τους χρήστες έτσι ώστε να χρησιμοποιούν το εξωτερικό όνομα DNS για το UPN. Οι χρήστες μπορούν να συνδεθούν σε οποιονδήποτε τομέα που είναι επιτρεπτός εντός του δάσους χρησιμοποιώντας το UPN τους. Στον τοπικό τομέα τους, μπορούν απλώς να χρησιμοποιήσουν το όνομα χρήστη τους αν το προτιμούν.
Τα δάση, τα δέντρα, οι τομείς, οι οργανωτικές μονάδες, οι ομάδες, οι χρήστες και οι υπολογιστές είναι όλα αντικείμενα αποθηκευμένα στη βάση δεδομένων ADDS. Ως εκ τούτου, μπορούν να διαχειριστούν γενικά ή ξεχωριστά .
Μια σημαντική διαφορά μεταξύ της υπηρεσίας καταλόγου Active Directory και μιας τυπικής βάσης δεδομένων είναι ότι η ADDS εκτός από ιεραρχική, είναι και πλήρως αποκεντρωμένη. Οι περισσότερες βάσεις δεδομένων Active Directory διανέμονται επίσης γεωγραφικά επειδή αντιπροσωπεύουν την πραγματική φύση ενός οργανισμού. Μόνο πολύ μικροί οργανισμοί που έχουν έναν μόνο ιστότοπο έχουν μια βάση δεδομένων που βρίσκεται εξ ολοκλήρου σε μία τοποθεσία.
Η διαχείριση μιας πλήρως κατανεμημένης βάσης δεδομένων είναι πολύ πιο δύσκολη από ό, τι η διαχείριση μιας βάσης δεδομένων που βρίσκεται σε μία μόνο περιοχή. Για απλοποίηση κατανεμημένων ζητημάτων βάσης δεδομένων, το ADDS εισάγει την έννοια της πολλαπλής αναπαραγωγής. Αυτό σημαίνει ότι παρόλο που ολόκληρη η δασική βάση δεδομένων αποτελείται από κατανεμημένες εγγραφές, οι εγγραφές αυτές ανάλογα με τη θέση τους εντός της λογικής ιεραρχίας του δάσους, μπορεί να περιέχουν ή να μην περιέχουν τις ίδιες πληροφορίες. Μέσα από μία δομή multimaster, το ADDS μπορεί να δεχτεί τοπικές αλλαγές και να διασφαλίσει τη συνέπεια μεταδίδοντας τις πληροφορίες ή τις αλλαγές σε όλες τις άλλες εγγραφές εντός του τομέα ή του δάσους. Αυτό είναι μία από τις λειτουργίες του αντικειμένου ελεγκτή τομέα (Domain Controller) στον κατάλογο. Εκτός από την αναπαραγωγή multimaster, το ADDS υποστηρίζει την έννοια ενός ελεγκτή τομέα μόνο για ανάγνωση (Read-Only Domain Controller – RODC). Το RODC εισήχθη στα WS08 για την προστασία των δεδομένων καταλόγου που είναι αποθηκευμένα σε απομακρυσμένους και μη ασφαλείς ελεγκτές τομέα. Παρ 'όλα αυτά, πρέπει πάντα οι DC προστατεύονται, οποιοδήποτε DC, επειδή είναι οι κινητήρες που παρέχουν πρόσβαση στο δίκτυο και σε όλα τα αντικείμενά του.

Οι μόνες εγγραφές που έχουν ακριβώς τις ίδιες πληροφορίες στη βάση δεδομένων AD είναι δύο ελεγκτές τομέα που βρίσκονται στον ίδιο τομέα. Κάθε μία από αυτές τις εγγραφές δεδομένων περιέχει πληροφορίες σχετικά με τον δικό της τομέα, καθώς και οποιεσδήποτε πληροφορίες έχουν προσδιοριστεί να ενδιαφέρουν ολόκληρο το δάσος από τους διαχειριστές δασών. Στο επίπεδο του δάσους, μπορούν να προσδιοριστούν οι πληροφορίες που θα διατίθενται σε ολόκληρο το δάσος επιλέγοντας τα αντικείμενα και τα χαρακτηριστικά από το σχήμα της βάσης δεδομένων των οποίων οι ιδιότητες θέλουμε να μοιραστούν μεταξύ όλων των δέντρων και τομέων. Επιπλέον, άλλες πληροφορίες σε ολόκληρο το δάσος περιλαμβάνουν το ίδιο το σχήμα βάσης δεδομένων και τη διαμόρφωση του δάσους ή τη θέση όλων των δασικών υπηρεσιών. Οι δημοσιευμένες πληροφορίες αποθηκεύονται στο Γενικό Κατάλογο (Global Catalog – GC). Το ADDS δημοσιεύει ορισμένα στοιχεία από προεπιλογή, όπως το περιεχόμενο των universal groups, αλλά υπάρχει και η δυνατότητα πρόσθεσης ή αφαίρεσης στοιχείων σύμφωνα με τις προτιμήσεις που επιθυμεί ο διαχειριστής. Για παράδειγμα, μπορεί ο διαχειριστής να αποφασίσει να συμπεριληφθούν οι φωτογραφίες των υπαλλήλων στον κατάλογο και να τις διαθέσει σε όλο το δάσος.

Ό, τι δημοσιεύεται στον Γενικό Κατάλογο κοινοποιείται από όλους τους ελεγκτές τομέα που έχουν αυτό το ρόλο στο δάσος. Ό, τι δεν δημοσιεύεται παραμένει εντός του τομέα. Ο διαχωρισμός αυτός των δεδομένων ελέγχει την ατομικότητα των τομέων. Ό, τι δεν δημοσιεύεται μπορεί να περιέχει διακριτές πληροφορίες που μπορεί να είναι της ίδιας φύση, ακόμη και να χρησιμοποιούν τις ίδιες τιμές και να περιέχονται σε άλλο τομέα. Ιδιότητες που δημοσιεύονται στον Γενικό Κατάλογο εντός ενός δάσους πρέπει να είναι μοναδικές, όπως και σε οποιαδήποτε άλλη βάση δεδομένων. Για παράδειγμα, μπορούν να υπάρχουν δύο John Smiths σε ένα δάσος αρκεί να είναι και οι δύο εντός διαφορετικών τομέων. Από τη στιγμή που το όνομα του αντικειμένου περιλαμβάνει το όνομα του κοντέινερ (σε αυτήν την περίπτωση, τον τομέα), το ADDS θα δει κάθε John Smith ως ένα διαφορετικό αντικείμενο. Φυσικά, και οι δύο John Smiths δεν θα μπορούν να χρησιμοποιήσουν το ίδιο UPN.

Το χώρος του καταλόγου, ή η βάση δεδομένων NTDS.DIT, βρίσκεται σε κάθε ελεγκτή τομέα. Περιλαμβάνει πολλά διαμερίσματα που αποθηκεύουν όλα τα δεδομένα που απαρτίζουν τον τομέα όπως φαίνεται στην εικόνα 6.22. Τρία στοιχεία βρίσκονται σε κάθε χώρο καταλόγου:

- το σχήμα
- η διαμόρφωση
- τα δεδομένα τομέα
- ο Γενικός Κατάλογος (Προαιρετικό)
- το διαμέρισμα εφαρμογών (Προαιρετικό).



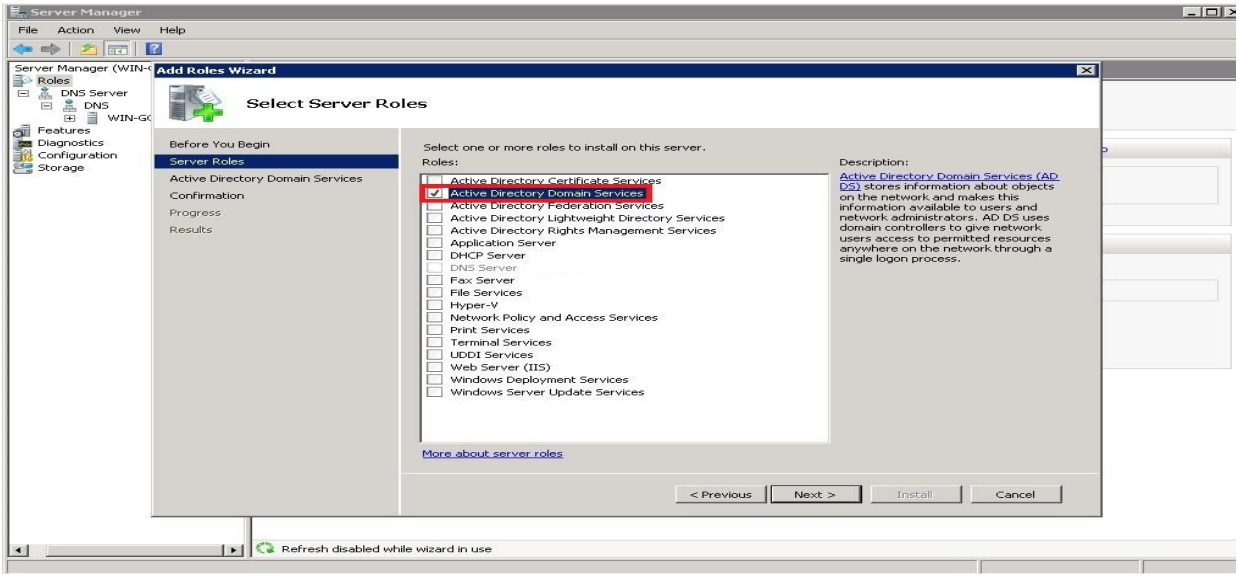
Εικόνα 6.22

Ο γενικός κατάλογος, το σχήμα και η διαμόρφωση περιέχουν κάθε πληροφορία που αναπαράγεται σε όλο το δάσος. Τα δεδομένα τομέα είναι πληροφορίες που αναπαράγονται μόνο εντός του τομέα. Η αναπαραγωγή μέσω τοπικών και απομακρυσμένων δικτύων ελέγχεται μέσω

περιφερειακών κατατμήσεων της βάσης δεδομένων. Οι οργανισμοί μπορούν να αποφασίσουν να δημιουργήσουν αυτά τα διαμερίσματα με βάση έναν αριθμό παραγόντων. Δεδομένου ότι ο τομέας είναι όριο πολιτικής ασφάλειας, έγκυροι οργανισμοί που εκτείνονται σε διάφορες γεωγραφικές τοποθεσίες που ελέγχουν μπορεί να θέλουν να δημιουργήσουν έναν μεμονωμένο τομέα που εκτείνεται σε αυτές τις τοποθεσίες. Προκειμένου να γίνει διαχωρισμός της κάθε περιοχής έτσι ώστε να ελεγχθεί
το ποσό και ο χρόνο αναπαραγωγής της βάσης δεδομένων μεταξύ περιοχών, ο τομέας θα χωριστεί σε ιστότοπους. Οι ιστότοποι είναι φυσικά διαμερίσματα που ελέγχουν την αναπαραγωγή δημιουργώντας όρια με βάση την διευθυνσιοδότηση του πρωτοκόλλου Διαδικτύου (IP).
Οι οργανισμοί που δεν είναι έγκυροι, έχουν ανεξάρτητες διαχειρίσεις , δεν ελέγχουν τις τοπικές τους τοποθεσίες ή μπορεί να έχουν αργούς συνδέσμους μεταξύ της κάθε τοποθεσίας και μπορούν να επιθυμούν περαιτέρω έλεγχο της αναπαραγωγής τους μέσω της δημιουργίας περιφερειακών τομέων. Οι τοπικοί τομείς μειώνουν σημαντικά την αναπαραγωγή, καθώς μόνο οι πληροφορίες αναπαράγονται σε όλο το δάσος από τοποθεσία σε τοποθεσία. Οι πληροφορίες σε ολόκληρο το δάσος υπερβαίνουν σπάνια το 20% των κοινών δασικών δεδομένων. Επιπλέον, οι οργανισμοί που έχουν μόνο τον έλεγχο ενός μέρους του χώρου ονομάτων των δασών θα πρέπει να είναι ιδιοκτήτες των δέντρων μέσα στο δάσος. Οργανισμοί που δεν μπορούν να εγγυηθούν ελάχιστο επίπεδο συναίνεσης ή εξουσίας μεταξύ ομάδων δημιουργούνται πάντα σε ξεχωριστά δάση.
Υπάρχει ένα ακόμη διαμέρισμα αναπαραγωγής στη βάση δεδομένων ADDS. Αυτό το διαμέρισμα εισήχθη με τα Windows Server 2003. Είναι το διαμέρισμα εφαρμογών. Αυτό το διαμέρισμα έχει πολλές δυνατότητες, όπως η δυνατότητα φιλοξενίας πολλών παρουσιών της ίδιας εφαρμογής και στοιχεία COM του ίδιου φυσικού μηχανήματος, αλλά για σκοπούς αναπαραγωγής, αυτό το διαμέρισμα μπορεί να οριστεί ως μια συγκεκριμένη ομάδα ελεγκτή τομέα διευθύνσεων IP ή ονομάτων DNS. Για παράδειγμα, το WS08 δημιουργεί αυτόματα ένα διαμέρισμα εφαρμογών σε ολόκληρο το δάσος για δεδομένα DNS σε ολόκληρο το δάσος. Επομένως αυτές οι πληροφορίες θα είναι διαθέσιμες σε όλους τους ελεγκτές τομέα μέσα στο δάσος. Αν φιλοξενούν επίσης το ρόλο DNS, τότε κάθε DC μπορεί να κάνει αυτές τις πληροφορίες διαθέσιμες στους χρήστες.

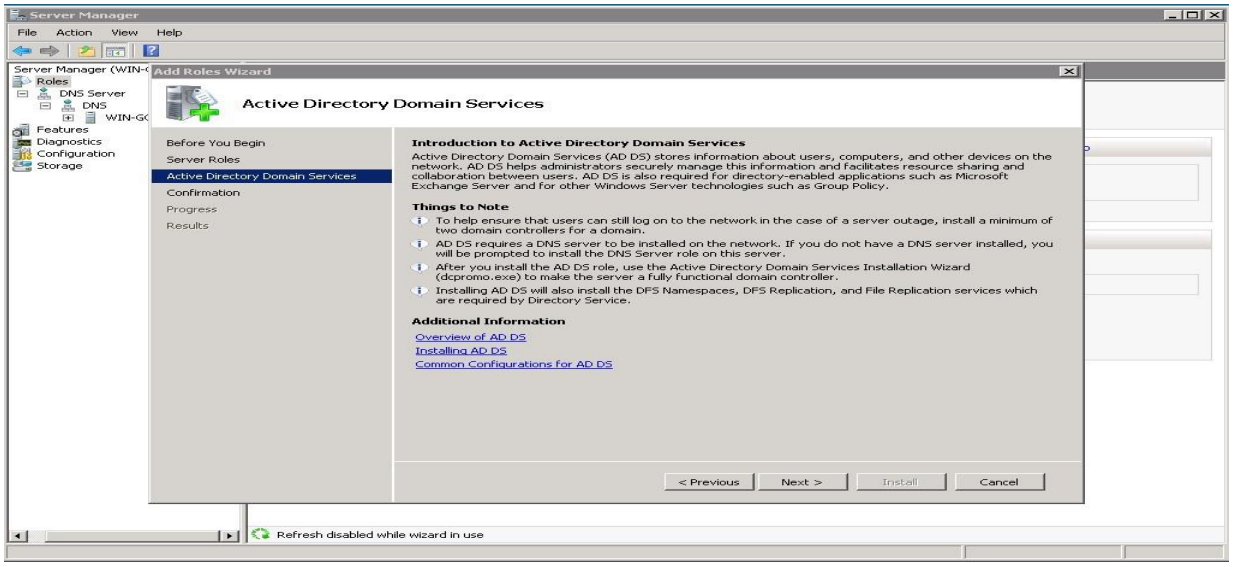
Εγκατάσταση υπηρεσίας ADDS

Ανοίγουμε το παράθυρο διαλόγου του Server Manager. Στη συνέχεια επιλέγουμε τους ρόλους και πατάμε κλικ στην επιλογή Add Roles. Θα μας εμφανιστεί το παράθυρο διαλόγου όπως φαίνεται στην εικόνα 6.23. Επιλέγουμε την υπηρεσία ADDS και στη συνέχεια πατάμε Επόμενο (Next).



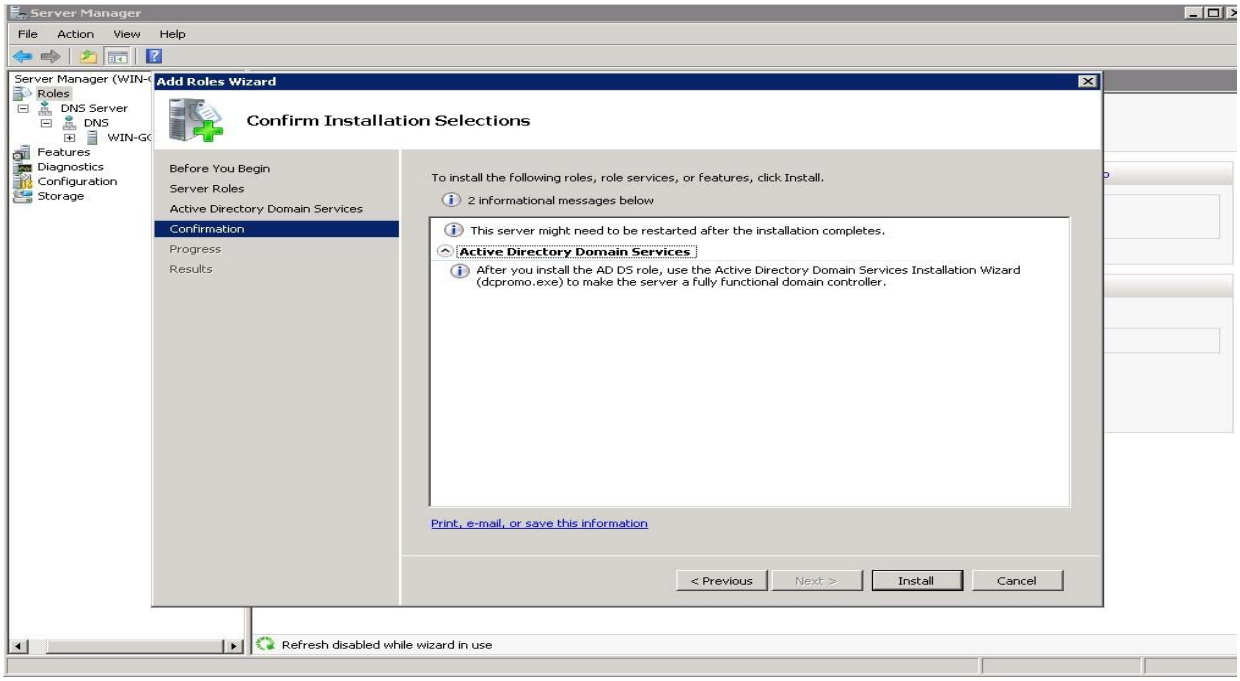
Εικόνα 6.23

Στη συνέχεια μας κάνει ένα overview της υπηρεσίας με τις δυνατότητες και τις επιλογές που μας παρέχει. Επιπρόσθετα παρέχονται και κάποια βοηθητικά link για να καταλάβουμε και να μας λυθούν οποιεσδήποτε απορίες τυχόν μπορεί να έχουμε για την υπηρεσία ADDS. Στην εικόνα 6.24 φαίνονται οι παρακάτω δυνατότητες. Στη συνέχεια πατάμε Επόμενο (Next).



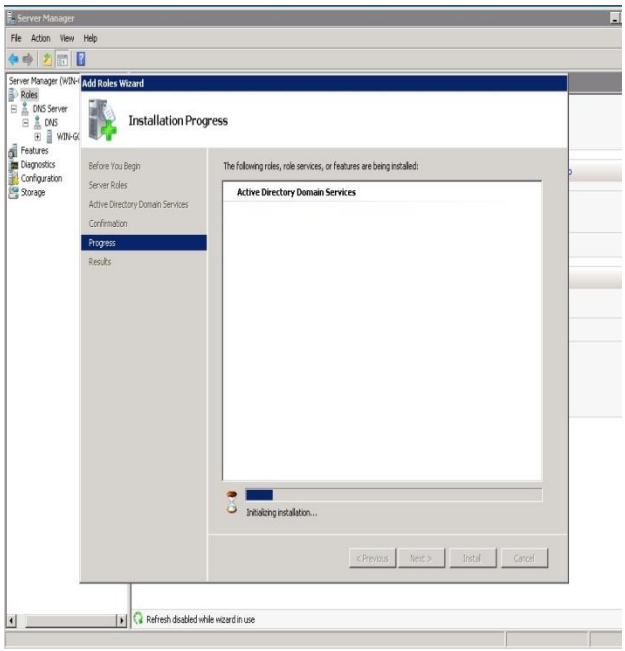
Εικόνα 6.24

Στο επόμενο παράθυρο διαλόγου το σύστημα μας ζητά να επιβεβαιώσουμε την επιλογή μας και αφού έχουμε ελέγξει ότι όλες τις επιλογές μας επιβεβαιώνουμε την επιλογή μας πατώντας στην επιλογή εγκατάστασης (Install) όπως φαίνεται στην εικόνα 6.25.

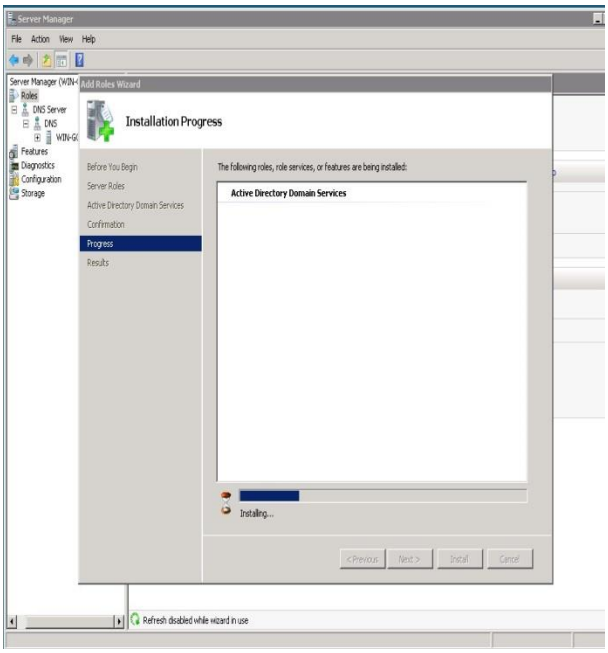


Εικόνα 6.25

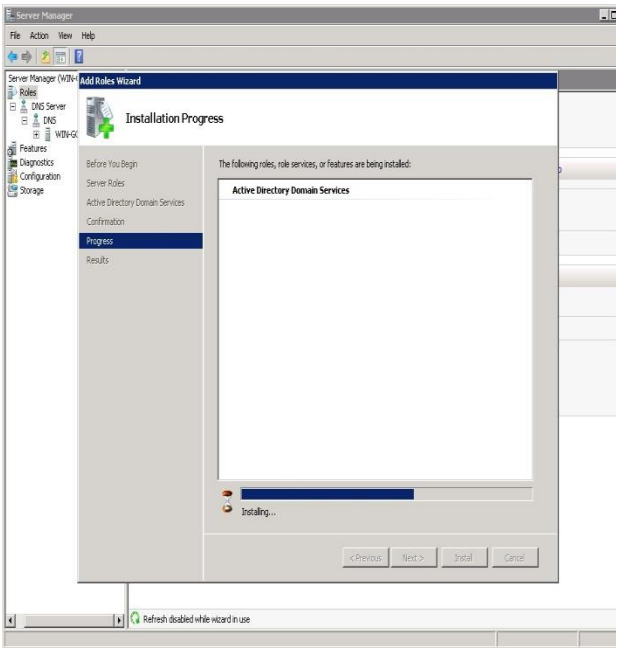
Στη συνέχεια το σύστημα ξεκινάει την εγκατάσταση της υπηρεσίας ADDS. Η πρόοδος φαίνεται στις παρακάτω εικόνες.



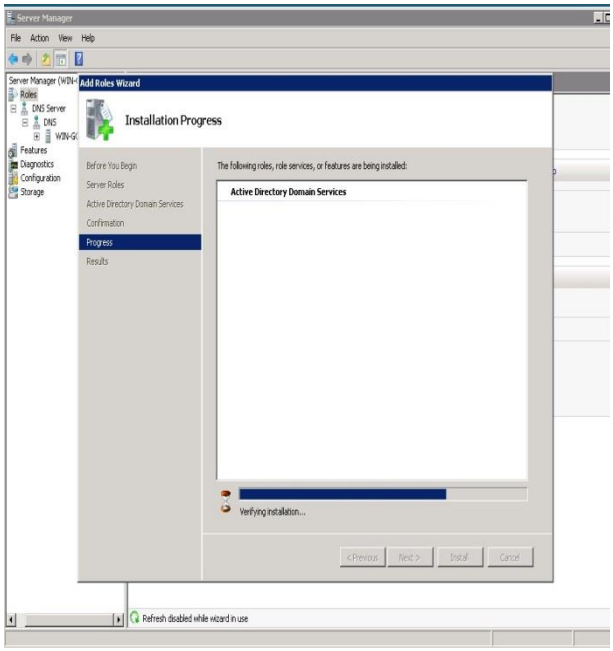
Εικόνα 6.26



Εικόνα 6.27

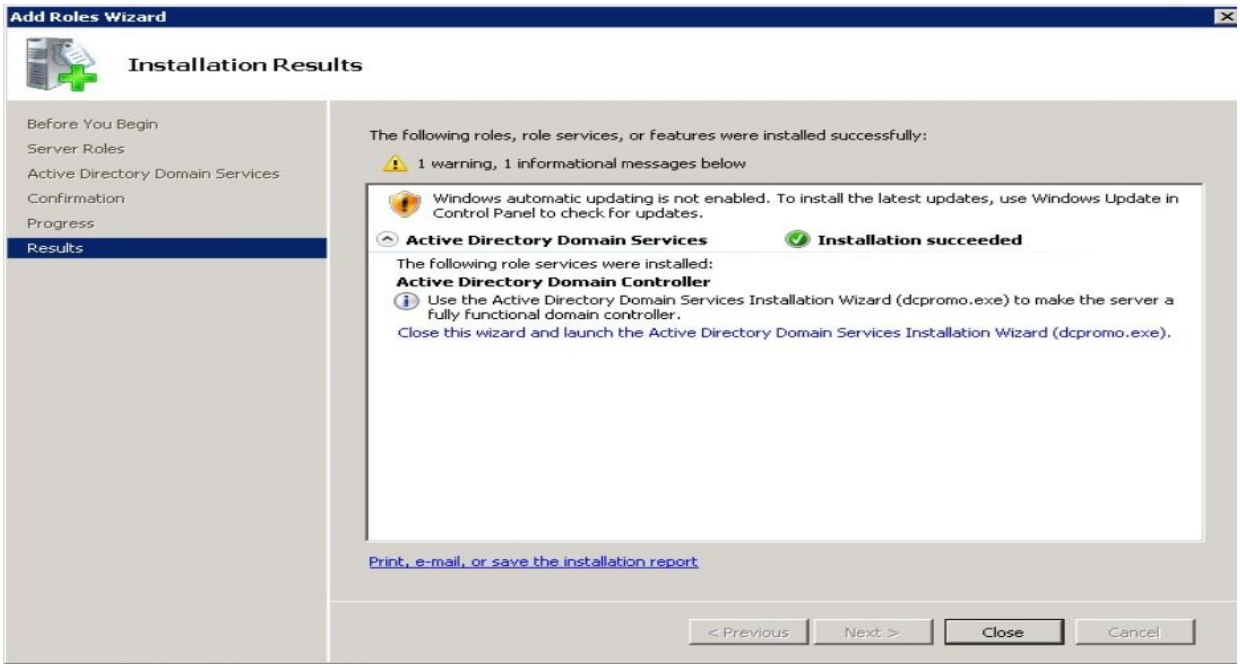


Εικόνα 6.28



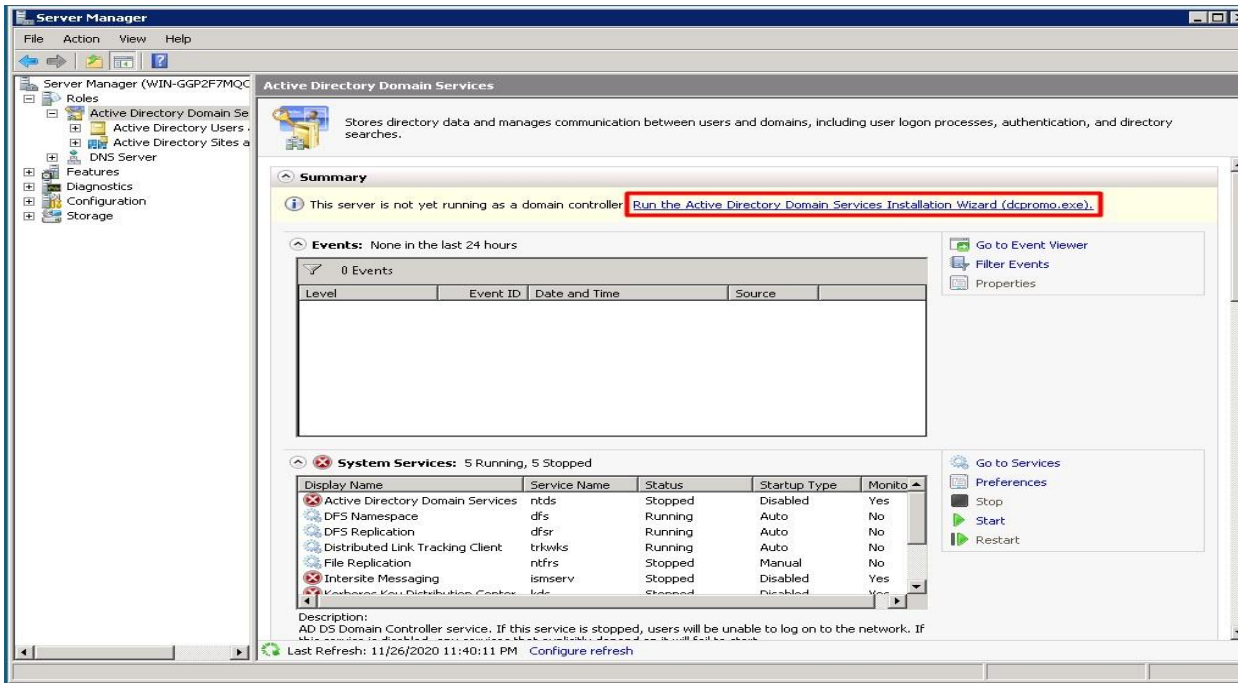
Εικόνα 6.29

Στη συνέχεια το σύστημα μας ενημερώνει ότι η εγκατάσταση της νέας υπηρεσίας ολοκληρώθηκε και ότι μπορούμε να παραμετροποιήσουμε το νέο ADDS με την βοήθεια του οδηγού ADDS. Στην συνέχεια πατάμε στην επιλογή κλείσιμο (Close) για να ολοκληρώσουμε την εγκατάσταση. Οι επιλογές μας φαίνονται στην εικόνα 6.30.



Εικόνα 6.30

Χρησιμοποιώντας τον οδηγό του Active Directory Domain Services Installation Wizard, ο οποίος φαίνεται στην εικόνα 6.31, θα ρυθμίσουμε – δημιουργήσουμε το νέο ADDS.

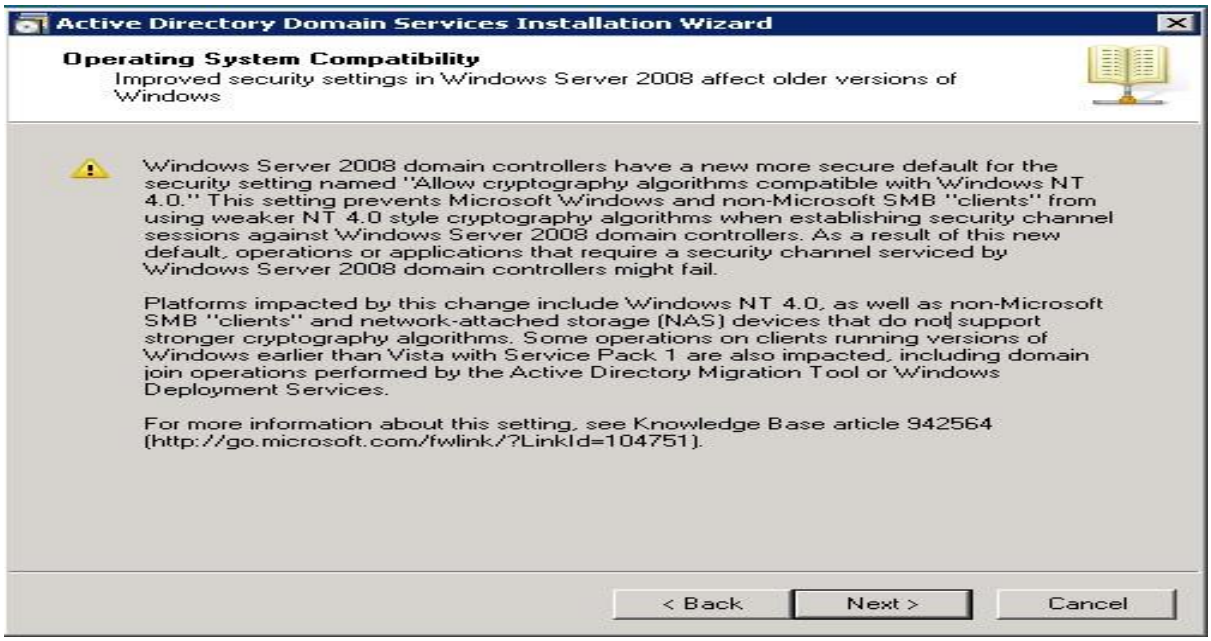


Εικόνα 6.31

Στο επόμενο παράθυρο διαλόγου που μας εμφανίζεται, όπως φαίνεται στην εικόνα 6.32, ξεκινάει ο οδηγός του Active Directory Domain Services Installation Wizard. Υπάρχει η επιλογή για advanced mode installation αν επιθυμούμε. Πατάμε Επόμενο (Next) για να συνεχίσουμε.

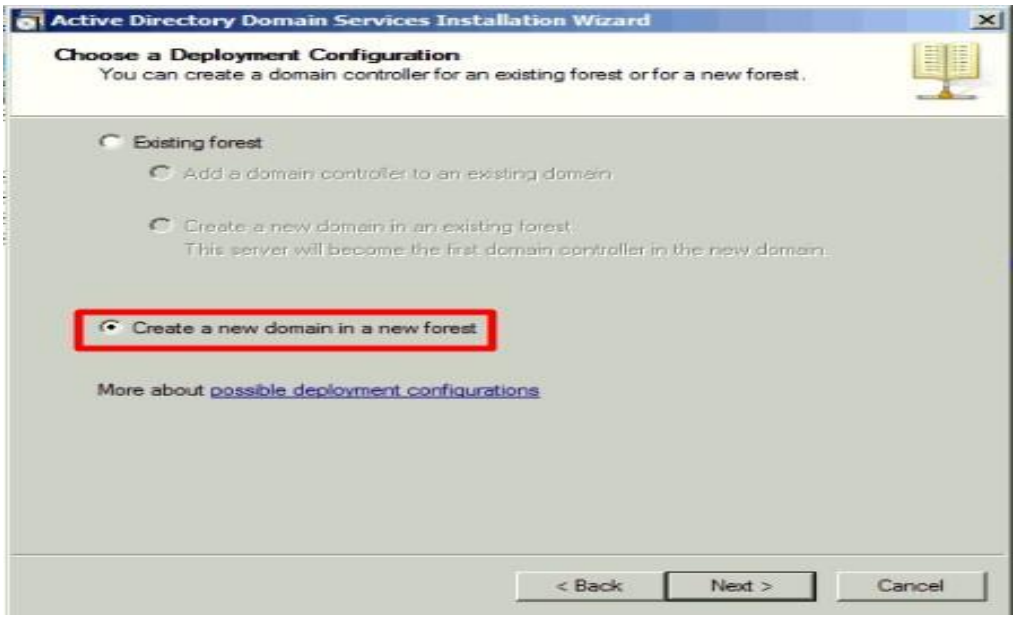
Εικόνα 6.32

Στο παράθυρο διαλόγου που μας εμφανίζεται, όπως φαίνεται στην εικόνα 6.33 γίνεται μια σύντομη παρουσίαση για τις έξτρα δυνατότητες που μας παρέχονται με τα Windows Server 2008. Πατάμε επόμενο για να συνεχίσουμε.



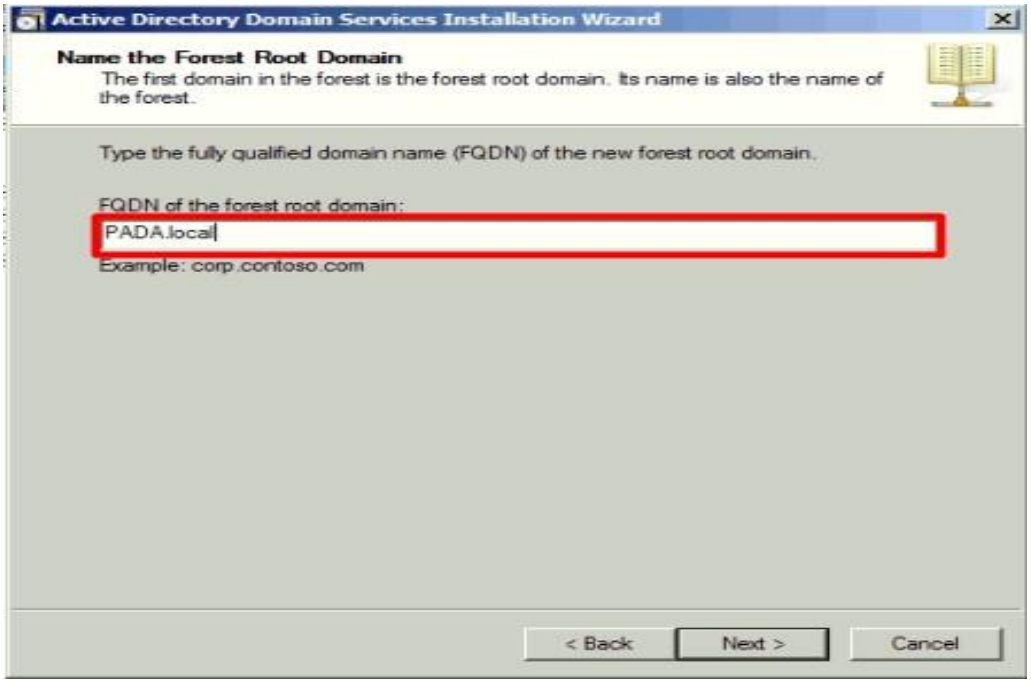
Εικόνα 6.33

Στη συνέχεια του οδηγού έχουμε την επιλογή να εγκαταστήσουμε το νέο ADDS σε ένα ήδη υπάρχον Domain Forest η να δημιουργήσουμε ένα δικό μας. Στην προκειμένη περίπτωση εμείς θα δημιουργήσουμε ένα δικό μας εφόσον δεν υπάρχει άλλο. Οι επιλογές αυτές φαίνονται στην εικόνα 6.34.



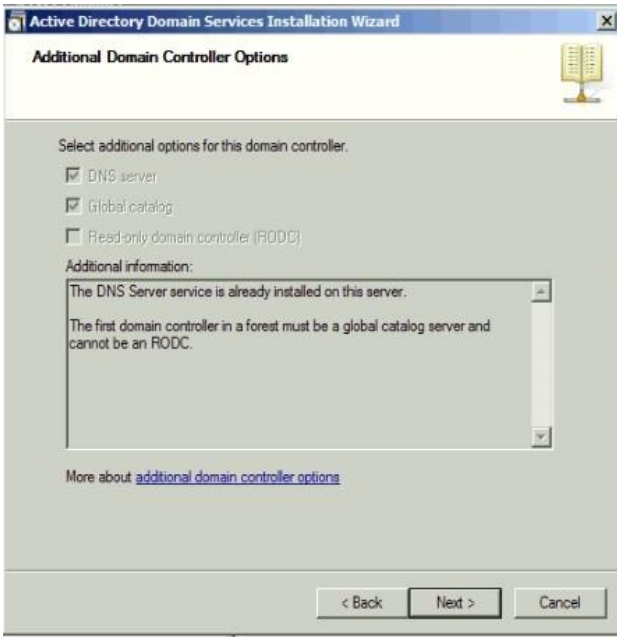
Εικόνα 6.34

Στη συνέχεια θα πρέπει να βάλουμε το όνομα του νέου Domain. Το εν λόγω Domain θα το ονομάσουμε PADA.local όπως φαίνεται και στην εικόνα 6.35.

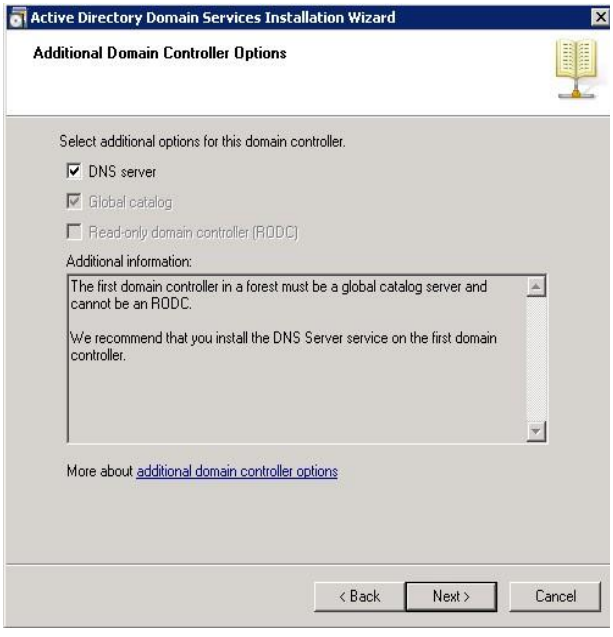


Εικόνα 6.35

Στη συνέχεια το σύστημά μας ελέγχει αν υπάρχει εγκατεστημένη η υπηρεσία DNS. Στις εικόνες 6.36 και 6.37 φαίνεται πως εμφανίζεται το παράθυρο διαλόγου εάν υπάρχει εγκατεστημένη η υπηρεσία ή θα πρέπει να εγκατασταθεί.

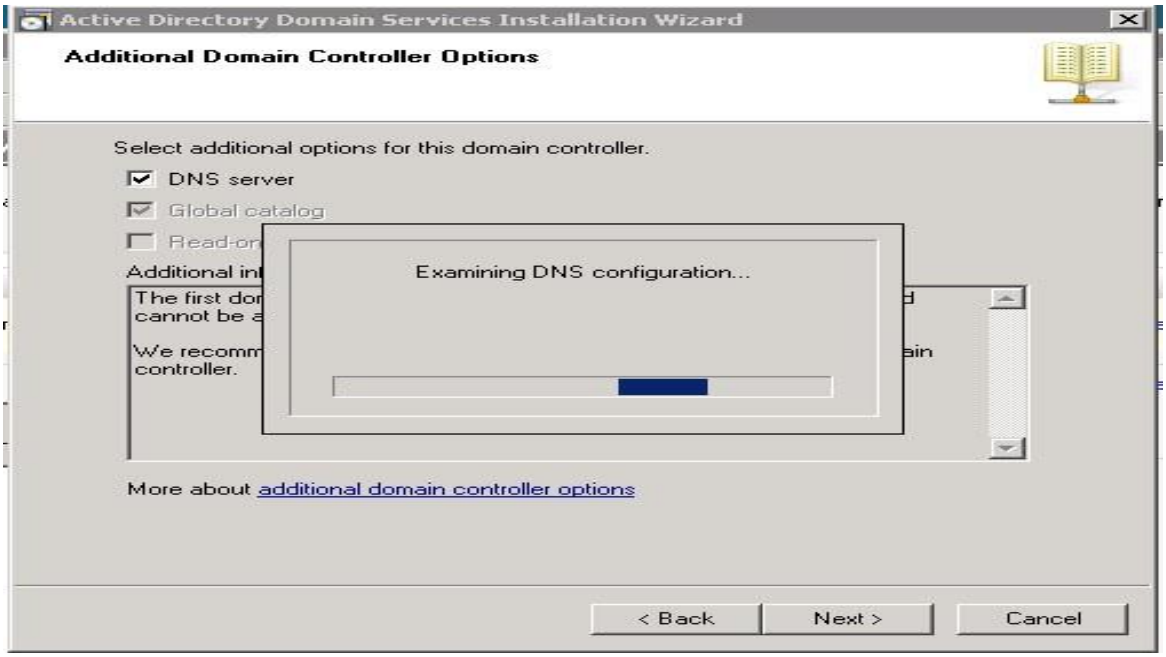


Εικόνα 6.36



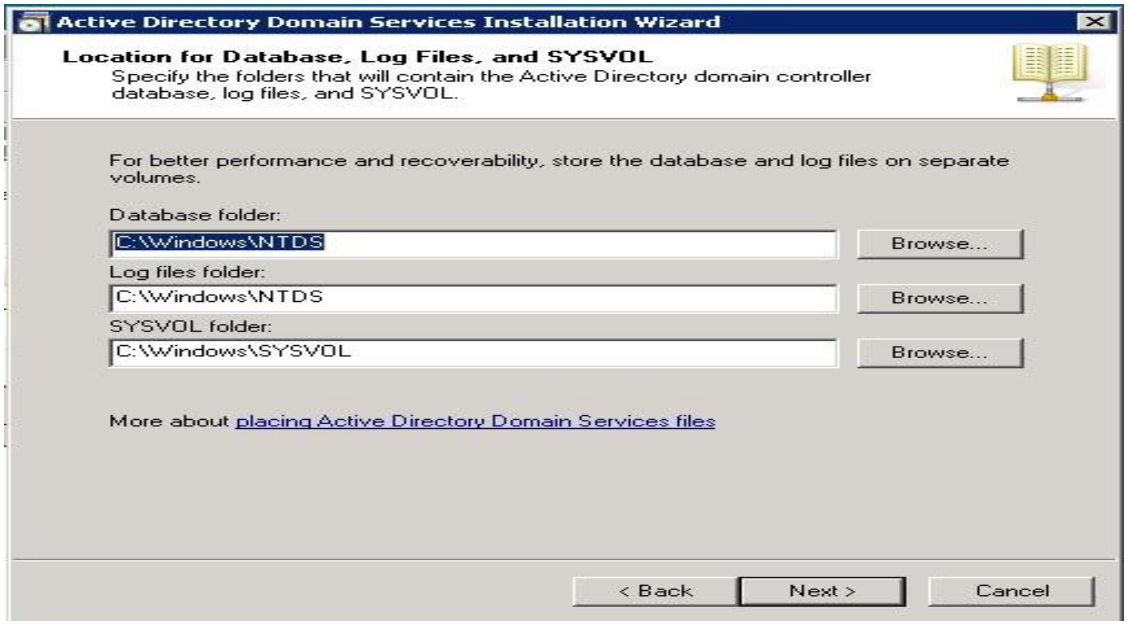
Εικόνα 6.37

Στη συνέχεια εφόσον έχουμε τοποθετήσει το νέο Domain, στην εικόνα 6.38 ελέγχεται εάν υπάρχει ήδη το νέο Domain προκειμένου να συνεχίσουμε στη δημιουργία του.



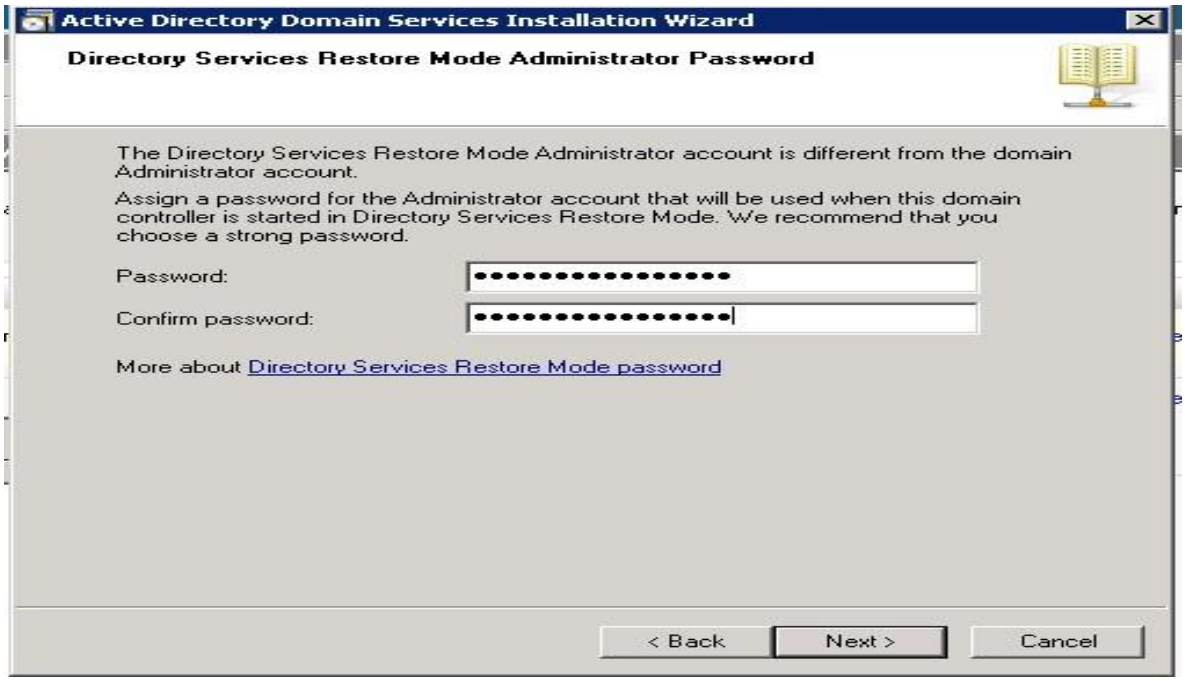
Εικόνα 6.38

Εφόσον δεν έχουμε κάποιο ίδιο Domain προχωράμε κανονικά στη δημιουργία του με την εμφάνιση του επόμενου παράθυρου διαλόγου όπως φαίνεται στην εικόνα 6.39. Στο συγκεκριμένο παράθυρο καθορίζουμε τα path των φακέλων που θα περιέχουν την βάση δεδομένων του Active Directory Domain Controller, log files καθώς και SYSVOL. Αφήνοντας τα default path πατάμε επόμενο για να συνεχίσουμε.



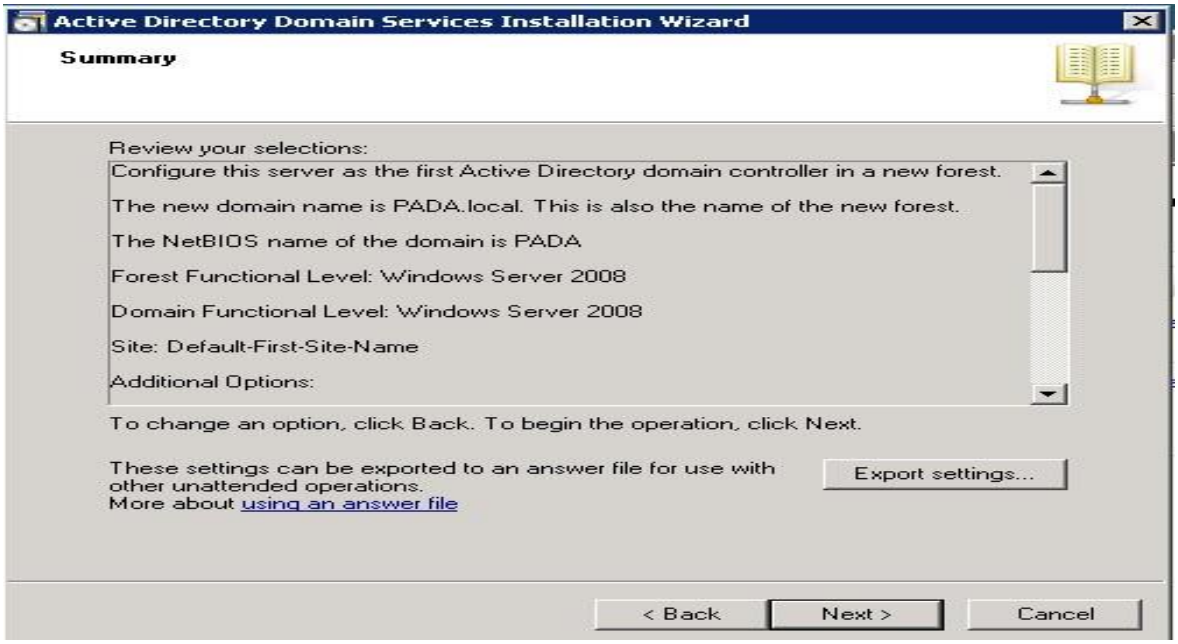
Εικόνα 6.39

Στη συνέχεια του οδηγού ζητείται από τον χρήστη να τοποθετήσει τον κωδικό του διαχειριστή που θα υφίσταται στο νέο Domain. Η διαδικασία φαίνεται στην εικόνα 6.40.



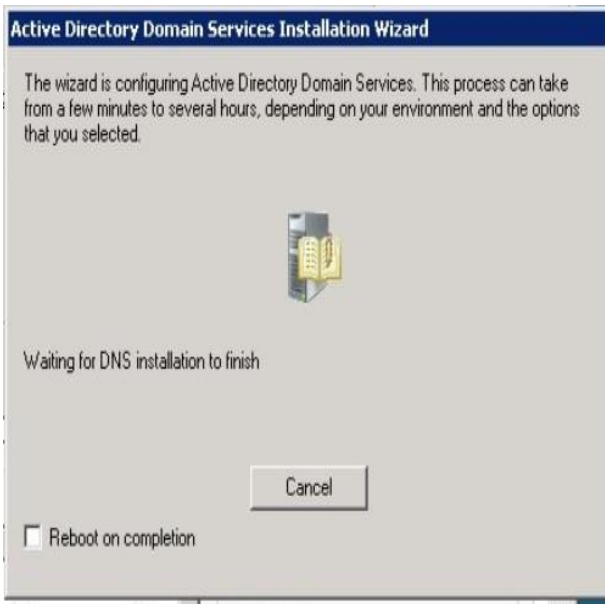
Εικόνα 6.40

Τέλος πριν από την εγκατάσταση των προτιμήσεων μας βλέπουμε ένα γενικό σύνολο με τις ρυθμίσεις του νέου ADDS που έχουμε επιλέξει. Μπορούμε να πάμε πίσω αν κάτι επιθυμούμε να το αλλάξουμε. Εφόσον είμαστε έτοιμοι πατάμε επόμενο όπως φαίνεται στην εικόνα 6.41.



Εικόνα 6.41

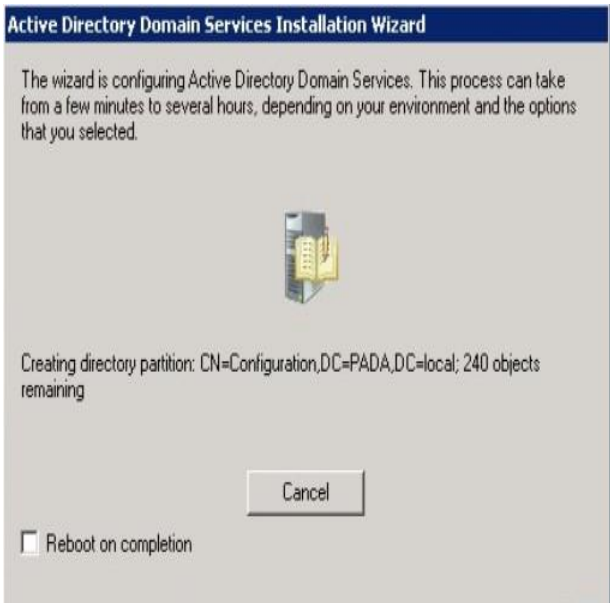
Στη συνέχεια το σύστημα ξεκινάει την εγκατάσταση του νέου controller της υπηρεσίας ADDS. Η πρόοδος φαίνεται στις παρακάτω εικόνες.



Εικόνα 6.42

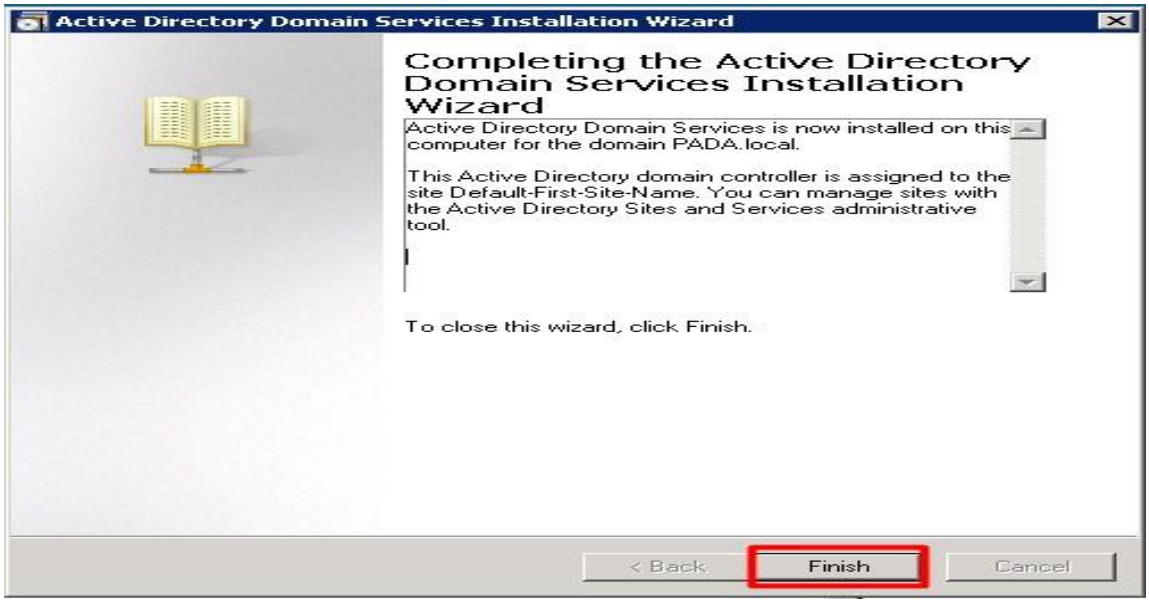
Εικόνα 6.43

Εικόνα 6.44



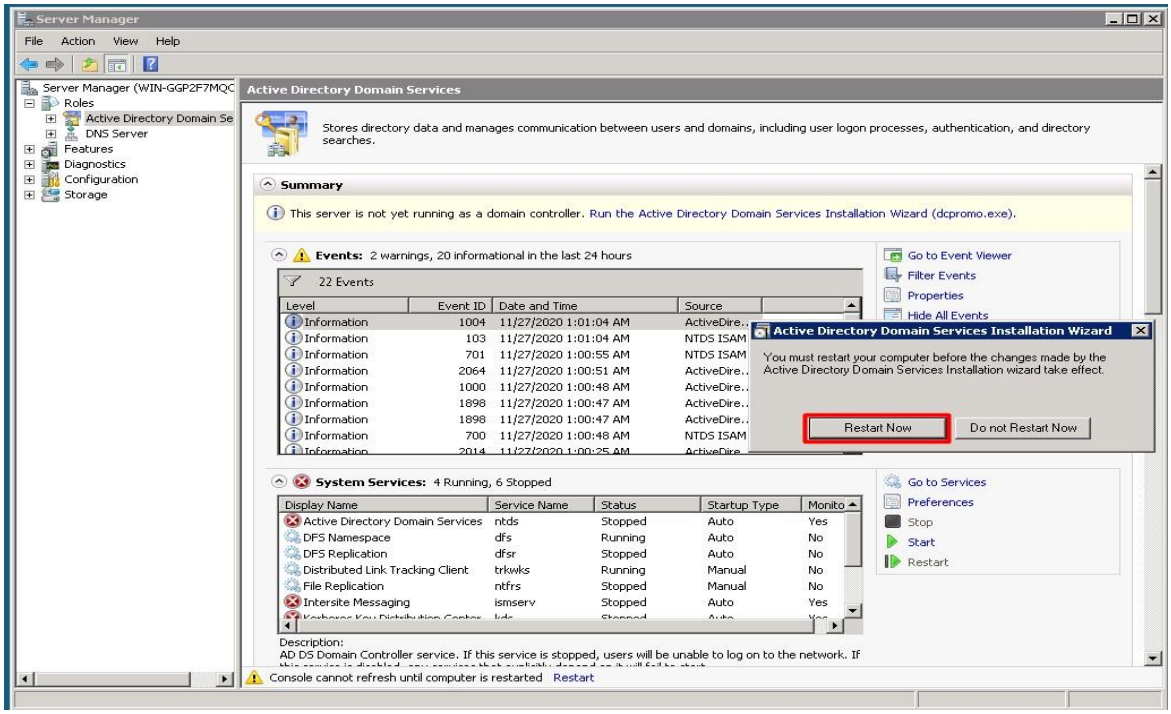
Εικόνα 6.45

Στη συνέχεια μόλις ολοκληρωθεί η εγκατάσταση του νέου controller πατάμε Τέλος (finish) για να εξέλθουμε από τον οδηγό, όπως φαίνεται στην εικόνα 6.46.



Εικόνα 6.46

Προκειμένου να εφαρμοστούν οι νέες ρυθμίσεις απαιτείται να γίνει επανεκκίνηση του συστήματος, όπως φαίνεται και στην εικόνα 6.47.



Εικόνα 6.47

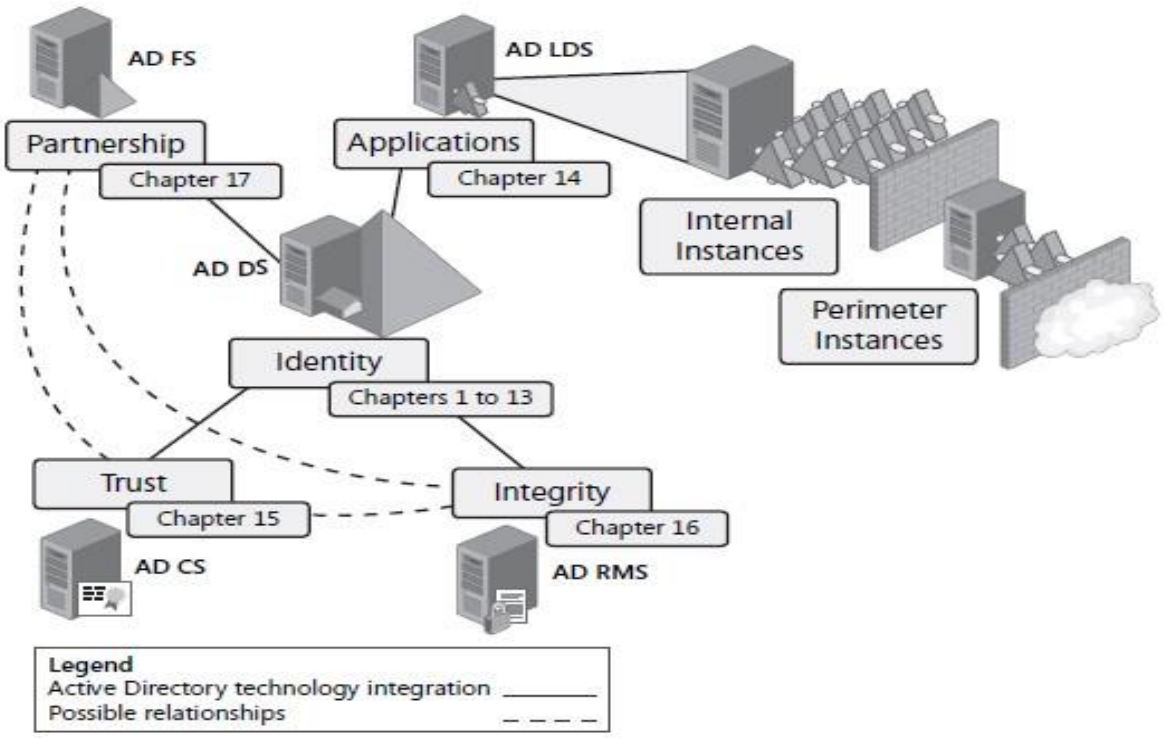
Μετά την επανεκκίνηση του συστήματος οι νέες ρυθμίσεις πραγματοποιήθηκαν και αυτό φαίνεται αμέσως από το παράθυρο διαλόγου κατά την είσοδο του συστήματος. Στην εικόνα 6.48 φαίνεται ότι πλέον είμαστε στο νέο Domain που το ονομάσαμε PADA.local.

Εικόνα 6.48

6.3.3. AD Lightweight Directory Services (ADLDS)

Από τις πέντε διαφορετικές τεχνολογίες Active Directory που διατίθενται στον Windows Server 2008, αυτή που μοιάζει περισσότερο με τις υπηρεσίες ADDS είναι η υπηρεσία καταλόγου Active Directory Lightweight Directory Services (ADLDS). Αυτό συμβαίνει επειδή το ADLDS δεν είναι τίποτα περισσότερο από ένα υποσύνολο των λειτουργιών του AD DS. Και οι δύο χρησιμοποιούν τον ίδιο βασικό κωδικό και οι δύο παρέχουν ένα πολύ παρόμοιο σύνολο χαρακτηριστικών. Το ADLDS, που παλαιότερα ονομαζόταν Active Directory Application Mode (ADAM), είναι μια τεχνολογία που έχει σχεδιαστεί για να υποστηρίζει εφαρμογές με δυνατότητα καταλόγου σε εφαρμογή ανά εφαρμογή και χωρίς να χρειάζεται να τροποποιηθεί το σχήμα της βάσης δεδομένων του Network Operating System (NOS) το οποίο τρέχει σε ADDS. Το ADLDS είναι ένα όφελος για τους διαχειριστές που θέλουν να χρησιμοποιήσουν directory enabled εφαρμογές χωρίς να τις ενσωματώσουν στον κατάλογο NOS. Οι υπηρεσίες τομέα Active Directory μπορούν επίσης να υποστηρίξουν τη χρήση εφαρμογών με δυνατότητα καταλόγου.
Ένα πολύ καλό παράδειγμα είναι ο Microsoft Exchange Server 2007. Όλες οι πληροφορίες χρήστη στον Exchange Server παρέχονται από τον κατάλογο. Όταν γίνεται εγκατάσταση του Exchange Server στο δίκτυό μας, η πρώτη ενέργεια που κάνει είναι η επέκταση του σχήματος ADDS, διπλασιάζοντας ουσιαστικά το μέγεθός του. Είναι πολύ σημαντικό να γνωρίζουμε ότι οι τροποποιήσεις σχήματος θα πρέπει να ληφθούν σοβαρά υπόψη γιατί, όταν προσθέτουμε ένα αντικείμενο ή ένα χαρακτηριστικό στο σχήμα ADDS, αυτό θα προστεθεί μόνιμα εκεί και δεν μπορεί να αφαιρεθεί. Μπορεί να απενεργοποίηση ή μετονομασία και να επαναχρησιμοποιήσουμε αυτά τα αντικείμενα, αλλά προτιμότερο είναι να μην έχουμε ατελή αντικείμενα στον κατάλογο NOS. Η προσθήκη στο σχήμα μιας τέτοιας εφαρμογής όπως ο Exchange Server είναι κατάλληλη επειδή μας παρέχει μια βασική υπηρεσία δικτύωσης, το e-mail.

Ωστόσο, όταν πρόκειται για άλλες εφαρμογές, ειδικά εφαρμογές που παρέχονται από κατασκευαστές λογισμικού τρίτων, θα πρέπει να γίνει προσεκτική εξέταση εάν πρέπει να ενσωματωθούν στον κατάλογο ADDS. Γι' αυτό το ADLDS είναι τόσο ευεργετικό. Επειδή μπορεί να υποστηρίξει πολλές εμφανίσεις ADLDS σε ένα μόνο διακομιστή (σε αντίθεση με το ADDS, που μπορεί να υποστηρίξει μόνο μία παρουσία ενός καταλόγου σε οποιοδήποτε δεδομένο διακομιστή), το ADLDS μπορεί να πληροί τις απαιτήσεις οποιασδήποτε εφαρμογής με δυνατότητα καταλόγου ακόμη και να παρέχει παρουσίες σε εφαρμογή ανά αίτηση. Επιπλέον, δεν χρειάζεται να έχουμε Enterprise διαχειριστή ή διαπιστευτήρια διαχειριστή σχήματος για την εκτέλεση οποιασδήποτε εργασίας με ADLDS, όπως θα έπρεπε να κάνουμε με το ADDS. Το ADLDS εκτελείται σε διακομιστές μελών ή αυτόνομους και απαιτεί μόνο δικαιώματα πρόσβασης τοπικού διαχειριστή για τη διαχείρισή του. Εξαιτίας αυτού, μπορεί επίσης να χρησιμοποιηθεί σε ένα περιμετρικό δίκτυο για να παρέχει υπηρεσίες ελέγχου ταυτότητας εφαρμογών ή Ιστού. Το ADLDS είναι μία από τις τέσσερις Active Directory τεχνολογίες που επιτρέπουν επέκταση την του οργανισμού μας έξω από το τείχος προστασίας στο cloud του Διαδικτύου, όπως φαίνεται και στην εικόνα 6.49.



Εικόνα 6.49

Κατανόηση του ADLDS

Όπως το ADDS, τα στιγμιότυπα ADLDS βασίζονται στο Lightweight Directory Access Protocol (LDAP) και παρέχει υπηρεσίες ιεραρχικής βάσης δεδομένων. Σε αντίθεση με τις σχεσιακές βάσεις δεδομένων, οι κατάλογοι LDAP έχουν βελτιστοποιηθεί για συγκεκριμένους σκοπούς και πρέπει να χρησιμοποιούνται όποτε χρειάζονται εκτελώντας γρήγορες αναζητήσεις πληροφοριών που θα υποστηρίζουν συγκεκριμένες εφαρμογές. Ο Πίνακας 6.1 περιγράφει τις σημαντικές διαφορές μεταξύ ενός καταλόγου LDAP και μιας σχεσιακής βάσης δεδομένων όπως είναι ο Microsoft SQL Server. Αυτή η σύγκριση μας βοηθά να καταλάβουμε πότε πρέπει να επιλέξουμε έναν κατάλογο LDAP για υποστήριξη μιας εφαρμογής μέσω σχεσιακής βάσης δεδομένων.

Κατάλογοι LDAP	Σχεσιακές βάσεις δεδομένων
Γρήγορη ανάγνωση και αναζητήσεις	Γρήγορες εγγραφές
Ο ιεραρχικός σχεδιασμός βάσεων δεδομένων βασίζεται συχνά στο σύστημα ονομάτων τομέα (DNS) ή το X.500 σύστημα ονομάτων.	Σχεδιασμός δομημένων δεδομένων που βασίζεται σε πίνακες που περιέχουν σειρές και στήλες. Οι πίνακες μπορούν να συνδεθούν μαζί.
Βασίζεται σε μια τυπική δομή σχήματος, ένα σχήμα το οποίο είναι επεκτάσιμο.	Δεν βασίζεται σε σχήματα.
Αποκεντρωμένη (κατανεμημένη) και βασιζόμενη στην αναπαραγωγή για τη διατήρηση της συνοχής των δεδομένων.	Αποθήκευση δεδομένων σε κεντρική τοποθεσία.
Η ασφάλεια εφαρμόζεται σε επίπεδο αντικειμένου.	Η ασφάλεια εφαρμόζεται σε επίπεδο γραμμής ή στήλης.

Επειδή η βάση δεδομένων είναι κατανεμημένη, η συνέπεια των δεδομένων δεν είναι απόλυτη - τουλάχιστον όχι μέχρι η αναπαραγωγή των αντικειμένων να είναι πλήρεις.	Επειδή η εισαγωγή δεδομένων είναι transactional, η συνέπεια των δεδομένων είναι απόλυτη και εγγυημένη ανά πάσα στιγμή.
Οι εγγραφές δεν είναι κλειδωμένες και μπορούν να τροποποιηθούν από δύο μέρη ταυτόχρονα. Η διαχείριση των συγκρούσεων πραγματοποιείται μέσω Update Sequence Numbers (USN).	Οι εγγραφές είναι κλειδωμένες και μπορούν να τροποποιηθούν μόνο ένα κάθε φορά.
Πίνακας 6.1	

Το ADLDS βασίζεται σε ADDS, αλλά δεν περιλαμβάνει όλες τις δυνατότητες του ADDS. Στον Πίνακα 6.2 περιγράφονται οι διαφορές στις δυνατότητες μεταξύ ADLDS και ADDS.

Χαρακτηριστικά	ADLDS	ADDS
Περιλαμβάνει περισσότερες από μία παρουσίες σε έναν διακομιστή.	√	
Περιλαμβάνει ανεξάρτητα σχήματα για κάθε παρουσία.	√	
Εκτελείται σε λειτουργικά συστήματα πελατών, όπως Windows Vista ή Windows Server 2008 μελών διακομιστή.	√	
Εκτελείται σε ελεγκτές τομέα.	√	√
Τα διαμερίσματα καταλόγου μπορούν να βασίζονται σε συμβάσεις ονομασίας X.500.	√	
Μπορεί να εγκατασταθεί ή να αφαιρεθεί χωρίς επανεκκίνηση.	√	
Η υπηρεσία μπορεί να διακοπεί ή να ξεκινήσει χωρίς επανεκκίνηση.	√	√
Υποστηρίζει πολιτική ομάδας		√
Περιλαμβάνει έναν κοινό κατάλογο.		√
Διαχειρίζεται αντικείμενα όπως σταθμούς εργασίας, διακομιστές μελών και ελεγκτές τομέα.		√
Υποστηρίζει εμπιστοσύνη μεταξύ τομέων και δασών.		√
Υποστηρίζει και ενσωματώνεται με υποδομές δημόσιου κλειδιού (PKI) και X.509 πιστοποιητικά.		√
Υποστηρίζει εγγραφές υπηρεσίας DNS (SRV) για τον εντοπισμό υπηρεσιών καταλόγου.		√
Υποστηρίζει διεπαφές προγραμματισμού εφαρμογών LDAP (API).	√	√
Υποστηρίζει API Active Directory Services Interface (ADSI).	√	√
Υποστηρίζει API ανταλλαγής μηνυμάτων (MAPI).		√
Υποστηρίζει αντικειμενική ασφάλεια και ανάθεση διαχειριστή.	√	√
Βασίζεται στην αναπαραγωγή πολλαπλών μεγεθών για συνέπεια δεδομένων.	√	√
Υποστηρίζει επεκτάσεις σχήματος και διαμερίσματα καταλόγου εφαρμογών.	√	√
Μπορεί να εγκαταστήσει ένα αντίγραφο από αφαιρούμενα μέσα.	√	√
Μπορεί να περιλαμβάνει αρχές ασφαλείας για την παροχή πρόσβασης σε διακομιστή Windows στο δίκτυο.		√
Μπορεί να περιλαμβάνει αρχές ασφαλείας για την πρόσβαση σε εφαρμογές και Web Υπηρεσίες.	√	√
Είναι ενσωματωμένο στα εργαλεία δημιουργίας αντιγράφων ασφαλείας των Windows Server 2008.	√	√
Πίνακας 6.2		

Όπως μπορούμε να δούμε από τα περιεχόμενα του Πίνακα 6.2, υπάρχουν πολλές ομοιότητες και διαφορές μεταξύ ADLDS και ADDS. Για παράδειγμα, είναι εύκολο να καταλάβουμε γιατί ο Exchange Server πρέπει να ενσωματωθεί με ADDS και όχι να βασιζόμαστε σε ADLDS, και αυτό επειδή ο Exchange Server απαιτεί πρόσβαση στην υπηρεσία καθολικού καταλόγου για εκτέλεση. Χωρίς αυτό, οι χρήστες ηλεκτρονικού ταχυδρομείου δεν θα μπορούσαν να αναζητήσουν παραλήπτες. Επειδή το ADLDS δεν υποστηρίζει τον καθολικό κατάλογο, ο Exchange Server δεν μπορεί να βασιστεί σε αυτόν. Ωστόσο, ο Exchange Server είναι μια εφαρμογή που απαιτεί πρόσβαση σε δεδομένα καταλόγου σε κάθε τοποθεσία του τομέα ή του δάσους. Ως εκ τούτου, βασίζεται επίσης στη θέση του ελεγκτή τομέα για να το διασφαλίσει ότι κάθε χρήστης μπορεί να διευθετήσει σωστά τα e-mail. Ωστόσο, το ADLDS παρέχει πολλές από τις ίδιες λειτουργίες με το ADDS. Για παράδειγμα, μπορούμε να δημιουργήσουμε παρουσίες με αντίγραφα που διανέμονται σε διάφορες τοποθεσίες στο δίκτυό μας, όπως και με τη θέση των ελεγκτών τομέα και στη συνέχεια να χρησιμοποιήσουμε την αναπαραγωγή πολλαπλών μεγεθών για να διασφαλίσουμε τη συνέπεια των δεδομένων. Εν ολίγοις, το ADLDS είναι μια ελαφριά, φορητή και πιο ευέλικτη έκδοση της υπηρεσίας καταλόγου που προσφέρει το ADDS.

Σενάρια AD LDS

Μερικά από τα σενάρια που θα μπορούσαμε να εξετάσουμε για να αποφασίσουμε αν θα βασιστούμε σε ADLDS ή ADDS φαίνονται παρακάτω:

- Όταν οι εφαρμογές μας πρέπει να βασίζονται σε έναν κατάλογο LDAP, εξετάζουμε το ενδεχόμενο να χρησιμοποιήσουμε το ADLDS αντί για ADDS. Το ADLDS μπορεί συχνά να φιλοξενείται στον ίδιο διακομιστή με την εφαρμογή, παρέχοντας υψηλές ταχύτητες και τοπική πρόσβαση σε δεδομένα καταλόγου. Αυτό θα μείωνε την κίνηση αναπαραγωγής επειδή όλα τα απαιτούμενα δεδομένα είναι τοπικά. Επιπλέον, μπορούμε να ομαδοποιήσουμε την παρουσία ADLDS με την εφαρμογή κατά την ανάπτυξη. Για παράδειγμα, εάν έχουμε μία εφαρμογή ανθρώπινου δυναμικού που πρέπει να βασίζεται σε προσαρμοσμένες πολιτικές για να διασφαλίσει ότι οι χρήστες μπορούν να έχουν πρόσβαση μόνο σε συγκεκριμένα περιεχόμενα όταν το αντικείμενο χρήστη περιέχει ένα σύνολο συγκεκριμένων χαρακτηριστικών, μπορούμε να αποθηκεύσουμε αυτά τα χαρακτηριστικά και τις πολιτικές στο ADLDS.
- Εάν βασιστούμε στο ADLDS για την παροχή δεδομένων που σχετίζονται με λογαριασμούς χρηστών στο ADDS θα πρέπει να γνωρίζουμε ότι για να το για υποστηρίξει απαιτεί επεκτάσεις στο σχήμα του ADDS. Η χρήση του ADLDS σε αυτό το σενάριο παρέχει τα πρόσθετα δεδομένα χρήστη χωρίς τροποποίηση του σχήματος ADDS. Για παράδειγμα, εάν έχουμε μια κεντρική εφαρμογή που παρέχει μια φωτογραφία κάθε υπαλλήλου στον οργανισμό μας και συσχετίζει αυτήν τη φωτογραφία με τον λογαριασμό ADDS του χρήστη, μπορούμε να αποθηκεύσουμε τις φωτογραφίες σε μια παρουσία ADLDS. Αποθηκεύοντας τις φωτογραφίες στο ADLDS σε κεντρική τοποθεσία συνδέονται απευθείας με τους λογαριασμούς χρηστών στο ADDS. Επειδή όμως είναι στο ADLDS, δεν αναπαράγονται με όλα τα άλλα δεδομένα του ADDS, πετυχαίνοντας έτσι την μείωση του εύρος ζώνης που χρειάζεται για την αναπαραγωγή.
- Μπορούμε να βασιστούμε σε μια παρουσία ADLDS για την παροχή υπηρεσιών ελέγχου ταυτότητας για μια εφαρμογή Web όπως το Microsoft SharePoint Portal

Server σε περιμετρικό δίκτυο ή extranet. Το ADLDS μπορεί να υποβάλει ερώτημα για την εσωτερική δομή ADDS μέσω τείχους προστασίας για τη λήψη πληροφοριών λογαριασμού χρήστη και να το αποθηκεύσει με ασφάλεια στο περιμετρικό δίκτυο. Αυτό αποφεύγει είτε την ανάπτυξη του ADDS στην περίμετρο είτε να συμπεριλαμβάνονται οι ελεγκτές τομέα από το εσωτερικό δίκτυο στη περίμετρο.

- Συγκέντρωση διαφόρων repositories ταυτότητας σε έναν μόνο κατάλογο. Χρησιμοποιώντας έναν μετακατευθυντικό κατάλογο υπηρεσίας, όπως τα Microsoft Identity Integration Server (MIIS), Microsoft Identity Lifecycle Διαχειριστής (MILM) ή το δωρεάν πακέτο δυνατοτήτων ολοκλήρωσης ταυτότητας (IIFP), μπορούμε να αποκτήσουμε δεδομένα από διάφορες πηγές και να τα ενοποιήσουμε σε μια παρουσία ADLDS. Τα MIIS και MILM υποστηρίζουν την παροχή δεδομένων από μια μεγάλη ποικιλία πηγών όπως τα δάση ADDS, SQL Βάσεις δεδομένων διακομιστή, υπηρεσίες LDAP τρίτων και πολλά άλλα. Το IIFP είναι ένα υποσύνολο των MIIS και υποστηρίζει την ενοποίηση δεδομένων μεταξύ ADDS, ADLDS και Exchange Server. Χρησιμοποιώντας αυτές τα λύσεις μειώνονται τα έξοδα διαχείρισης της ταυτότητας, ορίζοντας μία μόνο κύρια πηγή και παροχή όλων των άλλων repositories από αυτήν την πηγή.
- Παροχή υποστήριξης για εφαρμογές σε τμήματα. Σε ορισμένες περιπτώσεις, τα τμήματα μπορεί να απαιτούν πρόσθετες πληροφορίες ταυτότητας, πληροφορίες που δεν σχετίζονται με κανένα άλλο τμήμα εντός του οργανισμού. Ενσωματώνοντας αυτές τις πληροφορίες σε ένα ADLDS για παράδειγμα, το τμήμα έχει πρόσβαση σε αυτό χωρίς να επηρεάζει την υπηρεσία καταλόγου για ολόκληρο τον οργανισμό.
- Παροχή υποστήριξης για κατανεμημένες εφαρμογές. Εάν η αίτησή μας διανέμεται και απαιτεί πρόσβαση σε δεδομένα σε διάφορες τοποθεσίες, μπορούμε να βασιστούμε στο ADLDS επειδή ADLDS παρέχει τις ίδιες δυνατότητες αναπαραγωγής πολλαπλών μεταδόσεων με το ADDS.
- Μετεγκατάσταση εφαρμογών καταλόγου παλαιού τύπου σε ADLDS. Εάν ο οργανισμός μας λειτουργεί παλαιού τύπου εφαρμογές που βασίζονται σε έναν κατάλογο LDAP, μπορούμε να μεταφέρουμε τα δεδομένα σε ADLDS παρουσία και τυποποίηση με τεχνολογίες καταλόγου Active Directory.
- Παροχή υποστήριξη για την τοπική ανάπτυξη. Επειδή το ADLDS μπορεί να εγκατασταθεί σε σταθμούς εργασίας πελάτη, μπορούμε να παρέχουμε στους προγραμματιστές φορητούς καταλόγους μίας παρουσίας που μπορούν να τους χρησιμοποιήσουν για την ανάπτυξη προσαρμοσμένων εφαρμογών που απαιτούν πρόσβαση σε δεδομένα ταυτότητας. Η ανάπτυξη με το ADLDS είναι πολύ απλούστερη και πιο εύκολα διαχειρίσιμη στον περιορισμό της από την ανάπτυξη με ADDS.
- Επιπλέον, κατά την αξιολόγηση εμπορικών εφαρμογών με δυνατότητα καταλόγου, θα πρέπει να προτιμάμε πάντα μια εφαρμογή που θα βασίζεται στο ADLDS ή στον προκάτοχό του, ADAM, προτού επιλέξουμε αυτό που βασίζεται σε τροποποιήσεις σχήματος ADDS. Ανάπτυξη εφαρμογών διαφημίσεων με τη χρήση φορητών καταλόγων είναι πολύ ευκολότερη και έχουν πολύ μικρότερο αντίκτυπο στο δίκτυό μας από την ανάπτυξη εφαρμογών που θα τροποποιήσουν το σχήμα του καταλόγου NOS για πάντα.

Κάθε ένα από αυτά τα σενάρια αντιπροσωπεύει μια πιθανή χρήση του ADLDS. Οι τυπικές εφαρμογές πρέπει περιλαμβάνουν καταλόγους λευκών σελίδων, εφαρμογές

προσανατολισμένες στην ασφάλεια και στη διαμόρφωση δικτύου καθώς και policy store εφαρμογές. Όπως μπορούμε να δούμε, το ADLDS είναι πολύ πιο φορητό και εύπλαστο. Οποτεδήποτε πρέπει να σκεφτούμε τις τροποποιήσεις σχήματος στο ADDS, χωρίς σκέψη το ADLDS, σχεδόν σε κάθε περίπτωση θα προσφέρει μια καλύτερη επιλογή, διότι το ADDS πρέπει πάντα να είναι δεσμευμένο με τους καταλόγους NOS και πρέπει να περιλαμβάνει ενοποίηση μόνο με εφαρμογές που προσθέτουν λειτουργικότητα στις λειτουργίες καταλόγου NOS.

Δημιουργία παρουσιών AD LDS

Η διαδικασία εγκατάστασης ρόλου ADLDS μοιάζει πολύ με τη διαδικασία εγκατάστασης ADDS. Μετά την εγκατάσταση της υπηρεσίας ADLDS μέσα από τον Role Manager, δημιουργούμε ADLDS περιπτώσεις χρήσης της υπηρεσία με τον ίδιο τρόπο που αναπτύσσουμε το ADDS, χρησιμοποιώντας τον οδηγό εγκατάστασης υπηρεσιών τομέα Active Directory για να δημιουργήσουμε την παρουσία ADDS που θα χρησιμοποιήσουμε. Λόγω των ίδιων ριζών τους, πολλά από τα εργαλεία που χρησιμοποιούμε είναι το ίδιο διαχειρίσιμα.
Μπορούμε να δημιουργήσουμε παρουσίες ADLDS χρησιμοποιώντας τον οδηγό εγκατάστασης για τις υπηρεσίες καταλόγου Active Directory Lightweight. Ωστόσο, πρέπει να προετοιμαστούν πολλά στοιχεία πριν την δημιουργία του instance. Αυτά τα στοιχεία περιλαμβάνουν:

- ✓ Δημιουργία μονάδας δεδομένων για τον διακομιστή μας. Επειδή αυτός ο διακομιστής θα φιλοξενεί χώρους καταλόγων, τοποθετούμε αυτούς τους χώρους σε μια μονάδα δίσκου που είναι ξεχωριστή από το λειτουργικό σύστημα.
- ✓ Το όνομα που θα χρησιμοποιήσουμε για τη δημιουργία του instance. Θα πρέπει να χρησιμοποιήσουμε ουσιαστικά ονόματα, για παράδειγμα, το όνομα της εφαρμογής που θα συνδεθεί με αυτό το instance, για τον εντοπισμό instances. Αυτό το όνομα θα χρησιμοποιηθεί για την αναγνώριση του instance στον τοπικό υπολογιστή καθώς και για την ονομασία των αρχείων που αποτελούν το instance και την υπηρεσία που την υποστηρίζει.
- ✓ Οι πόρτες που σκοπεύουμε να χρησιμοποιήσουμε για να επικοινωνήσουμε με το instance. Τόσο ADLDS όσο και ADDS χρησιμοποιούν τις ίδιες πόρτες για επικοινωνία. Αυτές οι πόρτες είναι προεπιλεγμένες για το LDAP (389) και LDAP οι οποίες τρέχουν πάνω από τις πόρτες Secure Sockets Layer (SSL) ή Secure LDAP (636). Το ADDS χρησιμοποιεί δύο πρόσθετες πόρτες, την 3268 και 3269, οι οποίες χρησιμοποιούνται από το LDAP για πρόσβαση στον καθολικό κατάλογο και από το Secure LDAP για πρόσβαση στον καθολικό κατάλογο. Επειδή τα ADDS και ADLDS χρησιμοποιούν τις ίδιες πόρτες, αυτός είναι ένας άλλος καλός λόγος για να μην εκτελέσουμε και τους δύο ρόλους στον ίδιο διακομιστή. Ωστόσο, όταν ο οδηγός ανιχνεύει ότι οι θύρες 389 και 636 χρησιμοποιούνται ήδη, προτείνει 50000 και 50001 για κάθε πόρτα και στη συνέχεια χρησιμοποιεί άλλες πόρτες στην περιοχή 50000 για επιπλέον περιπτώσεις.
- ✓ Το όνομα του διαμερίσματος της εφαρμογής Active Directory που σκοπεύουμε να χρησιμοποιήσουμε για το instance. Θα πρέπει να χρησιμοποιήσουμε ένα διακεκριμένο όνομα (DN) για να δημιουργήσουμε το διαμέρισμα. Για παράδειγμα, θα μπορούσαμε να χρησιμοποιήσουμε CN = AppPartition1, DC = Contoso, DC = com. Ανάλογα με το πώς σκοπεύουμε να το χρησιμοποιήσουμε το instance, ίσως να χρειάζεται ή να μην χρειάζεται το διαμέρισμα εφαρμογής. Τα διαχωριστικά εφαρμογών ελέγχουν το πεδίο αναπαραγωγής για έναν χώρο καταλόγου. Για

παράδειγμα, όταν ενσωματώνουμε τα DNS δεδομένα στον κατάλογο, το ADDS δημιουργεί ένα διαμέρισμα εφαρμογής για να καταστήσει τα δεδομένα DNS διαθέσιμα σε κατάλληλα DC. Τα διαμερίσματα εφαρμογών για ADLDS μπορούν να δημιουργηθούν με έναν από τους παρακάτω τρεις τρόπους:

- όταν δημιουργούμε το instance,
- όταν εγκαθιστούμε την εφαρμογή στην οποία θα συνδεθεί το instance
- όταν δημιουργούμε το διαμέρισμα χειροκίνητα μέσω του εργαλείου LDP.exe.

Αν η εφαρμογή δεν δημιουργήσει αυτόματα διαμερίσματα εφαρμογών, θα τα δημιουργήσει με τον οδηγό.

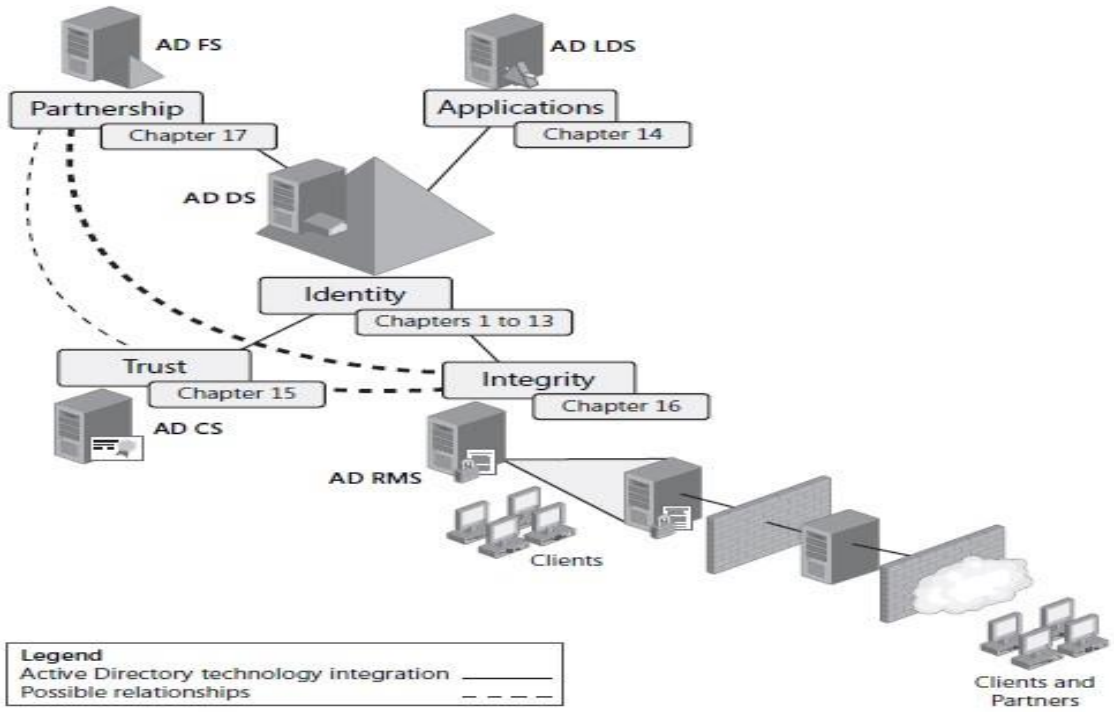
- ✓ Ένας λογαριασμός υπηρεσίας για την εκτέλεση της παρουσίας. Μπορούμε να χρησιμοποιήσουμε τον λογαριασμό υπηρεσίας δικτύου, αλλά εάν σκοπεύουμε να εκτελέσουμε πολλά instances είναι καλύτερο να χρησιμοποιήσουμε λογαριασμούς υπηρεσίας με όνομα σε κάθε περίπτωση. Καλό είναι να ακολουθούμε τις οδηγίες και τις απαιτήσεις λογαριασμών υπηρεσίας όπως παρακάτω:
  - ➢ Δημιουργούμε έναν λογαριασμό τομέα εάν βρισκόμαστε σε έναν τομέα. Διαφορετικά, χρησιμοποιούμε έναν τοπικό λογαριασμό (για παράδειγμα, σε ένα περιμετρικό δίκτυο).
  - ➢ Ονομάζουμε τον λογαριασμό με το ίδιο όνομα που δώσαμε και στο instance.
  - ➢ Εκχωρούμε έναν σύνθετο κωδικό πρόσβασης σε αυτόν τον λογαριασμό.
  - ➢ Ορισμός χρήστη έτσι ώστε να μην μπορεί να αλλάξει κωδικό πρόσβασης στις ιδιότητες του λογαριασμού του. Εκχωρούμε αυτήν την ιδιότητα για να διασφαλιστεί ότι κανείς δεν μπορεί να τροποποιήσει τον λογαριασμό του.
  - ➢ Ορισμός κωδικού πρόσβασης που δεν λήγει ποτέ στις ιδιότητες του λογαριασμού. Εκχωρούμε αυτήν την ιδιότητα για να βεβαιωθούμε ότι η υπηρεσία δεν αποτυγχάνει λόγω μιας πολιτικής κωδικού πρόσβασης.
  - ➢ Αντιστοιχίστε το Log On As A Service User απευθείας στο Local Security Policy για κάθε υπολογιστή που θα φιλοξενήσει αυτό το instance.
  - ➢ Εκχωρούμε τον Generate Security Audits User απευθείας στο Local Security Policy σε κάθε υπολογιστή που θα φιλοξενήσει αυτήν το instance για να υποστηρίζει τον έλεγχο λογαριασμού.
- ✓ Μια ομάδα που θα περιέχει τους λογαριασμούς χρηστών θα διαχειρίζονται την παρουσία. Η καλύτερη πρακτική για τις εκχωρήσεις αδειών είναι πάντα η χρήση ομάδων ακόμα κι αν είναι μόνο ένας λογαριασμός μέλος της ομάδας. Εάν το προσωπικό αλλάξει, μπορούμε πάντα να προσθέτουμε ή να αλλάξουμε μέλη της ομάδας χωρίς να χρειάζεται να προσθέσουμε ή να αλλάξουμε δικαιώματα. Εάν είμαστε σε έναν τομέα δημιουργούμε μια ομάδα τομέα, διαφορετικά δημιουργούμε μια τοπική ομάδα. Ονομάζουμε την ομάδα με το ίδιο όνομα που έχουμε εκχωρήσει στο instance. Έτσι θα είναι πιο εύκολο να παρακολουθούμε τον σκοπό της ομάδας. Προσθέτουμε τον δικό μας λογαριασμό στην ομάδα καθώς και στον λογαριασμό υπηρεσίας που δημιουργήσαμε νωρίτερα.
- ✓ Τυχόν πρόσθετα αρχεία LDIF που χρειαζόμαστε για το instance. Τοποθετούμε αυτά τα αρχεία στο %SystemRoot%/Φάκελος ADAM. Αυτά τα αρχεία θα εισαχθούν κατά τη δημιουργία του instance. Η εισαγωγή των αρχείων LDIF επεκτείνουν το σχήμα της παρουσίας που δημιουργούμε για να υποστηρίξουμε επιπλέον λειτουργίες. Για παράδειγμα, για να συγχρονίσουμε το ADDS με το ADLDS, θα εισάγουμε το MSAdamSyncMetadata.ldf. Εάν η εφαρμογή μας απαιτεί

προσαρμοσμένες τροποποιήσεις σχήματος, δημιουργούμε το αρχείο LDIF εκ των προτέρων και το εισάγουμε καθώς δημιουργούμε το instance.

6.3.4. Active Directory Rights Management Services (ADRMS)

Το Active Directory Rights Management Services (ADRMS), παλαιότερα γνωστό ως Rights Management Services, έχει σχεδιαστεί για να επεκτείνει την εμβέλεια του εσωτερικού μας δικτύου προς τον έξω κόσμο. Ωστόσο η επέκταση αυτή ισχύει για πνευματική ιδιοκτησία. Οι άνθρωποι άρχισαν να αγωνίζονται για τα Digital Rights Management (DRM) από τότε που άρχισαν να εργάζονται με υπολογιστές. Στις πρώτες μέρες της πληροφορικής, οι κατασκευαστές λογισμικού προσπάθησαν να προστατεύσουν το λογισμικό τους από κλοπή. Ακόμα και σήμερα, ορισμένοι προμηθευτές απαιτούν τη χρήση κλειδιών για την εκτέλεση του λογισμικό τους. Άλλοι έχουν καταφύγει σε διαδικασία έγκρισης και επικύρωσης μέσω Ιστού. Για παράδειγμα, με την κυκλοφορία των Windows Vista, η Microsoft εισήγαγε ένα νέο σχήμα αδειοδότησης, Μία επιλογή του οποίου είναι ένας διακομιστής διαχείρισης κλειδιών (KMS), για την επικύρωση των εκδόσεων με άδεια χρήσης των Microsoft Windows που χρησιμοποιούμε. Η δημιουργία λογισμικού δεν είναι η μόνη βιομηχανία που αγωνίζεται με τη διαχείριση δικαιωμάτων Η μουσική βιομηχανία βρίσκεται επίσης υπό πίεση για να καθορίσει τον καλύτερο τρόπο προστασίας της ψηφιακής μουσικής, μερικές φορές ακόμη και χρησιμοποιώντας αμφισβητήσιμες μεθόδους για να το πράξει. Για παράδειγμα, το 2005, ο Mark Russinovich, τώρα τεχνικός συνεργάτης της Microsoft Corporation, ανακάλυψε ότι η Sony BMG εγκατέστησε ένα root kit στο CD του προγράμματος αναπαραγωγής που ενεργοποιούνταν όταν οι χρήστες το φόρτωναν στους υπολογιστές τους. Αυτό το root kit έστελνε πληροφορίες playlist πίσω σε έναν κεντρικό διακομιστή που διαχειρίζεται η Sony μέσω του Διαδικτύου Αυτό οδήγησε σε μια σειρά από άρθρα και μια έντονη δραστηριότητα στο Διαδίκτυο σχετικά με τις προσεγγίσεις που χρησιμοποιούν οι πωλητές μουσικής για την προστασία του περιεχομένου τους.
Η μουσική και το λογισμικό δεν είναι τα μόνα αντικείμενα που χρειάζονται προστασία. Σε κέντρα δεδομένων παντού, οι άνθρωποι αρχίζουν να αναζητούν νέες τεχνολογίες για την προστασία της πνευματικής ιδιοκτησίας τους. Για παράδειγμα, το ηλεκτρονικό ταχυδρομείο διατηρεί αυτόματα ένα ίχνος συνομιλιών. Κάθε φορά που απαντάμε σε ένα μήνυμα, το αρχικό μήνυμα ενσωματώνεται στο δικό μας και ούτω καθεξής. Χωρίς DRM, οποιοσδήποτε μπορεί να αλλάξει το περιεχόμενο αυτής της ενσωματωμένης απόκρισης οποιαδήποτε στιγμή, αλλάζοντας τον τόνο ή τη φύση της συνομιλίας. Ακόμα χειρότερα, ο καθένας μπορεί να προωθήσει τη συνομιλία και να αλλάξει το περιεχόμενό της χωρίς καν να το καταλάβουμε. Ενσωματώνοντας την εφαρμογή DRM για την προστασία του περιεχομένου του ηλεκτρονικού ταχυδρομείου διασφαλίζεται ότι οι απαντήσεις δεν μπορούν ποτέ να τροποποιηθούν ακόμα κι αν είναι ενσωματωμένες σε άλλο μήνυμα. Το ίδιο ισχύει και για άλλα δικαιώματα πνευματικής ιδιοκτησίας - έγγραφα Microsoft Office Word, Microsoft παρουσιάσεις του Office PowerPoint και άλλα περιεχόμενα. Πολλοί οργανισμοί βασίζονται στην αξία της πνευματική τους ιδιοκτησίας. Η απώλεια αυτής της ιδιοκτησίας ή η κατάχρησή της, η αντιγραφή ή η κλοπή της μπορεί προκαλούν ανείπωτες ζημιές στις λειτουργίες τους. Δεν χρειάζεται να είμαστε μια μεγάλη επιχείρηση για να κερδίσουμε από κάποια μορφή διαχείρισης δικαιωμάτων.
Το ADRMS μας επιτρέπει να προστατεύουμε την πνευματική μας ιδιοκτησία μέσω της ενσωμάτωσης πολλών χαρακτηριστικών. Στην πραγματικότητα, εκτός από την άμεση

ενοποίηση με τις υπηρεσίες τομέα Active Directory DS, τα ADRMS μπορούν επίσης να βασίζονται τόσο στις υπηρεσίες πιστοποιητικών Active Directory (AD CS) όσο και στην υπηρεσία Active Directory Υπηρεσίες Ομοσπονδίας (AD FS). Το AD CS μπορεί να δημιουργήσει πιστοποιητικά δημόσιας υποδομής (PKI) ότι το ADRMS μπορεί να ενσωματωθεί σε έγγραφα. Το AD FS επεκτείνει τις πολιτικές ADRMS πέραν του τείχος προστασίας και υποστηρίζει την προστασία της πνευματικής ιδιοκτησίας μεταξύ των συνεργατών όπως φαίνεται στην εικόνα 6.50.

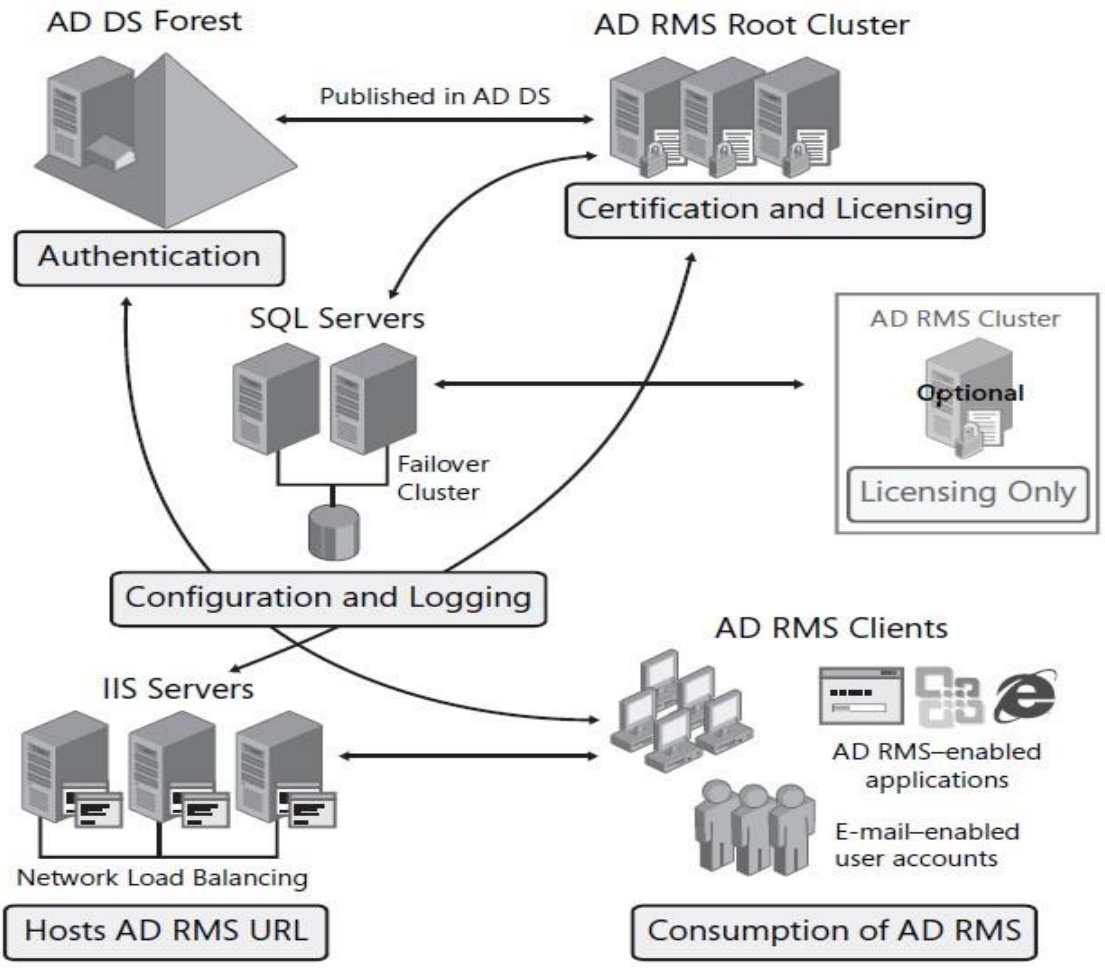


Εικόνα 6.50

Κατανόηση ADRMS

Το ADRMS είναι μια ενημερωμένη έκδοση του Microsoft Windows Rights Management Services το οποίο ήταν διαθέσιμο στις υπηρεσίες του Microsoft Windows Server 2003. Με αυτήν την έκδοση, η Microsoft έχει συμπεριλάβει πολλές νέες δυνατότητες που επεκτείνουν τη λειτουργικότητα που περιλαμβάνεται στο ADRMS. Ωστόσο, τα σενάρια που χρησιμοποιούνται για την ανάπτυξη ADRMS παραμένουν τα ίδια. Το ADRMS συνεργάζεται με έναν ειδικό πελάτη ADRMS για την προστασία ευαίσθητων πληροφοριών. Παρέχεται προστασία μέσω του ρόλου διακομιστή ADRMS, ο οποίος έχει σχεδιαστεί για την παροχή πιστοποιητικών και αδειών διαχείρισης. Οι πληροφορίες — διαμόρφωση και καταγραφή — διατηρούνται σε μια βάση δεδομένων. Σε περιβάλλοντα δοκιμών, μπορούμε να βασιστούμε στην εσωτερική βάση δεδομένων των Windows (WID) που περιλαμβάνεται στα Windows Server 2008, αλλά σε περιβάλλοντα παραγωγής, πρέπει να βασιζόμαστε σε μια επίσημη μηχανή βάσης δεδομένων όπως ο Microsoft SQL Server 2005 ή ο Microsoft SQL Server 2008 που εκτελείται σε ξεχωριστή υπηρεσία. Αυτό θα παρέχει τη δυνατότητα load balancing της υπηρεσίας ADRMS μέσω της εγκατάστασης πολλαπλών διακομιστών που εκτελούν αυτόν τον ρόλο. Το WID δεν υποστηρίζει απομακρυσμένες συνδέσεις. Επομένως, μόνο ένα ο διακομιστής μπορεί να το

χρησιμοποιήσει. Οι υπηρεσίες πληροφοριών Διαδικτύου (IIS) 7.0 παρέχουν τις υπηρεσίες Web στις οποίες βασίζονται το ADRMS και η υπηρεσία Microsoft Message Queue διασφαλίζει τον συντονισμό συναλλαγών σε κατανεμημένα περιβάλλοντα. Ο πελάτης ADRMS παρέχει πρόσβαση σε δυνατότητες ADRMS στην επιφάνεια εργασίας. Επιπλέον, ένας κατάλογος ADDS παρέχει ολοκληρωμένο έλεγχο ταυτότητας και διαχείρισης. Το ADRMS βασίζεται στο ADDS για έλεγχο ταυτότητας χρηστών και επαλήθευσης σε όσους επιτρέπεται να χρησιμοποιούν την υπηρεσία. Η υποδομή ADRMS φαίνεται στην εικόνα 6.51.



Εικόνα 6.51

Την πρώτη φορά που θα εγκαταστήσουμε έναν διακομιστή ADRMS, θα δημιουργηθεί από προεπιλογή ένα σύμπλεγμα ρίζας ADRMS. Το σύμπλεγμα ρίζας έχει σχεδιαστεί για να διεκπεραιώνει αιτήματα πιστοποίησης και αδειοδότησης. Μόνο ένα σύμπλεγμα ρίζας μπορεί να υπάρχει σε ένα δάσος ADDS. Μπορούμε επίσης να εγκαταστήσουμε διακομιστές μόνο με άδεια χρήσης, οι οποίοι αυτόματα σχηματίζουν ένα σύμπλεγμα αδειοδότησης. Τα συμπλέγματα είναι διαθέσιμα μόνο εάν έχουμε αναπτύξει τη βάση δεδομένων ADRMS σε ξεχωριστό διακομιστή. Κάθε φορά που προσθέτουμε έναν νέο διακομιστή ADRMS είτε με ρόλο τη ρίζα είτε με την αδειοδότηση, ενσωματώνεται αυτόματα στο αντίστοιχο υπάρχον σύμπλεγμα. Η Microsoft συνιστά να βασιζόμαστε περισσότερο στον ριζικό ρόλο παρά στον ρόλο μόνο για αδειοδότηση για δύο λόγους:

- Τα σύνολα ρίζας χειρίζονται όλες τις λειτουργίες AD RMS και, επομένως, είναι πολυλειτουργικά.
- Οι συστάδες μόνο ρίζας και αδειοδότησης είναι ανεξάρτητες, δηλαδή δεν μπορούν να μοιραστούν την εξισορρόπηση φορτίου της υπηρεσίας.

Εάν εγκαταστήσουμε όλους τους διακομιστές μας ως διακομιστές ρίζας, φορτώνουν αυτόματα την ισορροπία μεταξύ τους. Μετά την ολοκλήρωση της υποδομής, μπορούμε να ενεργοποιήσουμε εφαρμογές παραγωγής πληροφοριών όπως επεξεργαστές κειμένου, εργαλεία παρουσίασης, πελάτες e-mail και προσαρμοσμένες εσωτερικές εφαρμογές οι οποίες θα είναι βασισμένες στο ADRMS για την παροχή υπηρεσιών προστασίας πληροφοριών. Καθώς οι χρήστες δημιουργούν τις πληροφορίες, αυτοί καθορίζουν ποιοι θα είναι σε θέση να διαβάσουν, να γράψουν, να τροποποιήσουν, να εκτυπώσουν, να μεταφέρουν και να χειριστούν με άλλο τρόπο τις πληροφορίες. Επιπλέον, μπορούμε να δημιουργήσουμε πρότυπα πολιτικής που μπορούν να εφαρμόσουν μια δεδομένη διαμόρφωση σε έγγραφα καθώς δημιουργούνται.
Τα δικαιώματα χρήσης ενσωματώνονται απευθείας στα έγγραφα που δημιουργούμε έτσι ώστε οι πληροφορίες να παραμένουν προστατευμένες ακόμα κι αν κινούνται πέρα από τη ζώνη εξουσίας μας. Για παράδειγμα, εάν ένα προστατευμένο έγγραφο φεύγει από τις εγκαταστάσεις μας και φτάνει έξω από το δίκτυό μας, θα παραμείνει προστατευμένο επειδή οι ρυθμίσεις ADRMS είναι μόνιμες. Το ADRMS προσφέρει ένα σύνολο υπηρεσιών Web, επιτρέποντάς μας να το επεκτείνουμε και να ενσωματώσουμε τις δυνατότητές του στις δικές μας εφαρμογές παραγωγής πληροφοριών. Επειδή είναι υπηρεσίες Web, οι οργανισμοί μπορούν να τις χρησιμοποιήσουν για να ενσωματώσουν δυνατότητες ADRMS ακόμη και σε μη περιβάλλοντα Windows.

Νέες δυνατότητες ADRMS

Οι υπηρεσίες διαχείρισης δικαιωμάτων Active Directory περιλαμβάνουν πολλές νέες δυνατότητες:

- Το AD RMS είναι πλέον ένας ρόλος διακομιστή που είναι ενσωματωμένος στον Windows Server 2008. Στις προηγούμενες εκδόσεις, οι δυνατότητες που υποστηρίζονται από ADRMS παρέχονταν σε ένα πακέτο που απαιτούσε ξεχωριστή λήψη. Επιπλέον, η εγκατάσταση του διαχειριστή διακομιστή παρέχει όλα τα dependencies και απαιτούμενες εγκαταστάσεις εξαρτημάτων. Επίσης, εάν δεν εμφανίζεται απομακρυσμένη βάση δεδομένων κατά τη διάρκεια εγκατάστασης, ο διαχειριστής διακομιστή θα εγκαταστήσει αυτόματα την εσωτερική βάση δεδομένων των Windows.
- Όπως συμβαίνει με τους περισσότερους ρόλους διακομιστή των Windows Server 2008, το ADRMS διαχειρίζεται μέσω μιας κονσόλα διαχείρισης της Microsoft (MMC). Οι προηγούμενες εκδόσεις παρείχαν διαχείριση μόνο μέσω διεπαφής ιστού.
- Το ADRMS περιλαμβάνει άμεση ενσωμάτωση με τις υπηρεσίες Active Directory Federation Services, επιτρέποντάς μας την επέκταση στις πολιτικές διαχείρισης δικαιωμάτων πέρα από το τείχος προστασίας με τους συνεργάτες μας. Αυτό σημαίνει ότι οι συνεργάτες μας δεν χρειάζονται τις δικές τους υποδομές ADRMS και μπορούν να βασίζονται στο δικό μας μέσω του ADFS για πρόσβαση στις δυνατότητες ADRMS. Στις προηγούμενες εκδόσεις, μπορούσαμε να βασιστούμε μόνο στα Windows Live ID για την ενοποίηση υπηρεσιών RMS. Με την ενσωμάτωση ADRMS και ADFS, δεν χρειάζεται πλέον να βασιζόμαστε σε τρίτο μέρος για την προστασία των πληροφοριών. Ωστόσο, για χρήση ομοσπονδίας,

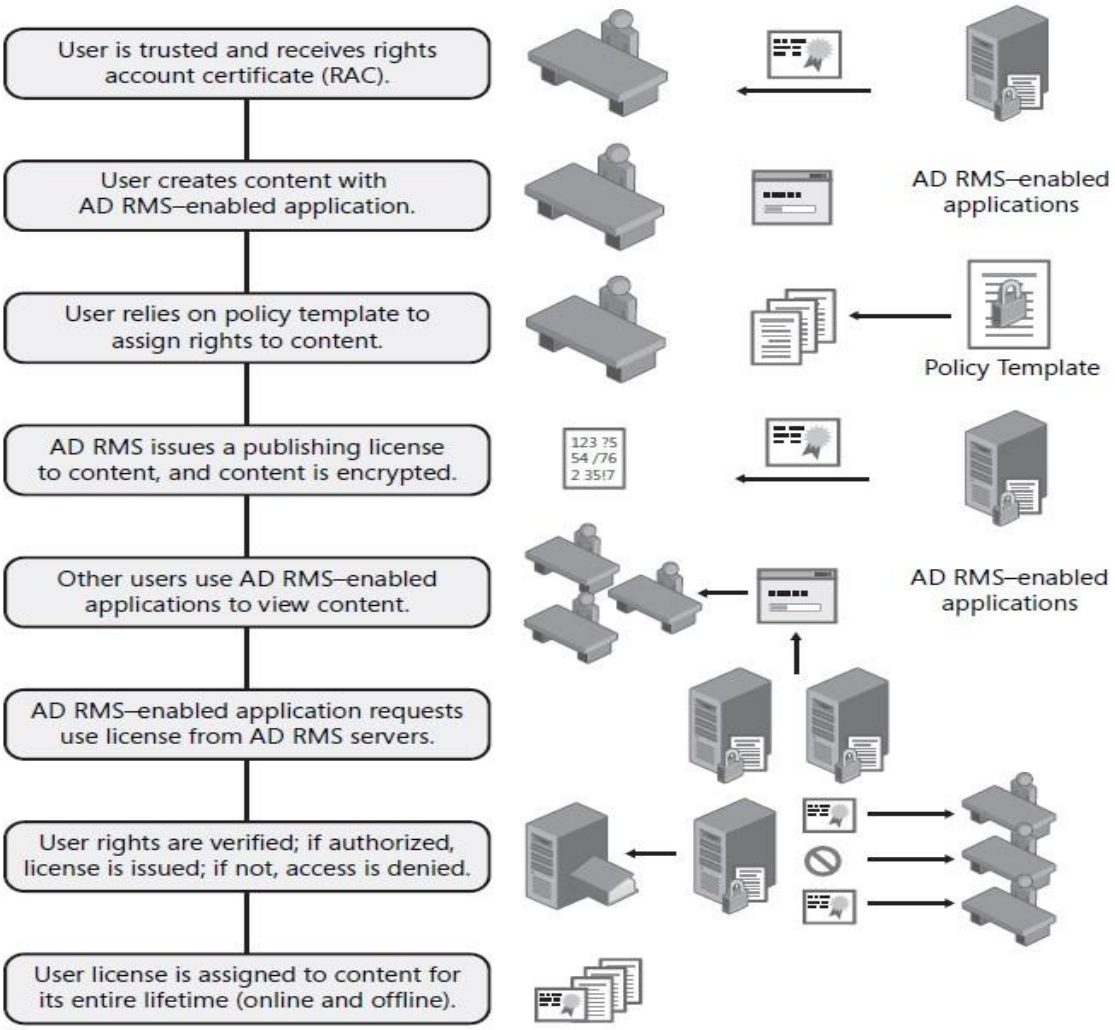
πρέπει να έχουμε καθιερώσει ενοποιημένη εμπιστοσύνη πριν εγκαταστήσουμε το ADRMS επέκταση που ενσωματώνεται στο ADFS και πρέπει να χρησιμοποιήσουμε τον πιο πρόσφατο πελάτη RMS.

- Οι διακομιστές AD RMS εγγράφονται αυτόματα όταν δημιουργούνται. Η εγγραφή δημιουργεί έναν διακομιστή με πιστοποιητικό άδειας χρήσης (SLC), το οποίο παρέχει στο διακομιστή το δικαίωμα συμμετοχής στην ADRMS δομή. Οι παλαιότερες εκδόσεις απαιτούσαν πρόσβαση στο Κέντρο Εγγραφής της Microsoft μέσω του Διαδικτύου για την έκδοση και υπογραφή του SLC. Το ADRMS βασίζεται σε πιστοποιητικό αυτό-εγγραφής που περιλαμβάνεται στα Windows Server 2008. Εξαιτίας αυτού, μπορούμε τώρα να εκτελέσουμε ADRMS σε μεμονωμένα δίκτυα χωρίς να απαιτείται οποιουδήποτε είδους πρόσβαση στο Διαδίκτυο.
- Το AD RMS περιλαμβάνει νέους ρόλους διαχείρισης, ώστε να μπορούμε να εκχωρήσουμε συγκεκριμένες ADRMS εργασίες χωρίς να χρειάζεται να παραχωρήσουμε υπερβολικά δικαιώματα διαχείρισης. Τέσσερις τοπικοί διοικητικοί ρόλοι δημιουργούνται:
    - *ADRMS Enterprise Administrators*, οι οποίοι μπορούν να διαχειριστούν όλες τις πτυχές του ADRMS. Αυτή η ομάδα περιλαμβάνει τον λογαριασμό χρήστη που χρησιμοποιείται για την εγκατάσταση του ρόλου καθώς και την ομάδα με τους τοπικούς διαχειριστές.
    - *Διαχειριστές προτύπων ADRMS*, οι οποίοι υποστηρίζουν τη δυνατότητα ανάγνωσης πληροφοριών σχετικά με την υποδομή ADRMS καθώς και για τη λίστα, τη δημιουργία, την τροποποίηση και τα δικαιώματα εξαγωγής policy templates.
    - *AD RMS Auditors*, που επιτρέπει στα μέλη να διαχειρίζονται αρχεία καταγραφής και αναφορές. Οι ελεγκτές έχουν πρόσβαση μόνο για ανάγνωση σε πληροφορίες υποδομής ADRMS.
    - *Υπηρεσία ADRMS*, η οποία περιέχει τον λογαριασμό υπηρεσίας ADRMS που προσδιορίστηκε κατά τη διάρκεια της εγκατάστασης ρόλων.

Επειδή καθεμία από αυτές τις ομάδες είναι τοπική, δημιουργούμαι αντίστοιχες ομάδες στον κατάλογο ADDS και εισάγουμε αυτές τις ομάδες στις τοπικές ομάδες σε κάθε διακομιστή ADRMS. Όταν πρέπει να εκχωρήσουμε δικαιώματα σε έναν διαχειριστικό ρόλο, το μόνο που χρειάζεται να κάνουμε είναι να προσθέσουμε τον λογαριασμό χρήστη στην ομάδα στο ADDS.

Όταν προστατεύουμε πληροφορίες μέσω ADRMS, βασιζόμαστε στον διακομιστή ADRMS για την έκδοση πιστοποιητικών λογαριασμού δικαιωμάτων. Αυτά τα πιστοποιητικά προσδιορίζουν τις αξιόπιστες οντότητες — χρήστες, ομάδες, υπολογιστές, εφαρμογές ή υπηρεσίες - που μπορούν να δημιουργήσουν και να δημοσιεύσουν περιεχόμενο με δικαιώματα. Μετά ένας εκδότης περιεχομένου ο οποίος είναι έμπιστος, μπορεί να εκχωρήσει δικαιώματα και προϋποθέσεις στο περιεχόμενο που δημιουργεί. Κάθε φορά που ένας χρήστης θεσπίζει πολιτική προστασίας σε ένα έγγραφο, το ADRMS εκδίδει μια άδεια για το περιεχόμενο. Με την ενσωμάτωση αυτής της άδειας στο περιεχόμενο, το ADRMS το δεσμεύει ότι η άδεια συνδέεται μόνιμα και δεν απαιτεί πλέον πρόσβαση σε ADRMS σύστημα για την προστασία εγγράφων ή περιεχομένου. Τα δικαιώματα χρήσης ενσωματώνονται σε οποιαδήποτε μορφή δυαδικών δεδομένων που υποστηρίζει τη χρήση εντός ή εκτός του δικτύου μας, καθώς και στο διαδίκτυο ή εκτός σύνδεσης. Όταν το περιεχόμενο προστατεύεται, κρυπτογραφείται με ειδικά κλειδιά κρυπτογράφησης, όπως τα κλειδιά που δημιουργούνται όταν χρησιμοποιούμε το Active Directory Certificate Services(ADCS) Για να δουν τα δεδομένα, οι χρήστες πρέπει να έχουν πρόσβαση μέσω ενός προγράμματος περιήγησης ή εφαρμογής με δυνατότητα ADRMS. Εάν η εφαρμογή

δεν είναι ADRMS-enabled, οι χρήστες δεν θα μπορούν να χειριστούν τις πληροφορίες, επειδή η εφαρμογή δεν θα είναι σε θέση να διαβάσει την πολιτική προστασίας για να αποκρυπτογραφήσει σωστά τα δεδομένα. Όταν άλλοι χρήστες έχουν πρόσβαση στο περιεχόμενο που προστατεύεται από δικαιώματα, οι πελάτες ADRMS ζητούν άδεια από το διακομιστή για τη χρήση. Εάν ο χρήστης είναι επίσης αξιόπιστη οντότητα, ο διακομιστής ADRMS εκδίδει αυτήν την άδεια χρήσης. Η άδεια χρήσης διαβάζει την άδεια προστασίας για αυτό το έγγραφο και εφαρμόζει αυτήν τη χρήση δικαιωμάτων στο έγγραφο για όλη τη διάρκεια ζωής του. Για να διευκολυνθεί η διαδικασία δημοσίευσης, οι έμπιστοι χρήστες μπορούν να δημιουργήσουν άδειες προστασίας από προκαθορισμένα πρότυπα που μπορούν να εφαρμοστούν μέσω των εργαλείων με τα οποία είναι ήδη εξοικειωμένα - word επεξεργαστές, πελάτες ηλεκτρονικού ταχυδρομείου και παρόμοια. Κάθε πρότυπο εφαρμόζει μια συγκεκριμένη προκαθορισμένη πολιτική χρήσης, όπως φαίνεται στην εικόνα 6.52.



Εικόνα 6.52

Σενάρια εγκατάστασης ADRMS

Κάθε οργανισμός έχει τις δικές του ανάγκες και απαιτήσεις για την προστασία των πληροφοριών. Γι' αυτό το λόγο, Το ADRMS υποστηρίζει διάφορα σενάρια ανάπτυξης. Αυτά τα σενάρια περιλαμβάνουν:

- *Ανάπτυξη μεμονωμένου διακομιστή*: Εγκατάσταση ADRMS σε έναν μόνο διακομιστή. Αυτό εγκαθιστά το WID ως τη βάση δεδομένων υποστήριξης. Επειδή όλα τα στοιχεία είναι τοπικά, δεν μπορούμε να το κλιμακώσουμε για υποστήριξη υψηλής διαθεσιμότητας. Συστήνεται η ανάπτυξη ενός μόνο διακομιστή σε περιβάλλοντα δοκιμής. Εάν θέλουμε να χρησιμοποιήσουμε αυτήν την ανάπτυξη για να δοκιμάσουμε το ADRMS πέρα από το τείχος προστασίας, θα πρέπει να προσθέσουμε τις κατάλληλες εξαιρέσεις στο ADRMS.
- *Εσωτερική ανάπτυξη*: Εγκατάσταση ADRMS σε πολλούς διακομιστές συνδεδεμένους σε έναν κατάλογο ADDS. Πρέπει να χρησιμοποιήσουμε έναν ξεχωριστό διακομιστή για να φιλοξενήσουμε τη βάση δεδομένων ADRMS. Διαφορετικά, δεν θα μπορεί να γίνει το load balancing του ρόλου AD RMS.
- *Ανάπτυξη Extranet*: Όταν οι χρήστες είναι φορητοί και δεν παραμένουν εντός των ορίων του δικτύου μας, πρέπει να αναπτύξουμε το ADRMS σε ένα extranet - ένα ειδικό περιμετρικό δίκτυο που παρέχει εσωτερικές υπηρεσίες σε εξουσιοδοτημένους χρήστες. Σε αυτό το σενάριο, θα πρέπει να διαμορφώσουμε κατάλληλες εξαιρέσεις τείχους προστασίας και προσθήκη μιας ειδικής διεύθυνσης URL extranet σε έναν εξωτερικό διακομιστή ιστού για να επιτρέπονται εξωτερικές συνδέσεις πελατών.
- *Ανάπτυξη πολλών δασών*: Όταν έχουμε υπάρχουσες συνεργασίες που βασίζονται σε ADDS δάση εμπιστοσύνης, πρέπει να εκτελέσουμε μια πολύπλευρη ανάπτυξη. Σε αυτήν την περίπτωση, πρέπει να αναπτύξουμε πολλαπλές εγκαταστάσεις ADRMS, μία σε κάθε δάσος. Στη συνέχεια, εκχωρούμε ένα Secure Sockets Layer (SSL) πιστοποιητικό σε κάθε τοποθεσία Web που φιλοξενεί τα συμπλέγματα ADRMS σε κάθε δάσος. Επίσης θα πρέπει να επεκτείνουμε το σχήμα ADDS για να συμπεριλάβει αντικείμενα ADRMS. Στην περίπτωση που χρησιμοποιούμε ήδη τον Microsoft Exchange Server σε κάθε δάσος, οι επεκτάσεις θα υπάρχουν ήδη. Ο λογαριασμός υπηρεσίας ADRMS - ο λογαριασμός που εκτελεί την υπηρεσία - θα πρέπει να είναι αξιόπιστος σε κάθε δάσος.
- *ADRMS με ανάπτυξη ADFS*: Μπορούμε επίσης να επεκτείνετε το ADRMS root cluster σε άλλα δάση μέσω της υπηρεσίας Active Directory Federation Services. Για να το κάνουμε αυτό, θα πρέπει να προετοιμάσουμε τα παρακάτω:
    1. Εκχώρηση ενός πιστοποιητικού SSL στην τοποθεσία Web που φιλοξενεί το σύμπλεγμα ρίζας ADRMS. Αυτό θα εξασφαλίσει ασφαλείς επικοινωνίες μεταξύ του συμπλέγματος και του διακομιστή πόρων ADFS.
    2. Εγκατάσταση συμπλέγματος ρίζας.
    3. Προετοιμασία μιας ομοσπονδιακής σχέση εμπιστοσύνης πριν πραγματοποιηθεί εγκατάσταση του Identity Federation Support ρόλου υπηρεσίας του ADRMS.
    4. Δημιουργία μιας εφαρμογής με γνώμονα τα δικαιώματα στον διακομιστή συνεργατών πόρων ADFS και για τα δύο, την πιστοποίηση και τα pipepline αδειοδότησης του ADRMS.
    5. Εκχώρηση δημιουργίας ελέγχων ασφαλείας του χρήστη απευθείας στον λογαριασμό υπηρεσίας ADRMS.

6. Ορισμός URL συμπλέγματος extranet σε ADRMS και στη συνέχεια εγκατάσταση ταυτότητας ADRMS Identity Federation Support μέσω Server Manager.

- *Ανάπτυξη διακομιστή μόνο με άδεια χρήσης*: Σε σύνθετα περιβάλλοντα δασών, μπορούμε εάν θέλουμε την ανάπτυξη ενός συμπλέγματος ADRMS μόνο για αδειοδότηση εκτός από το σύμπλεγμα ρίζας. Σε αυτήν την περίπτωση, θα πρέπει πρώτα να εκχωρήσουμε ένα πιστοποιητικό SSL στην τοποθεσία Web που φιλοξενεί το ριζικό σύμπλεγμα ADRMS και στη συνέχεια να εγκαταστήσουμε το σύμπλεγμα ρίζας.
- *Αναβάθμιση των Windows RMS σε ADRMS*: Εάν κάνουμε αναβάθμιση από μία υπάρχουσα εγκατάσταση Windows RMS, πρέπει να εκτελέσουμε τα ακόλουθα βήματα:
    1. Θα πρέπει να βεβαιωθούμε ότι τα συστήματα RMS μας έχουν αναβαθμιστεί σε RMS Service Pack 1 πριν από την αναβάθμιση.
    2. Δημιουργία αντιγράφων ασφαλείας όλων των διακομιστών και δημιουργία αντιγράφων ασφαλείας της βάσης δεδομένων διαμόρφωσης και αποθήκευση του σε ασφαλές σημείο.
    3. Εάν χρησιμοποιούμε εγγραφή εκτός σύνδεσης για να ρυθμίσουμε το περιβάλλον RMS των Windows, θα πρέπει να βεβαιωθούμε ότι η εγγραφή έχει ολοκληρωθεί πριν από την αναβάθμιση.
    4. Εάν έχουμε ήδη σημεία σύνδεσης υπηρεσίας στην υπηρεσία καταλόγου Active Directory, θα πρέπει να βεβαιωθούμε ότι χρησιμοποιούν την ίδια διεύθυνση URL για την αναβάθμιση.
    5. Εάν η βάση δεδομένων των Windows RMS εκτελεί Microsoft SQL Server Desktop Engine (MSDE), πρέπει να πραγματοποιήσουμε αναβάθμιση σε SQL Server πριν από την αναβάθμιση σε ADRMS.
    6. Καθαρισμός της ουράς μηνυμάτων RMS για να βεβαιωθούμε ότι όλα τα μηνύματα είναι γραμμένα στη βάση δεδομένων καταγραφής RMS πριν από την αναβάθμιση.
    7. Αναβάθμιση του συμπλέγματος ρίζας πριν από την αναβάθμιση του διακομιστή μόνο με άδεια χρήσης. Αυτό θα παρέχει το αυτο-υπογεγραμμένο SLC του ριζικού συμπλέγματος στον διακομιστή αδειών χρήσης όταν πραγματοποιηθεί η αναβάθμιση.
    8. Αναβάθμιση όλων των άλλων διακομιστών στο σύμπλεγμα RMS.

Αυτά τα σενάρια παρέχουν τις πιο κοινές δομές ανάπτυξης για ADRMS.

Κατανόηση των πιστοποιητικών AD RMS

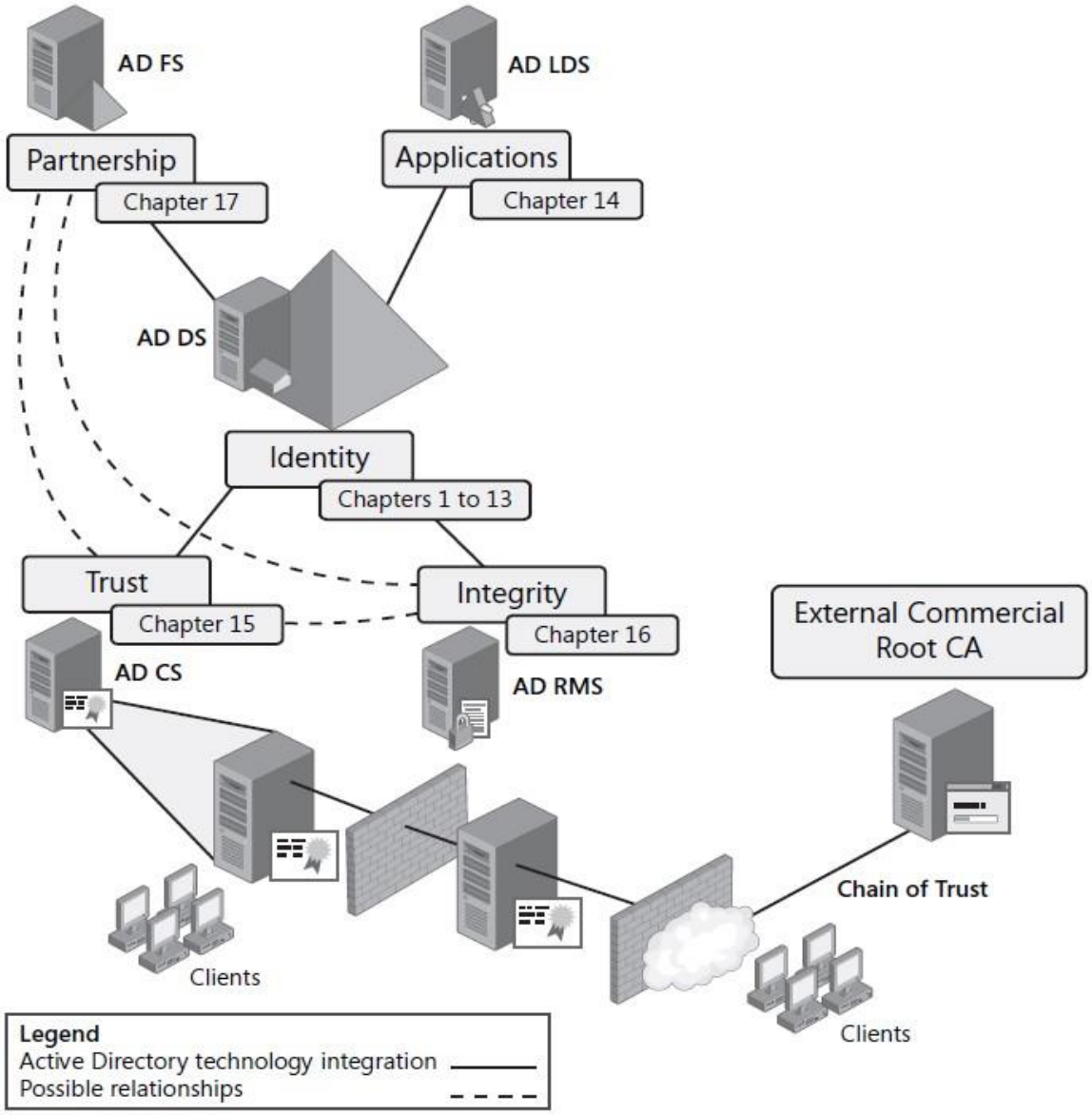
Επειδή κρυπτογραφεί και υπογράφει δεδομένα, το ADRMS, όπως το ADCS, βασίζεται σε πιστοποιητικά και τα εκχωρεί στους διάφορους χρήστες στην υποδομή ADRMS. Χρησιμοποιεί επίσης άδειες που βρίσκονται με μορφή Extensible Rights Markup Language (XrML). Επειδή αυτές οι άδειες είναι ενσωματωμένες στο περιεχόμενο που δημιουργούν οι χρήστες, είναι επίσης μια μορφή πιστοποιητικού. Όπως το ADCS, η ιεραρχία ADRMS σχηματίζει μια αλυσίδα εμπιστοσύνης που επικυρώνει το πιστοποιητικό ή την άδεια χρήσης όταν χρησιμοποιείται. Στον Πίνακα 6.3 περιγράφονται τα διάφορα πιστοποιητικά που χρειάζονται σε μια υποδομή ADRMS.

Πιστοποιητικό	Περιεχόμενο
Server licensor certificate (SLC)	Το SLC είναι ένα αυτό-υπογεγραμμένο πιστοποιητικό που δημιουργήθηκε κατά τη ρύθμιση ADRMS του πρώτου διακομιστή σε ένα σύμπλεγμα ρίζας. Άλλα μέλη του συμπλέγματος ρίζας θα μοιραστούν αυτό το SLC. Εάν δημιουργήσουμε ένα σύμπλεγμα μόνο για άδειες, θα δημιουργηθεί το δικό του SLC το οποίο θα μοιραστεί με μέλη του συμπλέγματος του. Η προεπιλεγμένη διάρκεια για ένα SLC είναι 250 χρόνια.
Rights account certificate (RAC)	Τα RAC εκδίδονται σε αξιόπιστους χρήστες που διαθέτουν λογαριασμό με δυνατότητα ηλεκτρονικού ταχυδρομείου σε ADDS. Τα RAC δημιουργούνται όταν ο χρήστης προσπαθεί για πρώτη φορά να ανοίξει περιεχόμενο με προστατευμένα δικαιώματα. Τα τυπικά RAC αναγνωρίζουν τους χρήστες σε σχέση με τους υπολογιστές τους και έχουν διάρκεια 365 ημερών. Τα προσωρινά RAC δεν συνδέουν τον χρήστη με έναν συγκεκριμένο υπολογιστή και ισχύει μόνο για 15 λεπτά. Το RAC περιέχει το δημόσιο κλειδί του χρήστη καθώς και το ιδιωτικό του κλειδί. Το ιδιωτικό κλειδί είναι κρυπτογραφημένο με το ιδιωτικό κλειδί του υπολογιστή.
Client licensor certificate (CLC)	Αφού ο χρήστης διαθέτει RAC και ξεκινήσει μια εφαρμογή με δυνατότητα ADRMS, η εφαρμογή στέλνει αυτόματα ένα αίτημα για CLC στο ADRMS σύμπλεγμα. Ο υπολογιστής-πελάτης πρέπει να είναι συνδεδεμένος για να λειτουργήσει αυτή η διαδικασία, αλλά μετά την απόκτηση του CLC, ο χρήστης μπορεί να εφαρμόσει πολιτικές ADRMS ακόμη και εκτός σύνδεσης. Επειδή το CLC είναι συνδεδεμένο με το RAC του πελάτη, ακυρώνεται αυτόματα όταν το RAC ανακαλείται. Το CLC περιλαμβάνει το δημόσιο κλειδί του δικαιοπάροχου πελάτη, το ιδιωτικό άδεια χρήσης του πελάτη κλειδί που είναι κρυπτογραφημένο από το δημόσιο κλειδί του χρήστη και το ADRMS δημόσιο κλειδί του συμπλέγματος. Το ιδιωτικό κλειδί CLC χρησιμοποιείται για την κρυπτογράφηση περιεχομένου.
Machine certificate	Την πρώτη φορά που χρησιμοποιείται μια εφαρμογή με δυνατότητα ADRMS, δημιουργείται ένα πιστοποιητικό μηχανήματος. Ο πελάτης ADRMS στα Windows διαχειρίζεται αυτόματα τη διαδικασία αυτή με το σύμπλεγμα ADRMS. Αυτό το πιστοποιητικό δημιουργεί ένα είδος κλειδαριάς στον υπολογιστή για να συσχετίσει το πιστοποιητικό του μηχανήματος με το προφίλ χρήστη. Το πιστοποιητικό μηχανήματος περιέχει το δημόσιο κλειδί για τον ενεργοποιημένο υπολογιστή. Το ιδιωτικό κλειδί περιέχεται στο πλαίσιο κλειδώματος του υπολογιστή.
Publishing license	Η άδεια δημοσίευσης δημιουργείται όταν ο χρήστης αποθηκεύει περιεχόμενο με ενεργοποιημένη την προστασία δικαιωμάτων. Αυτή η άδεια παραθέτει τους χρήστες που μπορούν να χρησιμοποιήσουν το περιεχόμενο και υπό ποιες προϋποθέσεις καθώς και τα δικαιώματα που έχει κάθε χρήστης στο περιεχόμενο. Αυτή η άδεια περιλαμβάνει το συμμετρικό κλειδί περιεχομένου για την αποκρυπτογράφηση περιεχομένου καθώς και το δημόσιο κλειδί του συμπλέγματος.

Use license	Η άδεια χρήσης εκχωρείται σε έναν χρήστη που ανοίγει περιεχόμενο που προστατεύεται από δικαιώματα. Συνδέεται με το RAC του χρήστη και παραθέτει τα δικαιώματα πρόσβασης που έχει ο χρήστης στο περιεχόμενο. Εάν το RAC δεν είναι διαθέσιμο, ο χρήστης δεν μπορεί να επεξεργαστεί με το περιεχόμενο που προστατεύεται από δικαιώματα. Περιέχει το συμμετρικό κλειδί για την αποκρυπτογράφηση περιεχομένου. Αυτό το κλειδί είναι κρυπτογραφημένο με το δημόσιο κλειδί του χρήστη.
Πίνακας 6.3	

6.3.5. A D Certificate Services & Public Key Infrastructures (ADCS & PKI)

Οι υποδομές δημόσιου κλειδιού (PKI) γίνονται βασικά στοιχεία υποδομής για όλες τις σύγχρονες οργανώσεις. Σχεδόν κάθε οργανισμός σήμερα έχει κάποια χρήση για πιστοποιητικά δημόσιου κλειδιού. Είτε πρόκειται για την ασφαλή ασύρματη επικοινωνία, για την παροχή ασφαλών εμπορικών υπηρεσιών σε ιστοσελίδες, για την ενσωμάτωση εικονικών ιδιωτικών δικτύων Secure Sockets Layer (SSL), ή ακόμη και μόνο υπογραφή e-mail και αναγνώριση του εαυτού μας σε περιβάλλοντα Web, όλοι οι οργανισμοί παντού χρησιμοποιούν πιστοποιητικά PKI. Με τα πιστοποιητικά PKI έρχεται η ίδια η υποδομή - μια υποδομή που πρέπει πρώτα να δημιουργήσουμε και μετά να τη διαχειριστούμε. Η Microsoft έχει συμπεριλάβει τη δυνατότητα δημιουργίας και συντήρησης PKI απευθείας στο λειτουργικό σύστημα εδώ και μερικά χρόνια. Στην περίπτωση του Windows Server 2008, αυτή η δυνατότητα παρέχεται από Active Directory Certificate Services (ADCS), γνωστές απλώς ως υπηρεσίες πιστοποιητικών σε προηγούμενες εκδόσεις των Microsoft Windows. Εξαιτίας αυτού, οι οργανισμοί επιλέγουν τώρα να εφαρμόσουν και να διαχειριστούν τις δικές τους υποδομές.
Ωστόσο, η ίδια η φύση των PKIs είναι ότι δεν βασίζονται μόνο σε λογισμικό. Επειδή τα πιστοποιητικά PKI έχουν σχεδιαστεί για να αποδεικνύουν σε άλλους ότι είμαστε αυτό που λέμε ότι είμαστε, πρέπει να εφαρμόσουμε διοικητικές διαδικασίες που έχουν σχεδιαστεί για να αποδεικνύουν αποτελεσματικά ότι κάθε άτομο που λαμβάνει ένα πιστοποιητικό από μας είναι όποιος ισχυρίζεται ότι είναι. Παρέχοντας πιστοποιητικά στο κάθε άτομο στον οργανισμό μας, του παρέχουμε ένα αναμφισβήτητο εργαλείο - ένα εργαλείο που εγγυάται την ταυτότητα κάθε ατόμου. Οι υποδομές δημόσιου κλειδιού έχουν σχεδιαστεί για να χτίσουν έναν κόσμο εμπιστοσύνης σε ένα αναξιόπιστο περιβάλλον. Στην πραγματικότητα, τα PKI μπορούν να χρησιμοποιηθούν για την επέκταση της εξουσίας που έχει ο οργανισμός σας πέρα από τα όρια του δικτύου που ελέγχει. Αν και Active Directory Domain Services (ADDS), ως δίκτυο κατάλογος λειτουργικού συστήματος (NOS), αποσκοπεί κυρίως στην παροχή ελέγχου ταυτότητας και εξουσιοδότησης εντός των ορίων του εταιρικού δικτύου, το ADCS, όπως και οι υπόλοιπες τρεις Active Directory υπηρεσίες, έχουν σχεδιαστεί για να παρέχουν αυτές τις υπηρεσίες τόσο σε εσωτερικά όσο και σε εξωτερικά δίκτυα. Ωστόσο, όταν επεκτείνουμε την εξουσία του οργανισμού μας πέρα από τα όρια του δικτύου μας με AD CS, θα πρέπει να βασιζόμαστε σε μια αρχή εμπορικού πιστοποιητικού τρίτου μέρους (CA) για την υποστήριξη των αξιώσεων που δημιουργούνται μέσω των πιστοποιητικών που δημοσιεύουμε., όπως στην εικόνα 6.53.



Εικόνα 6.53

Για παράδειγμα, όταν μεταβαίνουμε σε μια τοποθεσία Web χρησιμοποιώντας το πρωτόκολλο Secure Hypertext Transfer Protocol (HTTPS) που περιέχει ένα πιστοποιητικό SSL, αυτό το πιστοποιητικό αποδεικνύει ότι είμαστε πραγματικά αυτοί που δηλώνουμε ότι είμαστε. Όταν επαληθεύσουμε το πιστοποιητικό, βλέπουμε ότι περιλαμβάνει το όνομα διακομιστή, το όνομα οργανισμού και την αρχή έκδοσης πιστοποιητικών. Το πιστοποιητικό λειτουργεί με το πρόγραμμα περιήγησής σας, επειδή προγράμματα περιήγησης όπως ο Microsoft Internet Explorer ή ο Firefox περιλαμβάνουν ήδη μια λίστα με αξιόπιστες εμπορικές αρχές που διαχειρίζονται τη διαδικασία πιστοποίησης ως επιχείρηση. Η λίστα αξιόπιστων CAs ενημερώνεται αυτόματα μέσω των μηχανισμών ενημέρωσης για το δικό μας επιλεγμένο λειτουργικό σύστημα. Στα Windows Vista και Windows Server 2008, ελέγχεται αυτή η ενημέρωση μέσω μιας ρύθμισης

πολιτικής ομάδας που είναι ενεργοποιημένη από προεπιλογή. Σε παλαιότερα λειτουργικά συστήματα Windows, η ενημέρωση των πιστοποιητικών Trusted Root ήταν ένα στοιχείο των Windows, το οποίο ήταν προσβάσιμο μέσω του Πίνακα Ελέγχου. Όταν εκδίδουμε τα δικά μας πιστοποιητικά — πιστοποιητικά που δεν προέρχονται από εξωτερικές CAs— πρέπει να συμπεριλάβουμε τον δικό μας οργανισμό ως αξιόπιστο CA στους υπολογιστές των ατόμων που θα χρησιμοποιούν αυτά τα πιστοποιητικά. Μπορούμε να το κάνουμε αυτό όταν συνεργαζόμαστε με τους χρήστες του δικού μας οργανισμού επειδή ελέγχουμε τους υπολογιστές τους, αλλά όταν οι χρήστες είναι άνθρωποι με υπολογιστές των οποίων δεν ελέγχουμε, τότε δημιουργούνται προβλήματα. Ζητώντας τους να δεχτούν το δικό μας πιστοποιητικό είναι σαν να τους ζητάμε να μας εμπιστεύονται όταν δεν μας γνωρίζουν. Αυτός είναι ένας λόγος για τον οποίο οι αρχιτεκτονικές PKI κατασκευάζονται όπως είναι. Ουσιαστικά, κάθε μέλος του public key infrastructure συνδέεται σε μια ιεραρχία που καταλήγει στην κορυφή του CA. Αυτή η CA είναι τελικά υπεύθυνη για καθένα από τα πιστοποιητικά που περιλαμβάνονται στην αλυσίδα. Για παράδειγμα, εάν λάβουμε ένα πιστοποιητικό από τον οργανισμό μας και ο οργανισμός μας έλαβε το κύριο πιστοποιητικό του από έναν αξιόπιστο εμπορικό CA, το πιστοποιητικό μας θα είναι αυτόματα αξιόπιστο, επειδή κάθε πρόγραμμα περιήγησης εμπιστεύεται ήδη την εμπορική CA. Όπως μπορούμε να φανταστούμε, αυτό το εξωτερικό CA πρέπει να χρησιμοποιεί ένα αυστηρό πρόγραμμα επικύρωσης.

Πολλές τεχνολογίες βασίζονται στη λειτουργία πιστοποιητικών PKI. Ένα πολύ καλό παράδειγμα είναι ο Microsoft Exchange Server 2007. Επειδή ο Exchange Server χωρίζεται σε διάφορους ρόλους — Hub Transport, Πρόσβαση πελάτη, Mailbox και άλλα - και επειδή μεταφέρει ιδιωτικές πληροφορίες μέσω TCP/IP συνδέσεων, κάθε διακομιστής δημιουργεί αυτόματα ένα αυτό-υπογεγραμμένο πιστοποιητικό κατά την εγκατάσταση. Τότε, μέσω της χρήσης αυτών των πιστοποιητικών, το ηλεκτρονικό ταχυδρομείο μεταφέρεται μέσω ασφαλών συνδέσεων. Αυτό λειτουργεί καλά για εσωτερικές επικοινωνίες, αλλά μόλις ανοίξετε τις πόρτες για επικοινωνία με τον έξω κόσμο, για παράδειγμα, η παροχή Microsoft Outlook Web Access (OWA) σε υπαλλήλους εκτός του εσωτερικού μας δικτύου, πρέπει να αντικατασταθεί το αυτό-υπογεγραμμένο πιστοποιητικό με ένα που έχουμε αγοράσει από έναν έγκυρο προμηθευτή. Διαφορετικά, κανένας από τους χρήστες σας δεν θα μπορεί να έχει πρόσβαση στο OWA από εξωτερικές τοποθεσίες Διαδικτύου. Σε ορισμένες περιπτώσεις, η εφαρμογή PKI εσωτερικού έχει νόημα μόνο επειδή αποδεικνύει ποιος είμαι μόνο για τον εαυτό μας, αλλά γίνεται πιο δύσκολο και ακόμη περιττό όταν ασχολούμαστε με το διαδίκτυο.

Οι υπηρεσίες πιστοποιητικών Active Directory παρέχουν μια ποικιλία υπηρεσιών σχετικά με υποδομές δημόσιου κλειδιού και τη χρήση πιστοποιητικών γενικά. Χρησιμοποιώντας τον Windows Server 2008 και το ADCS, μπορούμε να υποστηρίξουμε τα ακόλουθα σενάρια χρήσης πιστοποιητικών:

- Μπορούμε να κρυπτογραφήσουμε όλα τα αρχεία δεδομένων. Ένα από τα πιο κοινά προβλήματα στην πληροφορική σήμερα είναι η απώλεια ή κλοπή συστημάτων κινητών υπολογιστών. Εάν τα δεδομένα είναι κρυπτογραφημένα, η απώλεια είναι μικρή, αλλά εάν τα δεδομένα είναι χωρίς προστασία, θα μπορούσε να επηρεάσει την ικανότητά μας να δημιουργούμε επιχειρήσεις. Με τα Windows Server 2008 και Windows Vista, μπορούμε να κρυπτογραφήσετε όλα τα αρχεία δεδομένων χρήστη αυτόματα μέσω του Group Policy objects και να επιβάλλουν ισχυρούς κωδικούς πρόσβασης που απαιτούνται για την περαιτέρω προστασία τους. Το σύστημα κρυπτογράφησης αρχείων (EFS) βασίζεται σε πιστοποιητικά για το κλείδωμα και το ξεκλείδωμα κρυπτογραφημένων αρχείων.

- Μπορούμε να κρυπτογραφήσουμε όλες τις απομακρυσμένες επικοινωνίες. Ο Windows Server 2008 περιλαμβάνει και το IPSec και Secure Sockets Tunneling Protocol (SSTP) εικονικές ιδιωτικές συνδέσεις δικτύου. Και οι δύο βασίζονται σε πιστοποιητικά για τον έλεγχο ταυτότητας της αρχής και του τελικού σημείου της επικοινωνίας.
- Μπορούμε να ασφαλίσουμε όλα τα μηνύματα e-mail. Ο Windows Server 2008 περιλαμβάνει υποστήριξη για Secure Επεκτάσεις αλληλογραφίας πολλαπλών χρήσεων (S/MIME), το τυπικό πρωτόκολλο ασφαλείας ηλεκτρονικού ταχυδρομείου. Τα υπογεγραμμένα μηνύματα προστατεύονται από παραβίαση και αποδεικνύουν ότι προέρχονται από το σωστό πρόσωπο.
- Μπορούμε να ασφαλίσουμε όλες τις συνδέσεις. Χρησιμοποιώντας έξυπνες κάρτες μπορούμε να χρησιμοποιήσουμε πιστοποιητικά για την υποστήριξη της σύνδεσης και διασφαλίσουμε ότι όλοι οι χρήστες, ειδικά οι διαχειριστές, είναι αυτοί που λένε ότι είναι.
- Μπορούμε να ασφαλίσουμε όλες τις τοποθεσίες Web. Με τη χρήση των Windows Server 2008 και Internet Information Υπηρεσίες (IIS) 7.0, μπορούμε να ασφαλίσουμε όλες τις επικοινωνίες στους ιστότοπούς μας, διασφαλίζοντας την ασφάλεια όλων των συναλλαγών των πελατών μας.
- Μπορούμε να ασφαλίσουμε τους διακομιστές μας για να διασφαλίσουμε την αυθεντικότητά τους. Για παράδειγμα, όταν εκχωρούμε πιστοποιητικά σε διακομιστές σε μία υποδομή προστασίας πρόσβασης δικτύου (NAP) ή σε οποιαδήποτε άλλη ασφαλή εξυπηρέτηση, οι υπολογιστές στο δίκτυό μας θα γνωρίζουν ότι εργάζονται με τους δικούς μας διακομιστές και όχι με άλλους διακομιστές που προσπαθούν να πλαστοπροσωπήσουν τους δικούς μας.
- Μπορούμε να ασφαλίσουμε όλες τις ασύρματες επικοινωνίες. Με τη χρήση των Windows Server 2008 και Windows Vista, μπορούμε να διασφαλίσουμε ότι όλες οι ασύρματες επικοινωνίες προέρχονται από αξιόπιστα τελικά σημεία.
- Μπορούμε να προστατεύσουμε όλα τα δεδομένα από παραβίαση. Με τη χρήση του Active Directory Rights Management Services (ADRMS), μπορούμε να βασιστούμε στον Windows Server 2008 για προστασία από παραβίαση ή κακή χρήση όλων των πληροφοριών που δημιουργούνται.

Επιπλέον, θα πρέπει να εξετάσουμε το ενδεχόμενο να εκδώσουμε ένα πιστοποιητικό σε όλους τους υπαλλήλους μας για να τους βοηθήσουμε να πιστοποιήσουν ποιοι είναι σε όλες τις συναλλαγές τους στο Διαδίκτυο. Επίσης θα πρέπει να λάβουμε υπόψη μας ότι όλα τα εξωτερικά πιστοποιητικά πρέπει να περιλαμβάνουν μια αξιόπιστη CA για να τους επιτρέψει να λειτουργούν αυτόματα με οποιοδήποτε πρόγραμμα περιήγησης.

Κατανόηση του Active Directory Certificate Services

Το Active Directory Certificate Services είναι ο μηχανισμός στον οποίο βασίζεται ο Windows Server 2008 για τη διαχείριση δημόσιων πιστοποιητικών κλειδιού. Χρησιμοποιώντας το ADCS, μπορούμε να δημιουργήσουμε μια ολοκληρωμένη ιεραρχία PKI που μπορεί να χρησιμοποιηθούν για την έκδοση και διαχείριση πιστοποιητικών εντός του οργανισμού μας. Το AD CS αποτελείται από πολλά συστατικά:

- **Certificate authorities:** CAs είναι οι διακομιστές που χρησιμοποιούνται για την έκδοση και τη διαχείριση πιστοποιητικών. Λόγω της ιεραρχικής φύσης ενός PKI, το ADCS υποστηρίζει τόσο τη ρίζα όσο και την υποδεέστερη ή θυγατρικές CAs. Το root CA συνήθως εκδίδει πιστοποιητικά για δευτερεύουσες CAs, κάτι που επιτρέπει με τη σειρά τους την έκδοση πιστοποιητικών σε χρήστες, υπολογιστές και υπηρεσίες. Η δευτερεύουσα CA μπορεί να εκδώσει πιστοποιητικά μόνο όταν το δικό του πιστοποιητικό είναι έγκυρο. Όταν λήξει αυτό το πιστοποιητικό, η δευτερεύουσα CA πρέπει να ζητήσει ανανέωση πιστοποιητικού από τη ρίζα της CA. Γι 'αυτό το λόγο, οι ρίζες CA έχουν συχνά διάρκεια πιστοποιητικού που είναι πολύ μεγαλύτερη από οποιαδήποτε από τους υφισταμένους τους. Με τη σειρά τους, οι δευτερεύουσες CAs έχουν συνήθως διάρκεια πιστοποιητικού μεγαλύτερη από αυτά που εκδίδουν σε χρήστες, υπολογιστές ή υπηρεσίες.
- **CA Web Enrollment:** Χρησιμοποιώντας Web Enrollment, οι χρήστες μπορούν να συνδεθούν με την CA μέσω ενός προγράμματος περιήγησης στο Web για να ζητήσουν πιστοποιητικά, να πραγματοποιήσουν εγγραφές έξυπνων καρτών ή να λάβουν Certificate Revocation Lists (CRL). Τα CRL παρέχουν στους χρήστες της υποδομής δημόσιου κλειδιού μία λίστα πιστοποιητικών που έχουν ακυρωθεί ή ανακληθεί από τον οργανισμό μας. Τα συστήματα βασίζονται στους διακομιστές CA PKI poll για να λαμβάνουν CRL κάθε φορά που τους παρουσιάζεται ένα πιστοποιητικό τους. Εάν το πιστοποιητικό που τους παρουσιάζεται περιλαμβάνεται σε αυτήν τη λίστα, απορρίπτεται αυτόματα.
- **Online responder:** Αυτή η υπηρεσία έχει σχεδιαστεί για να ανταποκρίνεται σε συγκεκριμένα αιτήματα επικύρωσης πιστοποιητικών μέσω του διαδικτυακού πρωτοκόλλου κατάστασης πιστοποιητικού (OCSP). Με τη χρήση διαδικτυακού ανταποκριτή (OR), το σύστημα που βασίζεται στο PKI δεν χρειάζεται να αποκτήσει ένα πλήρες CRL και μπορεί υποβάλει αίτημα επικύρωσης για ένα συγκεκριμένο πιστοποιητικό. Ο διαδικτυακός ανταποκριτής αποκωδικοποιεί το αίτημα επικύρωσης και καθορίζει εάν το πιστοποιητικό είναι έγκυρο. Όταν καθορίζει την κατάσταση του ζητούμενου πιστοποιητικού, στέλνει πίσω μια κρυπτογραφημένη απάντηση που περιέχει τις πληροφορίες στον αιτούντα. Η χρήση διαδικτυακών ανταποκριτών είναι πολύ πιο γρήγορη και πιο αποτελεσματική παρά τη χρήση CRL. Το AD CS περιλαμβάνει διαδικτυακούς ανταποκριτές ως νέα δυνατότητα στα Windows Server 2008.
- **Network Device Enrollment Service:** Συσκευές που χρησιμοποιούν λειτουργικά συστήματα χαμηλού επιπέδου, όπως οι δρομολογητές και τα switches, μπορούν επίσης να συμμετέχουν σε ένα PKI μέσω του Network Device Enrollment Service (NDES) χρησιμοποιώντας το πρωτόκολλο εγγραφής απλού πιστοποιητικού (SCEP), ένα πρωτόκολλο που αναπτύχθηκε από την Cisco Systems, Inc. Αυτές οι συσκευές συνήθως δεν συμμετέχουν σε έναν κατάλογο ADDS και, επομένως, δεν έχουν λογαριασμούς ADDS. Ωστόσο, μέσω του NDES και το SCEP, μπορούν

επίσης να γίνουν μέρος της ιεραρχίας PKI που διατηρείται και διαχειρίζεται από την εγκατάσταση ADCS.

Αυτά τα τέσσερα στοιχεία αποτελούν τον πυρήνα της υπηρεσίας ADCS στον Windows Server 2008.

Δημιουργία ιεραρχίας CA

Ένα ζήτημα κατά τον σχεδιασμό της ιεραρχίας CA είναι η ασφάλεια. Επειδή μια ιεραρχία CA βασίζεται στην αλυσίδα πιστοποιητικών, εναποθέτει κινδύνους οποιαδήποτε έκθεση ενός ανώτατου επιπέδου ή ρίζας CA που διακυβεύεται αυτόματα όλα τα πιστοποιητικά που βασίζονται σε αυτό. Αυτός είναι ένας λόγος για τον οποίο θα πρέπει να ασφαλιστούν οι ρίζες CA όσο το δυνατόν περισσότερο. Στην πραγματικότητα, μια κοινή πρακτική είναι η δημιουργία μιας κλιμακωτής ιεραρχίας CA και η εκτός σύνδεση κορυφαίων μελών μιας κλιμακωτής αρχιτεκτονικής. Η λογική είναι ότι εάν ένας διακομιστής είναι εκτός σύνδεσης, είναι εξίσου ασφαλής όπως μπορεί να είναι. Ωστόσο, ο καθορισμός του αριθμού των επιπέδων στην αρχιτεκτονική ADCS εξαρτάται από πολλούς άλλους παράγοντες. Θα πρέπει να λάβουμε υπόψη το μέγεθος και τη γεωγραφική κατανομή του δικτύου μας. Πρέπει επίσης να προσδιορίσουμε τη σχέση εμπιστοσύνης που θα χρειαστεί να υπάρχει μεταξύ των CA και τους κατόχους του πιστοποιητικού. Κάθε φορά που παρουσιάζεται ένα πιστοποιητικό, θα πρέπει να επικυρώνεται είτε μέσω CRL είτε μέσω διαδικτυακού ανταποκριτή, οπότε για να χρησιμοποιηθούν τα πιστοποιητικά, πρέπει να υπάρχει κάποιου είδους συνδεσιμότητα.

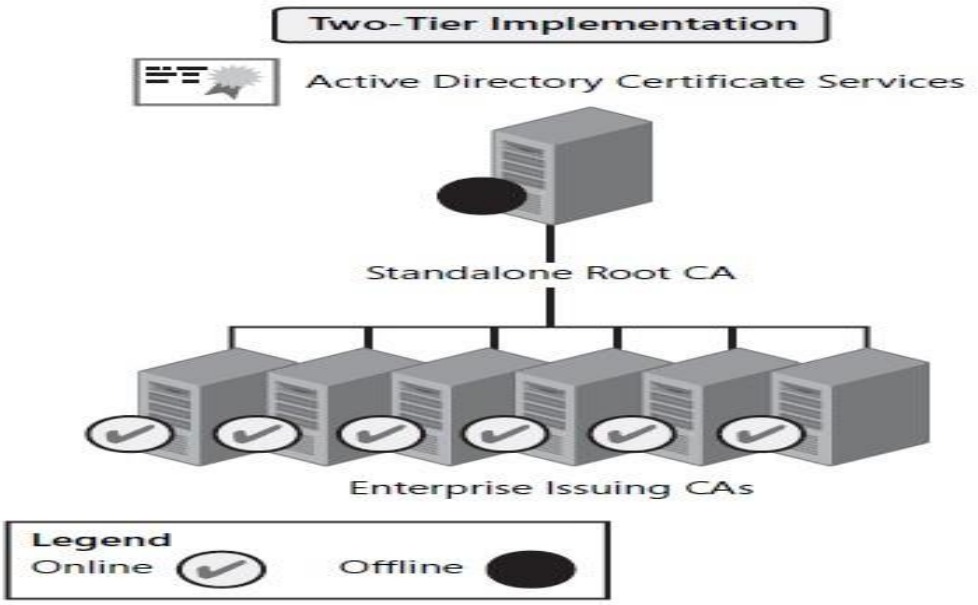
Θα πρέπει να εξετάσουμε τα πιθανά σενάρια που σκοπεύουμε να υποστηρίξουμε με την ανάπτυξη ADCS. Θα πρέπει να απαντηθούν ερωτήματα όπως:

- Θα υπάρχει αλληλεπίδραση με άτομα ή συνεργάτες εκτός του δικτύου
- Θα χρησιμοποιηθούν έξυπνες κάρτες
- Θα χρησιμοποιηθούν ασύρματα δίκτυα
- Θα χρησιμοποιήσουμε το IPSec ή το νέο SSTP.

Όποτε χρειαστεί να πιστοποιήσουμε την ταυτότητα μιας συσκευής, μιας εφαρμογής ή ενός χρήστη, θα πρέπει να το κάνουμε βασιζόμενοι στο ADCS και, ενδεχομένως, στις αρχές εμπορικών πιστοποιητικών τρίτων. Όταν θα έχουμε όλες τις απαντήσεις σε αυτές τις ερωτήσεις, μπορούμε να προχωρήσουμε στον σχεδιασμό της ADCS.

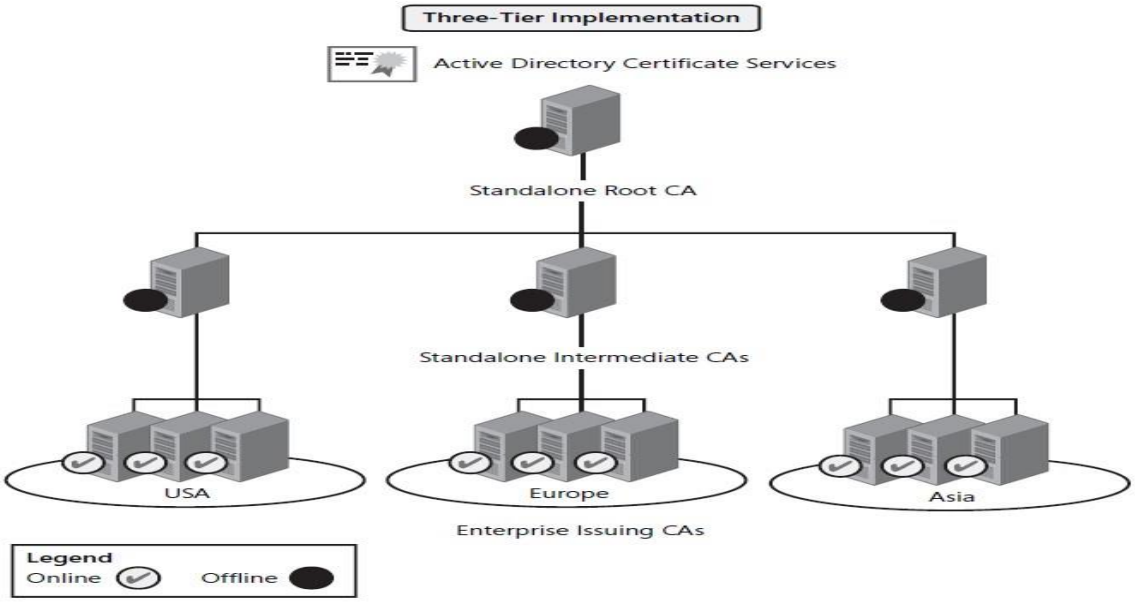
Για τον σχεδιασμό του ADCS θα πρέπει να λάβουμε υπόψη τα εξής:

- ✓ Η δημιουργία μιας κλιμακωτής ιεραρχίας με μία μόνο ρίζα CA συνίσταται σε πολύ σπάνιες περιπτώσεις, σε περιπτώσεις που πιστεύουμε ότι η ρίζα CA δεν μπορεί να τεθεί σε κίνδυνο σε καμία περίπτωση.
- ✓ Δημιουργία ιεραρχίας δύο επιπέδων με ρίζα CA και έκδοση CA όταν πρέπει να προστατέψουμε το root CA, και αυτό γιατί το μέγεθος του οργανισμού μας και ο σκοπός της ιεραρχίας δεν δικαιολογούν μια πιο περίπλοκη ιεραρχία. Σε αυτό το μοντέλο, μπορούμε να απομακρύνουμε τη ρίζα CA εκτός σύνδεσης για προστασία, όπως φαίνεται στην εικόνα 6.54.



Εικόνα 6.54

- ✓ Δημιουργία τριών επιπέδων ιεραρχίας με ρίζα CA, ενδιάμεσες CA και έκδοση CA όταν χρειαζόμαστε υψηλότερα επίπεδα ασφάλειας και υψηλή διαθεσιμότητα για τις εκδόσεις CA και το μοντέλο διαχείρισης, ο πληθυσμός χρηστών και το γεωγραφικό εύρος δικαιολογούν το επιπλέον κόστος της πρόσθετης βαθμίδας. Πολλές ενδιάμεσες CA χρησιμοποιούνται συχνά για την υποστήριξη διαφορετικών πολιτικών σε διαφορετικά περιβάλλοντα σε αυτό το μοντέλο. Εάν θα χρησιμοποιήσουμε αυτό το μοντέλο θα πρέπει να βάλουμε τις δύο ρίζες και τις ενδιάμεσες CA εκτός σύνδεσης για την προστασία τους, όπως φαίνεται εικόνα 6.55.



Εικόνα 6.55

- ✓ Δημιουργία περισσότερων από τριών επιπέδων πραγματοποιείται μόνο σε πολύ περίπλοκα περιβάλλοντα που απαιτούν μέγιστη ασφάλεια όπου η υποδομή CA πρέπει να προστατεύεται ανά πάσα στιγμή.

Όπως μπορούμε να κατανοήσουμε, όσο περισσότερα επίπεδα δημιουργούμε σε μια ιεραρχία, τόσο υψηλότερο είναι το επίπεδο πολυπλοκότητας και οι όροι διαχείρισης και διοίκησης. Ωστόσο, όσο πιο περίπλοκη είναι η ιεραρχία μας, τόσο πιο ασφαλής μπορεί να είναι. Επίσης, θα πρέπει να σκεφτούμε ποιος τύπος CA είναι κατάλληλος για να αναπτυχθεί σε κάθε επίπεδο.

Βέλτιστες πρακτικές για αναπτύξεις ADCS

Οι αρχιτεκτονικές που χρησιμοποιούν δύο ή περισσότερες βαθμίδες αντιπροσωπεύουν τις πιο κοινές εφαρμογές του ADCS. Όταν σχεδιάζουμε την υποδομή ADCS, θα πρέπει να λάβουμε υπόψη τα ακόλουθα:

- Αποφυγή των μονόπλευρων ιεραρχιών όσο το δυνατόν περισσότερο, επειδή είναι πολύ δύσκολο να προστατευθούν.
- Οι ρίζες και οι ενδιάμεσες CA (εάν εφαρμοστούν) πρέπει να αποσυρθούν το συντομότερο δυνατό μετά τη θέση της υποδομής. Για το λόγο αυτό, αυτές οι CA είναι εξαιρετικοί υποψήφιοι για εικονικοποίηση μέσω των Windows Server 2008 Hyper-V. Δημιουργούμε μια εικονική μηχανή (VM), εγκαθιστούμε τον ρόλο ADCS Standalone CA και, στη συνέχεια, αποθηκεύουμε την κατάσταση του μηχανήματος το συντομότερο δυνατό.
- Εξετάζουμε το ενδεχόμενο να καταργήσουμε τα αρχεία VM για τη ρίζα CA από τον κεντρικό διακομιστή μόλις ληφθεί εκτός σύνδεσης. Αποθηκεύουμε το ασφαλές VM σε θησαυροφυλάκιο κάποιου τύπου.
- Εάν χρησιμοποιούμε εικονικοποίηση για την υποστήριξη της ανάπτυξης ADCS, ασφαλίζουμε τα VMs όσο περισσότερο μπορούμε. Είναι πολύ πιο εύκολο να απομακρυνθούμε με ένα VM από ό, τι με έναν φυσικό διακομιστή.
- Εξετάζουμε το ενδεχόμενο δημιουργίας VM που δεν διαθέτουν ή έχουν απενεργοποιήσει τις συνδέσεις δικτύου για τις ρίζες και τις ενδιάμεσες CA. Αυτό εξασφαλίζει ακόμη υψηλότερο επίπεδο προστασίας. Τα πιστοποιητικά μεταφέρονται από αυτούς τους διακομιστές μέσω συσκευών USB ή δισκέτας.
- Ελέγχουμε τις αφαιρούμενες συσκευές σε ριζικές και ενδιάμεσες CA μέσω προστασίας συσκευών από τις ρυθμίσεις στην κονσόλα τοπικής πολιτικής ασφαλείας. Αυτό προσθέτει ένα επιπλέον επίπεδο προστασίας.
- Θα πρέπει να βεβαιωθούμε ότι οι διαχειριστές CA είναι ιδιαίτερα αξιόπιστα άτομα. Ελέγχουν ολόκληρη την ιεραρχία της CA και, εξαιτίας αυτού, βρίσκονται σε πολύ υψηλή θέση εμπιστοσύνης.
- Ασφαλίζουμε καλά το κέντρο δεδομένων που φιλοξενεί τις CA. Ελέγχουμε την πρόσβαση στο κέντρο δεδομένων και χρησιμοποιούμε όσο το δυνατόν περισσότερο τις διαχειριστικές συνδέσεις έξυπνων καρτών.
- Εξετάζουμε το ενδεχόμενο να χρησιμοποιήσουμε μόνο ένα root CA αλλά προσθέτοντας διαθεσιμότητα μέσω πολλαπλών εγκαταστάσεων CA μόλις φτάσουμε στα ενδιάμεσα και στα επίπεδα έκδοσης της ιεραρχίας.
- Δεν μπορούμε να αλλάξουμε το όνομα ενός διακομιστή μετά την εγκατάσταση της υπηρεσίας ADCS, οπότε θα πρέπει να σχεδιάσουμε τα δικά μας ονόματα των

διακομιστών προσεκτικά και να βεβαιωθούμε ότι μπορούμε να τα διατηρήσουμε για πολύ καιρό.
- Δεν μπορούμε να αλλάξουμε μια CA από Standalone σε Enterprise ή το αντίστροφο εφόσον έχει ήδη εγκατασταθεί η υπηρεσία ADCS.
- Ως γενική πρακτική, καλύτερα να μην εγκαθιστούμε την υπηρεσία ADCS σε DC. Αν και μπορεί να πραγματοποιηθεί, είναι φρονιμότερο να διατηρήσουμε ανεξάρτητο το ρόλο του διακομιστή ADDS από όλους τους άλλους ρόλους εκτός από το Domain Name System (DNS).

Πρόσθετες απαιτήσεις προγραμματισμού

Όπως προαναφέρθηκε, ο σχεδιασμός και η ανάπτυξη μιας ιεραρχίας CA δεν είναι μόνο μια τεχνική δραστηριότητα. Πρέπει να έχουμε τις κατάλληλες διοικητικές διαδικασίες για να υποστηρίξουμε τη χρήση πιστοποιητικών στο δίκτυό μας. Χρειάζονται τρεις επιπλέον σκέψεις να καλυφθούν πριν προχωρήσουμε στην εγκατάσταση του ADCS:

- Θα πρέπει να σκεφτούμε πώς θα υποστηρίξουμε την εγγραφή πιστοποιητικών.
- Θα πρέπει να σκεφτούμε πώς θα γίνεται η ανανέωση των πιστοποιητικών.
- Θα πρέπει να δημιουργήσουμε μια δήλωση πρακτικής πιστοποιητικού (Certificate Practice Statement).

Το πρώτο επικεντρώνεται στον τρόπο με τον οποίο σκοπεύουμε να υποστηρίξουμε τις αιτήσεις πιστοποιητικών και τη διανομή τους. Ένα πιστοποιητικό χρησιμοποιείται για να προσδιορίσει διεξοδικά τον κάτοχό του εάν είναι χρήστης, μια μηχανή ή μια εφαρμογή. Επομένως, θα πρέπει να δημιουργήσουμε μια διαδικασία αναγνώρισης αιτούντος προς επικύρωση. Δεν θέλουμε να εκδώσουμε ένα πιστοποιητικό στον John Kane όταν δεν είμαστε σίγουροι ότι ο αιτών είναι στην πραγματικότητα ο John Kane. Οι αρχές έκδοσης πιστοποιητικών τρίτων χρησιμοποιούν διάφορους τύπους διαδικασιών για αυτήν την επικύρωση, η πιο αυστηρή από την οποία θα περιλαμβάνει επίσκεψη στο άτομο που ζητά το πιστοποιητικό από εξουσιοδοτημένο νόμιμο εκπρόσωπο της CA. Αυτό σημαίνει συνάντηση κατά πρόσωπο και μετά την επικύρωση του αιτούντος, μπορούμε να του εκχωρήσουμε το πιστοποιητικό σε αυτό το όνομα. Για να προστατεύσουμε περαιτέρω το πιστοποιητικό, μπορούμε να το αποθηκεύσουμε σε ένα διακριτικό υλικό όπως μία έξυπνη κάρτα και να το παράσχουμε στον αιτούντα. Από εκεί και έπειτα είναι ευθύνη του αιτούντα η προστασία του πιστοποιητικού και του διακριτικού που περιέχει. Ωστόσο, εάν σκοπεύουμε να χρησιμοποιήσουμε την αυτόματη εγγραφή μέσω εταιρικών CA, πρέπει να βεβαιωθούμε ότι οι χρήστες έχουν επικυρωθεί σωστά προτού τους δοθεί πρόσβαση στο δίκτυό μας. Βασιζόμαστε σε κάποια μορφή επίσημης ταυτότητας, όπως διαβατήριο ή άλλος κυβερνητικός μηχανισμός ταυτότητας. Αυτό πρέπει ήδη να αποτελεί μέρος των διαδικασιών και των πολιτικών του ανθρώπινου δυναμικού μας.

Το δεύτερο σκέλος αφορά τη διάρκεια ζωής του πιστοποιητικού. Τα πιστοποιητικά συνήθως περιλαμβάνουν δύο ζεύγη κλειδιών: ένα ιδιωτικό κλειδί και ένα δημόσιο κλειδί. Όταν κρυπτογραφούμε τα δεδομένα, χρησιμοποιούμε το ιδιωτικό κλειδί για να το κάνουμε. Όταν άλλοι αποκρυπτογραφούν τα δεδομένα, συνήθως χρησιμοποιούν το δημόσιο κλειδί μας για να το κάνουν. Όσο περισσότερο χρησιμοποιούμε ένα ζεύγος κλειδιών πιστοποιητικού, τόσο πιο επιρρεπές είναι να δεχθεί επίθεση ή να εκτεθεί . Όταν ανανεώνουμε ένα πιστοποιητικό, η ανανέωση δημιουργεί ένα νέο ζεύγος κλειδιών για το πιστοποιητικό. Επομένως, πρέπει να σχεδιάσουμε τη διάρκεια ζωής του πιστοποιητικού

και τις ανανεώσεις του προσεκτικά. Στην πραγματικότητα, πρέπει να μετριάσουμε τη βασική ζωή των κλειδιών υπό τον κίνδυνο να μην εκτεθούν. Επιπλέον, πρέπει να διασφαλίσουμε ότι η κλιμακωτή ιεραρχία μας περιλαμβάνει επίσης κλιμακωτές ζωές. Μία ρίζα CA θα πρέπει να έχει τη μεγαλύτερη διάρκεια ζωής και μετά οι ενδιάμεσες CA εάν τις χρησιμοποιούμε, μετά οι CA που εκδίδουν και στη συνέχεια αυτές που δίνουν πιστοποιητικά. Για παράδειγμα, μπορούμε να χρησιμοποιήσετε ένα κενό 10 ετών για κάθε επίπεδο στην αρχιτεκτονική μας, δηλαδή εκχώρηση 10 χρόνων σε κάθε επίπεδο. Σε μια αρχιτεκτονική τριών επιπέδων, χρησιμοποιούμε 30 χρόνια για τη ρίζα CA, 20 χρόνια για τις ενδιάμεσες CA και 10 χρόνια για τις CA που τα εκδίδουν. Τότε μπορούμε να ορίσουμε ένα ή δύο χρόνια στα πιστοποιητικά που εκδίδουμε. Ο λόγος για αυτήν την ιεραρχία διάρκειας είναι ότι από τη στιγμή που ένα πιστοποιητικό λήγει για έναν διακομιστή, όλα τα δευτερεύοντα πιστοποιητικά λήγουν επίσης. Έτσι προστατευόμαστε ενάντια σε αυτό το ενδεχόμενο και δίνουμε πολύ μεγάλη διάρκεια στους διακομιστές. Στο τρίτο σκέλος θα πρέπει να σχεδιάσουμε και να προετοιμάσουμε τη δήλωση πρακτικής πιστοποιητικού. Τα CPS βασίζονται στις πολιτικές πιστοποιητικών που δημιουργούμε. Οι πολιτικές αυτές καθορίζουν τις ευθύνες του οργανισμού έκδοσης για κάθε τύπο πιστοποιητικού που εκδίδει. Ο οργανισμός έκδοσης είναι τελικά υπεύθυνος για οποιοδήποτε αδίκημα ή κατάχρηση των πιστοποιητικών που εξέδωσε. Εξαιτίας αυτού, θα πρέπει να εμπλακεί το νομικό τμήμα, το τμήμα ανθρωπίνου δυναμικού και τα τμήματα ασφαλείας του οργανισμού μας για να βοηθήσουν στον καθορισμό των πολιτικών που χρησιμοποιούνται για κάθε τύπο πιστοποιητικού και στη συνέχεια δημιουργείται το CPS. Το CPS πρέπει να συμπεριλαμβάνει πολλά στοιχεία, όπως έναν σαφή ορισμό του ποιοι είμαστε, μια λίστα με τις πολιτικές πιστοποιητικών μας, μια γενική δήλωση των διαδικασιών που χρησιμοποιούμε για την έκδοση, εκχώρηση και ανάκληση πιστοποιητικών. Με αυτόν τον τρόπο προστατεύουμε το CA. Ένα άλλο σημαντικό στοιχείο που πρέπει να συμπεριληφθεί στο CPS είναι η πολιτική ανάκλησης που χρησιμοποιούμε. Η ανάκληση συμβαίνει όταν πρέπει να γίνει ακύρωση ενός πιστοποιητικού για οποιονδήποτε λόγο. Συνήθως όταν κάποιος δεν συμμορφώνεται με την πολιτική που ορίσαμε για τον συγκεκριμένο τύπο πιστοποιητικού. Θα πρέπει να έχουμε στο νου μας ότι η ανάκληση είναι η μόνη μέθοδος που έχουμε για την ακύρωση ενός πιστοποιητικού όταν χρησιμοποιείται κατά λάθος. Το CPS θα πρέπει να είναι διαθέσιμο στο κοινό, τόσο στους εσωτερικούς όσο και στους εξωτερικούς χρήστες CA. Αυτό συνήθως σημαίνει τη διάθεσή του σε κάποια μορφή στο Διαδίκτυο ή μέσω intranets. Στον Πίνακα 6.4 φαίνονται οι δυνατότητες ADCS ανά έκδοση των Windows Server 2008.

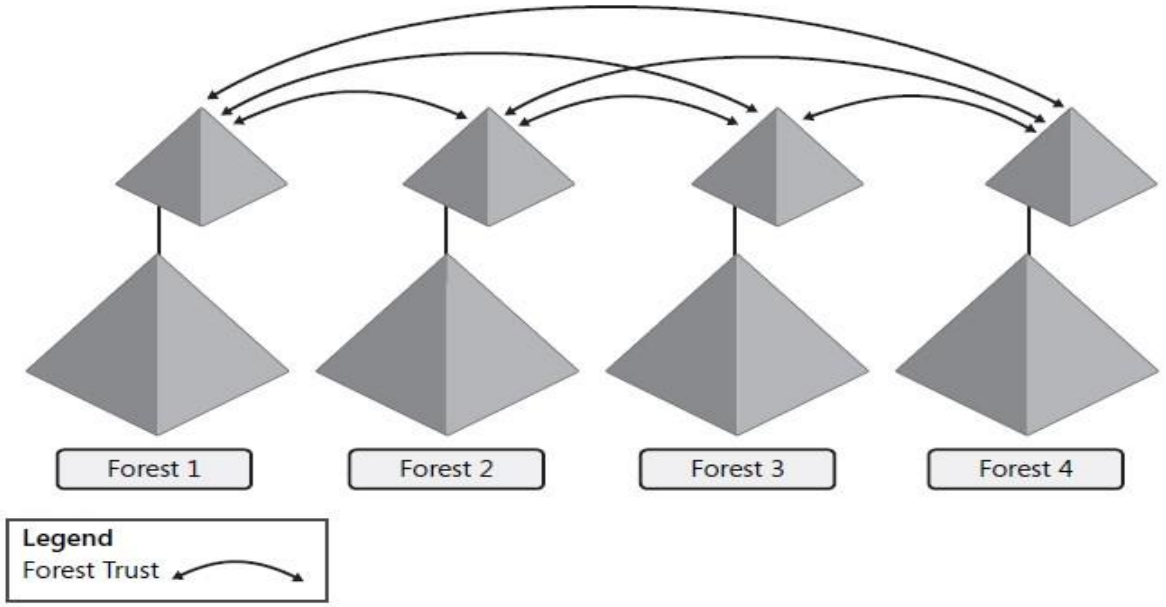
Υποστηριζόμενα στοιχεία και Χαρακτηριστικά	Web	Standard	Enterprise	Datacenter
Standalone certificate authority		√	√	√
Enterprise certificate authority			√	√
Network Device Enrollment Service (NDES)			√	√
Online responder service			√	√
Βασικό αρχείο			√	√
Διαχωρισμός ρόλου			√	√
Certificate Manager restrictions			√	√
Delegated enrollment agent restrictions			√	√

Πίνακας 6.4

6.3.6. Active Directory Federation Services (ADFS)

Οι οργανισμοί αγωνίζονται για την εξασφάλιση των δικτύων τους από τον έξω κόσμο από τότε που εφευρέθηκε το Διαδίκτυο. Η βασική αρχή είναι ότι κάθε οργανισμός που έχει μια διεπαφή μεταξύ του δικτύου και του Διαδικτύου έχει επίσης ένα περιμετρικό δίκτυο κάποιου είδους. Σε πολλές περιπτώσεις, οι οργανισμοί καταβάλλουν μεγάλη προσπάθεια εφαρμόζοντας ειδικές τεχνολογίες ασφαλείας, όπως συστήματα ανίχνευσης εισβολής, με τη βασική προϋπόθεση ενός περιμετρικού δικτύου είναι η διατήρηση του τείχους προστασίας που περιέχει όσο το δυνατόν πιο ασφαλή. Αυτό όμως μπορεί να επηρεάσει τις πιθανές συνεργασίας. Στις πρώτες μέρες των τομέων Microsoft Windows με Microsoft Windows NT, η Microsoft παρείχε τη δυνατότητα δημιουργίας εμπιστοσύνης μεταξύ τομέων για την υποστήριξη αλληλεπιδράσεων τομέα. Με την κυκλοφορία των ADDS στα Windows 2000, η Microsoft παρουσίασε την έννοια της εμπιστοσύνης και τα υποστηριζόμενα εμπιστευτικά πεδία μεταξύ τομέων. Τομείς μέσα στο ίδιο δάσος χρησιμοποιούσαν αυτόματες μεταβατικές καταπιστεύσεις και τομείς από διαφορετικά δάση χρησιμοποιούσαν σαφή εμπιστοσύνη όταν ήθελαν να μοιραστούν περιβάλλοντα ασφαλείας. Με την κυκλοφορία των Microsoft Windows Server 2003, η Microsoft επέκτεινε την έννοια της μεταβατικής εμπιστοσύνης σε δάση με την εισαγωγή δασικών εμπιστευμάτων. Χρησιμοποιώντας μια δασική εμπιστοσύνη, οι συνεργάτες μπορούν να επεκτείνουν το πλαίσια ασφαλείας του εσωτερικού τους δάσους για να εμπιστεύονται άλλα δάση εταίρους. Ωστόσο, η εφαρμογή της εμπιστοσύνης των δασών είχαν δύο σημαντικές επιπτώσεις:

- Πρώτον, απαιτεί το άνοιγμα συγκεκριμένων πορτών στο τείχος προστασίας για την υποστήριξη του τομέα ADDS.
- Δεύτερον, εάν οι συνεργασίες μεγαλώσουν πολύ, μπορεί να γίνουν εξαιρετικά δυσκίνητες στη διαχείριση πολλαπλών καταπιστεύσεων. Όπως φαίνεται στην εικόνα 6.56. Η χρήση εμπιστοσύνης μπορεί να μην είναι ο καλύτερος τρόπος για την εφαρμογή συνεργασιών.



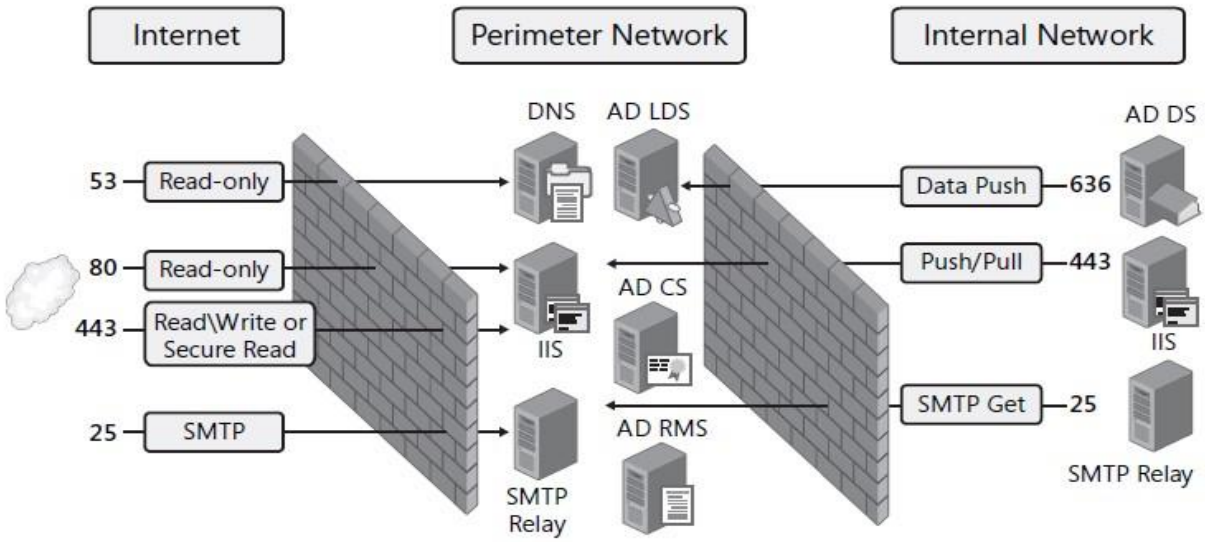
Εικόνα 6.56

Αν και η εμπιστοσύνη των δασών μπορεί να γίνει πολύ περίπλοκη, έχουν επίσης αντίκτυπο στους μηχανισμούς προστασίας. Για παράδειγμα, η κυκλοφορία ADDS θα διέρχεται μέσω του LDAP στη πόρτα TCP/IP 389 ή, κατά προτίμηση, μέσω ασφαλούς LDAP (LDAP/S) στην πόρτα 636. Επιπλέον, εάν πρέπει να μεταφορά της κυκλοφορίας του καθολικού καταλόγου (GC), θα πρέπει να χρησιμοποιήσουμε τη πόρτα 3268 ή κατά προτίμηση την πόρτα 3269 στο LDAP/S. Ωστόσο, τα τείχη προστασίας έχουν σχεδιαστεί για να αποτρέπουν την ανεπιθύμητη κίνηση. Ανοίγοντας όμως ατελείωτους αριθμούς TCP/IP πορτών δεν είναι λύση.

Τα παραδοσιακά περιμετρικά δίκτυα έχουν δύο στρώματα προστασίας. Το πρώτο προστατεύει τα περιμετρικά δίκτυα από εξωτερική πρόσβαση. Το δεύτερο προστατεύει τα εσωτερικά δίκτυα από την περίμετρο. Η ίδια η περίμετρος παρέχει μια σειρά υπηρεσίες όπως Active Directory Certificate Services (ADCS), Active Directory Rights Management Services (ADRMS) και σε ορισμένες περιπτώσεις, Active Directory Lightweight Directory Υπηρεσίες (ADLDS). Το ADDS προορίζεται αποκλειστικά για εσωτερικά δίκτυα. Το ιδανικό εξωτερικό τείχος προστασίας χρησιμοποιεί ένα σετ βασικών από πόρτες. Αυτά τα σετ περιλαμβάνουν:

- Πόρτα 53, η οποία χρησιμοποιείται για κυκλοφορία συστήματος ονομάτων τομέα (DNS). Συνήθως παρέχεται κίνηση DNS με τρόπο μόνο για ανάγνωση.
- Πόρτα 80, η οποία χρησιμοποιείται από δεδομένα ανοιχτού Hypertext Transfer Protocol (HTTP). Η πόρτα 80 χρησιμοποιείται συνήθως για πρόσβαση μόνο για ανάγνωση, επειδή δεν είναι ασφαλής.
- Πόρτα 443, για Secure HTTP ή Hypertext Transfer Protocol Secure (HTTPS). Διαβιβάσεις στη πόρτα 443 ασφαλίζονται μέσω του Secure Sockets Layer (SSL) ή του Transport Layer Security (TLS), τα οποία και τα δύο βασίζονται σε Certificate Authority (CA) πιστοποιητικά για την κρυπτογράφηση δεδομένων. Εξαιτίας αυτού, οι επικοινωνίες στη θύρα 443 υποστηρίζουν την ανάγνωση-εγγραφή ή λειτουργίες ασφαλής ανάγνωση δεδομένων.
- Πόρτα 25, η οποία χρησιμοποιείται για το Simple Mail Transfer Protocol (SMTP). Είναι απαραίτητο ρίσκο γιατί κανείς δεν μπορεί να εργαστεί χωρίς πρόσβαση σε e-mail.

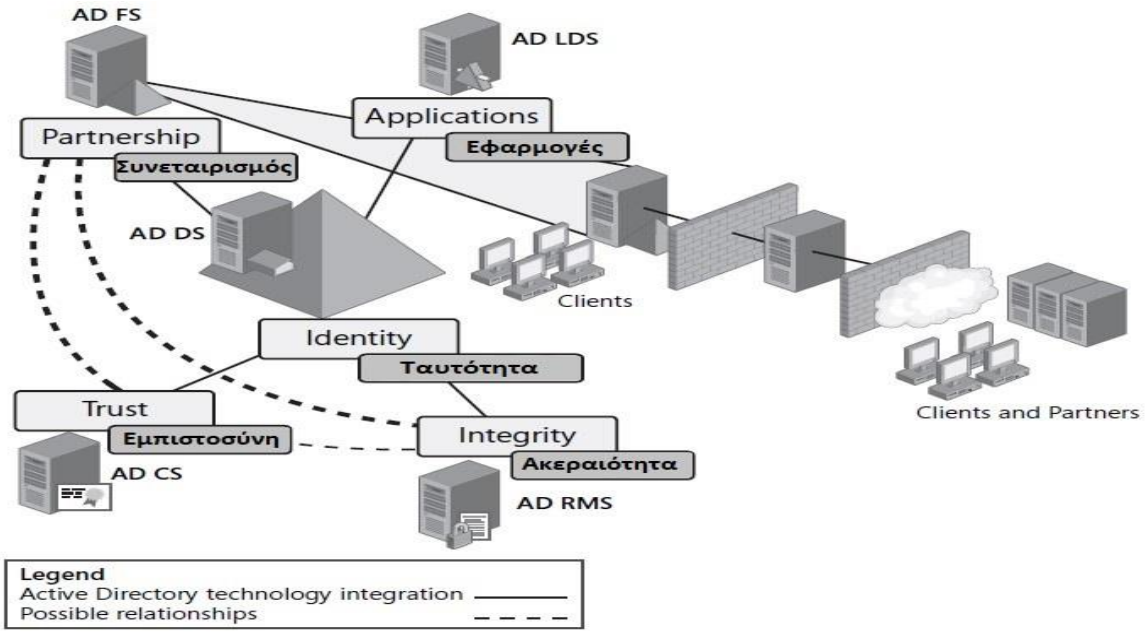
Όλες οι άλλες πόρτες θα πρέπει ιδανικά να είναι κλειστές. Το εσωτερικό τείχος προστασίας θα έχει μερικές ακόμη ανοιχτές πόρτες, ανάλογα με τις τεχνολογίες που χρησιμοποιούμε στην περίμετρο, όπως φαίνεται στην εικόνα 6.57. Για παράδειγμα, εάν χρησιμοποιούμε ADLDS για παροχή υπηρεσιών ελέγχου ταυτότητας για εφαρμογές Web στην περίμετρο, ίσως θελήσουμε να έχουμε μονόδρομους συγχρονισμούς από τον εσωτερικό μας ADDS κατάλογο για την παροχή των δικών μας λογαριασμών χρήστη. Εάν χρησιμοποιούμε Υπηρεσίες πληροφοριών Διαδικτύου (Internet Information Services), ίσως θελήσουμε να προωθήσουμε και να τραβήξουμε δεδομένα στις τοποθεσίες Web της περιμέτρου. Αυτή είναι η βάση ενός ασφαλούς περιμετρικού σχεδιασμού.



Εικόνα 6.57

Υπηρεσίες Ομοσπονδίας Active Directory (ADFS)

Η υπηρεσία Active Directory Federation Services (ADFS), μία από τις τεχνολογίες Active Directory, περιλαμβάνεται στα Windows Server 2008. Η τεχνολογία τύπου Active Directory έχει σχεδιαστεί για την επέκταση του εσωτερικού μας δικτύου στον έξω κόσμο όπως φαίνεται και στην εικόνα 6.58.



Εικόνα 6.58

Το ADFS έχει σχεδιαστεί για να παρέχει παρόμοια λειτουργικότητα με τη δασική εμπιστοσύνη ή τη αποκλειστική εμπιστοσύνη αλλά όχι μέσω των παραδοσιακών θυρών LDAP TCP/IP αλλά μέσω των κοινών θυρών HTTP. Στην πραγματικότητα, το ADFS χρησιμοποιεί τη θύρα 443 επειδή όλες οι επικοινωνίες εμπιστοσύνης ADFS είναι

ασφαλείς και κρυπτογραφημένες. Με αυτόν τον τρόπο, μπορούμε να βασιστούμε στο ADCS για να παρέχει πιστοποιητικά για κάθε διακομιστή στην εφαρμογή ADFS. Το ADFS μπορεί επίσης να επεκτείνει την ανάπτυξη ADRMS και να παρέχει ομοσπονδία υπηρεσιών διαχείρισης πνευματικής ιδιοκτησίας μεταξύ εταίρων.
Για την επέκταση της εσωτερικής μας αρμοδιότητας, το ADFS παρέχει επεκτάσεις σε εσωτερικά δάση και επιτρέπει στους οργανισμούς να δημιουργήσουν συνεργασίες χωρίς να χρειάζεται να ανοίξουν επιπλέον πόρτες στα τείχη προστασίας τους. Βασικά, το ADFS βασίζεται στον εσωτερικό κατάλογο ADDS κάθε συνεργάτη για να παρέχει έλεγχο ταυτότητας για υπηρεσίες extranet ή περιμέτρου. Όταν ένας χρήστης προσπαθεί να πραγματοποιήσει έλεγχο ταυτότητας σε μια εφαρμογή ενσωματωμένη στο ADFS, ο η υπηρεσία ADFS θα κάνει αντλήσει δεδομένα από τον εσωτερικό κατάλογο για έλεγχο ταυτότητας. Εάν ο χρήστης έχει πρόσβαση στον εσωτερικό κατάλογο, θα του έχει παραχωρηθεί πρόσβαση και στην εξωτερική εφαρμογή. Το κύριο πλεονέκτημα αυτού είναι ότι κάθε συνεργάτης του οργανισμού πρέπει να διαχειρίζεται μόνο δεδομένα ελέγχου ταυτότητας στο εσωτερικό δίκτυο. Το ADFS κάνει τα υπόλοιπα. Εν ολίγοις, το ADFS θα πρέπει να χρησιμοποιείται όποτε θέλουμε να εφαρμόσουμε μια συνεργασία με άλλους οργανισμούς που βασίζονται επίσης σε εσωτερικούς καταλόγους ADDS. Όταν πρέπει να παρέχουμε υπηρεσίες ελέγχου ταυτότητας στο περιμετρικό δίκτυο, αλλά οι χρήστες ή οι οργανισμοί που θέλουμε να αλληλεπιδράσουν, δεν έχουν εσωτερικούς καταλόγους ADDS, ή το εύρος της συνεργασίας δεν δικαιολογείται για ανάπτυξη ADFS, τότε θα πρέπει να βασιστούμε στο ADLDS.

Κατανόηση του Active Directory Federation Services

Σε γενικές γραμμές, το ADFS είναι σαν ένας κινητήρας ενιαίας σύνδεσης (single sign-on - SSO) που επιτρέπει στους χρήστες των εξωτερικών μας εφαρμογών που βασίζονται στο Web για πρόσβαση και έλεγχο ταυτότητας μέσω προγράμματος περιήγησης. Αυτό δεν είναι τόσο διαφορετικό από τη χρήση ενός εξωτερικού καταλόγου ADLDS που είναι συνδεδεμένος με τον εσωτερικό κατάλογό μας. Ωστόσο, το βασικό χαρακτηριστικό του ADFS είναι ότι για τον έλεγχο ταυτότητας ενός πελάτη, χρησιμοποιεί τον εσωτερικό κατάλογο ελέγχου ταυτότητας του ίδιου τομέα του χρήστη και δεν διαθέτει δικό του κατάλογο. Χρησιμοποιεί επίσης τον αυθεντικό έλεγχο ταυτότητας που πραγματοποίησε ο πελάτης στο δικό του δίκτυο και μεταβιβάζει αυτόν τον έλεγχο ταυτότητας σε όλες τις εφαρμογές Web με δυνατότητα ADFS.
Τα πλεονεκτήματα είναι ξεκάθαρα. Οι οργανισμοί πρέπει να διαχειρίζονται μόνο ένα κατάλογο ελέγχου ταυτότητας για τους δικούς τους χρήστες και δεν χρειάζεται να διαχειρίζονται καθόλου τα δευτερεύοντες καταλόγους. Η χρήση ενός καταλόγου ADLDS για έλεγχο ταυτότητας extranet προσθέτει γενικό διαχειριστικό φόρτο, επειδή ο οργανισμός χρειάζεται να διαχειρίζεται το δικό του εσωτερικό κατάλογο και τον εξωτερικό κατάλογο ή οποιοδήποτε κατάλογο γενικά. Οι χρήστες επίσης πρέπει συχνά να θυμούνται πολλούς κωδικούς πρόσβασης και κωδικούς πρόσβασης για να συνδεθούν σε κάθε ένα από αυτούς τους καταλόγους. Αυτό το ADFS το απλοποιεί επειδή συνδυάζει την εσωτερική ταυτότητα ADDS του χρήστη και την προβάλλει στον εξωτερικό κόσμο. Οι χρήστες πρέπει να κάνουν έλεγχο ταυτότητας μόνο μία φορά: όταν συνδέονται στο δικό τους δίκτυο. Χρησιμοποιώντας το ADFS, μπορούμε να δημιουργήσουμε συνεργασίες

μεταξύ επιχειρήσεων (B2B) με πολύ λίγα γενικά έξοδα. Σε αυτές τις συνεργασίες B2B, οι οργανισμοί χωρίζονται σε δύο κατηγορίες:

- *Οργάνωση πόρων (Resource organization)*: Όταν οργανισμοί έχουν εκθέσει πόρους όπως Web ιστότοπους — ηλεκτρονικό εμπόριο ή συνεργασία — αποφασίζουν να χρησιμοποιήσουν το ADFS για να απλοποιήσουν τον έλεγχο ταυτότητας επεξεργασία σε αυτούς τους πόρους, σχηματίζοντας συνεργασίες με άλλους οργανισμούς - προμηθευτές, συνεργάτες και ούτω καθεξής. Ο οργανισμός που σχηματίζει τη συνεργασία θεωρείται ο πόρος οργανισμός επειδή φιλοξενεί τους κοινόχρηστους πόρους στο περιμετρικό του δίκτυο.
- *Οργάνωση λογαριασμού (Account organization)*: Όταν οι οργανισμοί συνάπτουν σχέση ADFS με οργανώσεις πόρων, θεωρούνται οι οργανισμοί λογαριασμών επειδή διαχειρίζονται τους λογαριασμούς που χρησιμοποιούνται για την πρόσβαση στους κοινόχρηστους πόρους σε σχήματα SSO.

Το ADFS υποστηρίζει έναν πρόσθετο τρόπο ελέγχου ταυτότητας. Σε μια σχεδίαση SSO ιστού, θα γίνει έλεγχος ταυτότητας στους χρήστες από οπουδήποτε στο Διαδίκτυο. Μετά την πιστοποίηση τέτοιων χρηστών, το ADFS εξετάζει τα χαρακτηριστικά των χρηστών σε ADDS ή σε καταλόγους ADLDS για να προσδιορίσει ποιοι από αυτούς που ισχυρίζονται ότι είναι χρήστες πρέπει να έχουν πρόσβαση στην εφαρμογή. Για την υποστήριξη αυτής της ομοσπονδίας ταυτότητας, το ADFS βασίζεται σε τέσσερις υπηρεσίες ρόλου.

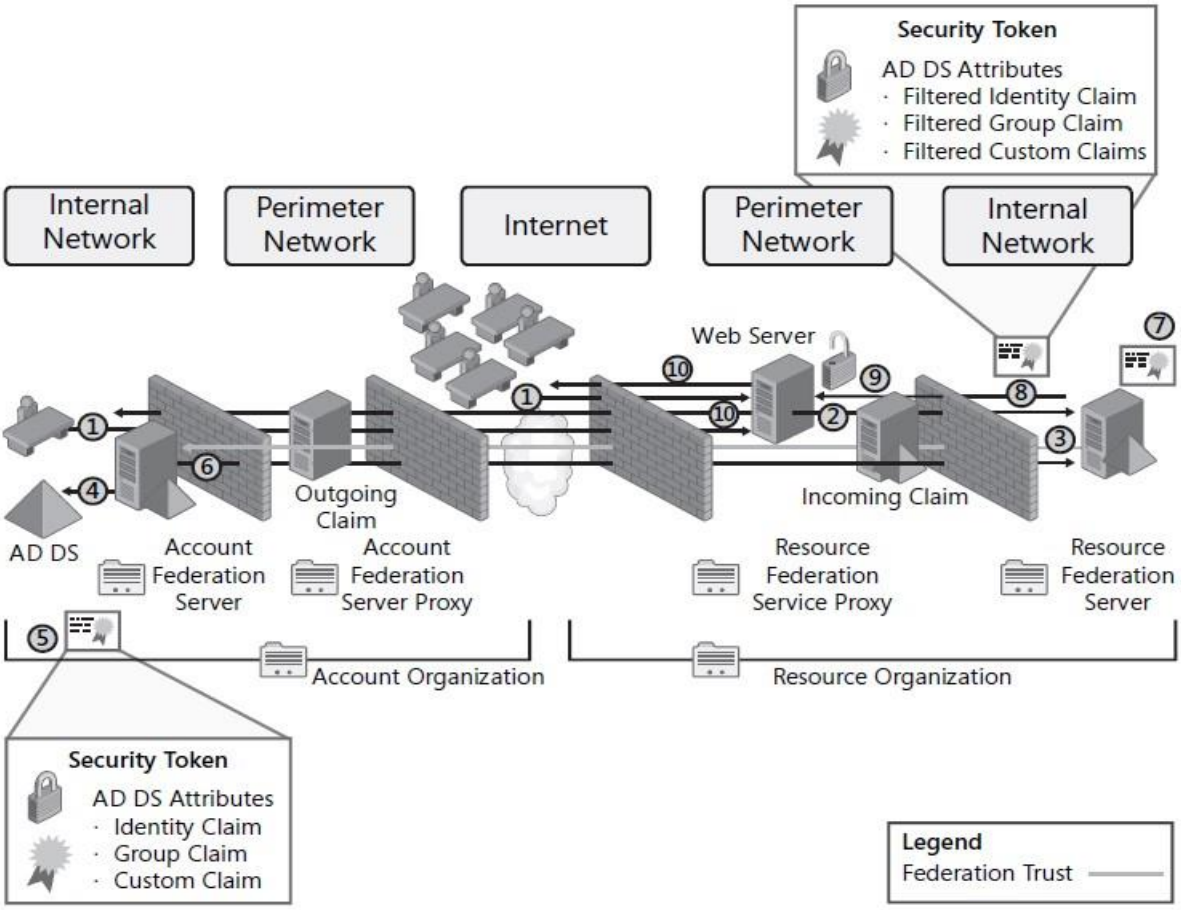
- ✓ *Υπηρεσία ομοσπονδίας (Federation Service)*: Αυτή η υπηρεσία διαμορφώνεται από τους διακομιστές που μοιράζονται μια πολιτική εμπιστοσύνης. Ο διακομιστής federation θα δρομολογήσει αιτήματα ελέγχου ταυτότητας στον κατάλληλο κατάλογο πηγής για τη δημιουργία διακριτικών ασφαλείας για τον χρήστη που ζητά πρόσβαση.
- ✓ *Συνδυασμός υπηρεσίας ομοσπονδίας (Federation Service Proxy)*: Για να λάβουμε τα αιτήματα ελέγχου ταυτότητας από τον χρήστη, την ομοσπονδία, ο διακομιστής βασίζεται σε έναν διακομιστή μεσολάβησης που βρίσκεται στο περιμετρικό δίκτυο. Ο πληρεξούσιος συλλέγει πληροφορίες ελέγχου ταυτότητας από το πρόγραμμα περιήγησης του χρήστη μέσω του WS-Federation Passive Requestor Profile (WS-F PRP), μια υπηρεσία ADFS Web, και την μεταβιβάζει στην ομοσπονδία υπηρεσία.
- ✓ *Claims-Aware Agent*: Ένας πράκτορας βρίσκεται στον διακομιστή Web και ξεκινά ερωτήματα ασφαλείας, απαιτώντας token, στην υπηρεσία ομοσπονδίας. Κάθε απαίτηση χρησιμοποιείται για τη χορήγηση ή την άρνηση πρόσβασης σε μια δοθείσα αίτηση. Εφαρμογές ASP.NET που μπορούν να εξετάσουν τις διάφορες απαιτήσεις που περιέχονται στο διακριτικό ασφαλείας ADFS του χρήστη θεωρούνται εφαρμογές που γνωρίζουν τις απαιτήσεις. Αυτές οι εφαρμογές μπορούν να βασίζονται στις απαιτήσεις για να προσδιορίσουν εάν ο χρήστης έχει πρόσβαση στην εφαρμογή. Δύο παραδείγματα εφαρμογών που γνωρίζουν απαιτήσεις είναι το ADRMS και το Microsoft Office SharePoint Server 2007.
- ✓ *Windows Token-based Agent*: Αυτός είναι ένας εναλλακτικός πράκτορας που μπορεί να μετατρέψει την ασφάλεια ADFS σε διακριτικό πρόσβασης Windows NT σε επίπεδο πλαστοπροσωπίας για εφαρμογές που βασίζονται σε μηχανισμούς ελέγχου ταυτότητας των Windows αντί για άλλους ελέγχους ταυτότητας που βασίζονται σε Web μεθόδους.

Επειδή βασίζεται σε μια τυπική υπηρεσία Web, το ADFS δεν χρειάζεται να βασίζεται μόνο στο ADDS υποστήριξη ομόσπονδων ταυτοτήτων. Οποιαδήποτε υπηρεσία καταλόγου

που συμμορφώνεται με το πρότυπο WS-Federation μπορεί να συμμετάσχει σε μια ένωση ταυτότητας ADFS. Παρόλο που οι υπηρεσίες Federation υπήρχαν στον Windows Server 2003 R2, το ADFS έχει βελτιωθεί σημαντικά στον Windows Server 2008 για τη διευκόλυνση των διαδικασιών εγκατάστασης και διαχείρισης. Το ADFS υποστηρίζει επίσης περισσότερες εφαρμογές Web από την αρχική έκδοση.

Η διαδικασία ελέγχου ταυτότητας AD FS

Μετά τη δημιουργία συνεργασιών ADFS, καθίσταται διαφανές για τους χρήστες να συνδέονται σε εξωτερικές εφαρμογές ιστού που περιλαμβάνονται στη συνεργασία. Σε ένα τυπικό σενάριο ADFS, όταν ένας χρήστης συνδέεται σε μια εφαρμογή που γνωρίζει τα αξιώματα ενός extranet, το ADFS προβλέπει αυτόματα τα διαπιστευτήρια του χρήστη και περιγράφει τις αξιώσεις που περιλαμβάνονται στα χαρακτηριστικά του λογαριασμού ADDS του χρήστη, όπως φαίνεται στην εικόνα 6.59.



Εικόνα 6.59

1. Ένας χρήστης ο οποίος βρίσκεται εντός ενός εσωτερικού δικτύου ή στο Διαδίκτυο και θέλει να έχει πρόσβαση σε μια εφαρμογή ιστού με γνώμονα τις αξιώσεις σε ένα extranet. Αυτός ο χρήστης ανήκει σε έναν από τους λογαριασμούς του οργανισμού που είναι μέλη της συνεργασίας ADFS.

2. Ο αντιπρόσωπος που γνωρίζει τις αξιώσεις στον διακομιστή Web επαληθεύει με έναν Resource Federation Server (RFS) στους πόρους του οργανισμού για να ελέγξει εάν έχει παραχωρηθεί πρόσβαση στον πελάτη. Επειδή το αίτημα πρέπει να διασχίσει ένα τείχος προστασίας, ο πράκτορας επικοινωνεί πρώτα με έναν διακομιστή μεσολάβησης της ομοσπονδίας (FSP), ο οποίος στη συνέχεια έρχεται σε επαφή με τον εσωτερικό διακομιστή ομοσπονδίας.
3. Επειδή δεν έχει λογαριασμό για τον χρήστη, αλλά έχει σχέση ομοσπονδίας με το χώρο καταλόγου στον λογαριασμό του οργανισμού - μια εμπιστοσύνη ομοσπονδίας, στην πραγματικότητα – ο διακομιστής πόρων του οργανισμού ελέγχει με έναν Account Federation Server(AFS) στο εσωτερικό δίκτυο του οργανισμού για τον προσδιορισμό των δικαιωμάτων πρόσβασης του χρήστη. Αυτά τα δικαιώματα πρόσβασης παρατίθενται με τη μορφή αξιώσεων, τα οποία είναι χαρακτηριστικά που συνδέονται με το αντικείμενο λογαριασμού του χρήστη στο ADDS.
4. Ο διακομιστής ομοσπονδίας στον λογαριασμό του οργανισμού συνδέεται άμεσα με τον εσωτερικό οργανισμό ADDS και αποκτά δικαιώματα πρόσβασης στον κατάλογο μέσω ενός ερωτήματος LDAP. Ο λογαριασμός χρήστη μπορεί επίσης να βρίσκεται σε ένα χώρο καταλόγου ADLDS.
5. Ο διακομιστής ομοσπονδίας του λογαριασμού του οργανισμού δημιουργεί το διακριτικό ασφαλείας ADFS του χρήστη. Αυτό το διακριτικό περιλαμβάνει το αναγνωριστικό χρήστη, τη λίστα των αξιώσεων που περιλαμβάνονται στο ADDS του λογαριασμού χρήστη και το ψηφιακό πιστοποιητικό του AFS.
6. Το AFS ανταποκρίνεται στο RFS με τα δικαιώματα πρόσβασης του πελάτη που περιέχονται στο υπογεγραμμένο διακριτικό ασφαλείας μέσω του διακομιστή μεσολάβησης. Αυτή είναι μια εξερχόμενη αξίωση.
7. Το RFS αποκρυπτογραφεί το token και εξάγει τις αξιώσεις για τον χρήστη από την εισερχόμενη απαίτηση. Στη συνέχεια χαρτογραφεί τις αξιώσεις στον οργανισμό που ισχυρίζεται ότι διατηρεί και εφαρμόζει ένα φιλτράρισμα πολιτικής για τη συγκεκριμένη αιτούμενη εφαρμογή ιστού.
8. Οι φιλτραρισμένες αξιώσεις στη συνέχεια συσκευάζονται και πάλι σε ένα υπογεγραμμένο διακριτικό ασφαλείας, το οποίο αποστέλλεται στον διακομιστή Web στο extranet του οργανισμού πόρων δημοσιεύοντάς το στη διεύθυνση URL που περιλαμβάνονται στο αρχικό αίτημα της εφαρμογής Web. Σε αυτήν την περίπτωση, η υπογραφή για το το διακριτικό βασίζεται είτε στο ψηφιακό πιστοποιητικό RFS είτε σε κλειδί περιόδου λειτουργίας Kerberos επειδή τα συστήματα βρίσκονται στο ίδιο δίκτυο.
9. Ο διακομιστής Ιστού βασίζεται στον αντιπρόσωπό του που γνωρίζει τις αξιώσεις για να αποκρυπτογραφήσει το διακριτικό ασφαλείας του χρήστη, αναζητά τις αξιώσεις του χρήστη και, στη συνέχεια, παραχωρεί πρόσβαση στην εφαρμογή βάσει των αξιώσεων του διακριτικού.
10. Για να υποστηρίξει τη μεμονωμένη σύνδεση, ο ADFS πράκτορας Web κατευθύνει το πρόγραμμα περιήγησης του χρήστη να γράψει ένα τοπικό cookie ελέγχου ταυτότητας για το χρήστη, ώστε να μην χρειαστεί να εκτελέσει αυτήν την αναζήτηση ξανά την επόμενη φορά που θα πρέπει να γίνει έλεγχος ταυτότητας κατά τη διάρκεια αυτής της περιόδου σύνδεσης.

Κάθε συνεργάτης μπορεί να χρησιμοποιήσει τους δικούς του χώρους εσωτερικού καταλόγου για να παρέχει στους χρήστες πρόσβαση σε εφαρμογές extranet. Αυτό απλοποιεί τη διαχείριση πρόσβασης, αλλά για να γίνει αυτό, κάθε συνεργάτης πρέπει να εφαρμόσει εμπιστοσύνη της ομοσπονδίας. Η εμπιστοσύνη της ομοσπονδίας βασίζεται στους συνεργάτες που έχουν τουλάχιστον μία ομοσπονδία ADFS εγκατεστημένη στα δίκτυά τους. Η κατεύθυνση της εμπιστοσύνης εκτελείται πάντα από τον συνεργάτη πόρων στον συνεργάτη του λογαριασμού. Όταν ο χρήστης χρησιμοποιεί δημόσιο ή οικιακό υπολογιστή που δεν είναι μέρος του τομέα ADDS του οργανισμού, μπορεί να χρησιμοποιήσει μια ειδική ιστοσελίδα ADFS, η οποία θα επιτρέψει σε αυτόν τον χρήστη να επιλέξει ποιο λογαριασμό του οργανισμού θα χρησιμοποιήσει. Αυτή η ιστοσελίδα παρέχει επίσης logon screens που μπορούν να υποστηρίξουν είτε έλεγχο ταυτότητας που βασίζεται σε φόρμες είτε ενσωματωμένα στα Windows. Αυτό επιτρέπει στους εξωτερικούς χρήστες να έχουν πρόσβαση στις εφαρμογές extranet, ακόμη και αν δεν χρησιμοποιούν εταιρικούς υπολογιστές. Εάν δεν θέλουμε να δημιουργήσουμε μια ιστοσελίδα που περιλαμβάνει μια λίστα λογαριασμών οργανώσεων επειδή δεν θέλουμε να δημοσιεύονται τα ονόματα του οργανισμού για λόγους ασφαλείας, μπορούμε να συμπεριλάβουμε τον λογαριασμό του οργανισμού απευθείας στη συμβολοσειρά ερωτήματος για την πρόσβαση στον πόρο.

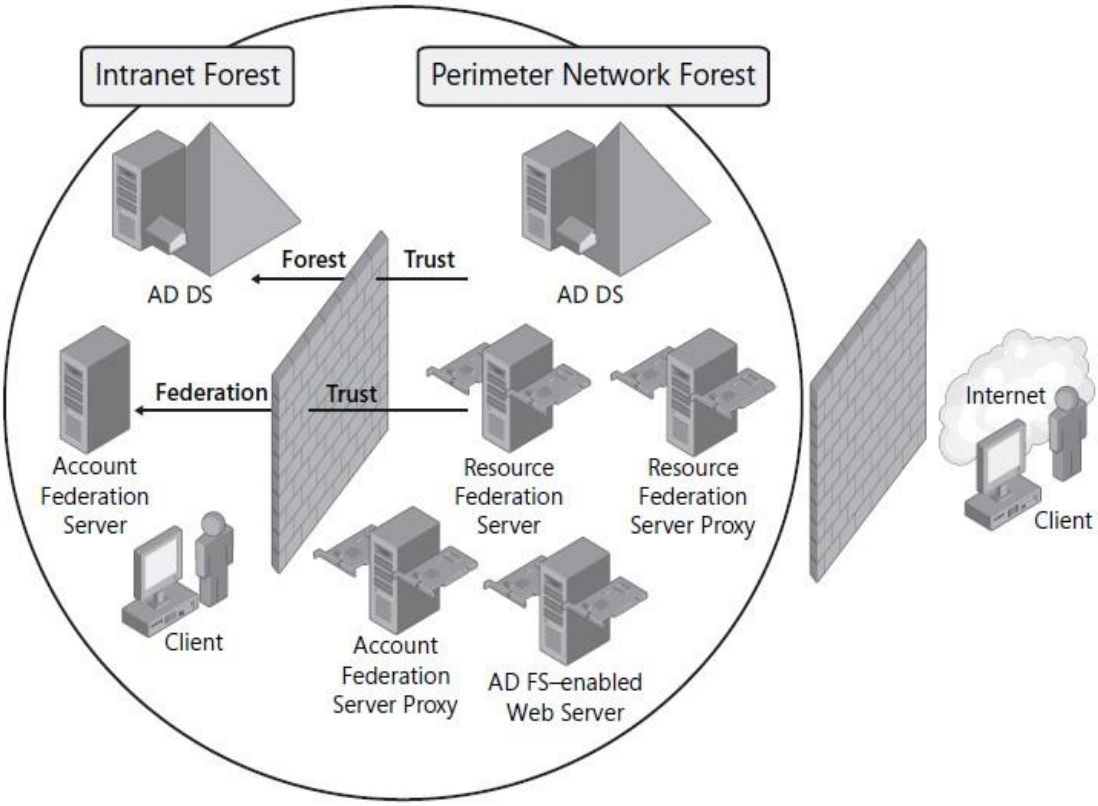
AD FS Designs

Το ADFS υποστηρίζει τρεις διαμορφώσεις ή αρχιτεκτονικά σχέδια, ανάλογα με τον τύπο του B2B που πρέπει να δημιουργήσουμε. Καθένα περιλαμβάνει τις δικές του ιδιαιτερότητες, και το καθένα υποστηρίζει ένα ειδικό σενάριο εταιρικής σχέσης.

- *Federated Web SSO*: Αυτό το μοντέλο εκτείνεται συνήθως σε πολλά τείχη προστασίας επειδή συνδέει εφαρμογές που περιέχονται σε ένα extranet με έναν οργάνισμό πόρων στον εσωτερικό κατάλογο των λογαριασμών του οργανισμού. Η μόνη εμπιστοσύνη που υπάρχει σε αυτό το μοντέλο είναι η εμπιστοσύνη ομοσπονδίας, η οποία είναι πάντα μονόδρομη εμπιστοσύνη από τον οργανισμό πόρων στον οργανισμό λογαριασμού. Αυτό είναι το πιο κοινό σενάριο ανάπτυξης ADFS, το οποίο το είδαμε στην εικόνα 6.41.

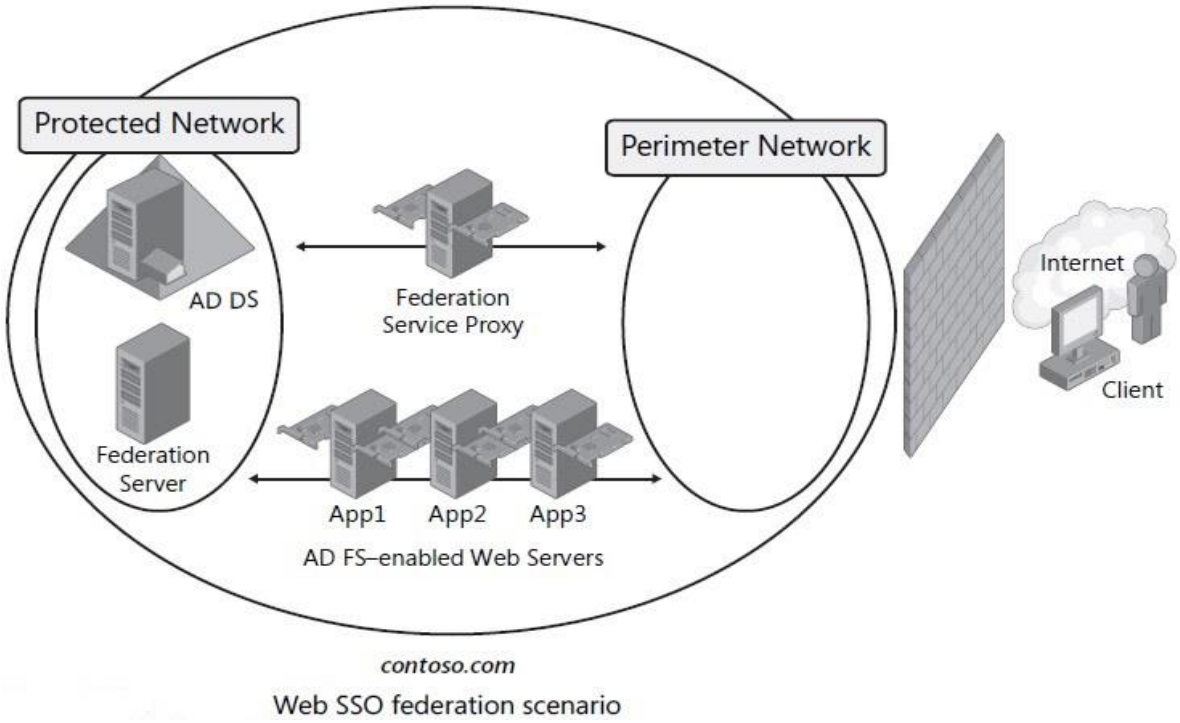
- *Federated Web SSO with Forest Trust*: Σε αυτό το μοντέλο, ο οργανισμός χρησιμοποιεί δύο ADDS δάση. Το ένα είναι το εσωτερικό δάσος και το δεύτερο είναι ένα εξωτερικό δάσος που βρίσκεται μέσα ένα περιμετρικό δίκτυο. Μια δασική εμπιστοσύνη δημιουργείται μεταξύ του δάσους στο περιμετρικό δίκτυο και το εσωτερικό δάσος. Επιπλέον, δημιουργείται μια εμπιστοσύνη ομοσπονδίας μεταξύ του διακομιστή συνένωσης πόρων, ο οποίος βρίσκεται εντός της περιμέτρου και η συνένωση λογαριασμού διακομιστή, που βρίσκεται στο εσωτερικό δίκτυο. Σε αυτό το σενάριο, οι εξωτερικοί χρήστες έχουν λογαριασμούς στο περιμετρικό δάσος και οι εσωτερικοί χρήστες έχουν λογαριασμούς στο εσωτερικό δάσος. Τα συστήματα ADFS συνδυάζουν τα δικαιώματα πρόσβασης από τους λογαριασμούς και στα δύο δάση στις εφαρμογές της περιμέτρου. Εξαιτίας αυτού, οι εσωτερικοί χρήστες έχουν πρόσβαση στις εφαρμογές τόσο από το εσωτερικό δίκτυο όσο και από το

Διαδίκτυο, ενώ οι εξωτερικοί χρήστες έχουν πρόσβαση στις εφαρμογές μόνο από το Διαδίκτυο, όπως φαίνεται στην εικόνα 6.60.



Εικόνα 6.60

- *Web SSO*: Όταν όλοι οι χρήστες μιας εφαρμογής extranet είναι εξωτερικοί και δεν έχουν λογαριασμούς εντός τομέα ADDS, πρέπει να αναπτύξουμε μόνο ένα SSO Web. Το μοντέλο Web SSO επιτρέπει στους χρήστες να κάνουν έλεγχο ταυτότητας μόνο μία φορά σε πολλές εφαρμογές Web. Ωστόσο, αυτό το μοντέλο βασίζεται σε διακομιστές Web πολλαπλών υπολογιστών - διακομιστές που περιλαμβάνουν τουλάχιστον δύο κάρτες δικτύων διασύνδεσης (NIC), μία που είναι συνδεδεμένη με το εξωτερικό δίκτυο και μία που είναι συνδεδεμένο στο εσωτερικό δίκτυο. Οι διακομιστές Web αποτελούν μέρος του εσωτερικού ADDS τομέα και συνδέονται σε αυτόν μέσω του εσωτερικού NIC. Οι πελάτες έχουν πρόσβαση στις εφαρμογές μέσω του εξωτερικού NIC. Ο Federation Service Proxy παρέχει επίσης πολλές υπηρεσίες πρόσβαση τόσο στο εξωτερικό όσο και στο εσωτερικό δίκτυο, όπως φαίνεται στην εικόνα 6.61.



Εικόνα 6.61

Τα πιο συνηθισμένα σενάρια είναι το πρώτο και το τελευταίο αλλά, ιδανικά, όλα τα μέλη της identity federation deployment θα έχουν τον δικό τους κατάλογο ADDS και θα λειτουργούν ως λογαριασμοί ενός οργανισμού με αποτέλεσμα την στρατηγική ανάπτυξης.

Κατανόηση των ADFS components

Εκτός από τις διάφορες υπηρεσίες ρόλου που υποστηρίζονται από το ADFS, αυτή η τεχνολογία βασίζεται σε πολλά συστατικά. Αυτά περιλαμβάνουν:

- Claims
- Cookies
- Certificates

Καθένα από αυτά τα τρία συστατικά παρέχει πρόσθετη υποστήριξη στη διαδικασία ADFS.

ADFS Claims

Στην πιο βασική τους μορφή, τα claims είναι δηλώσεις που κάνει κάθε συνεργάτης σε μια σχέση ADFS για τους χρήστες του. Τα claims μπορούν να βασίζονται σε διάφορες τιμές, για παράδειγμα, ονόματα χρηστών, κλειδιά πιστοποιητικού, ομαδικές συνδρομές, ειδικά προνόμια ή περισσότερα. Τα claims αποτελούν τη βάση της εξουσιοδότησης. Το ADFS στέλνει στην εφαρμογή Web. Τα claims μπορούν να ληφθούν με τρεις τρόπους:

- Ο διακομιστής λογαριασμού ομοσπονδίας μπορεί να υποβάλει ερώτημα στον εσωτερικό κατάλογο για claims και τους παρέχει σε έναν συνεργάτη πόρων.
- Ο λογαριασμός του οργανισμού μπορεί να παρέχει claims σε έναν διακομιστή συνένωσης πόρων, ο οποίος στη συνέχεια τα διαβιβάζει στην εφαρμογή πόρων αφού φιλτραριστούν.

- Η υπηρεσία ομοσπονδίας ρωτά το κατάλογο (ADDS ή ADLDS) για τα claims και στη συνέχεια τους παρέχει στην εφαρμογή πόρων αφού φιλτραριστούν.

Το ADFS μπορεί να υποστηρίξει τρεις τύπους claims:

- **Identity claim type**: Κάθε claim που βασίζεται στην ταυτότητα του χρήστη εμπίπτει σε αυτήν την κατηγορία. Πρέπει να υπάρχει τουλάχιστον ένας τύπος claim ταυτότητας σε κάθε claim για security tokens παράγονται από μια λίστα claim.
    - Αυτό μπορεί να περιλαμβάνει ένα κύριο όνομα χρήστη (UPN), το οποίο αντιπροσωπεύει την ταυτότητα του χρήστη σε μορφή που μοιάζει με διεύθυνση ηλεκτρονικού ταχυδρομείου (όνομα χρήστη @ λογαριασμός τομέα). Θα πρέπει να λάβουμε υπόψη ότι ακόμα και αν υπάρχουν πολλά UPN για λογαριασμό χρήστη, μόνο ένα μπορεί να χρησιμοποιηθεί σε έναν τύπο claim ταυτότητας. Εάν πρέπει να κοινοποιηθούν άλλα UPN στο claim, αυτά πρέπει να οριστούν ως προσαρμοσμένος τύπος claim. Όταν περιλαμβάνεται με άλλους τύπους claim ταυτότητας, το UPN έχει την υψηλότερη προτεραιότητα.
    - Μπορεί επίσης να είναι μια διεύθυνση e-mail (όνομα χρήστη @ email domain). Όπως και το UPN, μόνο μία διεύθυνση e-mail μπορεί να κοινοποιηθεί ως τύπος claim e-mail. Όλα τα άλλα e-mail, διευθύνσεις, εάν απαιτούνται, πρέπει να αναφέρονται ως προσαρμοσμένοι τύποι claim. Όταν περιλαμβάνεται με άλλους τύπους claim ταυτότητας, η διεύθυνση ηλεκτρονικού ταχυδρομείου έχει τη δεύτερη υψηλότερη προτεραιότητα.
    - Μπορούμε να βασιστούμε σε κοινά ονόματα, τα οποία δεν είναι τίποτα περισσότερο από αυθαίρετες σειρές χαρακτήρων. Δεν υπάρχει μέθοδος που μπορούμε να χρησιμοποιήσουμε για να εγγυηθούμε την μοναδικότητα ενός κοινού ονόματος. Επομένως, χρειάζεται προσοχή όταν χρησιμοποιούμε αυτόν τον τύπο claim. Όταν περιλαμβάνεται με άλλους τύπους claim ταυτότητας, το κοινό όνομα έχει τη χαμηλότερη προτεραιότητα.
- **Group claim type**: Οι συνδρομές ομάδας στις οποίες ανήκει ένας χρήστης μπορούν επίσης να χρησιμοποιηθούν σε ένα claim. Επειδή ένας χρήστης μπορεί να ανήκει σε πολλές ομάδες, μπορούμε να παρέχουμε πολλούς τύπους claim ομάδας σε ένα claim. Για παράδειγμα, ο ίδιος χρήστης μπορεί να ανήκει στον ελεγκτή, τον προγραμματιστή και τον χρήστη ομάδες σε μια εφαρμογή.
- **Custom claim type**: Εάν πρέπει να παρέχονται προσαρμοσμένες πληροφορίες για έναν χρήστη, για παράδειγμα, ένας προσαρμοσμένος αριθμός αναγνώρισης, όπως αριθμός τραπεζικού λογαριασμού ή αριθμός υπαλλήλου, θα το βάζαμε σε έναν προσαρμοσμένο τύπο claim.

Κατά την διάρκεια επεξεργασίας των claim, αυτά φιλτράρονται από τον διακομιστή ομοσπονδίας. Αυτό μειώνει το σύνολο αριθμός claim που πρέπει να έχει ένας οργανισμός. Εάν το φιλτράρισμα δεν ήταν διαθέσιμο, τότε ο οργανισμός θα ήταν υπεύθυνος για τη χαρτογράφηση κάθε claim για κάθε συνεργάτη. Αυτό θα αύξανε πολύ τον αριθμό των claim προς διαχείριση.

ADFS Cookies

Εκτός από τα claim, το ADFS λειτουργεί με cookies, τα οποία εγγράφονται στα προγράμματα περιήγησης των χρηστών κατά τη διάρκεια της περιόδου σύνδεσης Web που πιστοποιούνται μέσω ADFS. Τρεις τύποι cookie χρησιμοποιούνται από το ADFS:

- **Cookies ελέγχου ταυτότητας**: Επειδή η πρώτη εμφάνιση ενός ελέγχου ταυτότητας ADFS μπορεί να απαιτεί μερικές συναλλαγές, το ADFS δημιουργεί ένα cookie ελέγχου ταυτότητας για να τοποθετηθεί μέσα στο πρόγραμμα περιήγησης του χρήστη για υποστήριξη SSO έξτρα ελέγχων. Αυτό το cookie θα συμπεριλάβει όλα τα claim του χρήστη. Τα cookie ελέγχου ταυτότητας εκδίδονται από το ADFS πράκτορας ιστού και την ίδια την υπηρεσία ομοσπονδίας. Η εμπιστοσύνη στον πράκτορα Web αποφεύγει την ανάγκη τοποθέτησης ζευγών δημόσιων και ιδιωτικών κλειδιών στο διακομιστή. Όταν ο πράκτορας Web δημιουργεί έλεγχο ταυτότητας cookie, χρησιμοποιεί απλώς το υπάρχον διακριτικό ασφαλείας που δημιουργείται από την ομοσπονδία υπηρέτη. Ο διακομιστής ομοσπονδίας, ωστόσο, πρέπει να έχει ζεύγη κλειδιών, επειδή βασίζεται σε αυτά τα κλειδιά ζευγάρια για να υπογράψουν διακριτικά ασφαλείας. Αυτό το cookie είναι υπογεγραμμένο, αλλά δεν είναι κρυπτογραφημένο. Αυτός είναι ένας ακόμη λόγος έτσι ώστε όλες οι επικοινωνίες σε αυτήν τη διαδικασία να κρυπτογραφούνται είτε μέσω TLS είτε SSL. Επίσης, επειδή είναι μια συνεδρία cookie, διαγράφεται μετά το κλείσιμο της συνεδρίας.
- **Λογαριασμός Partner Cookies**: Κατά τη διαδικασία ελέγχου ταυτότητας, ο πελάτης θα πρέπει να ανακοινώσει τον λογαριασμό συνεργάτη με τον οποίο έχει συνδρομή. Εάν αυτή η ανακοίνωση έχει έγκυρο διακριτικό, η διαδικασία ADFS γράφει ένα cookie στον πελάτη, ώστε να μπορεί να βασίζεται σε αυτό το cookie αντί να χρειάζεται να εκτελέσει ξανά την ανακάλυψη συνεργατών την επόμενη φορά που ο πελάτης θα πραγματοποιήσει έλεγχο ταυτότητας. Αυτό το cookie δεν είναι υπογεγραμμένο ή κρυπτογραφημένο. Είναι ένα μακρόχρονο και επίμονο cookie.
- **Cookies αποσύνδεσης**: Κάθε φορά που η υπηρεσία ομοσπονδίας εκχωρεί ένα διακριτικό, ο συνεργάτης πόρων ή διακομιστής προορισμού που είναι συνδεδεμένος με το διακριτικό προστίθεται σε ένα cookie αποσύνδεσης Το cookie αποσύνδεσης στη συνέχεια χρησιμοποιείται για τη διευκόλυνση ενός τεχνητού ελέγχου ταυτότητας, για παράδειγμα, προσωρινά αποθηκευμένα cookie, λειτουργίες καθαρισμού στο τέλος μιας περιόδου λειτουργίας χρήστη. Αυτό το cookie δεν είναι υπογεγραμμένο ή κρυπτογραφημένο. Είναι ένα cookie περιόδου λειτουργίας που διαγράφεται ως μέρος εργασιών καθαρισμού.

ADFS Certificate

Για την εξασφάλιση ασφαλών επικοινωνιών, η εφαρμογή ADFS χρησιμοποιεί διάφορους τύπους πιστοποιητικών. Στην πραγματικότητα, το ADFS μπορεί να βασιστεί στην ανάπτυξη ADCS για να αποκτήσει τα πιστοποιητικά που χρειάζεται. Κάθε διακομιστής ρόλος μιας ανάπτυξης ADFS θα βασίζεται σε πιστοποιητικά. Ο τύπος πιστοποιητικού που απαιτείται από τον κάθε ρόλο εξαρτάται από τον σκοπό του.

- **Διακομιστές ομοσπονδίας (Federation servers)**: Ο διακομιστής ομοσπονδίας πρέπει να διαθέτει πιστοποιητικό ελέγχου ταυτότητας διακομιστή και ένα πιστοποιητικό υπογραφής διακριτικών εγκατεστημένο πριν να εκτελέσει οποιεσδήποτε λειτουργίες ADFS και γίνει πλήρως λειτουργικός. Επιπλέον, η πολιτική εμπιστοσύνης που αποτελεί το βασικό δόγμα της σχέσης ομοσπονδίας βασίζεται στο πιστοποιητικό επαλήθευσης. Το τελευταίο δεν είναι τίποτα περισσότερο από το δημόσιο κλειδί του πιστοποιητικού υπογραφής διακριτικών.
  - *Certificate*: Το πιστοποιητικό ελέγχου ταυτότητας διακομιστή είναι ένα πιστοποιητικό ελέγχου ταυτότητας SSL που διασφαλίζει την κυκλοφορία ιστού μεταξύ του διακομιστή συνένωσης και του διακομιστή μεσολάβησης ομοσπονδίας ή οι πελάτες στο Web. Τα πιστοποιητικά SSL συνήθως ζητούνται και εγκαθίστανται μέσω των υπηρεσιών IIS Διευθυντής.
  - Κάθε φορά που ο διακομιστής ομοσπονδίας δημιουργεί ένα διακριτικό ασφαλείας, πρέπει να υπογράφει ψηφιακά το διακριτικό με το πιστοποιητικό υπογραφής διακριτικών. Η υπογραφή πιστοποιητικών διασφαλίζει ότι δεν μπορεί να παραβιαστεί κατά τη διέλευση. Το πιστοποιητικό υπογραφής διακριτικών αποτελείται από ιδιωτικό και δημόσιο κλειδί.
  - Όταν υπάρχουν περισσότεροι από ένας διακομιστές ομοσπονδίας σε μια ανάπτυξη θα πρέπει να πραγματοποιείται μια διαδικασία επαλήθευσης μεταξύ διακομιστών. Για να γίνει αυτό, κάθε διακομιστής πρέπει να έχει πιστοποιητικά επαλήθευσης για όλους τους άλλους διακομιστές. Το πιστοποιητικό επαλήθευσης αποτελείται από το δημόσιο κλειδί του πιστοποιητικού υπογραφής διακριτικών για διακομιστής ομοσπονδίας. Αυτό σημαίνει ότι το πιστοποιητικό είναι εγκατεστημένο στο διακομιστή προορισμού χωρίς το αντίστοιχο ιδιωτικό κλειδί του.
- **Federation Service proxies**: Οι διακομιστές μεσολάβησης ομοσπονδίας πρέπει να διαθέτουν πιστοποιητικό ελέγχου ταυτότητας διακομιστή, κρυπτογραφημένο σε SSL επικοινωνίες με πελάτες Web. Πρέπει επίσης να διαθέτουν πιστοποιητικό ελέγχου ταυτότητας πελάτη για έλεγχο ταυτότητας της ομοσπονδίας διακομιστή κατά τη διάρκεια των επικοινωνιών. Αυτό το πιστοποιητικό μπορεί να είναι οποιουδήποτε τύπου πιστοποιητικό ελέγχου ταυτότητας πελάτη εφ 'όσον βασίζεται σε εκτεταμένη χρήση κλειδιού (EKU). Τόσο το ιδιωτικό όσο και το δημόσιο κλειδί για αυτό το πιστοποιητικό αποθηκεύονται στον διακομιστή μεσολάβησης. Το δημόσιο κλειδί αποθηκεύεται επίσης στην ομοσπονδία διακομιστών και στην πολιτική εμπιστοσύνης. Όταν εργάζεστε με αυτόν τον τύπο πιστοποιητικού στην Κονσόλα ADFS, ονομάζονται ομοσπονδιακά πιστοποιητικά διακομιστή μεσολάβησης υπηρεσίας.
- **AD FS Web agents**: Κάθε διακομιστής Ιστού με δυνατότητα ADFS που φιλοξενεί τον πράκτορα ιστού ADFS πρέπει να έχουν επίσης πιστοποιητικό ελέγχου

ταυτότητας διακομιστή για να διασφαλίσουν την επικοινωνία του με πελάτες στο Web. Το ADFS μπορεί εύκολα να βασιστεί στο ADCS για τη λήψη και τη διαχείριση αυτών των πιστοποιητικών. Λάβετε υπόψη, ωστόσο, ότι επειδή πολλοί από τους ρόλους ADFS είναι στραμμένοι προς τα έξω, τα πιστοποιητικά πρέπει να είναι από μια αξιόπιστη αρχή πιστοποίησης · Διαφορετικά, θα πρέπει να τροποποιήσετε το Trusted CA για κάθε πελάτης Ιστού.

6.4. Ασφάλεια

6.4.1. Η ασφάλεια στον οργανισμό

Η ασφάλεια είναι δύσκολο θέμα στον τομέα της πληροφορικής. Στο παρελθόν υπήρξαν, και στο μέλλον θα υπάρχουν, σημαντικές απειλές για την ασφάλεια σε οποιονδήποτε χρησιμοποιεί υπολογιστές, ειδικά με λειτουργικά συστήματα Windows. Είτε μέσω επιθέσεων ιών, trojan, worms, root kit ή άλλο κακόβουλο κώδικα στον υπολογιστή ή στον διακομιστή, επιθέσεις υπηρεσίας (DDoS) σε διακομιστές συστήματος ονομάτων τομέα (DNS), κωδικών πρόσβασης ή κλοπής ταυτότητας κτλ, όλοι διατρέχουν κίνδυνο. Όσοι οργανισμοί που δεν κάνουν τίποτα για την ασφάλεια των συστημάτων τους είναι ευάλωτοι και κινδυνεύουν να χάσουν τα πάντα, ακόμη και την ίδια τους την ύπαρξη. Η ασφάλεια είναι ένα προαπαιτούμενο ζήτημα ανεξάρτητα από το μέγεθος του οργανισμού. Είτε αναφερόμαστε σε ένα υπολογιστή που διαχειρίζεται ένα μικρό κατάστημα είτε σε έναν διακομιστή πρέπει να δοθεί ιδιαίτερη προσοχή στην ασφάλεια των πόρων του. Κακόβουλοι χάκερ στο Διαδίκτυο ακολουθούν τα προϊόντα σας.

Η Microsoft, ως κατασκευαστής των Windows, παρέχει εργαλεία και οδηγίες για την ασφάλεια των συστημάτων που τρέχουν τα λειτουργικά της. Η ασφάλεια όμως έχει δικό της κύκλο ζωής. Η ασφάλεια δεν είναι μόνο μια τεχνική λειτουργία, περιλαμβάνει όλους τους χρήστες της υποδομής του οργανισμού. Ακόμα κι αν παρέχουμε τα πιο αυστηρά τεχνικά επίπεδα ασφάλειας στα συστήματά μας, όλα αυτά μπορεί να καταρρεύσουν εάν οι χρήστες δεν το γνωρίζουν τις δικές τους ευθύνες στο θέμα της ασφαλείας.

Γενικά οι οργανισμοί που χρησιμοποιούν την τεχνολογία της Microsoft διατρέχουν μεγαλύτερο κίνδυνο. Ο μεγαλύτερος προμηθευτής λειτουργικού συστήματος στον κόσμο είναι η Microsoft ως εκ’ τούτου είναι ο νούμερο ένα στόχος για τους hacker. Αυτό φυσικά δεν σημαίνει ότι οι τεχνολογίες της Microsoft είναι χειρότερες από άλλες όσον αφορά την ασφάλεια και άλλα ελαττώματα.

Ο στόχος της Microsoft με τα Windows Server είναι το σύστημα να είναι “Ασφαλής από προεπιλογή και Ασφαλής κατά την ανάπτυξη". προσπαθώντας με τις νέες τεχνολογίες της να αποκλείσει απειλές για την ασφάλεια που βρέθηκαν στο παρελθόν.

Φυσικά παρόλη την προσπάθεια της Microsoft να κάνει ασφαλές το λειτουργικό σύστημα, οι λειτουργίες ασφαλείας θα το προστατεύσουν μόνο εάν εφαρμοστούν σωστά.

Βασικά στοιχεία ασφαλείας

Η ασφάλεια είναι ένα ζήτημα που περιλαμβάνει σχεδόν τα πάντα μέσα στο δίκτυο. Το αντικείμενο της ασφάλειας είναι η προστασία των πληροφοριών. Για να επιτευχθεί αυτό, πρέπει να εφαρμοστεί ένα σύστημα προστασίας με στρώσεις (layer) που θα παρέχει τη δυνατότητα εκτέλεσης των ακόλουθων δραστηριοτήτων:

- Προσδιορισμός των ατόμων καθώς εισέρχονται στο δίκτυό.
- Προσδιορισμός κατάλληλα επίπεδα πρόσβασης για άτομα που εργάζονται στο δίκτυό, και απόδοση των κατάλληλων δικαιωμάτων πρόσβασης.
- Προσδιορισμός ότι το άτομο που τροποποιεί τα δεδομένα είναι το άτομο το οποίο έχει εξουσιοδότηση τροποποίησης των δεδομένων.
- Παροχή εγγύησης του απόρρητου των πληροφοριών μόλις αποθηκευτούν στο δίκτυό του οργανισμού.

- Εξασφάλιση της διαθεσιμότητας των πληροφοριών μόλις αποθηκευτούν στο δίκτυό του οργανισμού.
- Διασφάλιση την ακεραιότητας των δεδομένων που είναι αποθηκευμένα στο δίκτυό του οργανισμού.
- Παρακολούθηση των δραστηριοτήτων στο δίκτυό του οργανισμού.
- Έλεγχος των συμβάντων ασφαλείας εντός του δικτύου και ασφαλής αποθήκευση των ιστορικών δεδομένων ελέγχου.
- Δημιουργία τις κατάλληλών διοικητικών δραστηριοτήτων για την διασφάλιση ότι το δίκτυο είναι ασφαλής ανά πάσα στιγμή.

Για καθεμία από αυτές τις δραστηριότητες, υπάρχουν διάφορα πεδία αλληλεπίδρασης:

- Οι άνθρωποι του οργανισμού αλληλοεπιδρούν με συστήματα σε τοπικό επίπεδο. Αυτά τα συστήματα πρέπει να είναι προστατευμένα, ανεξάρτητα από το αν είναι συνδεδεμένα ή όχι σε δίκτυο.
- Το Intranet αλληλοεπιδρά με απομακρυσμένα συστήματα. Αυτά τα συστήματα πρέπει επίσης να είναι προστατεύονται ανά πάσα στιγμή, είτε βρίσκονται στο τοπικό δίκτυο (LAN) είτε το δίκτυο ευρείας περιοχής (WAN).
- Τα διαδικτυακά συστήματα που θεωρούνται δημόσια πρέπει επίσης να προστατεύονται από επιθέσεις όλων των τύπων. Αυτά βρίσκονται σε χειρότερη κατάσταση, επειδή εκτίθενται έξω από τα όρια του εσωτερικού δικτύου.
- Extranet Αυτά τα συστήματα συχνά θεωρούνται εσωτερικά, αλλά εκτίθενται σε συνεργάτες, προμηθευτές ή / και πελάτες. Η κύρια διαφορά μεταξύ συστημάτων extranet και Internet είναι έλεγχος ταυτότητας - ενώ ενδέχεται να υπάρχει αναγνώριση σε ένα σύστημα Internet, στη πρόσβαση σε περιβάλλον extranet απαιτείται πάντα έλεγχος ταυτότητας.

Ανεξάρτητα από το εύρος της, η ασφάλεια είναι μια δραστηριότητα (όπως όλες οι δραστηριότητες πληροφορικής) που βασίζεται σε τρία κλειδιά στοιχεία: άτομα, υπολογιστές και διαδικασίες:

- Οι άνθρωποι είναι οι εκτελεστές της διαδικασίας ασφαλείας. Είναι επίσης οι κύριοι χρήστες της.
- Οι υπολογιστές αντιπροσωπεύουν τεχνολογία. Περιλαμβάνουν μια σειρά εργαλείων και εξαρτημάτων για την υποστήριξη της διαδικασίας ασφαλείας.
- Οι διαδικασίες αποτελούνται από πρότυπα ροής εργασίας, διαδικασίες και πρότυπα για την εφαρμογή της ασφάλειας.

Η ενσωμάτωση αυτών των τριών στοιχείων βοηθάει ώστε να σχεδιαστεί μια πολιτική ασφάλειας που ισχύει για ολόκληρο τον οργανισμό.

6.4.2. Σχεδιασμός μιας πολιτικής ασφαλείας

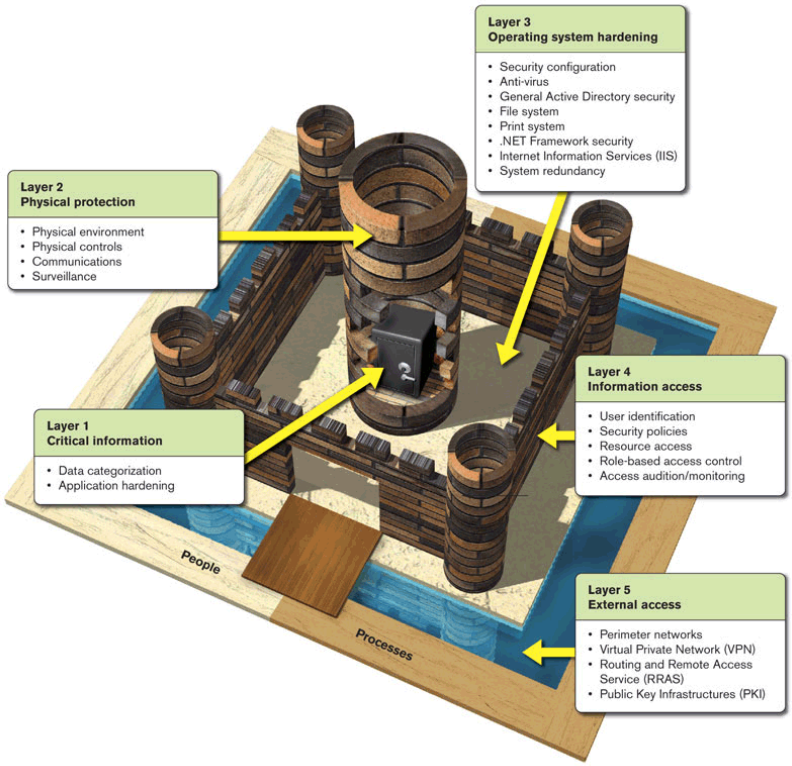
Ο σχεδιασμός μιας πολιτικής ασφαλείας είναι μόνο ένα βήμα στον κύκλο ζωής της ασφαλείας, αλλά, δυστυχώς, είναι δεν είναι πάντα το πρώτο βήμα. Οι άνθρωποι συχνά σκέφτονται την πολιτική ασφάλειας μόνο αφού υπάρξουν θύματα απειλής για την ασφάλεια.

Όπως κάθε άλλη διαδικασία σχεδιασμού, πρέπει να αξιολογηθεί το επιχειρηματικό μοντέλο και να προσδιοριστούν και να αναθεωρηθούν οι τρέχουσες πολιτικές ασφαλείας, εάν υπάρχουν. Στη συνέχεια, θα πρέπει να προσδιοριστούν ποια κοινά πρότυπα ασφαλείας θα εφαρμοστούν εντός του οργανισμού. Αυτά θα περιλαμβάνουν τεχνικές και μη τεχνικές πολιτικές και διαδικασίες. Ένα παράδειγμα τεχνικής πολιτικής θα ήταν οι παράμετροι ασφαλείας που θα οριστούν σε κάθε υπολογιστή στον οργανισμό. Μια μη τεχνική πολιτική θα ασχοληθεί τις συνήθειες που πρέπει να αναπτύξουν οι χρήστες για να επιλέγουν σύνθετους κωδικούς πρόσβασης και να τους προστατεύουν.

Το Σύστημα Άμυνας του Κάστρου (Castle Defense System)

Ο καλύτερος τρόπος για να ορίσουμε μια πολιτική ασφάλειας είναι να χρησιμοποιήσουμε ένα μοντέλο. Το μοντέλο που θα αναλύσουμε είναι το Castle Defense System (CDS). Στα μεσαιωνικά χρόνια, οι άνθρωποι χρειάζονταν να προστατεύουν τους ίδιους και τα υπάρχοντά τους μέσω του σχεδιασμού ενός αμυντικού συστήματος που βασίστηκε κυρίως σωρευτικά

εμπόδια εισόδου, ή όπως θα λέγαμε σήμερα, η άμυνα σε βάθος. Ένα κάστρο χρησιμοποιείται, επειδή είναι μια εικόνα που είναι γνωστή σχεδόν σε όλους. Αν έχετε επισκεφθεί ποτέ ένα μεσαιωνικό κάστρο ή έχετε δει μια ταινία με μεσαιωνικό θέμα θα θυμάστε ότι η πρώτη γραμμή άμυνας είναι συχνά η τάφρος. Η τάφρος είναι ένα φράγμα που έχει σχεδιαστεί για να σταματά τους ανθρώπους από το να φτάσουν στο τείχος του κάστρου. Οι τάφροι περιλαμβάνουν συχνά επικίνδυνα πλάσματα (αλιγάτορες, πιράνχας) που θα προσθέσουν ένα δεύτερο επίπεδο προστασίας εντός του ίδιου φραγμού. Στη συνέχεια, υπάρχουν τα τείχη του κάστρου. Αυτά έχουν σχεδιαστεί για να αποκρούσουν τους εχθρούς. Στην κορυφή των τοίχων μικρές οπές που επιτρέπουν στους τοξότες να πυροβολούν τον εχθρό, ενώ εξακολουθούν να είναι σε θέση να κρύβονται. Υπάρχουν πόρτες διαφόρων μεγεθών μέσα στους τοίχους, μια πύλη και μια γέφυρα για την πόρτα πάνω από την τάφρο. Σε όλα τα σημεία εισόδου έχουν τοποθετηθεί φρουροί. Για άλλη μια φορά, είναι πολλαπλά επίπεδα προστασίας που εφαρμόζονται στο ίδιο επίπεδο. Το



Εικόνα 6.62

τρίτο αμυντικό στρώμα είναι η αυλή μέσα στα τείχη του κάστρου. Αυτό έχει σχεδιαστεί ως «Πεδίο θανάτωσης» έτσι ώστε αν οι εχθροί καταφέρουν να παραβιάσουν τα τείχη του κάστρου, θα βρεθούν μέσα σε μια εσωτερική ζώνη που δεν προσφέρει κάλυψη από επιτιθέμενους που βρίσκονται είτε στο εξωτερικά τείχη του κάστρου ή εντός του ίδιου του κάστρου. Το τέταρτο στρώμα άμυνας είναι το ίδιο το κάστρο. Αυτό είναι το κύριο κτίριο μέσα στο οποίο βρίσκονται τα κοσμηματοπωλεία. Είναι σχεδιασμένο να είναι υπερασπίζεται από μόνο του, οι σκάλες είναι στενές και τα δωμάτια είναι διατεταγμένα για να συγχέουν τον εχθρό. Το πέμπτο και τελευταίο στρώμα προστασίας είναι το θησαυροφυλάκιο που βρίσκεται στην καρδιά του κάστρου. Είναι δύσκολο να προσεγγιστεί και να φυλάσσεται ιδιαίτερα.

Φυσικά, αυτή είναι μια στοιχειώδης περιγραφή των αμυντικών που περιλαμβάνονται σε ένα κάστρο όπου Μεσαιωνικοί μηχανικοί δούλεψαν πολύ σκληρά για να συμπεριλάβουν πολλαπλά αμυντικά συστήματα σε κάθε επίπεδο προστασίας. Αλλά εξυπηρετεί το σκοπό του. Ένα σύστημα άμυνας πληροφορικής μπορεί να σχεδιαστεί στο ίδιο μοτίβο ως CDS. Ακριβώς όπως το CDS, το σύστημα προστασίας πληροφορικής απαιτεί επίπεδα προστασίας. Σύμφωνα λοιπόν με αυτό το μοντέλο πέντε επίπεδα προστασίας φαίνονται κατάλληλα. Ξεκινώντας από το εσωτερικό αυτά είναι:

- **Επίπεδο 1:** Κρίσιμες πληροφορίες. Η καρδιά του συστήματος είναι οι πληροφορίες που θέλετε να προστατεύσετε. Αυτό είναι το θησαυροφυλάκιο πληροφοριών.
- **Επίπεδο 2:** Φυσική προστασία. Τα μέτρα ασφάλειας φυσικής προστασίας πρέπει πάντα να ξεκινούν με ένα επίπεδο φυσικής προστασίας για συστήματα πληροφοριών. Αυτό συγκρίνεται με το ίδιο το κάστρο.
- **Επίπεδο 3:** «Σκλήρυνση» του λειτουργικού συστήματος. Μόλις εφαρμοστούν οι φυσικές άμυνες πρέπει να «σκληρύνετε» το λειτουργικό σύστημα κάθε υπολογιστή για να περιορίσετε την πιθανότητα επίθεσης όσο το δυνατόν περισσότερο. Αυτή είναι η αυλή.
- **Επίπεδο 4:** Πρόσβαση σε πληροφορίες. Όταν δίνετε πρόσβαση στα δεδομένα σας, θα πρέπει να βεβαιωθείτε ότι όλοι είναι εξουσιοδοτημένοι και ελεγμένοι. Αυτό είναι το τείχος του κάστρου και οι πόρτες που ανοίγετε μέσα από αυτό.
- **Επίπεδο 5:** Εξωτερική πρόσβαση. Το τελευταίο επίπεδο προστασίας αφορά τον εξωτερικό κόσμο. Περιλαμβάνει το περιμετρικό δίκτυο και όλες τις άμυνες του. Είναι η τάφρος του κάστρου.

Αυτό είναι το Σύστημα Άμυνας του Κάστρου (CDS). Για να γίνει πλήρης πολιτική ασφάλειας, πρέπει να συμπληρώνεται από δύο στοιχεία: άτομα και διαδικασίες. Αυτά τα δυο στοιχεία περιβάλλουν το CDS και συμπληρώνουν την εικόνα πολιτικής ασφαλείας που αντιπροσωπεύει. Ο καθορισμός των διαφόρων επιπέδων άμυνας δεν είναι η μόνη απαίτηση για μια πολιτική ασφάλειας, αλλά είναι ένα σημείο εκκίνησης. Υπάρχουν πολλές άλλες δραστηριότητες οι οποίες θα πρέπει να εκτελεσθούν για να συμπληρωθεί ο ορισμός της πολιτικής ασφαλείας. Αυτά αποτελούν τη βάση του σχεδιαγράμματος ασφαλείας.

Το σχέδιο ασφαλείας

Όπως αναφέρθηκε προηγουμένως, η πολιτική ασφάλειας είναι μόνο το πρώτο βήμα για ένα ολοκληρωμένο σχέδιο ασφαλείας. Μόλις δημιουργηθεί η πολιτική, πρέπει να σχεδιαστούν και να εφαρμοστούν οι άμυνες του συστήματος οι οποίες πρέπει να παρακολουθούνται, να δοκιμάζονται και να ενημερώνονται τακτικά. Οι τέσσερις δραστηριότητες διαχείρισης ασφαλείας (σχεδιασμός πολιτικής, αμυντικός σχεδιασμός, παρακολούθηση και δοκιμές) είναι το σχέδιο ασφαλείας. Το κλειδί για ένα σωστό σχέδιο ασφαλείας είναι να γνωρίζουμε τι πρέπει να καλύψουμε και να μάθουμε γιατί χρειάζεται να καλύπτεται. Το πρώτο μέρος, τι πρέπει να καλύψουμε, περιγράφεται στο CDS. Προσδιορίζει όλους τους τομείς που απαιτούν προστασία από την πολιτική ασφάλειας και βοηθά να είμαστε προετοιμασμένοι για κάθε πιθανότητα.

Το επόμενο είναι ο αμυντικός σχεδιασμός. Εδώ, το πρώτο βήμα βρίσκεται γνωρίζοντας τον τύπο των επιθέσεων που μπορεί να αντιμετωπισθούν. Μερικά παραδείγματα περιλαμβάνουν:

- **Παραβίαση ασφαλείας κατά λάθος.** Αυτές οι επιθέσεις προκαλούνται συνήθως από χρήστες ή διαχειριστές συστήματος. Προέρχονται από την έλλειψη ευαισθητοποίησης για θέματα ασφάλειας. Για παράδειγμα, οι χρήστες που δεν προστατεύουν τους κωδικούς πρόσβασης, επειδή δεν γνωρίζουν τις συνέπειες, μπορεί να είναι η αιτία τυχαίων επιθέσεων. Ομοίως, οι διαχειριστές που τοποθετούν χρήστες σε λάθος ομάδες ασφαλείας και τους εκχωρήσουν λάθος δικαιώματα μπορούν επίσης να είναι η αιτία της παραβίασης.
- **Εσωτερική επίθεση.** Αυτές είναι μία από τις σημαντικότερες πηγές επιθέσεων. Στην πραγματικότητα, ήταν η κύρια πηγή επίθεσης, αλλά με τον πολλαπλασιασμό επιθέσεων που βασίζονται στο Διαδίκτυο, η σημασία τους σε σχέση με όλες τις άλλες επιθέσεις έχει μειωθεί. Προέρχονται από το εσωτερικό δίκτυο. Η πηγή τους μπορεί να είναι το προσωπικό του οργανισμού ή άλλο προσωπικό στο οποίο επιτρέπεται η πρόσβαση στο εσωτερικό δίκτυο. Αυτές οι επιθέσεις είναι συχνά αποτέλεσμα της έλλειψης επαγρύπνησης. Το εσωτερικό προσωπικό συχνά υποθέτει ότι εσωτερικά το δίκτυο προστατεύεται και όλοι όσοι έχουν πρόσβαση σε αυτό μπορούν να είναι αξιόπιστοι.
- **Κοινωνική μηχανική**. Για άλλη μια φορά, αυτές οι επιθέσεις προέρχονται από την έλλειψη συνειδητοποίησης. Αυτές προκαλούνται από εξωτερικές πηγές που πλαστοπροσωπούν εσωτερικό προσωπικό και παραπλανούν τους χρήστες να αποκαλύψουν εμπιστευτικές πληροφορίες, για παράδειγμα, κάποιος που καλεί έναν χρήστη ενώ πλαστοπροσωπεί το γραφείο βοήθειας και ζητά από τον χρήστη τον κωδικό πρόσβασής του, επειδή στον οργανισμό είναι κοινή πρακτική για το προσωπικό του γραφείου βοήθειας να ζητάει από τους χρήστες τον κωδικό πρόσβασής τους. Δεν υπάρχει λόγος το γραφείο βοήθειας προσωπικού να ζητά από τους χρήστες τον κωδικό πρόσβασης τους.
- **Οργανωτική επίθεση**. Αυτές οι επιθέσεις προέρχονται από ανταγωνιστικούς οργανισμούς που θέλουν να διεισδύσουν στον οργανισμό και να ανακαλύψουν τα εμπορικά μυστικά του.
- **Αυτοματοποιημένες επιθέσεις.** Αυτές είναι τώρα ένας από τους πιο συνηθισμένους τύπους επιθέσεων. Βασικά ένας εξωτερικός υπολογιστής σαρώνει

διευθύνσεις Διαδικτύου μέχρι να βρει μια απάντηση. Μόλις βρει μια διεύθυνση σαρώνει αυτήν τη διεύθυνση για να ανακαλύψει τα τρωτά της σημεία. Αυτές οι επιθέσεις έχουν γίνει εξαιρετικά εξελιγμένες σήμερα..

- **Κατανεμημένη άρνηση υπηρεσίας (DDoS).** Αυτές οι επιθέσεις έχουν σχεδιαστεί για να υπερφορτώνουν τη λειτουργία μιας υπηρεσίας στο δίκτυό. Προέρχονται συχνά από διάφορες πηγές. Επιθέσεις που στοχεύουν γενικές τεχνολογίες της Microsoft και όχι έναν οργανισμό συγκεκριμένα είναι εξαιρετικά παραδείγματα επιθέσεων DDoS.
- **Επιθέσεις ιών.** Αυτές οι επιθέσεις έχουν τη μορφή ιών, σκουληκιών ή Δούρειων ίππων και έχουν σχεδιαστεί για να διεισδύσουν στα συστήματά του οργανισμού ώστε να προκαλέσουν κάποια μορφή ζημιάς τόσο σε υπηρεσίες όσο και σε δεδομένα.
- **Κακόβουλα e-mail ή phishing**. Αυτές οι επιθέσεις στοχεύουν το ανυποψίαστο θύμα από παρασύροντάς το να εκτελέσει μια ενέργεια που θα δώσει στον εισβολέα πρόσβαση στο σύστημά του. Η εκπαίδευση των χρηστών είναι ένας από τους καλύτερους τρόπους για την αποτροπή αυτών των τύπων επίθεσης.

Κάθε τύπος επίθεσης απαιτεί διαφορετική στρατηγική άμυνας. Τα περισσότερα καλύπτονται με το CDS, αλλά πρέπει επίσης να καθοριστούν οι διαδικασίες που περιλαμβάνουν επιθέσεις και αντιδράσεις σε επιθέσεις. Αυτός είναι ο πυρήνας του αμυντικού σχεδιασμού.

Ασφάλεια των Windows Server 2008

Η Microsoft έχει δημιουργήσει έναν εξαιρετικό οδηγό για την ασφάλεια των τεχνολογιών των Windows Server 2008, τον Οδηγό Ασφαλείας WS08. Αυτός ο οδηγός χρησιμοποιεί μια προσέγγιση που είναι παρόμοια με το CDS που χρησιμοποιούμε εδώ για να περιγράψουμε την ασφάλεια στα Windows Server 2008.

Ο Windows Server 2008 είναι ένα από τα βασικά στοιχεία της πρωτοβουλίας Trusted Computing Initiative της Microsoft. Ως εκ τούτου, η Microsoft έχει επανεξετάσει και βελτιώσει τις βασικές δυνατότητες ασφαλείας που περιλαμβάνονται στις προηγούμενες εκδόσεις. Τεχνολογίες όπως το Kerberos, το σύστημα αρχείων κρυπτογράφησης (EFS), η υποδομή δημόσιου κλειδιού (PKI), η έξυπνη κάρτα και η βιομετρική υποστήριξη, και ειδικά οι υπηρεσίες τομέα Active Directory, για να αναφέρουμε μερικές, είναι σημαντικές βελτιώσεις σε σχέση με τις βασικές δυνατότητες ασφαλείας παλαιότερων εκδόσεων των Windows, όπως το NT.

Με τα WS08, η Microsoft έχει βελτιώσει αυτές τις δυνατότητες, καθώς έχεις προσθέσει και νέες δυνατότητες ασφαλείας. Το .NET Framework από μόνο του είναι μια σημαντική βελτίωση της ασφάλειας από μόνη της, επειδή φέρνει μαζί του την έννοια του διαχειριζόμενου κώδικα, κώδικα που ταιριάζει εντός των ορίων που έχουν ορισθεί. Ενισχύει σημαντικά την ικανότητα εκτέλεσης ασφαλούς κώδικα, επειδή παρέχει το περιβάλλον εκτέλεσης για λογισμικό, περιορίζοντας την πιθανότητα σφαλμάτων στον κώδικα που εκτελείτε. Προσδιορίζει επίσης εάν ο κώδικας υπογράφεται ψηφιακά από κάποιον έμπιστο, καθώς και την προέλευσή του, διασφαλίζοντας υψηλότερο βαθμό εμπιστοσύνης στο περιβάλλον εκτέλεσης.

Επιπλέον, τα WS08 προσφέρουν πολλές άλλες νέες και βελτιωμένες δυνατότητες που βοηθούν στην ασφάλεια του συστήματος σε όλα τα επίπεδα. Φυσικά, το ιδανικό επίπεδο προστασίας που μπορεί να αποκτηθεί με τα WS08 εξαρτάται από τον πελάτη που χρησιμοποιείτε. Τα χαρακτηριστικά ασφαλείας του WS08 περιλαμβάνουν:

- **Πολιτικές περιορισμού λογισμικού.** Αυτές οι πολιτικές μπορούν να ελέγχουν ποιος κώδικας επιτρέπεται να εκτελείται εντός του δικτύου. Αυτό περιλαμβάνει οποιονδήποτε τύπο κώδικα (εταιρικές εφαρμογές, εμπορικό λογισμικό, σενάρια, αρχεία δέσμης) και μπορεί ακόμη και να οριστεί σε επίπεδο Dynamic Link Library (DLL). Αυτό είναι ένα εξαιρετικό εργαλείο για να αποτραπεί την εκτέλεση κακόβουλων σεναρίων και στο δίκτυό του οργανισμού.
- **Η υποστήριξη ασύρματου LAN.** Περιλαμβάνει ειδικά αντικείμενα πολιτικής σχεδιασμένα για την υποστήριξη ασφαλούς ασύρματου δικτύου.
- **Ο έλεγχος ταυτότητας απομακρυσμένης πρόσβασης.** περιλαμβάνει μια δομή βάσει πολιτικής για τη διαχείριση απομακρυσμένης πρόσβασης και εικονικών ιδιωτικών συνδέσεων δικτύου μέσω ADDS. Αυτή η δυνατότητα επικεντρώνεται σε έναν βελτιωμένο διακομιστή ελέγχου ταυτότητας Διαδικτύου (IAS) και έναν διακομιστή απομακρυσμένου ελέγχου ταυτότητας (RADIUS).
- **Προστασία πρόσβασης δικτύου (NAP).** Εκτός από τις βελτιώσεις στην απομακρυσμένη πρόσβαση, τα WS08 μπορούν πλέον να επιβάλλουν τα επίπεδα *'υγείας'* των πελατών πριν τους επιτραπεί να συνδεθούν στο δίκτυό. Το NAP μπορεί ακόμη και να ενημερώσει τους πελάτες προτού τους δοθεί πλήρης πρόσβαση στο δίκτυο.
- **Τείχος προστασίας διακομιστή.** Με προηγμένη ασφάλεια Προκειμένου να διευκολυνθούν οι συνδέσεις που κάνουν τα απομακρυσμένα συστήματα με τους διακομιστές, τα WS08 παρέχουν μια ολοκληρωμένη διεπαφή για ασφάλεια επιπέδου IP (IPSec), με στοιχεία ελέγχου εισερχόμενων και εξερχόμενων επικοινωνιών.
- **Λειτουργίες πολλαπλών δασών.** Τα δάση Υπηρεσιών τομέα υπηρεσίας καταλόγου Active Directory των WS08 μπορούν να χρησιμοποιούν εμπιστευτικά δίκτυα για να επεκτείνουν τις δυνατότητες ελέγχου ταυτότητας του καταλόγου τους με συνεργαζόμενους οργανισμούς. Επιπλέον, η χρήση των υπηρεσιών Active Directory Lightweight Directory Services (ADLDS) επιτρέπει να δημιουργηθεί ένας κατάλογος κεντρικού λειτουργικού συστήματος (NOS) και στη συνέχεια ο απαιτούμενος αριθμός καταλόγων εφαρμογών για να υποστηριχθούν οι εταιρικές ανάγκες εφαρμογών. Τέλος, οι υπηρεσίες Active Directory Federation Services (ADFS) επιτρέπουν την συνεργασία με συνεργαζόμενους οργανισμούς χωρίς να δημιουργηθεί εμπιστοσύνη στο δάσος, βασισμένο στους εσωτερικούς καταλόγους NOS του άλλου οργανισμού.
- **Η υποδομή δημόσιου κλειδιού.** Περιλαμβάνει βελτιωμένο PKI, Active Directory Certificate Services (ADCS), που υποστηρίζει αυτόματη εγγραφή και αυτόματη ανανέωση πιστοποιητικού X.509. Υποστηρίζει επίσης τη χρήση λιστών ανάκλησης πιστοποιητικών δέλτα (CRL), απλοποιώντας τη διαδικασία διαχείρισης CRL.
- **Ασφάλεια διακομιστή Web.** Οι υπηρεσίες πληροφοριών Internet (IIS) έκδοση 7 είναι ασφαλείς από προεπιλογή. Δεν εγκαθίσταται από προεπιλογή και, μόλις εγκατασταθεί, θα προβάλλει περιεχόμενο μόνο με βάση εγκατεστημένα στοιχεία.

- **Προσωρινή και offline προστασία αρχείων.** Τα WS08 υποστηρίζουν την κρυπτογράφηση προσωρινών και εκτός σύνδεσης αρχείων, καθώς και την προστασία κρυπτογραφημένων δεδομένων κατά τη μεταφορά, μέσω του πρωτοκόλλου Secure Sockets Tunneling Protocol (SSTP).
- **Διαχείριση διαπιστευτηρίων.** Το Credential Manager μπορεί να αποθηκεύσει με ασφάλεια κωδικούς πρόσβασης και ψηφιακά πιστοποιητικά (X.509). Αυτό υποστηρίζει την απρόσκοπτη πρόσβαση σε πολλές ζώνες ασφαλείας.
- **Η κρυπτογράφηση λειτουργίας πυρήνα.** Υποστηρίζει εγκεκριμένους κρυπτογραφικούς αλγόριθμους Federal Information Processing Standard (FIPS). Αυτό σημαίνει ότι τόσο κυβερνητικοί όσο και μη κυβερνητικοί οργανισμοί μπορούν να επωφεληθούν από αυτήν την ενότητα κρυπτογραφίας για να διασφαλίσουν τις επικοινωνίες πελατών / διακομιστών. Το WS08 εφαρμόζει επίσης το Suite B κρυπτογραφικοί αλγόριθμοι που ορίζονται από την κυβέρνηση των ΗΠΑ. Αυτό σημαίνει ότι υποστηρίζει κρυπτογράφηση δεδομένων, ψηφιακές υπογραφές και ανταλλαγές κλειδιών, καθώς και κατακερματισμό, επιτρέποντας σε τρίτους προμηθευτές να βασίζονται σε αυτήν την υποδομή για να δημιουργήσουν πιο ολοκληρωμένες λύσεις ασφαλείας.
- **Το Digest Authentication Protocol (DAP)**. Περιλαμβάνει ένα νέο πακέτο ασφάλειας digest που υποστηρίζεται τόσο από τις υπηρεσίες IIS όσο και από τις υπηρεσίες τομέα Active Directory.
- **Ψηφιακά υπογεγραμμένα πακέτα Windows Installer.** Υποστηρίζει τη συμπερίληψη ψηφιακών υπογραφών στα πακέτα του Windows Installer, έτσι ώστε οι διαχειριστές να μπορούν να διασφαλίσουν ότι εγκαθίστανται μόνο αξιόπιστα πακέτα στο δίκτυο, ειδικά σε διακομιστές.
- **Πολλαπλές πολιτικές κωδικού πρόσβασης.** Το ADDS υποστηρίζει την εφαρμογή πολλαπλών πολιτικών κωδικού πρόσβασης, επιτρέποντάς στον οργανισμό να απαιτεί πολύ περίπλοκους κωδικούς πρόσβασης για διαχειριστές και λιγότερο περίπλοκους κωδικούς πρόσβασης για τελικούς χρήστες.
- **Ο έλεγχος πρόσβασης βάσει ρόλου.** Περιλαμβάνει τη διαχείριση εξουσιοδότησης, η οποία υποστηρίζει τη χρήση ελέγχων πρόσβασης βάσει ρόλων (RBAC) για εφαρμογές. Οι εγγραφές RBAC μπορούν να είναι είτε σε Extensible Markup Language (XML) είτε σε Active Directory.
- **Αντιπροσωπεία ελέγχου ταυτότητας.** Υποστηρίζει περιορισμένη εκχώρηση. Αυτό σημαίνει ότι μπορούν να καθοριστούν ποιοι διακομιστές είναι αξιόπιστοι για την πλαστοπροσωπία των χρηστών στο δίκτυο. Μπορεί επίσης να προσδιοριστεί για ποιες υπηρεσίες είναι αξιόπιστος ο διακομιστής.
- **Διαχείριση δικαιωμάτων και απαρίθμηση βάσει πρόσβασης**. Είναι δυνατή η προβολή δικαιωμάτων μέσω του πλαισίου διαλόγου *Ιδιότητες* για αντικείμενα αρχείων και φακέλων. Επίσης, οι χρήστες θα μπορούν να βλέπουν μόνο αντικείμενα στα οποία έχουν πρόσβαση, σε αντίθεση με προηγούμενες εκδόσεις, όπου οι χρήστες θα μπορούσαν να δουν όλο το περιεχόμενο ενός φακέλου σε κοινή χρήση, ακόμη και αν δεν μπορούσαν να ανοίξουν τα έγγραφα.
- **Περιορισμένη πρόσβαση σε όλους**. Η ομάδα Everyone συνεχίζει να περιλαμβάνει πιστοποιημένους χρήστες και επισκέπτες, αλλά τα μέλη της ομάδας *Ανώνυμοι* δεν αποτελούν πλέον μέρος της ομάδας Everyone.

- **Το Auditing Auditing στα WS08 βασίζεται πλέον σε λειτουργίες.** Αυτό σημαίνει ότι είναι πιο περιγραφικό και προσφέρει την επιλογή των λειτουργιών που θα ελέγχουν τους χρήστες ή τις ομάδες. Μπορούν επίσης να ελεγχθούν οι αλλαγές ADDS και να χρησιμοποιηθούν τις αναφορές ελέγχου για να αντιστραφούν αυτές οι αλλαγές εάν πραγματοποιήθηκαν κατά λάθος.
- **Επαναφορά προεπιλογών.** Το εργαλείο Οδηγός διαμόρφωσης ασφαλείας (SCW) είναι ποιο απλό στην χρήση του με την βοήθεια του οποίου μπορούν να εφαρμοστούν ξανά τις ρυθμίσεις ασφαλείας του υπολογιστή από πρότυπα βάσης.
- **Προαιρετικά υποσυστήματα.** Τα προαιρετικά υποσυστήματα, όπως το POSIX (υποστήριξη για εφαρμογές UNIX), δεν είναι εγκατεστημένα από προεπιλογή.
- **Μικροί διακομιστές.** Μέσω της χρήσης του Core Server, μπορούν να αναπτυχθούν διακομιστές που παρέχουν ένα περιορισμένο σύνολο υπηρεσιών και μια μικρότερη πιθανότητα επίθεσης.
- **Ελεγκτές τομέα μόνο για ανάγνωση (RODCs).** Τα RODC παρέχουν μια πιο ασφαλή πλατφόρμα ελεγκτή τομέα (DC) για υποκαταστήματα ή περιμετρικά δίκτυα. Τα RODCS είναι δύσκολο να δεχθούν επίθεση, επειδή θα αποθηκεύουν προσωρινά τους κωδικούς πρόσβασης βάσει των πολιτικών χρήστη που έχουν ορισθεί. Επιπλέον, υπάρχει η δυνατότητα να επαναφερθούν αυτόματα τυχόν κρυφοί κωδικοί πρόσβασης σε περίπτωση κλοπής ενός RODC.
- **Περιορισμένοι ρόλοι και δυνατότητες.** Κάθε ρόλος ή χαρακτηριστικό εγκαθιστά μόνο στοιχεία που είναι απολύτως απαραίτητα για την εκτέλεση του. Αυτό σας επιτρέπει να ελέγχετε ακριβώς τι είναι εγκατεστημένο στους διακομιστές σας.
- **Ασφάλεια υπηρεσιών.** Οι υπηρεσίες είναι περιορισμένες και εκτελούνται μόνο σε συγκεκριμένα περιβάλλοντα. Επιπλέον, σε κάθε υπηρεσία επιτρέπεται μόνο η πρόσβαση σε στοιχεία του συστήματος που σχετίζονται με αυτήν.
- **Κρυπτογράφηση μονάδας δίσκου BitLocker.** Υπάρχει η δυνατότητα να κρυπτογραφηθούν πλήρως οι μονάδες δίσκου του συστήματος σε απομακρυσμένους διακομιστές, ώστε οι κακόβουλοι χρήστες να μην έχουν πρόσβαση στα περιεχόμενά τους.
- **Έλεγχος λογαριασμού χρήστη (UAC).** Με το UAC, οι διαχειριστές γνωρίζουν συνεχώς πότε χρησιμοποιούν πραγματικά αυξημένα διαπιστευτήρια για την εκτέλεση εργασιών, επειδή φαίνεται όταν ζητείτε εξουσιοδότηση. Αυτό παρέχει ένα επιπλέον επίπεδο προστασίας. Φυσικά, κάθε διαχειριστής θα πρέπει να λειτουργεί ως τυπικός χρήστης και να χρησιμοποιεί διαχειριστικά δικαιώματα μόνο όταν χρειάζεται να εκτελέσει μια διαχειριστική εργασία.
- **Προστασία πληροφοριών.** Με το Active Directory Rights Management Protection (ADRMS), μπορεί να διασφαλιστεί πλήρως το περιεχόμενο της πνευματικής ιδιοκτησίας, διασφαλίζοντας ότι δεν μπορεί να παραβιαστεί.
- **Έλεγχος συσκευής.** Μέσω του ελέγχου της συσκευής, μπορεί να διασφαλιστεί ότι κακόβουλοι χρήστες δεν μπορούν να συνδέσουν συσκευές Universal Serial Bus (USB) στους διακομιστές ή ακόμα και στους σταθμούς εργασίας , προκειμένου να κλέψουν το περιεχόμενο των κοινόχρηστων φακέλων ή των συνεργαζόμενων περιβαλλόντων.

Αυτή δεν είναι μια ολοκληρωμένη λίστα με όλες τις δυνατότητες ασφαλείας του Windows Server 2008, αλλά είναι μια λίστα με τις πιο σημαντικές δυνατότητες για δίκτυα. Αυτές οι

δυνατότητες, μαζί με τις βασικές δυνατότητες που προέρχονται από προηγούμενες εκδόσεις των Windows, αρκούν για να σχεδιαστεί το Castle Defense System.

Ασφάλεια στις ομάδες πόρων

Θα ακολουθηθεί μία διπλή προσέγγιση στον σχεδιασμό του CDS. Η πρώτη επικεντρώνεται στην ομάδα πόρων (resource pools). Αυτή η ομάδα πρέπει να περιλαμβάνει πολύ αυστηρές στρατηγικές προστασίας. Ως εκ τούτου, το CDS για ομάδες πόρων θα απαιτήσει να δοθεί ιδιαίτερη προσοχή στα επίπεδα που προσδιορίζονται στον Πίνακα 6.5.

Επίπεδο	Περιεχόμενο	Σχόλια
Επίπεδο 1	Κατηγοριοποίηση δεδομένων	Ιδιαίτερη προσοχή στα αρχεία που χρησιμοποιούνται για εικονικές μηχανές
	Ασφάλεια εφαρμογής	Ασφάλεια στο Hyper-V
Επίπεδο 2	Φυσικό περιβάλλον	Τα data center πρέπει να έχουν επαρκή ενέργεια και ψύξη
	Φυσικός έλεγχος	Οι server δεν θα πρέπει να είναι προσβάσιμοι χωρίς εξουσιοδότηση
	Επικοινωνίες	Οι διαχειριστές θα πρέπει να γνωρίζουν τις πολιτικές ασφαλείας
	Επιτήρηση	Να τηρούνται αρχεία εισόδου-εξόδου για τους διαχειριστές
Επίπεδο 3	Ρυθμίσεις ασφαλείας	Χρειάζονται ιδιαίτερη προσοχή τα ακόλουθα: - Διαμόρφωση πυρήνα διακομιστή - Ασφάλεια εφαρμογής - Ρυθμίσεις οδηγού διαμόρφωσης ασφαλείας για διακομιστές - Περιορισμένες εγκαταστάσεις ρόλων σε κάθε κεντρικό υπολογιστή. - Διαμόρφωση μηχανών εικονικής διαχείρισης BitLocker Drive Encryption - Έλεγχος λογαριασμού χρήστη (UAC) για όλους τους διαχειριστές - Έλεγχος συσκευής για να διασφαλιστεί ότι μη εγκεκριμένο USB οι μονάδες δίσκου δεν μπορούν να συνδεθούν σε κανέναν φυσικό διακομιστή.
	Anti-malware	Ρύθμιση του Windows Defender σε συνεργασία με κατάλληλα antivirus.

	ADDS ασφάλεια	Αυστηρή διαχείριση δικαιωμάτων και πολιτικές περιορισμού λογισμικού
	Σύστημα αρχείων	Ασφάλεια στο σύστημα αρχείων και απαίτηση ψηφιακής υπογραφής του Windows Installer για third-party λογισμικό
	Σύστημα εκτυπώσεων	
	Ασφάλεια .NET Framework	
	Ασφάλεια IIS	Υλοποίηση Web security
Επίπεδο 4	Ταυτοποίηση χρηστών	Απαίτηση smart card ¨η two factor authentication για τους διαχειριστές
	Πολιτικές ασφαλείας	Καθορισμός κατάλληλων πολιτικών ασφαλείας για τους πόρους
	Πρόσβαση σε πόρους	
	Role-based έλεγχος πρόσβασης	
	Παρακολούθηση/Έλεγχος πρόσβασης	Ενεργοποίηση του ADDS auditing
Επίπεδο 5	Virtual private networks (VPNs)	Οι διαχειριστές απομακρυσμένα θα πρέπει να συνδέονται με VPN
	Δρομολόγηση και απομακρυσμένη πρόσβαση	Υλοποίηση αυθεντικοποίησης για απομακρυσμένη πρόσβαση
	Secure Sockets Tunneling Protocol (SSTP)	Όλες οι απομακρυσμένες προσβάσεις θα πρέπει να είναι encrypted
	Υποδομή δημόσιου κλειδιού (PKI)	Υλοποίηση ADCS
	Network Access Protection (NAP)	Υλοποίηση NAP για να διασφαλιστεί ότι όλες οι συσκευές που συνδέονται στο δίκτυο έχουν το κατάλληλο επίπεδο “υγείας”

Πίνακας 6.5

Ασφάλεια στις εικονικές υπηρεσίες

Παρόμοια, οι εικονικές υπηρεσίες απαιτούν επίσης μια ειδική εφαρμογή του CDS. Σε αυτήν την περίπτωση, εστιάζουμε στα στοιχεία που προσδιορίζονται στον Πίνακα 6.6.

Οι εικονικές υπηρεσίες απαιτούν περισσότερη προσοχή στις ρυθμίσεις ασφαλείας, επειδή έχουν σχεδιαστεί για να αλληλεπιδρούν με τους τελικούς χρήστες. Ορισμένες τεχνολογίες ασφαλείας προορίζονται για τις εικονικές υπηρεσίες. Για παράδειγμα, υπάρχει μικρή ανάγκη εκτέλεσης του Server Core στα VSO, καθώς είναι εικονικές μηχανές. Είναι πιο σημαντικό να βεβαιωθούμε ότι εφαρμόζετε το κατάλληλο επίπεδο ασφάλειας σε μια πλήρη εγκατάσταση του WS08 από το να αναπτύξουμε Server Core σε εικονικές μηχανές. Στη συνέχεια αυτού του κεφαλαίου θα χρησιμοποιηθεί αυτός ο διαχωρισμός για να κατανοήσουμε καλύτερα πότε η ασφάλεια εφαρμόζετε στο σύνολο των πόρων, πότε σε εικονικές υπηρεσίες και πότε στα δύο.

Επίπεδο	Περιεχόμενο	Σχόλια
Επίπεδο 1	Κατηγοριοποίηση δεδομένων	Ιδιαίτερη προσοχή στα αρχεία που χρησιμοποιούνται για εικονικές μηχανές
	Ασφάλεια εφαρμογής	Ο κώδικας που δημιουργείτε για να τρέξει στις εικονικές μηχανές θα πρέπει να είναι ασφαλής
Επίπεδο 2	Φυσικό περιβάλλον	
	Φυσικός έλεγχος	
	Επικοινωνίες	Οι διαχειριστές και όλοι οι χρήστες θα πρέπει να γνωρίζουν τις πολιτικές ασφαλείας
	Επιτήρηση	Ότι είναι δυνατόν θα πρέπει να εφαρμόζετε
Επίπεδο 3	Ρυθμίσεις ασφαλείας	Χρειάζονται ιδιαίτερη προσοχή τα ακόλουθα: - Ασφάλεια εφαρμογής - Ρυθμίσεις οδηγού διαμόρφωσης ασφαλείας για διακομιστές - Περιορισμένες εγκαταστάσεις ρόλων σε κάθε εικονική μηχανή και μόνο με τα απαιτούμενα στοιχεία για την υπηρεσία που παρέχει. - Έλεγχος λογαριασμού χρήστη (UAC) για όλους τους χρήστες - Διαμόρφωση μηχανών εικονικής διαχείρισης BitLocker Drive Encryption - Έλεγχος συσκευής για να διασφαλιστεί ότι μη εγκεκριμένο USB οι μονάδες δίσκου δεν μπορούν να συνδεθούν σε κανέναν σημείο πρόσβασης συμπεριλαμβανομένου οποιοδήποτε υπολογιστή στο δίκτυο.
	Anti-malware	Ρύθμιση του Windows Defender σε συνεργασία με κατάλληλα antivirus.
	ADDS ασφάλεια	- Αυστηρή διαχείριση δικαιωμάτων και πολιτικές περιορισμού λογισμικού - Εφαρμογή πολιτικής κωδικών πρόσβασης ώστε να υπάρχει η απαίτηση πολύπλοκων κωδικών για τους διαχειριστές.
	Σύστημα αρχείων	Ασφάλεια στο σύστημα αρχείων και απαίτηση ψηφιακής υπογραφής του Windows Installer για third-party λογισμικό

	Σύστημα εκτυπώσεων	Υλοποίηση πλήρους στρατηγικής ασφαλείας για όλους τους εκτυπωτές.
	Ασφάλεια .NET Framework	Ισχύει για οποιοδήποτε μηχάνημα που έχει ρόλο εφαρμογής ή οποιοδήποτε μηχάνημα που περιλαμβάνει PowerShell
	Ασφάλεια IIS	Υλοποίηση Web security
Επίπεδο 4	Ταυτοποίηση χρηστών	- Απαίτηση smart card ή two factor authentication για τους διαχειριστές - Περιβάλλοντα που χρειάζονται υψηλή προστασία θα πρέπει να χρησιμοποιούν η two factor authentication για όλους τους χρήστες
	Πολιτικές ασφαλείας	Καθορισμός κατάλληλων πολιτικών ασφαλείας για το δίκτυο των VSO
	Πρόσβαση σε πόρους	- Έλεγχος της πρόσβασης σε πόρους. - Χρήση του ADLDS για προσαρμοσμένη πρόσβαση σε πόρους εφαρμογών.
	Role-based έλεγχος πρόσβασης	Υλοποίηση σε κάθε εφαρμογή όπου είναι εφικτό
	Παρακολούθηση/Έλεγχος πρόσβασης	Ενεργοποίηση του ADDS auditing
	Digital Rights Management (DRM)	Χρήση του ADRMS ώστε να εφαρμοστεί το DRM σε όλα τα έγγραφα που προστατεύονται από πνευματικά δικαιώματα ή με οποιονδήποτε άλλο τρόπο.
Επίπεδο 5	Virtual private networks (VPNs)	Απαίτηση VPN για όλες τις απομακρυσμένες συνδέσεις
	Δρομολόγηση και απομακρυσμένη πρόσβαση	Υλοποίηση αυθεντικοποίησης για απομακρυσμένη πρόσβαση
	Secure Sockets Tunneling Protocol (SSTP)	Όλες οι απομακρυσμένες προσβάσεις θα πρέπει να είναι encrypted
	Υποδομή δημόσιου κλειδιού (PKI)	Υλοποίηση ADCS
	Network Access Protection (NAP)	Υλοποίηση NAP για να διασφαλιστεί ότι όλες οι συσκευές που συνδέονται στο δίκτυο έχουν το κατάλληλο επίπεδο “υγείας”

Πίνακας 6.6

6.4.3. Εφαρμογή της πολιτικής ασφαλείας (Εφαρμογή του Castle Defense System)

Δεδομένου ότι σχεδιάζετε ένα νέο παράλληλο δίκτυο VSO που βασίζεται στα WS08, υπάρχει η δυνατότητα, και θα πρέπει, να ελεγχθεί ολόκληρη την υποδομή ασφαλείας, ειδικά επειδή έχετε τώρα υπάρχουν υποδομές για διαχείριση. Συνεπώς για να το κάνουμε αυτό βασιζόμαστε στο CDS. Εξετάζουμε καθένα από τα πέντε επίπεδα του και προσδιορίζουμε εάν απαιτούνται αλλαγές ή τροποποιήσεις στην υπάρχουσα προσέγγιση ασφαλείας.

Επίπεδο 1 - Κρίσιμες πληροφορίες

Οι οργανισμοί που θέλουν να λειτουργήσουν μέσα σε ένα δίκτυο, πρέπει να μοιράζονται δεδομένα. Πρέπει επίσης συχνά να επιτρέπουν στους χρήστες να αποθηκεύουν δεδομένα τοπικά στους σκληρούς τους δίσκους. Αυτό δεν είναι τόσο μεγάλο ζήτημα όταν ο χρήστης διαθέτει σταθμό εργασίας εντός του οργανισμού, επειδή έχει σχεδιαστεί για να παραμένει εντός του εσωτερικού δικτύου και έχουν εφαρμοστεί σε αυτόν πολιτικές ασφαλείας, αλλά καθίσταται κρίσιμο όταν ο σκληρός δίσκος εγκαταλείψει τις εγκαταστάσεις . Είναι το επίπεδο κινδύνου που πρέπει να προσδιοριστεί έτσι ώστε οι λύσεις που σχεδιάζονται για την προστασία των δεδομένων να είναι κατάλληλες.
Τα δεδομένα λοιπόν θα πρέπει να κατηγοριοποιηθούν. Αυτή η κατηγοριοποίηση πρέπει να ξεκινήσει με απογραφή όλων των δεδομένων στο δίκτυό του οργανισμού. Μόλις γίνει αυτό, μπορούμε να ομαδοποιήσουμε τα δεδομένα σε τέσσερις κατηγορίες:

- Δημόσιες πληροφορίες που μπορούν να κοινοποιούνται δημόσια εντός και εκτός του δικτύου.
- Εσωτερικές πληροφορίες που σχετίζονται με οργανωτικές λειτουργίες. Θεωρείται ιδιωτικό, αλλά όχι εμπιστευτικό. Ως εκ τούτου, θα πρέπει να προστατεύεται σε κάποιο βαθμό.
- Εμπιστευτικές πληροφορίες που δεν πρέπει να κοινοποιούνται σε μη εξουσιοδοτημένο προσωπικό. Για παράδειγμα, δεδομένα προσωπικού όπως μισθοί.
- Μυστικές πληροφορίες που είναι κρίσιμες για τη λειτουργία του οργανισμού. Εάν αυτές οι πληροφορίες κοινοποιούνται σε λάθος μέρη, ο ίδιος ο οργανισμός μπορεί να κινδυνεύει.

Για κάθε κατηγορία δεδομένων, θα πρέπει επίσης να προσδιοριστεί ποια στοιχεία κινδυνεύουν. Για παράδειγμα, εάν τα δεδομένα που βρίσκονται στον ιστότοπο του οργανισμού, δεδομένα δηλαδή που θεωρούνται δημόσια, τροποποιούνται χωρίς να το γνωρίζει ο οργανισμός, η φήμη του οργανισμού μπορεί να διακινδυνεύσει. Εάν τα δεδομένα μισθοδοσίας έχουν διαρρεύσει στον οργανισμό, θα χαθεί η εμπιστοσύνη των υπαλλήλων και πιθανώς θα υπάρχει μεγάλη δυσαρέσκεια εργαζομένων.

Οι πληροφορίες αποτελούνται από δύο στοιχεία: δεδομένα και έγγραφα. Τα δεδομένα συνήθως αποθηκεύονται σε δομημένους πίνακες και συνήθως βρίσκονται σε κάποιο τύπο βάσης δεδομένων. Τα έγγραφα περιέχουν μη δομημένα δεδομένα και βρίσκονται εντός διακριτών αντικειμένων, όπως αρχεία κειμένου, παρουσιάσεις, εικόνες ή άλλους τύπους εγγράφων. Και οι δύο τύποι πληροφοριών απαιτούν προστασία. Τα έγγραφα

προστατεύονται μέσω των δυνατοτήτων των συστημάτων αποθήκευσης αρχείων. Τα δεδομένα προστατεύονται σε δύο επίπεδα. Πρώτον, προστατεύεται μέσω των ίδιων μηχανισμών με τα έγγραφα, επειδή οι βάσεις δεδομένων αποθηκεύουν πληροφορίες σε αρχεία όπως τα έγγραφα. Δεύτερον, προστατεύεται μέσω των χαρακτηριστικών του συστήματος βάσης δεδομένων που χρησιμοποιείται για την αποθήκευσή τους. Για παράδειγμα, ο Microsoft SQL Server, ο οποίος αποθηκεύει βάσεις δεδομένων σε αρχεία .mdb, προσφέρει επίσης πολλές δυνατότητες ασφαλείας για τα δεδομένα που περιέχονται σε αυτά τα αρχεία. Εξαιτίας αυτού, οι οργανισμοί πρέπει επίσης να προσέχουν τη ασφάλεια των εφαρμογών, ειδικά όταν πρόκειται για δεδομένα, εάν θέλουν να προστατεύσουν απόλυτα τις πληροφορίες τους. Σε αυτήν την περίπτωση, αυτό σημαίνει να διασφαλιστεί ότι οι τρύπες ασφαλείας έχουν αφαιρεθεί όσο το δυνατόν περισσότερο στις εφαρμογές που έχει αναπτύξει ή αγοράσει ο οργανισμός. Σημαίνει επίσης ότι τα χαρακτηριστικά ασφαλείας της βάσης δεδομένων έχουν εφαρμοστεί για την προστασία των δεδομένων που περιέχει. Οι σειρές και οι στήλες που περιέχουν εμπιστευτικές και ασφαλείς πληροφορίες πρέπει να είναι ασφαλείς σε επίπεδο βάσης δεδομένων, ίσως ακόμη και κρυπτογραφημένες, και η πρόσβασή τους πρέπει να ελέγχετε.

Επίπεδο 2 - Φυσική προστασία

Το δεύτερο επίπεδο ασφάλειας έγκειται στη φυσική προστασία των υπολογιστικών συστημάτων. Η φυσική προστασία ασχολείται με διάφορα θέματα. Για παράδειγμα, ένας διακομιστής που βρίσκεται κάτω από μια σκάλα δεν μπορεί να θεωρηθεί ασφαλής με κανένα τρόπο. Αυτό το επίπεδο ασχολείται κυρίως με τις ομάδες πόρων, αλλά επεκτείνεται και στα υπολογιστικά συστήματα που είναι συνδεδεμένα στο δίκτυό του οργανισμού.
Τα στοιχεία που θα πρέπει να καλυφθούν στο επίπεδο φυσικής προστασίας περιλαμβάνουν:

- Γεωγραφική θέση. Η φυσική τοποθεσία των κτιρίων του οργανισμού είναι σε τοποθεσίες που απειλούνται από το περιβάλλον; Υπάρχει η πιθανότητα πλημμύρας, χιονοστιβάδων ή σπηλαίων που μπορεί να επηρεάσουν τα κτίρια στα οποία δραστηριοποιείτε; Βρίσκονται κοντά σε δρόμους όπου τα ατυχήματα ενδέχεται να επηρεάσουν το κτίριο;
- Κοινωνικό περιβάλλον. Γνωρίζει το προσωπικό του οργανισμού ότι η φυσική πρόσβαση σε οποιονδήποτε υπολογιστικό εξοπλισμό πρέπει να προστατεύεται ανά πάσα στιγμή; Γνωρίζουν ότι δεν πρέπει ποτέ να αποκαλύπτουν κωδικούς πρόσβασης σε καμία περίπτωση;
- Ασφάλεια κτιρίων Τα κτίριά του οργανισμού είναι ασφαλή; Αναγνωρίζονται οι επισκέπτες σε όλες τις τοποθεσίες; Οι επισκέπτες συνοδεύονται ανά πάσα στιγμή; Προστατεύεται η ηλεκτρική είσοδος του κτιρίου; Υπάρχουν αντίγραφα ασφαλείας, ειδικά για κέντρα δεδομένων; Προστατεύεται ο έλεγχος αέρα του κτηρίου και περιλαμβάνει εφεδρικό σύστημα; Υπάρχει καλό σχέδιο πυροπροστασίας σε όλα τα κτίρια; Είναι ασφαλής η καλωδίωση εντός και εκτός του κτιρίου; Είναι ασφαλείς οι ασύρματες εκπομπές;
- Κατασκευή κτιρίου. Είναι ασφαλής η κατασκευή του κτηρίου; Είναι οι τοίχοι στα κέντρα δεδομένων πυρίμαχοι; Είναι οι πόρτες κέντρων δεδομένων πυρίμαχες; Τα

δάπεδα καλύπτονται από αντιστατικό υλικό; Εάν υπάρχει γεννήτρια στις εγκαταστάσεις, βρίσκεται σε ασφαλή και προστατευμένη τοποθεσία; Προστατεύεται ο χώρος των υπολογιστών συστημάτων και των συστημάτων επικοινωνίας; Υπάρχουν στο κτίριο κάμερες ασφαλείας;

- Ασφάλεια διακομιστή. Οι διακομιστές βρίσκονται σε κλειδωμένα δωμάτια ή κλειδωμένα γραφεία σε όλες τις τοποθεσίες; Παρακολουθείται και προστατεύεται η πρόσβαση στα δωμάτια διακομιστών; Είναι οι ίδιοι οι διακομιστές ασφαλείς φυσικά; Ελέγχεται η πρόσβαση στον διακομιστή; Ο Windows Server 2008 υποστηρίζει τη χρήση έξυπνων καρτών για λογαριασμούς διαχειριστή. Σε πολύ ασφαλή περιβάλλοντα, θα πρέπει να εκχωρούνται έξυπνες κάρτες σε όλους τους διαχειριστές.
- Ασφάλεια BIOS. Όλες οι υπολογιστικές συσκευές θα πρέπει να έχουν κάποια μορφή προστασίας σε επίπεδο Basic Input Output System (BIOS). Για όλα τα συστήματα, οι ρυθμίσεις του BIOS πρέπει να προστατεύονται με κωδικό πρόσβασης, και όπως όλοι οι κωδικοί πρόσβασης, θα πρέπει να προστατεύονται ιδιαίτερα και να τροποποιούνται σε τακτική βάση. Τα εργαλεία διαχείρισης επιφάνειας εργασίας (DMI) επιτρέπουν τη συγκέντρωση της διαχείρισης κωδικών πρόσβασης BIOS.
- Ασφάλεια υπολογιστή. Είναι ασφαλείς οι σταθμοί εργασίας και οι φορητές συσκευές; Χρησιμοποιούνται συστήματα αναγνώρισης υλικού, όπως βιομετρικά και έξυπνες κάρτες, για κινητές συσκευές; Είναι ασφαλή τα δεδομένα στην κινητή συσκευή όταν η συσκευή βρίσκεται σε μεταφορά; Είναι ασφαλείς οι εξωτερικές συνδέσεις από τις κινητές συσκευές στο εσωτερικό δίκτυο; Ελέγχεται η σύνδεση των συσκευών USB;
- Ασφάλεια δικτύου. Είναι ασφαλές το δίκτυο και οι υπηρεσίες του; Για παράδειγμα είναι δυνατόν για κάποιον να εισαγάγει στους διακομιστές Dynamic Host Configuration Protocol (DHCP); Στα Windows Server 2008 οι διακομιστές DHCP πρέπει να έχουν εξουσιοδότηση να εκχωρούν διευθύνσεις, αλλά μόνο εάν είναι διακομιστές DHCP που βασίζονται σε Windows. Υπάρχει ασύρματο δίκτυο; Είναι ασφαλές;

Όλες οι φυσικές πτυχές των εγκαταστάσεων θα πρέπει να καταγραφούν και να τεκμηριωθούν. Η φυσική προστασία πρέπει να συμπληρώνεται από ένα πρόγραμμα παρακολούθησης. Κάθε υπάλληλος πρέπει να γνωρίζει ότι μπορεί και πρέπει να συμμετάσχει στην επιτήρηση τυχόν ύποπτης δραστηριότητας ή στην ειδοποίηση τυχόν ανεπιθύμητου συμβάντος που μπορεί να θέσει σε κίνδυνο τα πληροφοριακά συστήματα του οργανισμού.

Επίπεδο 3: «Σκλήρυνση» του λειτουργικού συστήματος

Το αντικείμενο της «σκλήρυνσης» του λειτουργικού συστήματος είναι να μειωθεί η επιφάνεια έκθεσης των συστημάτων του οργανισμού. Για επιτευχθεί αυτό, πρέπει να καταργηθεί οτιδήποτε δεν χρειάζεται σε ένα σύστημα. Τα Windows Server 2008 κάνουν καλή δουλειά από την αρχή επειδή εγκαθιστούν μόνο τα βασικά στοιχεία. Επιπλέον υπηρεσίες μπορούν να προστεθούν καθώς προστίθενται ρόλοι ή λειτουργίες. Επιπλέον,

οι υπηρεσίες IIS δεν εγκαθίστανται από προεπιλογή, γεγονός που διασφαλίζει ότι τα συστήματα που δεν το απαιτούν δεν το έχουν.
Αλλά ο περιορισμός του αριθμού των υπηρεσιών δεν είναι η μόνη δραστηριότητα που πρέπει να εκτελεσθεί. Πρέπει επίσης να καλυφθούν τα εξής:

- Διαμόρφωση ασφάλειας συστήματος
- Anti-malware
- Ασφάλεια στο Active Directory Domain Services
- Ασφάλεια συστήματος αρχείων
- Ασφάλεια συστήματος εκτύπωσης
- Ασφάλεια του .NET Framework
- Ασφάλεια του IIS
- Πλεονασμός συστήματος

Καθένα από αυτά τα στοιχεία απαιτεί ιδιαίτερη προσοχή τόσο για τις ομάδες πόρων όσο και για τις εικονικές υπηρεσίες.

Διαμόρφωση ασφάλειας συστήματος

Η διαμόρφωση ασφαλείας συστήματος περιλαμβάνει την εφαρμογή παραμέτρων ασφαλείας στο διακομιστή. Όταν εγκαθίσταται ένα μηχάνημα, ειδικά ένας διακομιστής, πρέπει να εκτελούνται ορισμένες τροποποιήσεις στην προεπιλεγμένη εγκατάσταση για να διασφαλιστεί ότι το μηχάνημά προστατεύεται. Αυτές οι δραστηριότητες εκτελούνται σε δύο επίπεδα:

- Το πρώτο επίπεδο επικεντρώνεται στην εκτέλεση ορισμένων τροποποιήσεων μετά την εγκατάσταση για λόγους ασφαλείας.
- Το δεύτερο επίπεδο περιλαμβάνει την εφαρμογή προτύπων ασφαλείας στο διακομιστή σύμφωνα με το ρόλο του. Το δεύτερο τμήμα της διαδικασίας διαμόρφωσης συστήματος βασίζεται στον Οδηγό Διαμόρφωσης Ασφαλείας για την αυτόματη εφαρμογή ρυθμίσεων ασφαλείας στο σύστημά.

Πολλά από τα στοιχεία που βρίσκονται στη λίστα ελέγχου μετά την εγκατάσταση μπορούν να αυτοματοποιηθούν μέσω της εφαρμογής προτύπων ασφαλείας.

Λίστα ελέγχου ασφαλείας μετά την εγκατάσταση

Για την καλύτερη ασφάλεια του διακομιστή θα πρέπει μετά την εγκατάσταση να γίνουν τα ακόλουθα:

- Μετονομασία του λογαριασμού διαχειριστή. Αυτή είναι μια δραστηριότητα που μπορεί να εκτελεστεί μέσω ενός προτύπου ασφαλείας, επειδή είναι μια ρύθμιση αντικειμένου πολιτικής ομάδας. Καλό είναι να χρησιμοποιηθεί ένα σύνθετο όνομα λογαριασμού και να εκχωρηθεί ένας σύνθετος κωδικό πρόσβασης.
- Αντιγραφή του λογαριασμού διαχειριστή για να δημιουργηθεί ένας εφεδρικός λογαριασμός.
- Δημιουργία ενός εικονικού λογαριασμού διαχειριστή και εκχώρηση μόνο δικαιωμάτων πρόσβασης επισκέπτη σε αυτόν. Χρήση ενός σύνθετου κωδικού πρόσβασης και για αυτόν τον λογαριασμό. Η δημιουργία εικονικού λογαριασμού

διαχειριστή χρησιμεύει ως παγίδα για χρήστες που θέλουν να προσπαθήσουν να αποκτήσουν πρόσβαση στον πραγματικό λογαριασμό διαχειριστή. Ελέγχοντας την πρόσβασή σε αυτόν το λογαριασμό μπορούμε για να δούμε ποιος προσπαθεί να διεισδύσει στα συστήματά του οργανισμού.

- Ο λογαριασμός επισκέπτη πρέπει να είναι απενεργοποιημένος.
- Επαλήθευση της λίστα των υπηρεσιών που εκτελούνται ώστε να και βεβαιωθούμε ότι είναι αυτές που πραγματικά χρειαζόμαστε. Επίσης πρέπει να τερματίσουμε οποιαδήποτε υπηρεσία θεωρείτε περιττή για αυτόν τον ρόλο διακομιστή.
- Επαλήθευση της λίστα ανοιχτών θυρών και κλείσιμο των θυρών που είναι περιττές για αυτόν τον ρόλο διακομιστή. Μπορούμε να προσδιορίσουμε τη λίστα ανοιχτών θυρών χρησιμοποιώντας την εντολή NETSTAT.
  netstat -a -n -o
  Η παράμετρος -a ζητά όλες τις θύρες, η παράμετρος -n ζητάει αριθμητική έξοδο για τις θύρες και η παράμετρος -o ζητά τη διαδικασία που σχετίζεται με τη θύρα.

Αυτό είναι για βασική ασφάλεια. Όλα τα υπόλοιπα μπορούν να εκτελεστούν μέσω του Οδηγού διαμόρφωσης ασφαλείας.

Πρότυπα ασφαλείας

Οι ρυθμίσεις ασφαλείας των Group Policy Objects αποθηκεύονται σε τρεις τοποθεσίες στον Windows Server 2008. Η πρώτη είναι στο ίδιο το GPO στην ενότητα
Πολιτικές → Ρυθμίσεις Windows → Ρυθμίσεις ασφαλείας και στις ρυθμίσεις παραμέτρων υπολογιστή και χρήστη. Η δεύτερη βρίσκεται σε ένα αρχείο προτύπου ασφαλείας. Σε πολλές περιπτώσεις, είναι καλύτερο να αποθηκεύουμε μια ρύθμιση σε ένα αρχείο προτύπου ασφαλείας, επειδή σχηματίζει αυτόματα ένα αντίγραφο ασφαλείας για τη ρύθμιση. Η τρίτη επιλογή μας επιτρέπει να δημιουργήσουμε πολύ πιο ολοκληρωμένες πολιτικές ασφαλείας μέσω του SCW. Οι πολιτικές ασφαλείας SCW μπορούν ακόμη και να ενσωματώσουν ρυθμίσεις προτύπων ασφαλείας.
Υπάρχουν διάφοροι τρόποι εφαρμογής προτύπων και ρυθμίσεων ασφαλείας. Το πρώτο είναι απευθείας μέσω ενός GPO εισάγοντας το πρότυπο σε αυτό. Αυτό γίνεται επιλέγοντας την εντολή Import Policy από το μενού περιβάλλοντος που εμφανίζεται όταν κάνουμε δεξί κλικ στο Security Settings στο Group Policy Editor. Αυτό εμφανίζει ένα παράθυρο διαλόγου που μας επιτρέπει να επιλέξουμε διαθέσιμα πρότυπα.
Τα εισαγόμενα πρότυπα μπορούν είτε να συγχωνευτούν είτε να αντικαταστήσουν όλες τις ρυθμίσεις ασφαλείας στο GPO. Η διαφορά εφαρμόζεται μέσω της επιλογής Clear This Database Before Importing στο πλαίσιο διαλόγου Import Policy. Με αυτήν την επιλογή θα διαγραφούν αυτόματα όλες οι ρυθμίσεις ασφαλείας στο GPO και θα εφαρμοστούν μόνο εκείνες που βρίσκονται στο πρότυπο.
Ο δεύτερος τρόπος είναι μέσω του Security Configuration Wizard. Αυτό το εργαλείο μάς επιτρέπει να δημιουργήσουμε μια ολοκληρωμένη πολιτική ασφαλείας για τους διακομιστές μας και, στη συνέχεια, να εφαρμόσουμε τις ρυθμίσεις σε μορφή προτύπου μέσω της Group Policy σε όλους τους διακομιστές των Windows. Μέσω των πολιτικών ασφαλείας, μπορούμε να διαμορφώσουμε τις ακόλουθες περιοχές ασφαλείας:

- Πολιτικές Λογαριασμού, Κωδικού Πρόσβασης, Κλειδώματος και Kerberos.

- Έλεγχος τοπικών πολιτικών, εκχωρήσεις δικαιωμάτων χρήστη και επιλογές ασφάλειας.
- Ρυθμίσεις καταγραφής συμβάντων για σύστημα, εφαρμογή, ασφάλεια, κατάλογο, αντιγραφή αρχείων και αρχεία καταγραφής υπηρεσίας DNS.
- Περιορισμένες ομάδες, Έλεγχος ιδιότητας μέλους ομάδας.
- Υπηρεσίες συστήματος, Λειτουργίες εκκίνησης και έλεγχος πρόσβασης για τις υπηρεσίες σε κάθε σύστημα.
- Έλεγχος πρόσβασης μητρώου για κλειδιά μητρώου.
- Σύστημα αρχείων, Έλεγχος πρόσβασης για φακέλους και αρχεία μέσω συστήματος αρχείων τεχνολογίας (NTFS).
- Πολιτικές ενσύρματου δικτύου (IEEE 802.3). Ελέγχει την πρόσβαση στο δίκτυο μέσω έξυπνων καρτών και άλλων ασφαλών συσκευών. Εφαρμόζει μεμονωμένη σύνδεση για το ενσύρματο δίκτυο.
- Τείχος προστασίας των Windows με ρυθμίσεις διακομιστή προηγμένων ελέγχων ασφαλείας και τείχος προστασίας υπολογιστή-πελάτη.
- Πολιτικές ασύρματου δικτύου (IEEE 802.11). Ελέγχει την πρόσβαση στο δίκτυο μέσω έξυπνων καρτών και άλλων ασφαλών συσκευών. Εφαρμόζει μεμονωμένη σύνδεση για το ασύρματο δίκτυο.
- Δημόσιο κλειδί. Ομαδοποιεί όλες τις πολιτικές που σχετίζονται με PKI. Για παράδειγμα, EFS, αξιόπιστες αρχές πιστοποιητικού ρίζας, αυτοματοποιημένη εκχώρηση πιστοποιητικών και άλλα.
- Πολιτικές περιορισμού λογισμικού. Ελέγχει ποιο λογισμικό επιτρέπεται να εκτελείται στο δίκτυο.
- Προστασία πρόσβασης δικτύου. Ελέγχει τη συμπεριφορά και την κατάσταση σύνδεσης υπολογιστών που δεν πληρούν τις απαιτήσεις υγείας.
- Πολιτικές ασφάλειας IP σε Active Directory Controls, ασφαλείς ρυθμίσεις επικοινωνίας μεταξύ πελατών και διακομιστών.

Το σύστημα βοήθειας των WS08 προσφέρει ολοκληρωμένες πληροφορίες σχετικά με καθεμία από αυτές τις ρυθμίσεις ασφαλείας. Από αυτά, μόνο τα πρώτα έξι επηρεάζονται από πρότυπα, και τρία από αυτά (υπηρεσίες συστήματος, μητρώο και ρυθμίσεις συστήματος αρχείων) είναι κατάλληλα για εφαρμογή τοπικών προτύπων ασφαλείας, επειδή ελέγχουν την πρόσβαση σε συγκεκριμένους τύπους αντικειμένων. Η εφαρμογή δικαιωμάτων ελέγχου πρόσβασης σε αρχεία, φακέλους, στο μητρώο και στη διαμόρφωση των υπηρεσιών συστήματος μπορεί να είναι αρκετά χρονοβόρα. Επομένως, είναι καλύτερο να διατηρήσουμε αυτές τις ρυθμίσεις σε τοπικά πρότυπα ασφαλείας παρά να τις ορίσουμε απευθείας σε επίπεδο GPO, επειδή τα τοπικά πρότυπα ασφαλείας εφαρμόζονται χειροκίνητα (ή αυτόματα), ενώ τα GPO εφαρμόζονται επάνω στα Active Directory Domain Services.
Οι τοπικές πολιτικές ασφαλείας ορίζονται κατά την εκκίνηση του υπολογιστή και παρακάμπτονται πάντα από τις ρυθμίσεις στις πολιτικές των αντικείμενων.
Σε αντίθεση με τις προηγούμενες εκδόσεις των Windows Server, ο Windows Server 2008 δεν περιλαμβάνει προεπιλεγμένα πρότυπα στο σύστημα. Υπάρχουν, ωστόσο, πρότυπα που εφαρμόζονται σε ορισμένους ρόλους συστήματος.
Για παράδειγμα, τα DCs περιλαμβάνουν ένα προεπιλεγμένο πρότυπο DC. Τα προεπιλεγμένα πρότυπα, όταν είναι διαθέσιμα, αποθηκεύονται στο:

% SYSTEMROOT% \ SECURITY \ TEMPLATES. Πρέπει να ελέγχουμε προσεκτικά τις ρυθμίσεις σε αυτά τα πρότυπα προτού τις εφαρμόσουμε. Να σημειωθεί ότι ακόμη και τα πρότυπα της Microsoft ισχύουν μόνο για τις τρεις βασικές ρυθμίσεις: υπηρεσίες συστήματος, αρχείο και μητρώο.

Επιπλέον, ο Οδηγός Ασφαλείας των Windows Server 2008 περιλαμβάνει πρότυπα βάσει ρόλων για διακομιστές μελών γενικά, ελεγκτές τομέα, διακομιστές εφαρμογών, διακομιστές αρχείων και εκτυπώσεων, διακομιστές υποδομής δικτύου και διακομιστές Web που εκτελούν IIS. Όλα βασίζονται σε ένα πρότυπο βάσης. Υπάρχουν δύο βασικές γραμμές: μία για διακομιστές μελών και μία για ελεγκτές τομέα. Εκτός από τη γραμμή βάσης διακομιστή μέλους, υπάρχουν στοιχειώδη πρότυπα για κάθε ρόλο διακομιστή μέλους. Πρότυπα ασφαλείας μπορούν να αποκτηθούν τόσο από τον Οδηγό Ασφαλείας WS08 όσο και από εμπορικούς προμηθευτές.

Δημιουργία προτύπων για τις τοπικές εφαρμογές

Όταν δημιουργούμε πρότυπα για μία τοπική εφαρμογή, για παράδειγμα κατά την εγκατάσταση του υπολογιστή, ιδανικό είναι να ξεκινήσουμε από ένα πρότυπο βάσης. Όσον αφορά τους διακομιστές, θα χρειαστούμε τουλάχιστον δύο πρότυπα βάσης: ένα για ελεγκτές τομέα και ένα για διακομιστές μελών. Αυτά τα πρότυπα βάσης πρέπει να περιλαμβάνουν μόνο τρεις τύπους ρυθμίσεων: σύστημα αρχείων, μητρώο και ρυθμίσεις υπηρεσίας συστήματος. (Άλλες ρυθμίσεις ασφαλείας θα καλυφθούν με πρότυπα για εισαγωγή σε αντικείμενα πολιτικής ομάδας.)
Θα πρέπει να προσδιορίσουμε ποιες ρυθμίσεις ταιριάζουν καλύτερα στον οργανισμό μας, αλλά ακολουθούν ορισμένες προτάσεις για καθεμία από τις τρεις κατηγορίες:

- Το μητρώο πρέπει να είναι όσο το δυνατόν πιο ασφαλές. Πρώτα, βεβαιωνόμαστε ότι η πρόσβαση στον επεξεργαστή μητρώου ελέγχεται στο δίκτυό μας. Αυτό γίνεται περιορίζοντας την πρόσβαση τόσο στο REGEDT32.EXE όσο και στο REGEDIT.EXE μέσω GPO. (User Configuration → Policies → Administrative Templates → System → Prevent access to registry editing tools)
- Στη συνέχεια, καλό είναι να ασφαλίσουμε κάποια συγκεκριμένα κλειδιά στο ίδιο το μητρώο. Ο ευκολότερος τρόπος για να ασφαλίσουμε κλειδιά μητρώου και κυψέλες είναι να διαδώσουμε κληρονομικά δικαιώματα από το γονικό κλειδί σε δευτερεύοντα κλειδιά. Αλλά σε ορισμένες περιπτώσεις, αυτό μπορεί να μην είναι δυνατό.
- Ασφαλίζουμε επίσης αρχεία και φακέλους. Στην ιδανική περίπτωση, θα ασφαλίσουμε φακέλους και όχι αρχεία. Για άλλη μια φορά, η διάδοση είναι προτιμότερη αλλά δεν ισχύει πάντα εδώ.
- Πρέπει να είμαστε προσεκτικοί όταν ασφαλίζουμε αρχεία και φακέλους και να βεβαιωνόμαστε ότι δε τροποποιούμε τις ρυθμίσεις ασφαλείας σε αντικείμενα που ασφαλίζονται αυτόματα από τα WS08. Για παράδειγμα, δεν είναι καλή ιδέα να αντικαταστήσουμε τις ρυθμίσεις ασφαλείας στο φάκελο Documents and Settings, καθώς τα WS08 πρέπει να διαχειρίζονται αυτές τις ρυθμίσεις κάθε φορά που δημιουργείται ένα νέο προφίλ χρήστη.
- Επίσης, ορίζουμε τις υπηρεσίες συστήματος στην κατάλληλη λειτουργία εκκίνησης:

Automatic για υπηρεσίες που πρέπει να ξεκινήσουν κατά την εκκίνηση του υπολογιστή, Automatic (Delayed Start) για υπηρεσίες που πρέπει να ξεκινήσουν αλλά δεν απαιτούνται κατά την εκκίνηση, Manual όταν επιτρέπεται η εκκίνηση ενός χρήστη ή μιας υπηρεσίας, αλλά δεν χρειάζεται να ξεκινήσει αυτόματα, και Disabled όταν δεν απαιτείται η υπηρεσία. Μπορείτε να καταργήσετε υπηρεσίες που βρίσκονται σε κατάσταση αναπηρίας.

- Τέλος, μπορούμε να εφαρμόσουμε ασφάλεια σε κάθε υπηρεσία, περιορίζοντας τα δικαιώματα πρόσβασης για την έναρξη, τη διακοπή και τον έλεγχο άλλων υπηρεσιών. Εάν ορίσουμε ασφάλεια στις υπηρεσίες, πρέπει να βεβαιωθούμε ότι συμπεριλαμβάνουμε πάντα τόσο το Administrators group όσο και το System account, διαφορετικά, ενδέχεται να αντιμετωπίσουμε προβλήματα κατά την έναρξη των υπηρεσιών. Από προεπιλογή, τρία αντικείμενα έχουν πρόσβαση: Administrators, System account και η Interactive group.

Διαμόρφωση προτύπων ασφαλείας

Αφού εντοπίσουμε τα κλειδιά μητρώου, τα αρχεία, τους φακέλους και τις υπηρεσίες που θέλουμε να τροποποιήσουμε, μπορούμε να προχωρήσουμε στη δημιουργία ή την τροποποίηση των προτύπων ασφαλείας μας. Το πρώτο πράγμα που πρέπει να κάνουμε είναι να δημιουργήσουμε ένα πρότυπο ασφαλείας και μια κονσόλα διαμόρφωσης, καθώς καμία δεν είναι διαθέσιμη από προεπιλογή.

1. Μεταβαίνουμε στο μενού Start, επιλέγουμε Run, πληκτρολογούμε MMC, στη συνέχεια πατάμε Enter.
2. Στην κονσόλα MMC, επιλέγουμε File → Add/Remove Snap-in.
3. Στο παράθυρο διαλόγου Add or Remove Snap-in, επιλέγουμε Security Templates και κάνουμε κλικ στο κουμπί Add. Επαναλαμβάνουμε τη λειτουργία με το Security Configuration and Analysis snap-in. Κάνουμε κλικ στο OK για να επιστρέψουμε στην κονσόλα. Επιλέγουμε στο File → Save, ονομάζουμε την κονσόλα Security Console και κάνουμε κλικ στο OK.
4. Μπορούμε να προσθέσουμε τα δικά μας πρότυπα μέσω αυτής της κονσόλας. Από προεπιλογή, τα νέα πρότυπα θα βρίσκονται στο φάκελο DOCUMENTS/SECURITY/TEMPLATES. Για να δημιουργήσουμε ένα νέο πρότυπο, κάνουμε δεξί κλικ στο φάκελό μας και επιλέγουμε New Template. Δίνουμε ένα όνομα και μια περιγραφή και κάνουμε κλικ στο OK για να δημιουργηθεί. Λαμβάνουμε υπόψη ότι ξεκινάμε το πρότυπο από το μηδέν και θα πρέπει να ορίσουμε όλες τις ρυθμίσεις. Μεταβαίνουμε στο νέο μας πρότυπο και τροποποιούμε τις ρυθμίσεις του. Αναπτύσσουμε το πρότυπο για να δούμε τα συστατικά του.
5. Για να ορίσουμε την ασφάλεια μητρώου, κάνουμε δεξί κλικ στο Registry και επιλέγουμε Add Key. Στο παράθυρο διαλόγου Add Key, εντοπίζουμε το κλειδί που θέλουμε να ασφαλίσουμε και κάνουμε κλικ στο OK. Αποφασίζουμε εάν θέλουμε να μεταδώσουμε δικαιώματα σε δευτερεύοντα κλειδιά, να επαναφέρουμε δικαιώματα σε δευτερεύοντα κλειδιά ή να αποκλείσουμε την αντικατάσταση δικαιωμάτων σε αυτό το κλειδί. Χρησιμοποιούμε το κουμπί Edit Security για να ορίσουμε τα κατάλληλα δικαιώματα ασφαλείας και κάνουμε κλικ στο OK.

Επαναλαμβάνουμε για κάθε κλειδί ή δευτερεύον κλειδί που θέλουμε να ασφαλίσουμε.

6. Για να ορίσουμε την ασφάλεια αρχείων ή φακέλων, κάνουμε δεξί κλικ File System και επιλέγουμε Add File. Στο πλαίσιο διαλόγου Add File, εντοπίζουμε το αρχείο ή το φάκελο που θέλουμε να ασφαλίσουμε και κάνουμε κλικ στο OK. Ορίζουμε τα κατάλληλα δικαιώματα ασφαλείας και κάνουμε κλικ στο OK. Αποφασίζουμε εάν θέλουμε να μεταδώσουμε δικαιώματα στο αρχείο ή στον φάκελο, να επαναφέρουμε τα δικαιώματα στο αρχείο ή στον φάκελο ή να αποκλείσουμε την αντικατάσταση δικαιωμάτων σε αυτό το αρχείο ή φάκελο. Επαναλαμβάνουμε για κάθε αρχείο ή φάκελο που θέλουμε να ασφαλίσουμε.
7. Για να ορίσουμε την ασφάλεια στις υπηρεσίες συστήματος, επιλέγουμε System Services. Κάνουμε διπλό κλικ στην κατάλληλη υπηρεσία στο δεξιό τμήμα του παραθύρου, επιλέγουμε Define This Policy Setting In The Template, επιλέγουμε τη λειτουργία έναρξης και, εάν απαιτείται, κάνουμε κλικ στην επιλογή Edit Security για να τροποποιήσουμε τις ρυθμίσεις ασφαλείας. Κάνουμε κλικ στο OK όταν τελειώσουμε. Επαναλαμβάνουμε για κάθε υπηρεσία που θέλουμε να τροποποιήσουμε.

Μπορούμε να χρησιμοποιήσουμε αυτήν την κονσόλα για να δημιουργήσουμε τα δικά μας πρότυπα ή να τροποποιήσουμε αυτά που αποκτάμε από άλλες πηγές. Βεβαιωνόμαστε ότι έχουμε δοκιμάσει πλήρως όλα τα πρότυπα που σκοπεύουμε να αναπτύξουμε.

Χρησιμοποιήστε πρότυπα τοπικής ασφάλειας

Τα τοπικά πρότυπα ασφάλειας μπορούν να εφαρμοστούν με δύο τρόπους, μέσω ενός γραφικού εργαλείου που ονομάζεται Security Configuration and Analysis ή μέσω ενός εργαλείου γραμμής εντολών που ονομάζεται SECEDIT. Και οι δύο έχουν τις χρήσεις τους. Και οι δύο μπορούν να χρησιμοποιηθούν για την ανάλυση και τη διαμόρφωση ενός συστήματος βάσει ενός προτύπου ασφαλείας.

Η διαμόρφωση και ανάλυση ασφάλειας είναι ένα συμπληρωματικό πρόγραμμα MMC που παρέχει μια γραφική προβολή στη διαμόρφωση και ανάλυση του συστήματος. Αυτό μπορεί να είναι αρκετά χρήσιμο, καθώς βασίζεται στην ίδια διεπαφή που χρησιμοποιείτε είτε για να δημιουργήσουμε πρότυπα είτε για να τροποποιήσουμε αντικείμενα πολιτικής ομάδας. Το Snap-in έχει ήδη εφαρμοστεί στη νέα Μας κονσόλα ασφαλείας. Αυτό μας δίνει ένα εργαλείο για τη δημιουργία, τροποποίηση, εφαρμογή, ανάλυση και εισαγωγή ρυθμίσεων πολιτικής ασφαλείας.

Για να αναλύσουμε έναν υπολογιστή και να τον συγκρίνουμε με μια δεδομένη πολιτική ασφαλείας, χρησιμοποιούμε την ακόλουθη διαδικασία:

1. Κάνουμε δεξί κλικ στο Security Configuration and Analysis στην κονσόλα ασφαλείας και επιλέγουμε Open database.
2. Στο πλαίσιο διαλόγου Open Database, εντοπίζουμε την κατάλληλη βάση δεδομένων ή πληκτρολογούμε ένα νέο όνομα βάσης δεδομένων και, στη συνέχεια, κάνουμε κλικ στο OK. Η προεπιλεγμένη ρύθμιση διαδρομής είναι DOCUMENTS \ SECURITY \ DATABASES.
3. Στη συνέχεια, θα πρέπει να επιλέξουμε το πρότυπο ασφαλείας που θέλουμε να χρησιμοποιήσουμε για ανάλυση. Αυτό πρέπει να είναι ένα πρότυπο που έχει

προετοιμαστεί εκ των προτέρων. Επιλέγουμε το κατάλληλο πρότυπο και κάνουμε κλικ στο OK.

4. Για να αναλύσουμε το σύστημά μας, κάνουμε δεξί κλικ στην επιλογή Security Configuration and Analysis και επιλέγουμε Analyze Computer Now.
5. Δεδομένου ότι για κάθε λειτουργία ανάλυσης ή διαμόρφωσης απαιτείται αρχείο καταγραφής, εμφανίζεται ένα παράθυρο διαλόγου για να μας ρωτήσει τη θέση του. Η προεπιλεγμένη ρύθμιση διαδρομής είναι
   DOCUMENTS \ SECURITY \ LOGS
   και το προεπιλεγμένο όνομα είναι το ίδιο με τη βάση δεδομένων. Πληκτρολογούμε το όνομα ενός νέου αρχείου καταγραφής, χρησιμοποιούμε το κουμπί Browse για να εντοπίσουμε ένα υπάρχον αρχείο ή κάνουμε κλικ στο OK για να αποδεχτούμε το προεπιλεγμένο όνομα.
6. Η ανάλυση ξεκινά. Μόλις ολοκληρωθεί η ανάλυση, μπορούμε να δούμε τη διαφορά στις ρυθμίσεις μεταξύ του προτύπου και του υπολογιστή. Απλώς μεταβαίνουμε σε μια ρύθμιση που θέλουμε να προβάλουμε και την επιλέγουμε. Οι διαφορές (εάν υπάρχουν) θα εμφανιστούν στο δεξιό τμήμα του παραθύρου.
7. Μπορούμε επίσης να προβάλουμε το αρχείο καταγραφής. Για να το κάνουμε αυτό, κάνουμε δεξί κλικ στο Security Configuration and Analysis και επιλέγουμε View Log. Το αρχείο καταγραφής θα εμφανιστεί στο δεξιό τμήμα του παραθύρου. Για να επιστρέψουμε στη βάση δεδομένων, απλώς διαγράφουμε το View Log στο μενού περιβάλλοντος.
8. Μπορούμε να τροποποιήσουμε τις ρυθμίσεις της βάσης δεδομένων ώστε να συμμορφώνονται με τις τιμές που θέλουμε να εφαρμόσουμε μεταβαίνοντας στην κατάλληλη τιμή και κάνοντας διπλό κλικ σε αυτήν. Επιλέγουμε Ορισμός αυτής της πολιτικής στη βάση δεδομένων, τροποποιούμε τη ρύθμιση και κάνουμε κλικ στο OK.
9. Χρησιμοποιούμε το δεξί κουμπί του ποντικιού για να εμφανιστεί το μενού περιβάλλοντος Security Configuration and Analysis και επιλέγουμε Save για να αποθηκεύσουμε τις τροποποιήσεις που κάνουμε στη βάση δεδομένων.
10. Για να διαμορφώσουμε έναν υπολογιστή με τις ρυθμίσεις στη βάση δεδομένων, επιλέγουμε Configure Computer Now από το ίδιο μενού περιβάλλοντος. Για άλλη μια φορά, θα πρέπει να καθορίσουμε τη θέση και το όνομα του αρχείου καταγραφής.
11. Κλείνουμε την κονσόλα ασφαλείας όταν τελειώσουμε.

Μπορούμε επίσης να αυτοματοποιήσουμε την εφαρμογή προτύπων σε διαφορετικά μηχανήματα με την χρήσης της εντολής SECEDIT. Μια τυπική εντολή για να γίνει αυτό θα μοιάζει με αυτό:

secedit / configigure / db filename.sdb / log filename.log

Επιπλέον, η χρήση του διακόπτη / verbose θα δημιουργήσει ένα αρχείο καταγραφής που είναι πολύ λεπτομερές. Εάν δεν έχει καθοριστεί αρχείο καταγραφής, το SECEDIT θα καταγράφει αυτόματα όλες τις πληροφορίες στο αρχείο SCESRV.LOG στο φάκελο

%WINDIR% \ SECURITY \ LOGS.

Ωστόσο, επειδή το πρότυπο τοπικής ασφάλειας επηρεάζει μόνο το σύστημα αρχείων, το μητρώο και τις υπηρεσίες συστήματος, πρέπει να διασφαλίσουμε ότι η εντολή που χρησιμοποιούμε ισχύει μόνο για αυτά τα τμήματα του προτύπου. Για να το κάνουμε αυτό, χρησιμοποιούμε την ακόλουθη εντολή:

secedit / configigure / db filename.sdb / log filename.log / areas REGKEYS FILESTORE SERVICES / quiet

Αυτή η εντολή θα διασφαλίσει ότι εφαρμόζονται μόνο οι κατάλληλες περιοχές, διασφαλίζοντας την εφαρμογή της γραπτής πολιτικής ασφαλείας μας. Επιπλέον, ο διακόπτης / silent θα διασφαλίσει ότι δεν θα παρέχονται σχόλια κατά την εφαρμογή του προτύπου.
Η εντολή SECEDIT μπορεί να εισαχθεί σε μια αυτόματη εγκατάσταση συστήματος για να διασφαλιστεί ότι οι υπολογιστές είναι ασφαλείς μόλις εγκατασταθούν. Το SECEDIT είναι επίσης χρήσιμο για την τακτική επαλήθευση της ρύθμισης ασφαλείας, καθώς περιλαμβάνει επίσης το διακόπτη / analyze. Τόσο η ανάλυση όσο και η διαμόρφωση μπορούν να αυτοματοποιηθούν μέσω του Task Scheduler στο Control Panel. Η εντολή SECEDIT πρέπει να καταγραφεί σε ένα σενάριο για να λειτουργήσει ο αυτοματισμός.
Αυτές δεν είναι οι μόνες λειτουργίες που μπορούν να εκτελεστούν μέσω του SECEDIT. Μπορούμε να μάθουμε περισσότερα σχετικά με αυτήν την εντολή μέσω του συστήματος βοήθειας WS08 ή απλά πληκτρολογώντας SECEDIT στη γραμμή εντολών.

Βέλτιστες πρακτικές προτύπων ασφαλείας

Υπάρχουν μερικά βασικά σημεία που πρέπει να θυμόμαστε όταν χρησιμοποιούμε πρότυπα ασφαλείας:

- Οι ρυθμίσεις που έχουν εισαχθεί σε ένα πρότυπο ασφαλείας δεν αποθηκεύονται στο GPO έως ότου το πρότυπο ασφαλείας έχει εισαχθεί σε αυτό.
- Το πρότυπο ασφαλείας μπορεί να εφαρμοστεί ξανά σε τακτική βάση για να διασφαλιστεί ότι οι ρυθμίσεις που ενδέχεται να έχουν τροποποιηθεί επαναφέρονται στις κατάλληλες τιμές.
- Η εφαρμογή προτύπου μέσω SECEDIT το εφαρμόζει μόνο στην τοπική πολιτική. Κάθε ρύθμιση διένεξης που εφαρμόζεται μέσω της Πολιτικής ομάδας θα αντικαταστήσει τη ρύθμιση Τοπικής πολιτικής. Για αυτόν τον λόγο, θα πρέπει να περιορίσουμε τις τοπικές ρυθμίσεις σε αρχεία, φακέλους, στο μητρώο και τις υπηρεσίες.
- Εάν αποφασίσουμε να χρησιμοποιήσουμε την επιλογή Clear Database δεδομένων κατά την εισαγωγή προτύπων σε GPO, αυτό σημαίνει ότι δεν πρέπει ποτέ να τροποποιούμε απευθείας τις ρυθμίσεις ασφαλείας στα GPO μας, επειδή αυτές οι τροποποιήσεις θα παρακαμφθούν κατά την εισαγωγή ενός προτύπου.
- Να τεκμηριώνουμε πάντα τις αλλαγές GPO μας, ακόμα κι αν είναι αποθηκευμένες σε ένα πρότυπο ασφαλείας.

Τα πρότυπα ασφαλείας είναι χρήσιμα, αλλά τα Windows Server 2008 περιλαμβάνουν ένα πολύ πιο ισχυρό εργαλείο που μπορεί να μας επιτρέψει να ελέγξουμε πολλά περισσότερα στοιχεία ασφαλείας, το Security Configuration Wizard.

Security Configuration Wizard

Όπως μπορούμε να δούμε, τα πρότυπα ασφαλείας αφορούν μόνο μια συγκεκριμένη επιλογή των στοιχείων που πρέπει να ελέγξουμε για να δημιουργήσουμε μια πλήρη πολιτική ασφάλειας. Ο Security Configuration Wizard ξεπερνά πολύ τα πρότυπα ασφαλείας που μπορούμε να δημιουργήσουμε. Μπορεί επίσης να εισαγάγει πρότυπα ασφαλείας για να συμπεριλάβει τις ρυθμίσεις τους σε οτιδήποτε εφαρμόζουμε μέσω του SCW. Επιπλέον, ο SCW μας επιτρέπει να διαμορφώσουμε τα εξής:
• Καλύτερες διαμορφώσεις υπηρεσιών μέσω διαμορφώσεων βάση ρόλων
• Καλύτερη ασφάλεια του δικτύου
• Καλύτερες ρυθμίσεις μητρώου
• Εφαρμογή πολιτικής ελέγχου
Αυτά είναι τα προεπιλεγμένα στοιχεία ελέγχου που θα βρούμε στο SCW. Επιπλέον, μας επιτρέπει να ελέγχουμε την ασφάλεια των υπηρεσιών IIS, αρκεί να επιλέξουμε τον ρόλο του διακομιστή Web στη σελίδα Server Roles του οδηγού. Ίσως το καλύτερο μέρος του SCW είναι ότι παρέχει πλήρεις εξηγήσεις για καθεμία από τις ρυθμίσεις που θα τροποποιήσει.
Επιπλέον, το SCW περιλαμβάνει μια αντίστοιχη γραμμή εντολών, SCWCMD.EXE, η οποία μας επιτρέπει να παράγουμε μαζικά την εφαρμογή πολιτικών ασφαλείας που δημιουργούνται μέσω της γραφικής διεπαφής του SCW. Το SCW παράγει έξοδο σε μορφή XML, η οποία είναι ασυμβίβαστη από προεπιλογή με GPO. Για να μετατρέψουμε την έξοδο SCW σε αναγνώσιμη μορφή για συμπερίληψη σε GPO, πρέπει να χρησιμοποιήσουμε την ακόλουθη εντολή:

scwcmd transform /p:PolicyFile.xml /g:GPOName

Αυτή η εντολή μετατρέπει το αρχείο XML σε νέο συμβατό GPO και πρέπει να εκτελείται με δικαιώματα διαχειριστή τομέα. Οι πολιτικές αποθηκεύονται στο φάκελο %SYSTEMROOT% \ SECURITY \ MSSCW \ POLICIES. Το GPO που προκύπτει θα περιλαμβάνει το περιεχόμενο του αρχείου SCW XML σε διάφορες ενότητες του GPO. Αυτές οι ρυθμίσεις θα περιλαμβάνουν περιεχόμενο για ρυθμίσεις ασφαλείας, πολιτικές ασφάλειας IP και τείχος προστασίας των Windows. Οι πολιτικές SCW είναι πολύ πιο ισχυρές από οποιοδήποτε άλλο στοιχείο για εφαρμογή ασφαλείας στα Windows. Αυτό το νέο GPO πρέπει στη συνέχεια να συνδεθεί με κατάλληλες Object Unities που θα εφαρμοστεί.
Μπορούμε να χρησιμοποιήσουμε το SCW για να δημιουργήσουμε νέες πολιτικές, να επεξεργαστούμε υπάρχουσες πολιτικές, να εφαρμόσουμε πολιτικές και ίσως το καλύτερο χαρακτηριστικό του, να επαναφέρουμε την εκχώρηση μιας πολιτικής ασφαλείας. Οι πολιτικές ασφαλείας δημιουργούνται από μια διαμόρφωση διακομιστή βάσης. Στην ιδανική περίπτωση, όπου θα δημιουργήσουμε διακομιστές βάσης για κάθε ρόλο που σκοπεύουμε να αναπτύξουμε, θα πρέπει να δημιουργήσουμε μια πολιτική βάσης από

καθέναν από αυτούς τους διακομιστές και να εφαρμόζουμε την πολιτική κάθε φορά που εργαζόμαστε με έναν νέο διακομιστή για οποιονδήποτε συγκεκριμένο ρόλο.

Ασφαλείς πόροι μέσω ελέγχου συσκευής

Τα Windows Vista εισήγαγαν μια νέα δυνατότητα για το λειτουργικό σύστημα Windows: τη δυνατότητα διαμόρφωσης αφαιρούμενων ελέγχων συσκευών μέσω της χρήσης Group Policy. Αυτό γίνεται μέσω του ελέγχου των εγκαταστάσεων συσκευών. Αυτό μας επιτρέπει να ελέγχουμε ποιες συσκευές μπορούν να εγκατασταθούν σε ένα σύστημα. Για παράδειγμα, θα αποτρέψει έναν κακόβουλο χρήστη να συνδέσει μια αφαιρούμενη μονάδα δίσκου και να απομακρυνθεί με τις εμπιστευτικές μας πληροφορίες.

Δημιουργούμε μια εγκεκριμένη λίστα συσκευών στο δίκτυό μας και τη συμπεριλαμβάνουμε στο GPO μας. Για παράδειγμα, ενδέχεται να επιτρέψουμε στους χρήστες να εγκαταστήσουν ποντίκια USB και πληκτρολόγια, αλλά να τους απαγορεύσουμε να εγκαταστήσουν συσκευές μνήμης Flash ή εξωτερικές μονάδες δίσκου. Τα iPod της Apple, για παράδειγμα, είναι επίσης στην πραγματικότητα μονάδες δίσκου που μπορούν να χρησιμοποιηθούν για τη μεταφορά πολύ μεγάλων ποσοτήτων πληροφοριών, το ίδιο ισχύει και για τα έξυπνα τηλέφωνα. Επειδή δεν μπορούμε να απαγορεύσουμε τη χρήση αυτών των τύπων συσκευών στο δίκτυό μας, πρέπει να ελέγξουμε τη χρήση τους μέσω ενός κατάλληλα σχεδιασμένου GPO.

Βεβαιωνόμαστε ότι έχουμε εφαρμόσει στοιχεία αφαιρούμενης συσκευής στην ομάδα πόρων, έτσι ώστε κανείς να μην μπορεί να συνδέσει μια μονάδα USB με έναν διακομιστή και να τη χρησιμοποιήσει για να αφαιρέσει αντίγραφα των εικονικών μας μηχανών. Επιπλέον, πρέπει να το εφαρμόσουμε σε υπολογιστές που είναι συνδεδεμένοι στο VSO για να διασφαλίσουμε ότι κανείς δεν μπορεί να χρησιμοποιήσει έναν υπολογιστή για να συνδέσει μια συσκευή και να διασχίσει κάπως τον τομέα VSO στον τομέα συγκέντρωσης πόρων και να κλέψει εικονικές μηχανές. Η καλύτερη προστασία είναι η πλήρης προστασία.

Ασφαλέστερα συστήματα με κρυπτογράφηση μονάδων δίσκου BitLocker

Με την κυκλοφορία των Vista, η Microsoft παρουσίασε το BitLocker Full Drive Encryption Το BitLocker μας επιτρέπει να κρυπτογραφούμε τα περιεχόμενα του τόμου του λειτουργικού μας συστήματος, ώστε οι κακόβουλοι εισβολείς να μην έχουν πρόσβαση σε αυτά. Το BitLocker χρησιμοποιείται κυρίως για κινητά συστήματα ή συστήματα που περιέχουν ευαίσθητα δεδομένα και εξέρχονται από τον χώρο του οργανισμού μας.

Το BitLocker μπορεί επίσης να χρησιμοποιηθεί για την προστασία των δίσκων του διακομιστή, καθώς τα WS08 υποστηρίζουν πλήρως τις δυνατότητές του. Μπορούμε, για παράδειγμα, να εφαρμόσουμε το BitLocker σε όλες τις εικονικές μηχανές μας, έτσι ώστε ακόμη και αν κάποιος κλέψει τα αρχεία που το συνθέτουν, δεν θα μπορεί να έχει πρόσβαση σε δεδομένα που ενδέχεται να βρίσκονται μέσα τους. Αυτό, ωστόσο, είναι ένα ακραίο μέτρο που θα εφαρμοζόταν μόνο σε πολύ ασφαλή περιβάλλοντα, επειδή οποιαδήποτε κρυπτογράφηση προσθέτει ένα ορισμένο ποσό επιβάρυνσης στη λειτουργία ενός διακομιστή. Ένα πιο πιθανό σενάριο είναι η κρυπτογράφηση των μονάδων διακομιστή κεντρικού υπολογιστή που βρίσκονται σε απομακρυσμένα γραφεία.

Με αυτόν τον τρόπο, εάν κάποιος απομακρυνθεί με έναν φυσικό διακομιστή σε απομακρυσμένο γραφείο, όχι μόνο δεν θα έχει πρόσβαση σε καμία από τις εικονικές μηχανές, αλλά και οι διακομιστές του κεντρικού υπολογιστή μας θα προστατεύονται επίσης. Για να μπορέσουμε να χρησιμοποιήσουμε το BitLocker, το σύστημά μας πρέπει να πληροί τις ακόλουθες προδιαγραφές:

- Να περιλαμβάνει δύο διαμερίσματα NTFS: έναν τόμο συστήματος και έναν τόμο λειτουργικού συστήματος. Ο τόμος του συστήματος είναι το διαμέρισμα εκκίνησης και απαιτεί μόνο περίπου 1,5 GB χώρου.
- Να περιλαμβάνει μια μονάδα USB flash και ένα BIOS που υποστηρίζει την ανάγνωση και εγγραφή σε μια μονάδα USB Flash κατά την εκκίνηση.
- Στην ιδανική περίπτωση, να περιλαμβάνει ένα μικροτσίπ Trusted Protection Module (TPM) έκδοση 1.2.
- Στην ιδανική περίπτωση επίσης, να περιλαμβάνει ένα αξιόπιστο BIOS που βασίζεται σε Trusted Computing Group (TCG).

Όπως μπορούμε να δούμε, το BitLocker μπορεί να εκτελεστεί μέσω της χρήσης εξωτερικής μονάδας USB Flash. Αυτή η μονάδα flash θα αποθηκεύσει το κλειδί κρυπτογράφησης που χρησιμοποιείται για να κλειδώσουμε και να ξεκλειδώσουμε το διαμέρισμα του λειτουργικού συστήματος. Ωστόσο, η χρήση μονάδας USB αποτελεί κίνδυνο, καθώς μπορεί να χαθεί ή να κλαπεί. Αυτός είναι ο λόγος για τον οποίο είναι ιδανικό να χρησιμοποιούμε έναν διακομιστή που διαθέτει τα πλήρη στοιχεία TPM. Σε αυτήν την περίπτωση, το κλειδί κρυπτογράφησης αποθηκεύεται με ασφάλεια στο τσιπ TPM και δεν μπορεί να κλαπεί.

Εάν οι κεντρικοί διακομιστές που χρησιμοποιούμε για απομακρυσμένα γραφεία περιλαμβάνουν αυτές τις δυνατότητες και σκοπεύουμε να κρυπτογραφήσουμε το περιεχόμενό τους, χρησιμοποιούμε την ακόλουθη διαδικασία.

1. Ξεκινάμε δημιουργώντας δύο διαμερίσματα κατά την εγκατάσταση. Και τα δύο διαμερίσματα πρέπει να είναι πρωτεύοντα διαμερίσματα. Επιπλέον, το μικρότερο διαμέρισμα πρέπει να οριστεί ως ενεργό. Και τα δύο διαμερίσματα πρέπει να μορφοποιηθούν με NTFS. Μπορούμε να χρησιμοποιήσουμε το μέσο εγκατάστασης για να δημιουργήσουμε αυτά τα διαμερίσματα.
2. Εγκαθιστούμε τον Server Core στο διαμέρισμα του λειτουργικού συστήματος.
3. Μόλις εγκατασταθεί ο Server Core, εκτελούμε τις διαμορφώσεις μετά την εγκατάσταση.
4. Στη συνέχεια, εγκαθιστούμε τη δυνατότητα BitLocker:
   start /w ocsetup BitLocker
   Επανεκκινούμε το σύστημα μόλις εγκατασταθεί το BitLocker.
5. Μόλις γίνει επανεκκίνηση του συστήματος, θα είμαστε έτοιμοι να διαμορφώσουμε το BitLocker. Ξεκινάμε παίρνοντας το BitLocker για τη λίστα συμβατών δίσκων. Βεβαιωνόμαστε ότι έχουμε μεταβεί στον κατάλληλο φάκελο για να το κάνουμε αυτό.
   cd\windows\system32
   cscript manage-bde.wsf -status
6. Τώρα, κρυπτογραφούμε τη μονάδα δίσκου συστήματος:
   cscript manage-bde.wsf –on C: -RecoveryPassword NumericalKey

–RecoveryKey BitLockerDrive –StartupKey BitLockerDrive
Το BitLockerDrive είναι το γράμμα μονάδας δίσκου που δώσαμε στο διαμέρισμα συστήματος. Το NumericalKey είναι ένας 48ψήφιος αριθμός, χωρισμένος σε οκτώ ομάδες έξι ψηφίων, χρησιμοποιώντας ενωτικά για να διαχωρίσουμε τις ομάδες. Κάθε ομάδα έξι ψηφίων πρέπει να διαιρείται με 11, αλλά δεν μπορεί να είναι μεγαλύτερη από 720.896.

7. Μπορούμε να επαναλάβουμε αυτήν την εντολή για να κρυπτογραφήσουμε οποιαδήποτε άλλη μονάδα δίσκου στον κεντρικό διακομιστή.

Αυτό είναι μια απλή εντολή με ισχυρά αποτελέσματα. Βεβαιωνόμαστε ότι προστατεύουμε το κλειδί κρυπτογράφησης και φροντίζουμε να αποθηκεύσουμε τον κωδικό πρόσβασης ανάκτησης.

Εγκατάσταση εργαλείων Anti-malware

Ένα άλλο επίπεδο ασφάλειας σε όλα τα συστήματα είναι η μηχανή anti-malware (AM). Η εφαρμογή ενός πλήρους περιβάλλοντος ασφαλείας απαιτεί τη χρήση μιας ολοκληρωμένης λύσης για την προστασία από ιούς, anti-spam, anti-spyware και γενικής κατάργησης κακόβουλου λογισμικού. Αυτή δεν είναι συνάρτηση των Windows Server 2008, αλλά τα WS08 προσφέρουν ειδικές διεπαφές προγραμματισμού εφαρμογών (API) για την υποστήριξη σάρωσης αρχείων και αντικειμένων σε ένα σύστημα. Περιλαμβάνουν επίσης το Windows Defender, τη δωρεάν μηχανή anti-spyware της Microsoft, αλλά μόνο το anti-spyware δεν αρκεί. Αυτός είναι ο λόγος για τον οποίο η Microsoft συνεργάστηκε εκτενώς με κατασκευαστές anti-malware λογισμικού για να διασφαλίσει ότι οι λύσεις τους λειτουργούν καλά υπό πίεση και αξιόπιστα σε κάθε περίπτωση.
Μια ολοκληρωμένη λύση κατά του κακόβουλου λογισμικού θα πρέπει να περιλαμβάνει τα ακόλουθα στοιχεία:

- Κεντρική διαχείριση τόσο των πελατών όσο και των διακομιστών
- Αυτόματη εγκατάσταση και ανάπτυξη σε υπολογιστές-πελάτες και διακομιστές
- Κονσόλα διαχείρισης της Microsoft (MMC) για εργασίες διαχείρισης
- Αυτόματη λήψη νέων υπογραφών anti-malware
- Μεταβλητά προγράμματα λήψης για τη διανομή του φόρτου εργασίας λήψης
- Αυτόματο διαμοιρασμό υπογραφών σε όλους τους πελάτες
- Αυτόματη σάρωση συστήματος
- Κεντρική συλλογή όλων των αποτελεσμάτων σάρωσης
- Δημιουργία ειδοποιήσεων για την ανακάλυψη κακόβουλου λογισμικού
- Δυνατότητες αφαίρεσης Root-kit
- Ενσωμάτωση και υποστήριξη για Server Core
- Κεντρική καραντίνα εντοπισμένου κακόβουλου λογισμικού και αυτόματου καθαρισμού του μηχανήματος
- Εντοπισμό ασυνήθιστης συμπεριφοράς για τον εντοπισμό άγνωστου κακόβουλου λογισμικού
- Παροχή διαχείρισης βάσει πολιτικής
- Υποστήριξη για επιθεώρηση συστήματος ηλεκτρονικού ταχυδρομείου και βάσης δεδομένων
- Υποστήριξη από τον κατασκευαστή για εκκαθάριση κακόβουλου λογισμικού

Όποια και αν είναι η λύση που επιλέγουμε, πρέπει να βεβαιωνόμαστε ότι είναι πλήρως λειτουργική πριν χρησιμοποιήσουμε οποιοδήποτε μέσο για να συνδεθούμε με τον εξωτερικό κόσμο.

Πολιτικές περιορισμού λογισμικού

Η στρατηγική κατά του κακόβουλου λογισμικού δεν μπορεί να ολοκληρωθεί χωρίς υποστήριξη από τα Windows Server 2008 και την Group Policy. Τα WS08 περιλαμβάνουν ένα ειδικό σύνολο ρυθμίσεων GPO που προσδιορίζουν τον κωδικό που επιτρέπεται να εκτελείται και να λειτουργεί σε ένα δίκτυο. Αυτές είναι οι πολιτικές περιορισμού λογισμικού (SRP).

Αυτό το σύνολο ρυθμίσεων GPO μάς επιτρέπει να ελέγχουμε έναν άγνωστο κωδικό στο δίκτυό μας. Αν και τα SRP μάς επιτρέπουν να ελέγχουμε πάνω από 38 τύπους αρχείων - βασικά οτιδήποτε θεωρείται ως κώδικας - υπάρχουν δύο τύποι αρχείων που πρέπει να ελέγχουμε απόλυτα: σενάρια (scripts) και μακροεντολές (macros). Οι περισσότερες άγνωστες απειλές έρχονται με τη μορφή ενός από αυτούς τους δύο τύπους αρχείων. Εφόσον ελέγχουμε τι συμβαίνει στο δίκτυό μας, θα πρέπει να προσδιορίσουμε ρητά τα σενάρια και τις μακροεντολές που έχουν εξουσιοδοτηθεί να εκτελούνται στο δίκτυό μας.

Ο ευκολότερος τρόπος για να το κάνουμε αυτό είναι να υπογράψουμε ψηφιακά τα σενάρια και τις μακροεντολές μας. Η υπογραφή τοποθετεί ένα πιστοποιητικό PKI εντός του κώδικα. Στη συνέχεια, μπορούμε να ορίσουμε SRP που αποκλείουν όλα τα σενάρια και τις μακροεντολές, εκτός από αυτά που έχουν υπογραφεί με το πιστοποιητικό μας. Τα SRP ορίζονται στο Computer Configuration → Windows Settings → Security Settings → Software Restriction Policies. Αυτή η ενότητα είναι κενή από προεπιλογή. Πρέπει να ξεκινήσουμε επιλέγοντας New Software Restriction Policies από το μενού περιβάλλοντος. Στη συνέχεια, πρέπει να προσδιορίσουμε τις επεκτάσεις που θέλουμε να απαγορεύσουμε, να αλλάξουμε τη βασική πολιτική και να προσδιορίσουμε το πιστοποιητικό που εμπιστευόμαστε. Βεβαιωνόμαστε ότι δεν συμπεριλαμβάνουμε το SRP στην προεπιλεγμένη πολιτική τομέα. Με αυτόν τον τρόπο, εάν πρέπει να την απενεργοποιήσουμε για κάποιο λόγο, δεν θα απενεργοποιήσουμε την global domain security policy.. Θα πρέπει επίσης να συμπεριλάβουμε αρχεία του Windows Installer σε αυτήν την πολιτική για να βεβαιωθούμε ότι έχει εγκατασταθεί μόνο αποδεκτός κώδικας στα δίκτυά μας.

Για ομάδες πόρων, εκχωρούμε αυτήν την πολιτική σε ολόκληρο τον τομέα. Αυτό θα επηρεάσει όλους τους κεντρικούς διακομιστές. Για VSO, μπορεί να είμαστε ικανοποιημένοι με την εκχώρηση αυτής της πολιτικής μόνο σε υπολογιστές. Σε αυτήν την περίπτωση, την εκχωρούμε μέσω του Global PC GPO που εφαρμόζεται σε επίπεδο PC.

Ασφάλεια Active Directory Domain Services

Το Active Directory Domain Services απαιτεί επίσης σημαντική ασφάλεια. Στην πραγματικότητα, ολόκληρος ο σχεδιασμός των καταλόγων που έχουμε δημιουργήσει μέχρι σήμερα έχει γίνει με γνώμονα την ασφάλεια. Το σύνολο πόρων βασίζεται σε ένα δάσος τομέα, το οποίο είναι ασφαλές επειδή μόνο οι διαχειριστές αλληλεπιδρούν με αυτό. Το δίκτυο VSO χρησιμοποιεί την έννοια του προστατευόμενου δασικού τομέα ρίζας

(PFRD) και ενός παιδιού τομέα παραγωγής, ο οποίος εξασφαλίζει περιεχόμενο σε ολόκληρο το δάσος επιτρέποντας στους χρήστες να αλληλεπιδρούν με τον τομέα παραγωγής. Επιπλέον, η ιδέα της δημιουργίας οργανωτικών μονάδων και της ανάθεσης ορισμένων δραστηριοτήτων διαχείρισης σε άλλα άτομα του οργανισμού μας είναι ένα σημαντικό μέρος του τομέα ασφαλείας για το ADDS. Αλλά ανεξάρτητα από τα μέτρα ασφαλείας που εφαρμόζουμε στους καταλόγους μας, θα έχουμε πάντα ένα κενό, ότι πρέπει να εμπιστευόμαστε έμμεσα τους διαχειριστές μας. Φυσικά, το ADDS μάς επιτρέπει να περιορίσουμε τα δικαιώματα που παραχωρούμε σε διαφορετικά επίπεδα διαχειριστών, αλλά παρόλα αυτά, οι διαχειριστές που ορίζουμε πρέπει να είναι αξιόπιστοι. Διαφορετικά, όλα όσα κάνουμε για να προστατέψουμε τον κατάλογο θα είναι άχρηστα.

Ένα καλό μέρος για να ξεκινήσουμε είναι η επιβολή ασφαλών διοικητικών συνηθειών. Οι διαχειριστές ADDS, τόσο σε επίπεδο τομέα όσο και σε επίπεδο διακομιστή μέλους, πρέπει να χρησιμοποιούν λογαριασμούς περιορισμένης πρόσβασης για την καθημερινή τους εργασία και να χρησιμοποιούν την εντολή Run as Administrator για την εκτέλεση εργασιών διαχείρισης. Επειδή τα WS08 υποστηρίζουν τη χρήση έξυπνων καρτών για διαχειριστές, θα ήταν καλή ιδέα να τις εφαρμόσουμε. Αυτό θα σήμαινε έλεγχο ταυτότητας δύο παραγόντων για όλους τους διαχειριστές του δικτύου. Τα WS08 το υποστηρίζουν πλήρως και μειώνουν το βάρος διαχείρισης της έξυπνης κάρτας λόγω των νέων δυνατοτήτων, όπως η αυτόματη εγγραφή και η αυτόματη ενημέρωση για πιστοποιητικά δημόσιου κλειδιού. Ωστόσο, οι έξυπνες κάρτες μπορεί να είναι δαπανηρές στην εφαρμογή και προσθέτουν ένα άλλο επίπεδο διαχείρισης σε ένα ήδη πολύπλοκο σύστημα. Εξαιτίας αυτού, θα πρέπει να εξετάσουμε την εφαρμογή τους μόνο σε πιο αυστηρά ελεγχόμενα περιβάλλοντα. Για να βεβαιωθούμε ότι οι κατάλογοι ADDS είναι ασφαλείς, πρέπει να εκτελέσουμε τις ακόλουθες ενέργειες:

- Σχεδιάζουμε τη δομή υπηρεσιών τομέα Active Directory με γνώμονα την ασφάλεια
- Βεβαιωνόμαστε ότι κάθε τομέας περιέχει τουλάχιστον δύο ελεγκτές τομέα για την προστασία των δεδομένων στον τομέα.
- Εκτελούμε τα δάση σε πλήρως λειτουργική λειτουργία για να επωφεληθούμε από τα πιο πρόσφατα χαρακτηριστικά ασφαλείας.
- Βεβαιωνόμαστε ότι όλες οι υπηρεσίες που σχετίζονται με τον κατάλογο χρησιμοποιούν ενσωματωμένο κατάλογο, χώρο αποθήκευσης δεδομένων, για παράδειγμα, DNS
- Βεβαιωνόμαστε ότι χρησιμοποιούμε μια δομημένη στρατηγική πολιτικής ομάδας
- Δημιουργούμε όσο το δυνατόν περισσότερες προσαρμοσμένες κονσόλες μόνο για ανάγνωση.
- Διανέμουμε κονσόλες μέσω Terminal Services και εκχωρούμε μόνο δικαιώματα ανάγνωσης και εκτέλεσης σε αυτά.
- Βεβαιωνόμαστε ότι όλα τα δεδομένα καταλόγου προστατεύονται και μπορούν να τροποποιηθούν μόνο από τα σωστά άτομα στον οργανισμό μας.
- Διαχειριζόμαστε αποτελεσματικά τις ομάδες για να εκχωρήσουμε δικαιώματα στον κατάλογο.
- Βεβαιωνόμαστε ότι οι ευαίσθητες πληροφορίες που είναι αποθηκευμένες στον τομέα είναι κρυμμένες από αδιάκριτα μάτια.
- Βεβαιωνόμαστε ότι οι ελεγκτές τομέα μας προστατεύονται φυσικά.
- Βεβαιωνόμαστε ότι οι ελεγκτές τομέα μας εφαρμόζουν συγκεκριμένες τοπικές πολιτικές ασφαλείας.

- Διαμορφώνουμε τις δύο προεπιλεγμένες πολιτικές ομάδας τομέα πριν από τη δημιουργία θυγατρικών τομέων για να επωφεληθούμε από τη μετάδοση πολιτικής κατά τη δημιουργία τομέα.
- Εκχωρούμε μόνο τα δικαιώματα διαχείρισης που απαιτούνται και τίποτα άλλο τόσο στους διαχειριστές υπηρεσιών όσο και στους διαχειριστές δεδομένων.
- Χρησιμοποιούμε τον ρόλο Read-Only Domain Controller ανάλογα με την περίπτωση.
- Ελέγχουμε προσεκτικά τα δικαιώματα τροποποίησης και τροποποιούμε τα δικαιώματα ιδιοκτησίας.
- Εφαρμόζουμε μια ισχυρή πολιτική καθολικού λογαριασμού στον κατάλογο για τους διαχειριστές και μια ισχυρή για τους χρήστες.
- Έλεγχος πρόσβασης ευαίσθητου αντικειμένου στον κατάλογο.
- Προστατεύουμε τον κωδικό πρόσβασης επαναφοράς καταλόγου.
- Βεβαιωνόμαστε ότι έχουμε μια ολοκληρωμένη πολιτική δημιουργίας αντιγράφων ασφαλείας καταλόγου.
- Επαληθεύουμε τακτικά την αναπαραγωγή καταλόγου και παρακολουθούμε τα αρχεία καταγραφής συστήματος, ειδικά το αρχείο καταγραφής εντοπισμού σφαλμάτων.

Ασφάλεια εντός του καταλόγου

Όπως τα Windows NTFS, ο κατάλογος παρέχει κληρονομική ασφάλεια. Αυτό σημαίνει ότι όλα τα θυγατρικά αντικείμενα κληρονομούν τις ρυθμίσεις ασφαλείας του γονικού αντικειμένου. Αυτό που είναι ιδιαίτερο στον κατάλογο είναι ο τρόπος μεταβίβασης των δικαιωμάτων.

Τα ρητά δικαιώματα παρακάμπτουν πάντα τα κληρονομούμενα δικαιώματα, ακόμη και τα δικαιώματα άρνησης. Αυτό σημαίνει ότι είναι δυνατό να ορίσουμε ένα δικαίωμα άρνησης σε ένα γονικό αντικείμενο και να ορίσουμε ένα δικαίωμα άδειας για το θυγατρικό αντικείμενο. Για παράδειγμα, μπορείτε να αρνηθούμε το δικαίωμα List Contents σε ένα Organizational Unit (OU) και να ορίσουμε το δικαίωμα Allow List Contents σε εάν θυγατρικό OU εντός του προηγούμενου OU. Τα άτομα στα οποία δεν επιτρέπεται η πρόσβαση στο γονικό OU δεν θα μπορούν ποτέ να δουν ή να τροποποιήσουν το περιεχόμενό του, ούτε θα μπορούν να περιηγηθούν στον κατάλογο στο θυγατρικό OU, αλλά θα μπορούν να αναζητήσουν τον κατάλογο για να εντοπίσουν τα περιεχόμενα μέσα στο παιδί OU.

Όπως το NTFS, ο κατάλογος προσφέρει δύο επίπεδα εκχώρησης δικαιωμάτων. Το πρώτο ομαδοποιεί αναλυτικά δικαιώματα σε κατηγορίες όπως Full Control, Read, Write, Execute και ούτω καθεξής. Για να προβάλουμε τις ρυθμίσεις ασφαλείας για ένα αντικείμενο, πρέπει να κάνουμε δεξί κλικ σε αυτό και να επιλέξουμε Properties (σε μία από τις κονσόλες ADDS). Κάνοντας κλικ στο κουμπί Advanced αυτού του παραθύρου διαλόγου οδηγούμαστε στα λεπτομερή δικαιώματα ασφαλείας Διάφοροι τύποι πληροφοριών είναι διαθέσιμοι εδώ. Αρχικά, μας δίνει πρόσβαση σε ειδικές λειτουργίες ασφαλείας, όπως Permissions, Audit, Owner, και Effective Permissions. Κάθε καρτέλα περιγράφει διαφορετικές πληροφορίες. Η καρτέλα Permissions, για παράδειγμα, προσδιορίζει εάν τα δικαιώματα κληρονομούνται και, εάν ναι, από ποιο container ή εάν είναι ρητά. Η καρτέλα Auditing προσδιορίζει τις πολιτικές ελέγχου που εφαρμόζονται στο

αντικείμενο. Η καρτέλα Owner παραθέτει τους διάφορους κατόχους αυτού του αντικειμένου. Τέλος, τα Effective Permissions μάς επιτρέπουν να προσδιορίσουμε τα προκύπτοντα δικαιώματα για μια δεδομένη αρχή ασφαλείας. Κάνουμε κλικ στην επιλογή Select για να εντοπίσουμε τον χρήστη ή την ομάδα για την οποία θέλουμε να δούμε τα Effective Permissions.

Εάν θέλουμε να προβάλουμε ή να εκχωρήσουμε συγκεκριμένα δικαιώματα, επιστρέφουμε στην καρτέλα Permissions και κάνουμε κλικ στην επιλογή Add or Edit. Αυτό εμφανίζει το παράθυρο διαλόγου Permissions Entry. Εδώ μπορούμε να εκχωρήσουμε συγκεκριμένα δικαιώματα σε χρήστες ή ομάδες.

Αυτό το επίπεδο λεπτομέρειας μπορεί να κάνει τη διαχείριση των αδειών καταλόγου αρκετά περίπλοκη. Διατηρούμε πάντα τα δικαιώματα καταλόγου μας όσο το δυνατόν πιο απλά και προσπαθούμε να χρησιμοποιούμε όσο το δυνατόν περισσότερα κληρονομικά δικαιώματα.

Πολιτικές κωδικού πρόσβασης

Στο ιδανικό περιβάλλον, θα θέλαμε πολύ ισχυρούς κωδικούς πρόσβασης για όλους όσους μπορούν συνδεθούν στο δίκτυό μας. Προφανώς, αυτό θα μπορούσε να συμβεί μόνο σε έναν τέλειο κόσμο. Πάντα θα υπάρχουν χρήστες που δυσκολεύονται να δουλέψουν με πολύ περίπλοκους κωδικούς πρόσβασης ή που πρέπει να γράψουν οτιδήποτε χρησιμοποιούν για να αποκτήσουν πρόσβαση σε ένα σύστημα εάν είναι περισσότεροι από μερικοί χαρακτήρες.

Στο παρελθόν, αυτό σήμαινε ότι έπρεπε να μειώσουμε την πολιτική κωδικών πρόσβασης στον χαμηλότερο κοινό παρονομαστή και να το κάνουμε τόσο απλό ή τόσο περίπλοκο όσο οι χρήστες μας μπορούν να χειριστούν. Αυτό συνέβαινε επειδή οι τομείς ADDS μπορούσαν να χειριστούν έναν μόνο λογαριασμό και, επομένως, την πολιτική κωδικού πρόσβασης ανά τομέα. Αλλά στα Windows Server 2008, αυτό δεν συμβαίνει πλέον. Πλέον το ADDS περιλαμβάνει λεπτομερείς πολιτικές κωδικού πρόσβασης (FGPPs), τη δυνατότητα καθορισμού πολλών πολιτικών κωδικού πρόσβασης σε έναν μόνο τομέα. Μαζί με τις πολιτικές κωδικού πρόσβασης, μπορούμε να εκχωρήσουμε διαφορετικούς περιορισμούς κλειδώματος λογαριασμού σε διαφορετικές ομάδες χρηστών.

Η δημιουργία FGPPs είναι αρκετά απλή. Ξεκινάμε καθορίζοντας σε ποιους χρήστες, ομάδες και OU σκοπεύουμε να βασιστούμε για να εφαρμόσουμε το FGPP. Στη συνέχεια συμπληρώνουμε τις νέες ομάδες που θέλουμε να δημιουργήσουμε, καθορίζουμε τα αντικείμενα ρυθμίσεων κωδικού πρόσβασης (PSO) που χρειαζόμαστε για να εφαρμόσουμε τις πολιτικές και τέλος, τα εφαρμόζουμε. Μπορούμε να δημιουργήσουμε όσα FGPP χρειαζόμαστε, αλλά καλό είναι να έχουμε τουλάχιστον δύο: ένα για διαχειριστές και ένα για χρήστες. Μπορούμε, φυσικά, να δημιουργήσουμε πολλά περισσότερα, αλλά καλό είναι να θυμόμαστε ότι όσο πιο περίπλοκο κάνουμε το περιβάλλον μας, τόσο πιο περίπλοκο θα είναι να το διαχειριστούμε και τόσο πιο πιθανό είναι να προκύψουν σφάλματα.

Έλεγχος ADDS

Τα Windows Server υποστήριξαν τον έλεγχο των συμβάντων ADDS από την πρώτη έναρξη της υπηρεσίας καταλόγου Active Directory στα Windows 2000. Τα ελεγμένα συμβάντα αποθηκεύονται στο αρχείο καταγραφής συμβάντων από προεπιλογή, αλλά αυτά τα συμβάντα ήταν ελλιπή, καθώς θα μας έλεγαν μόνο ότι ένα αντικείμενο είχε άλλαξε και τίποτα άλλο. Με τα WS08, η Microsoft βελτίωσε τις δυνατότητες ελέγχου καταλόγου. Τώρα δεν μπορούμε μόνο να δούμε ακριβώς τι έχει αλλάξει, αλλά και να δούμε προηγούμενες τιμές. Επιπλέον, μπορούμε ακόμη και να χρησιμοποιήσουμε αυτές τις προηγούμενες τιμές για να επαναφέρουμε τις ρυθμίσεις σε ό, τι ήταν πριν από την αλλαγή.

Οι κατάλογοι είναι περίτεχνα περιβάλλοντα. Με το ADDS, η Microsoft έχει εφαρμόσει ένα ισχυρό περιβάλλον που υποστηρίζει ταυτότητα και διαχείριση. Στην πραγματικότητα, πολλοί οργανισμοί που βασίζονται σε αυτήν την υπηρεσία καταλόγου δημιούργησαν πολύ περίπλοκες δομές καταλόγου και επέτρεψαν σε αρκετούς χειριστές να ελέγχουν διαφορετικά στοιχεία του καταλόγου. Στα Windows 2000, δεν υπήρχε παρακολούθηση ή προειδοποίηση όταν ένας χειριστής πραγματοποιούσε μια αλλαγή, για παράδειγμα, μετακίνηση μιας OU από τη μία θέση στην άλλη μέσα στον κατάλογο. Η μετακίνηση αντικειμένων είναι μια δύσκολη διαδικασία στο ADDS, καθώς μπορεί να αλλάξει σε μεγάλο βαθμό τη συμπεριφορά του συστήματος, επειδή τα εκχωρημένα GPO ενδέχεται να μην ισχύουν πλέον για αυτήν ή χειρότερα θα εφαρμοστούν λάθος GPO. Αυτός είναι ο λόγος για τον οποίο η Microsoft πρόσθεσε μια προειδοποίηση στα Windows Server 2003 κάθε φορά που οι χειριστές μετακινούσαν ένα αντικείμενο. Το πρόβλημα με αυτήν την προειδοποίηση, ωστόσο, είναι ότι παρείχε στους χειριστές τη δυνατότητα να την απενεργοποιήσουν, επαναφέροντας το σύστημα στις ρυθμίσεις των Windows 2000.

Στα WS08, η Microsoft πήγε ένα βήμα παραπέρα, πρόσθεσε μια νέα δυνατότητα προστασίας σε αντικείμενα που δημιουργήθηκαν στο ADDS. Κάθε φορά που δημιουργείται ένα αντικείμενο, προστατεύεται από τη διαγραφή από προεπιλογή. Αυτό σημαίνει ότι προστατεύεται επίσης και από τη μετακίνηση. Για να μετακινήσουμε ένα προστατευμένο αντικείμενο, πρέπει να προβάλλουμε την καρτέλα Object στο πλαίσιο διαλόγου Properties (μέσω της προβολής Advanced Features) και να διαγράψουμε το χαρακτηριστικό προστασίας. Αν και αυτό είναι ένα μεγάλο βήμα στην προστασία αντικειμένων καταλόγου από λανθασμένες λειτουργίες, δεν αρκεί. Γι' αυτό πρέπει να ενεργοποιήσουμε τον έλεγχο ADDS στους καταλόγους μας. Αυτή η λειτουργία πρέπει να εκτελείται τόσο σε ομάδες πόρων όσο και σε εικονικές υπηρεσίες.

Ο έλεγχος ADDS, όπως όλοι οι έλεγχοι, είναι μια διαδικασία δύο βημάτων. Αρχικά, ενεργοποιούμε τον έλεγχο στο κατάλληλο GPO. Εκεί καθορίζουμε ποια αντικείμενα πρέπει να ελεγχθούν. Ξεκινάμε ενεργοποιώντας το audit policy. Δεδομένου ότι θέλουμε να ελέγξουμε τα περιεχόμενα του καταλόγου, μπορούμε να το κάνουμε στην Default Domain Controllers Policy (DDCP)).

1. Χρησιμοποιούμε την Κονσόλα διαχείρισης πολιτικής ομάδας (GPMC) για να ξεκινήσετε το DDCP στο Group Policy Editor.
2. Μεταβαίνουμε στο Computer Settings → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy.

3. Εντοπίζουμε τη ρύθμιση Audit Directory Service Access, κάνουμε διπλό κλικ σε αυτήν και την διαμορφώνουμε την για να εντοπίσουμε επιτυχίες. Μπορούμε επίσης να τη διαμορφώσουμε για να εντοπίσουμε αστοχίες, αλλά μόνο εάν υποψιαζόμαστε ότι οι χειριστές προσπαθούν να κάνουν πράγματα που δεν επιτρέπεται. Ο στόχος αυτής της πολιτικής είναι να δει τι έχει αλλάξει και ενδεχομένως να έχει τη δυνατότητα να το αναιρέσει.
4. Κλείνουμε το Group Policy Editor.

Πλέον η πολιτική ελέγχου είναι ενεργοποιημένη. Θα ενημερωνόμαστε σε κάθε DC εντός πέντε λεπτών από την αλλαγή.

Τώρα πρέπει να πούμε στο ADDS ποια αντικείμενα θέλουμε να ελέγξουμε. Για παράδειγμα, εάν θέλουμε να ελέγξουμε όλες τις αλλαγές στη δομή People OU, συμπεριλαμβανομένων τυχόν αλλαγών στα αντικείμενα που περιέχει, χρησιμοποιούμε την ακόλουθη διαδικασία:

1. Μεταβαίνουμε στο Server Manager → Roles → Active Directory Domain Services → Active Directory Users and Computers. Βεβαιωθείτε ότι οι Advanced Features είναι ενεργοποιημένες στο μενού View.
2. Αναπτύξτσουμε τον κατάλογό μας μέχρι να δούμε το People OU. Κάνουμε δεξί κλικ για να δούμετο παράθυρο διαλόγου Properties.
3. Μεταβαίνουμε στην καρτέλα Security και κάνουμε κλικ στην επιλογή Advanced.
4. Μεταβαίνουμε στην καρτέλα Auditing. Κάνουμε κλικ επιλογή Add.
5. Επιλέγουμε Authenticated Users και κάνουμε κλικ στο OK.
6. Στο πλαίσιο διαλόγου Auditing Entry for People, επιλέγουμε Descendant User Objects στην αναπτυσσόμενη λίστα (το τελευταίο αντικείμενο στη λίστα), επιλέγουμε Write All Properties στην ενότητα Successful και κάνουμε κλικ στο OK για να κλείσετε το παράθυρο διαλόγου.
7. Κλείνουμε όλα τα άλλα παράθυρα διαλόγου.

Τώρα, κάθε φορά που τροποποιούμε ένα αντικείμενο στην ενότητα People, ένας αριθμός αναγνώρισης συμβάντος 4662 θα εμφανίζεται στο αρχείο καταγραφής συμβάντων ασφαλείας. Αυτή είναι η συμπεριφορά όλων των προηγούμενων εκδόσεων των Windows Server. Στα WS08, ωστόσο, μπορούμε να προχωρήσουμε πέρα από αυτό για να επεξεργαστούμε τέσσερις ακόμη δραστηριότητες:

- Πρόσβαση στην υπηρεσία καταλόγου
- Αλλαγές υπηρεσίας καταλόγου
- Αναπαραγωγή υπηρεσίας καταλόγου
- Λεπτομερής αναπαραγωγή υπηρεσίας καταλόγου

Δυστυχώς, αυτές οι πρόσθετες δραστηριότητες δεν διαθέτουν γραφική διεπαφή για να τις ενεργοποιήσουν. Πρέπει να χρησιμοποιήσουμε μια γραμμή εντολών. Για παράδειγμα, για τον έλεγχο αλλαγών στον κατάλογο, τη δραστηριότητα που παρέχει τις πιο ενδιαφέρουσες πληροφορίες, πρέπει να πληκτρολογήσουμε την ακόλουθη εντολή σε οποιοδήποτε DC:

```
auditpol /set /subcategory:"Directory Service Changes" /success:enable
```

Βεβαιωνόμαστε ότι έχουμε ανοίξει μια γραμμή εντολών με την επιλογή Run as Administrator.

Τώρα αν αλλάξουμε οποιοδήποτε αντικείμενο στην ενότητα People. Το σύστημα θα καταγράψει την αλλαγή. Για να δούμε το συμβάν, μεταβαίνουμε στο Server Manager → Diagnostics → Event Viewer → Windows Logs → Security. Θα πρέπει να δούμε κανονικά συμβάντα ADDS που έχουν αριθμό ID 4662, αλλά επιπλέον, θα πρέπει να δούμε ένα συμβάν 5136. Στην πραγματικότητα, ο έλεγχος ADDS προσθέτει τέσσερα νέα συμβάντα στο αρχείο καταγραφής.

Αυτά τα γεγονότα περιγράφονται λεπτομερώς στον Πίνακα 6.7.

Όπως μπορούμε να δούμε, ισχύουν διαφορετικές ρυθμίσεις ελέγχου για διαφορετικά αναγνωριστικά συμβάντων. Στην ιδανική περίπτωση, θα ελέγχουμε όσο το δυνατόν περισσότερες δραστηριότητες στον κατάλογό μας. Θα πρέπει να βεβαιωθούμε ότι έχουμε μια καλή στρατηγική για τη δημιουργία αντιγράφων ασφαλείας και την προστασία των αρχείων καταγραφής τα αποθηκεύουν πολύτιμες πληροφορίες.

Event ID	Περιγραφή
5136	Έχει τροποποιηθεί ένα χαρακτηριστικό του αντικειμένου
5137	Το αντικείμενο έχει δημιουργηθεί
5138	Το αντικείμενο έχει καταργηθεί
5139	Το αντικείμενο μετακινήθηκε εντός του τομέα

Πίνακας 6.7

Read-Only Domain Controllers (RODCs)

Οι ελεγκτές τομέα μόνο για ανάγνωση δεν αποτελούν αναδρομή στα Windows NT, παρά την ομοιότητά τους με τα εφεδρικά DC (BDC). Στα NT, μόνο ο κύριος ελεγκτής τομέα θα μπορούσε να γράψει οποιεσδήποτε ιδιότητες στον κατάλογο, κάθε άλλο DC ήταν σε read-only mode. Ενώ το RODC μοιάζει με το BDC, προσφέρει σημαντικά μεγαλύτερη προστασία από τον προκάτοχό του.

Τα RODCs είναι ελεγκτές τομέα που παρέχονται με μια ειδική προσωρινή μνήμη που μπορεί να αποθηκεύσει κωδικούς πρόσβασης χρηστών. Είναι σημαντικό να θυμόμαστε ότι κατά τη διάρκεια της διαδικασίας σύνδεσης, πρέπει να μπορούμε να επικοινωνήσουμε με έναν διακομιστή Global Catalog (GC) για να απαριθμήσουμε τα Universal Group Memberships, σε περίπτωση που υπάρχει πολιτική άρνησης σε μία από αυτές. Εάν δεν μπορούμε να συνδεθούμε σε ένα GC, τότε απορρίπτεται η σύνδεση. Το πρόβλημα με την επικοινωνία ενός GC είναι ότι απαιτεί σύνδεση WAN σε απομακρυσμένα γραφεία. Εάν τοποθετήσουμε ένα DC στον ιστότοπο αλλά χωρίς GC, τότε κάθε φορά που συνδέεται ένας χρήστης θα χρειάζεται σύνδεση WAN.

Οι προηγούμενες εκδόσεις του Windows Server περιλάμβαναν διάφορες δυνατότητες για να βοηθήσουν σε αυτήν τη διαδικασία. Για παράδειγμα, θα μπορούσαμε να ενεργοποιήσουμε το Universal Group Membership Caching (UGMC) στον ιστότοπο. Αυτό επιτρέπει στον χρήστη να συνδεθεί στο GC μία φορά και στη συνέχεια να αποθηκεύσει τις συνδρομές της ομάδας τοπικά για περίοδο οκτώ ωρών ή για τη διάρκεια του εισιτηρίου Kerberos που παραχωρείται στον χρήστη. Μετά από οκτώ ώρες, πρέπει να επικοινωνήσουμε ξανά με την GC για να ανακτήσουμε τις συνδρομές.

Τα RODC λειτουργούν με παρόμοιο τρόπο με το UGMC, αλλά αντί να αποθηκεύουν συνδρομές σε ομάδες, αποθηκεύουν κωδικούς πρόσβασης χρηστών μέσα σε μια προστατευμένη κρυφή μνήμη. Αυτό σημαίνει ότι οι χρήστες μπορούν να βασίζονται στο RODC για να συνδεθούν στον τομέα, αλλά το RODC εξακολουθεί να είναι ένας προστατευμένος πόρος. Σε περίπτωση κλοπής ενός RODC, μπορούμε να εκτελέσουμε κεντρική επαναφορά όλων των κωδικών πρόσβασης που είχαν αποθηκευτεί στο RODC, διασφαλίζοντας ότι ακόμη και αν ο κακόβουλος εισβολέας μπορεί να διαβάσει τους κωδικούς πρόσβασης, θα είναι ελάχιστα χρήσιμοι καθώς θα έχει γίνει επαναφορά.

Επιπλέον, μπορούμε να ελέγξουμε ποιοι κωδικοί πρόσβασης μπορούν να αποθηκευτούν σε οποιοδήποτε RODC στους τομείς μας. Να σημειωθεί ότι οι κωδικοί πρόσβασης διαχειριστή δεν αποθηκεύονται ποτέ σε RODC από προεπιλογή, επειδή παρέχουν πρόσβαση σε πάρα πολλούς πόρους. Η αποθήκευση κωδικού πρόσβασης είναι ιδιοκτησία του RODC και ιδιοκτησία λογαριασμών χρηστών. Στα RODC, ορίζουμε την πολιτική αναπαραγωγής κωδικού πρόσβασης. Τα αντικείμενα χρήστη περιλαμβάνουν επίσης μια καρτέλα Password Replication, η οποία μας δείχνει ποια RODCs αποθηκεύουν προσωρινά τους κωδικούς πρόσβασης.

Σε αντίθεση με το UGMC, τα RODCs μπορούν να συμπληρωθούν για να αποθηκεύσουν προσωρινά τους κωδικούς πρόσβασης. Για παράδειγμα, μπορούμε να δημιουργήσουμε τοπικές ομάδες χρηστών και να αποκτήσουμε το RODC για να συμπληρώσουμε εκ νέου όλους τους κωδικούς πρόσβασης. Αυτό γίνεται μέσω του κουμπιού για Advanced που βρίσκεται στην καρτέλα Password Replication Policy στο παράθυρο διαλόγου RODC's Property.

Τέλος, μπορούμε να επαναφέρουμε αυτόματα όλους τους κωδικούς πρόσβασης που είχαν αποθηκευτεί σε RODC σε περίπτωση κλοπής του. Απλώς διαγράφουμε τον λογαριασμό RODC από τον τομέα. Μόλις επιβεβαιώσουμε τη διαγραφή, θα έχουμε την επιλογή να επαναφέρουμε όλους τους κωδικούς πρόσβασης για τους λογαριασμούς που είναι αποθηκευμένοι στο κλεμμένο RODC. Θα πρέπει να αφιερώσουμε χρόνο για να εξαγάγετε τη λίστα των χρηστών των οποίων οι κωδικοί πρόσβασης επαναφέρθηκαν για να τους στείλουμε μια ανακοίνωση σχετικά με το γιατί επαναφέρθηκαν οι κωδικοί πρόσβασης.

Ασφάλεια συστήματος αρχείων

Το σύστημα αρχείων είναι επίσης ένα τμήμα του λειτουργικού συστήματος που πρέπει να υποστηρίζει ένα ασφαλές περιβάλλον. Όλες οι λειτουργίες δίσκου και αρχείων στα WS08 βασίζονται στη χρήση των πιο πρόσφατων δυνατοτήτων που υποστηρίζονται από το NTFS. Το ίδιο ισχύει και για την κρυπτογράφηση αρχείων. Χωρίς NTFS, δεν υπάρχει κρυπτογράφηση.

Μία από τις σημαντικές πτυχές της ασφαλούς διαχείρισης αρχείων είναι η δυνατότητα καταγραφής όλων των αλλαγών αρχείων και η ειδοποίηση οργανισμών σε περίπτωση μη εξουσιοδοτημένων αλλαγών. Αυτό μπορεί να γίνει σε κάποια μορφή με έλεγχο πρόσβασης σε αρχεία, αλλά για κρίσιμα αρχεία δεδομένων απαιτείται η βοήθεια ενός επαγγελματικού προγράμματος.

Επιπλέον, η ασφάλεια NTFS έχει βελτιωθεί σημαντικά στα Windows Server 2008. Όπως και τα αντικείμενα ADDS, χρησιμοποιεί την έννοια της κληρονομικότητας για να εφαρμόσει δικαιώματα πρόσβασης. Εφαρμόζει επίσης ισχυρές ρυθμίσεις ασφαλείας στην

ομάδα χρηστών για λόγους σταθερότητας. Αυτό σημαίνει ότι οι χρήστες δεν μπορούν πλέον να εκτελούν εφαρμογές παλαιού τύπου που τροποποιούν αρχεία που βρίσκονται σε ευαίσθητους φακέλους, όπως Program File και Windows. Οι διαχειριστές θα πρέπει να λάβουν ειδικά μέτρα για να διασφαλίσουν ότι οι εφαρμογές παλαιού τύπου θα λειτουργούν σε συστήματα Windows Server 2008 για κανονικούς χρήστες. Τα WS08 περιλαμβάνουν επίσης το Resource Protection των Windows, μια δυνατότητα που έχει σχεδιαστεί για την επιδιόρθωση αρχείων συστήματος και καταχωρίσεων μητρώου όταν καταστραφεί από εγκαταστάσεις λογισμικού ή άλλα ανεπιθύμητα συμβάντα.

Το σύστημα κρυπτογράφησης αρχείων

Το σύστημα κρυπτογράφησης αρχείων (EFS) είναι μέρος του NTFS που παίζει επίσης σημαντικό ρόλο στο Castle Defense System. Είναι ισχυρό επειδή η λειτουργία του είναι διαφανής για τους χρήστες μόλις ενεργοποιηθεί. Παρέχει επίσης περισσότερη προστασία αρχείων από ό, τι τα δικαιώματα, επειδή εάν οι κακόβουλοι εισβολείς αποκτήσουν φυσική πρόσβαση σε κρυπτογραφημένα αρχεία, δεν θα μπορούν να δουν το περιεχόμενό τους. Αυτό δεν ισχύει απαραίτητα με αρχεία που περιλαμβάνουν μόνο δικαιώματα NTFS. Το ιδανικό επίπεδο ασφάλειας είναι αυτό που χρησιμοποιεί τόσο τα δικαιώματα NTFS όσο και την κρυπτογράφηση.

Η κρυπτογράφηση ενεργοποιείται μέσω των ιδιοτήτων αρχείων ή φακέλων, ακριβώς όπως τα δικαιώματα. Μπορεί επίσης να εκτελεστεί με την εντολή CIPHER. Η κρυπτογράφηση είναι ιδιότητα αρχείου, εξαιτίας αυτού, δεν μπορεί να εφαρμοστεί εάν το αρχείο έχει συμπιεστεί. Αυτές οι δύο ιδιότητες είναι αμοιβαία αποκλειστικές. Τα αρχεία που αποτελούν μέρος του λειτουργικού συστήματος δεν μπορούν να κρυπτογραφηθούν, ούτε μπορούν να βρεθούν αρχεία στο φάκελο %SYSTEMROOT%. Τα WS08 υποστηρίζουν την κρυπτογράφηση δεδομένων που περιέχονται σε κοινές χρήσεις φακέλων. Ωστόσο, τα δεδομένα που περιέχονται σε κρυπτογραφημένα αρχεία που βρίσκονται σε κοινόχρηστα δίκτυα δεν είναι απαραίτητα κρυπτογραφημένα όταν μεταφέρονται από το κοινόχρηστο αρχείο στον τοπικό υπολογιστή. Εάν απαιτείται πλήρης κρυπτογράφηση, ακόμη και σε επίπεδο επικοινωνιών, πρέπει να χρησιμοποιηθούν πρόσθετες τεχνολογίες, όπως το Internet Protocol Security (IPSec) ή το Secure Socket Tunneling Protocol (SSTP).

Τα WS08 υποστηρίζουν την κρυπτογράφηση αρχείων εκτός σύνδεσης. Αυτή η ιδιότητα μπορεί να οριστεί σε επίπεδο GPO και να εφαρμοστεί μαζί με τις πολιτικές ανακατεύθυνσης φακέλων. Τα κρυπτογραφημένα αρχεία θα αποκρυπτογραφηθούν εάν αντιγραφούν σε τόμους που δεν είναι NTFS, επομένως οι χρήστες θα πρέπει να προειδοποιούνται για βέλτιστες πρακτικές για ασφαλή αρχεία. Επιπλέον, η κρυπτογράφηση δεν εμποδίζει τη διαγραφή αρχείων, εμποδίζει μόνο τους μη εξουσιοδοτημένους χρήστες να βλέπουν το περιεχόμενό τους. Εάν οι χρήστες έχουν δικαιώματα σε έναν κατάλογο που περιέχει κρυπτογραφημένα αρχεία, δεν θα μπορούν να δουν το περιεχόμενό τους, αλλά ενδέχεται να μπορούν να τα διαγράψουν. Τα κρυπτογραφημένα αρχεία εμφανίζονται σε πράσινο χρώμα στο Windows Explorer. Αυτό βοηθά τους χρήστες να αναγνωρίζουν γρήγορα τα αρχεία αυτά.

Η κρυπτογράφηση ενός αρχείου είναι μια απλή διαδικασία:

1. Ανοίγουμε το Windows Explorer.
2. Κάνουμε δεξί κλικ στο φάκελο που θέλουμε να κρυπτογραφήσουμε και επιλέγουμε Properties.
3. Κάνουμε κλικ στο κουμπί Advanced στην καρτέλα General.
4. Κάνουμε κλικ στην επιλογή Encrypt Contents To Secure Data και κάνουμε κλικ στο OK.
5. Κάνουμε κλικ στο OK για να κλείσουμε το παράθυρο διαλόγου Properties.
6. Το EFS θα μας ζητήσει να επιβεβαιώσουμε τη ρύθμιση που θέλουμε να εφαρμόσουμε. Επιλέγουμε Apply Changes To These Folders, Subfolders, And Files και κάνουμε κλικ στο OK.
7. Εάν οι εργασίες φακέλων δεν έχουν ενεργοποιηθεί, το EFS θα μας ζητήσει να τις ενεργοποιήσουμε. Κάνουμε κλικ στο Yes.

Τα κρυπτογραφημένα αρχεία θα εμφανίζονται πλέον με πράσινο χρώμα στο Windows Explorer. Η χρήση του EFS είναι τόσο απλή, αλλά υπάρχουν οδηγίες:

- Πρέπει να κρυπτογραφήσουμε φακέλους και όχι μεμονωμένα αρχεία.
- Πρέπει να διασφαλίσουμε ότι τα αρχεία εκτός σύνδεσης είναι κρυπτογραφημένα.
- Ολόκληρος ο φάκελος εγγράφων πρέπει να είναι κρυπτογραφημένος.
- Τόσο το %TEMP% όσο και το%TMP% πρέπει να κρυπτογραφηθούν για να βεβαιωθούμε ότι όλα τα προσωρινά αρχεία είναι επίσης κρυπτογραφημένα. Χρησιμοποιούμε ένα σενάριο που βασίζεται στην εντολή CIPHER κατά τη ρύθμιση του συστήματος για να ορίσουμε αυτούς τους φακέλους ως κρυπτογραφημένους.
- Πρέπει να κρυπτογραφήσουμε το spool folder στους διακομιστές εκτύπωσης.
- Πρέπει να συνδυάσουμε το EFS με το IPSec ή το SSTP για να εξασφαλίσουμε κρυπτογράφηση δεδομένων από άκρο σε άκρο.
- Πρέπει να χρησιμοποιούμε το Group Policy για τον έλεγχο της συμπεριφοράς του EFS στο δίκτυό μας.
- Χρησιμοποιούμε μια υποδομή δημόσιου κλειδιού WS08 (χρησιμοποιώντας ADCS) για τη διαχείριση πιστοποιητικών EFS και παραγόντων ανάκτησης.

Το EFS χρησιμοποιεί δημόσια και ιδιωτικά κλειδιά (πιστοποιητικά) για τη διαχείριση της διαδικασίας κρυπτογράφησης και ανάκτησης. Ο καλύτερος τρόπος για να διαχειριστούμε αυτά τα πιστοποιητικά είναι να χρησιμοποιήσουμε τις δυνατότητες PKI των Windows.

.NET Framework Ασφάλεια

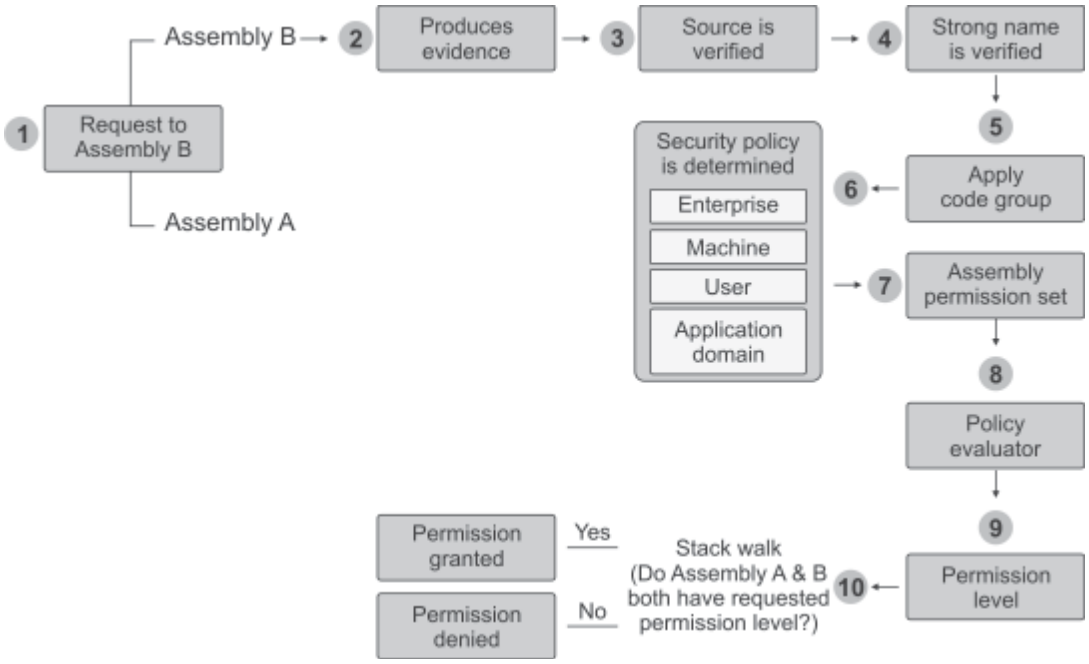
Το .NET Framework είναι μια άλλη πτυχή του λειτουργικού συστήματος η οποία χρειάζεται προστασία. Πρώτον, περιλαμβάνεται ως βασικό στοιχείο του λειτουργικού συστήματος WS08, καθώς η έκδοση 2 του Framework είναι εγκατεστημένη από προεπιλογή σε πλήρεις εγκαταστάσεις και η έκδοση 3 είναι διαθέσιμη ως δυνατότητα. Δεύτερον, παρέχει βασικές λειτουργίες για υπηρεσίες Web. Ως εκ τούτου, παρέχει τη μηχανή τόσο για τη λειτουργία όσο και για την εκτέλεση των υπηρεσιών Web. Είναι ευθύνη αυτού του κινητήρα να καθορίσει εάν μπορεί να εμπιστευτεί τον κώδικα που

πρόκειται να εκτελεστεί. Το Common Language Runtime (CLR) εφαρμόζει ασφάλεια με δύο διαφορετικούς τρόπους. Ο πρώτος είναι για διαχειριζόμενο κώδικα και ο δεύτερος για μη διαχειριζόμενο κώδικα. Η διαχειριζόμενη ασφάλεια κώδικα βρίσκεται στην καρδιά του CLR. Δύο πτυχές του κώδικα αξιολογούνται από το CLR προτού το επιτρέψει να τρέξει: η ασφάλεια του κώδικα και η συμπεριφορά του κώδικα. Για παράδειγμα, εάν ο κώδικας χρησιμοποιεί μια μέθοδο που αναμένει μια τιμή τεσσάρων byte, το CLR θα απορρίψει μια προσπάθεια επιστροφής μιας τιμής οκτώ byte. Με άλλα λόγια, το CLR εξασφαλίζει ότι ο διαχειριζόμενος κώδικας είναι ασφαλής και συμπεριφέρεται σωστά. Το πλεονέκτημα της χρήσης αυτής της προσέγγισης για την ασφάλεια είναι ότι οι χρήστες δεν χρειάζεται να ανησυχούν εάν ο κώδικας είναι ασφαλής πριν τον εκτελέσουν. Εάν είναι, το CLR θα τον εκτελέσει. Εάν δεν είναι, απλά δεν θα εκτελεστεί. Αλλά αυτό ισχύει μόνο για διαχειριζόμενο κώδικα. Επιτρέπεται η εκτέλεση μη διαχειριζόμενου κώδικα, αλλά δεν επωφελείται από αυτά τα μέτρα ασφαλείας. Για να εκτελέσουμε μη διαχειριζόμενο κώδικα, το CLR πρέπει να χρησιμοποιεί ένα συγκεκριμένο σύνολο δικαιωμάτων, δικαιώματα που μπορούν να ελεγχθούν αλλά που πρέπει να δηλωθούν καθολικά.

Η διαδικασία αξιολόγησης για διαχειριζόμενο κώδικα

Το CLR χρησιμοποιεί μια διαδικασία αξιολόγησης οκτώ βημάτων για διαχειριζόμενο κώδικα, όπως φαίνεται στην εικόνα 6.63. Χρησιμοποιεί τα ακόλουθα βήματα:

1. Όταν ένα assembly (ένα κομμάτι διαχειριζόμενου κωδικού) καλεί ένα άλλο assembly, το CLR αξιολογεί το επίπεδο άδειας για εφαρμογή στο νέο assembly.
2. Το πρώτο πράγμα που πρέπει να κάνει το νέο assembly είναι να παρέχει στοιχεία. Αυτά τα στοιχεία είναι, στην πραγματικότητα, ένα σύνολο απαντήσεων σε ερωτήματα που τίθενται από την πολιτική ασφάλειας του CLR.
3. Τρεις ερωτήσεις τίθενται σχετικά με την πηγή του assembly:
   α) Από ποια τοποθεσία αποκτήθηκε το assembly: Τα assemblies λαμβάνονται αυτόματα στον πελάτη από έναν ιστότοπο.
   β) Από ποιον Uniform Resource Locator (URL) προήλθε το assembly: Μια συγκεκριμένη διεύθυνση URL πρέπει να παρέχεται από το assembly.
   γ) Από ποια ζώνη αποκτήθηκε το assembly: Αυτό ισχύει για ζώνες του Internet Explorer όπως Internet, Intranet, Local Machine και ούτω καθεξής. Ορισμένες ζώνες είναι πιο αξιόπιστες από άλλες.
4. Το assembly πρέπει επίσης να παρέχει ένα κρυπτογραφικά ισχυρό αναγνωριστικό, που ονομάζεται strong name. Αυτό το αναγνωριστικό είναι μοναδικό και πρέπει να παρέχεται από τον συντάκτη του assembly. Το αναγνωριστικό δεν προσδιορίζει απαραίτητα τον συντάκτη, αλλά αναγνωρίζει τη διάταξη ως μοναδική.



Εικόνα 6.63

5. Τα στοιχεία συλλέγονται από μια σειρά διαφορετικών πηγών, όπως το ίδιο το CLR, το πρόγραμμα περιήγησης, το ASP.NET, το shell και ούτω καθεξής. Μόλις παρασχεθούν τα αποδεικτικά στοιχεία, το CLR αρχίζει να καθορίζει την πολιτική ασφαλείας που θα εφαρμοστεί. Πρώτον, εφαρμόζει τα αποδεικτικά στοιχεία σε τυπικές ομάδες κώδικα. Αυτές οι ομάδες περιέχουν τυπικές πολιτικές, ανάλογα με τη ζώνη από την οποία προέρχεται το assembly. Το .NET Framework περιλαμβάνει βασικές ομάδες κώδικα, αλλά οι διαχειριστές μπορούν να προσθέσουν τις δικές τους ή να τροποποιήσουν τις προεπιλεγμένες ομάδες.
6. Μόλις καθοριστεί η ομάδα κωδικών, ορίζεται η πολιτική. Αυτή η πολιτική μπορεί να οριστεί σε τρία επίπεδα και με αυτήν τη σειρά: Enterprise, Machine και User. Ένα τέταρτο επίπεδο περιλαμβάνει τον τομέα της εφαρμογής. Αυτός ο τομέας παρέχει ένα απομονωμένο περιβάλλον για να εκτελεστεί η εφαρμογή. Μια εφαρμογή που περιέχεται σε έναν τομέα δεν μπορεί να επηρεάσει οποιονδήποτε άλλο τομέα στον ίδιο υπολογιστή.
7. Μόλις οριστεί η πολιτική, δημιουργείται ένα αρχικό σύνολο δικαιωμάτων. Το assembly μπορεί να ρυθμίσει αυτό το σύνολο δικαιωμάτων με τρεις τρόπους:
   α) Πρώτον, μπορεί να προσδιορίσει το ελάχιστο σύνολο δικαιωμάτων που απαιτείται για την εκτέλεση.
   β) Δεύτερον, μπορεί να καθορίσει προαιρετικά δικαιώματα. Αυτά δεν είναι απολύτως απαραίτητα.
   γ) Τρίτον, μια σωστή συμπεριφορά μπορεί να απορρίψει άδειες που δεν απαιτεί και θεωρεί πολύ επικίνδυνες, μειώνοντας πραγματικά το σύνολο δικαιωμάτων που εκχωρείται από το CLR.
8. Όλοι αυτοί οι παράγοντες εξετάζονται από τον αξιολογητή πολιτικής.
9. Δημιουργείται ένα τελικό σύνολο δικαιωμάτων για το assembly.
10. Το τελευταίο στάδιο είναι το stack walk. Το CLR συγκρίνει το σύνολο δικαιωμάτων με εκείνο άλλων assemblies που εμπλέκονται στην αρχική κλήση για αυτό το

assembly. Εάν κάποιο από αυτά τα assemblies δεν έχει άδεια λειτουργίας με αυτό το σύνολο δικαιωμάτων, απορρίπτεται η άδεια εκτέλεσης. Εάν όλα είναι εντάξει, χορηγείται η άδεια εκτέλεσης.

Internet Information Server 7.0

Το IIS 7 είναι ασφαλές από προεπιλογή, επειδή έχει χωριστεί σε στοιχεία που εγκαθίστανται μόνο αν τα χρειαζόμαστε. Η ασφαλέστερη εγκατάσταση του IIS είναι, στην πραγματικότητα, αυτή που θα βρούμε στον Server Core, επειδή εξυπηρετεί μόνο στατικούς ιστότοπους από προεπιλογή. Επιπλέον, η Microsoft έχει βελτιώσει τα υπάρχοντα μοντέλα ασφαλείας σε παλαιότερες εκδόσεις των υπηρεσιών IIS. Για παράδειγμα, σε προηγούμενες εκδόσεις, οι υπηρεσίες IIS και ASP.NET ήταν ξεχωριστές οντότητες. Στο IIS 7, και τα δύο έχουν ενσωματωθεί σε ένα μοντέλο. Ενώ οι υπηρεσίες IIS εξακολουθούν να υποστηρίζουν προηγούμενες λειτουργίες, διαθέτει πλέον ένα ενιαίο μοντέλο ασφαλείας.

Όλοι οι ιστότοποι διαθέτουν μια ομάδα εφαρμογών, η οποία δημιουργείται αυτόματα. Αυτό διαχωρίζει τον ιστότοπο από όλους τους άλλους ιστότοπους ή εφαρμογές στον διακομιστή Web. Οι ομάδες εφαρμογών εκτελούνται από το NetworkService από προεπιλογή, περιορίζοντας και πάλι τα δικαιώματα πρόσβασης που διαθέτουν στον ίδιο τον διακομιστή. Για να βεβαιωθούμε ότι οι εφαρμογές μας εκτελούνται σε αυτό το πλαίσιο και μόνο σε αυτό το πλαίσιο, πρέπει τώρα να εγκαταστήσουμε το module Anonymous Authentication και, στη συνέχεια, να βεβαιωθούμε ότι το αρχείο WEB.CONFIG για την εφαρμογή περιλαμβάνει την ακόλουθη γραμμή:

```
<anonymousAuthentication enabled="true" username="" defaultLogonDomain="" />
```

Αφήνοντας κενές τις καταχωρήσεις τόσο για το όνομα τομέα όσο και για το όνομα χρήστη, διασφαλίζετε ότι το NetworkService χρησιμοποιείται για τη δημιουργία περιβάλλοντος ασφαλείας για τις εφαρμογές που εκτελούμε. Αυτό είναι μόνο ένα παράδειγμα αυξημένης ασφάλειας εντός του IIS. Το βασικό σημείο που πρέπει να θυμόμαστε όταν εργαζόμαστε με τον IIS είναι να εγκαταστήσουμε μόνο εκείνα τις module που πραγματικά χρειαζόμαστε και στη συνέχεια να βασιστούμε στον Security Configuration Wizard για να βοηθήσουμε στην ασφαλή εγκατάσταση της βασικής εγκατάστασης του IIS.

Επίπεδο 4 - Πρόσβαση σε πληροφορίες

Το 4ο Επίπεδο ασχολείται με την ταυτοποίηση χρήστη και την κατανομή δικαιωμάτων που του επιτρέπουν να λειτουργεί εντός του δικτύου μας. Όπως τα Windows 2003, τα Windows Server 2008 περιλαμβάνουν διάφορα πρωτόκολλα ασφαλείας για έλεγχο ταυτότητας και εξουσιοδότηση. Το πιο σημαντικό από αυτά για ένα εσωτερικό δίκτυο είναι το Kerberos, παρόλο που το NT LAN Manager (NTLM) εξακολουθεί να υποστηρίζεται. Ωστόσο, στο παράλληλο δίκτυο, υπάρχει ελάχιστη ανάγκη για NTLM, καθώς όλα τα μηχανήματα χρησιμοποιούν τα πιο πρόσφατα λειτουργικά συστήματα και τα δάση βρίσκονται σε πλήρη λειτουργία.

Το πρωτόκολλο Kerberos έχει πολλά πλεονεκτήματα έναντι του NTLM. Είναι ταχύτερο, πιο ασφαλές, πιο ευρέως αποδεκτό και απλούστερο στη χρήση. Ένα από τα καλύτερα

χαρακτηριστικά του είναι το γεγονός ότι μόλις πιστοποιήσει τους χρήστες, δεν χρειάζεται να επιστρέψουν στον διακομιστή για εξουσιοδότηση. Ενώ στο NTLM, ο χρήστης επιστρέφει συνεχώς στον διακομιστή για επικύρωση δικαιωμάτων και αδειών, στο Kerberos, ο χρήστης καλεί τα δικαιώματα και τα δικαιώματα εντός του διακριτικού πρόσβασης που παρέχεται από τον διακομιστή Kerberos. Αυτό το διακριτικό πρόσβασης έχει τη μορφή του εισιτηρίου Kerberos που παραχωρείται στον χρήστη κατά τη σύνδεση. Επιπλέον, με το Kerberos, ο διακομιστής επικυρώνει τον πελάτη, διασφαλίζοντας ότι είναι εξουσιοδοτημένος να παραχωρεί πρόσβαση χρήστη εντός του τομέα. Τέλος, το Kerberos υποστηρίζει επίσης έλεγχο ταυτότητας δύο παραγόντων. Αυτό μπορεί να έχει τη μορφή έξυπνης κάρτας ή βιομετρικής συσκευής, όπως συσκευή δακτυλικών αποτυπωμάτων.

Ένα από τα βασικά στοιχεία του Kerberos realm, το ισοδύναμο Kerberos ενός τομέα, είναι η χρονική σήμανση. Ο συγχρονισμός χρόνου είναι απαραίτητος στο Kerberos επειδή ο διακομιστής ελέγχου ταυτότητας αντιστοιχεί την ώρα του αιτήματος του πελάτη με το δικό του εσωτερικό ρολόι. Εάν ο χρόνος διαφέρει περισσότερο από τον προβλεπόμενο χρόνο, αυτό ορίζεται στις πολιτικές του λογαριασμού μας, ο διακομιστής Kerberos δεν θα αυθεντικοποιήσει τον χρήστη. Αυτός είναι ένας λόγος για τον οποίο η Microsoft έχει ενσωματώσει την υπηρεσία χρόνου στον ρόλο PDC Emulator Operations Master στο Active Directory Domain Services.

Έλεγχος ταυτότητας με Έξυπνη Κάρτα (Smart Card)

Ένα από τα πιο σημαντικά μέρη για έλεγχο ταυτότητας με Smart Card είναι οι λογαριασμοί διαχειριστή. Τα Windows Server 2008 υποστηρίζουν τη χρήση ελέγχου ταυτότητας δύο παραγόντων για διαχειριστές. Εάν θέλουμε να σχεδιάσουμε μια εξαιρετικά ασφαλή υποδομή, θα πρέπει να εκμεταλλευτούμε αυτήν τη δυνατότητα για όλους τους λογαριασμούς στους οποίους έχουν χορηγηθεί δικαιώματα διαχειριστή. Επιπλέον, οι διαχειριστές μας πρέπει να έχουν δύο λογαριασμούς: έναν λογαριασμό σε επίπεδο χρήστη για καθημερινές λειτουργίες και έναν λογαριασμό διαχειριστή για διαχειριστικές λειτουργίες. Θα πρέπει να συνδέονται ως χρήστες και θα πρέπει να εκτελούν τις διαχειριστικές τους δραστηριότητες μέσω της εντολής Run as Administrator, χρησιμοποιώντας την έξυπνη κάρτα τους για να συνδεθούν. Για την χρήση των Smart Cards χρειαζόμαστε υποδομή δημόσιου κλειδιού για να εκχωρήσουμε πιστοποιητικά στις Smart Cards.

Ασφαλής αναγνώριση χρήστη

Η αναγνώριση χρήστη συμβαίνει σε πολλά επίπεδα εντός ενός δικτύου των WS08. Ο πιο προφανής έλεγχος ταυτότητας γίνεται μέσω του τομέα ADDS. Για αυτό, πρέπει να ορίσουμε καθολικές πολιτικές λογαριασμού για ολόκληρο το σύμπλεγμα και να τις βελτιώσουμε σε κάθε τομέα. Επιπλέον, ο έλεγχος ταυτότητας εμφανίζεται σε σενάρια μεταξύ δασών. Τα WS08 επεκτείνουν την έννοια της εμπιστοσύνης μέσα στο δάσος σε πολλαπλά δάση μέσω της εμπιστοσύνης δασών. Για να το πετύχουμε αυτό, πρέπει να δημιουργήσουμε εμπιστοσύνη. Δύο άλλες περιοχές ελέγχου ταυτότητας στα WS08 βρίσκονται στα: Web server και Web service ή .NET Framework authentication. Ο έλεγχος ταυτότητας Web server εκτελείται μέσω των υπηρεσιών IIS και χρησιμοποιεί μια

σειρά τεχνικών ελέγχου ταυτότητας. Ο έλεγχος ταυτότητας .NET Framework βασίζεται σε ρόλο και μπορεί να είναι συγκεκριμένος για κάθε εφαρμογή.

Έλεγχος ταυτότητας χρήστη σε Active Directory Domain Services

Στα δίκτυα Windows, κάθε αρχή ασφαλείας αναγνωρίζεται από έναν μοναδικό αριθμό, το αναγνωριστικό ασφαλείας ή το SID. Οι αρχές ασφαλείας περιλαμβάνουν τα πάντα, από υπολογιστές έως χρήστες έως ομάδες και ούτω καθεξής. Το SID χρήστη περιλαμβάνεται στο διακριτικό πρόσβασης για κάθε χρήστη. Όταν οι πληροφορίες στο διακριτικό πρόσβασης χρησιμοποιούνται για να προσδιορίσουν εάν ένας χρήστης έχει πρόσβαση σε ένα αντικείμενο, τα SID του χρήστη συγκρίνονται με τη λίστα των SID που συνιστούν τη λίστα ελέγχου πρόσβασης (DACL) του αντικειμένου για τον προσδιορισμό του επιπέδου άδειας του χρήστη έχει σε αυτό το αντικείμενο. Με άλλα λόγια, κάθε αρχή ασφαλείας στα WS08 αναγνωρίζεται ως αριθμός και όχι όνομα.

Ο αντίκτυπος αυτού είναι ότι η ιδιοκτησία αντικειμένων προσδιορίζεται από τα SID. Όταν δημιουργούμε ξανά ένα αντικείμενο, όπως έναν λογαριασμό χρήστη, του εκχωρούμε διαφορετικό SID. Όταν δημιουργούμε το παράλληλο δίκτυο VSO, θα μεταφέρουμε λογαριασμούς από τον αρχικό τομέα στον νέο τομέα παραγωγής, πράγμα που σημαίνει ότι όλοι οι χρήστες μας θα έχουν νέα SID. Όταν συμβεί αυτό, οι χρήστες μας θα έχουν πρόσβαση στα αρχεία και τους φακέλους τους μέσω του αρχικού τους SID. Όταν μεταφέρονται από τους αρχικούς διακομιστές αρχείων στους διακομιστές αρχείων στο παράλληλο δίκτυο VSO, θα πρέπει επίσης να εκτελέσουμε μετάφραση ασφαλείας για να αντικαταστήσουμε τα παλιά SID με νέα.

Διαμόρφωση των Default Domain Policies

Η προεπιλεγμένη πολιτική τομέα είναι η πολιτική λογαριασμού για τον τομέα. Δεδομένου ότι μόνο μία πολιτική μπορεί να περιέχει πληροφορίες λογαριασμού, αυτές οι πληροφορίες πρέπει να καθοριστούν σε έναν μόνο τομέα. Πρέπει να είμαστε προσεκτικοί όταν εργαζόμαστε με αυτήν την πολιτική, επειδή δεν μπορεί να απενεργοποιηθεί. Εάν κάνουμε λάθος κατά την επεξεργασία αυτής της πολιτικής, θα επηρεάσουμε ολόκληρο τον τομέα. Αυτός είναι ένας λόγος για μια δομημένη στρατηγική διαχείρισης αλλαγών του Group Policy. Στην πραγματικότητα, αυτό που πρέπει να κάνουμε είναι να ορίσουμε την πολιτική στον ριζικό τομέα έτσι ώστε να είναι όσο το δυνατόν πληρέστερη. Αυτή η πολιτική πρέπει να αντιστοιχεί στις ρυθμίσεις που απαιτούνται από τον global τομέα παραγωγής παιδιών. Θα μεταδοθεί στους τομείς των παιδιών κατά τη δημιουργία τους. Στη συνέχεια, μπορούμε να κάνουμε τροποποιήσεις όπως απαιτείται σε κάθε θυγατρικό τομέα.

Τα στοιχεία που πρέπει να καλυφθούν σε αυτήν την πολιτική λογαριασμού περιγράφονται στον Πίνακα 6.8. Όλα τα στοιχεία που περιγράφονται σε αυτόν τον πίνακα βρίσκονται στο Computer Configuration → Policies → Windows Components → Security Settings branch of Group Policy.

Όλες αυτές οι ρυθμίσεις εφαρμόζονται σε επίπεδο τομέα για να διασφαλιστεί ότι επηρεάζουν κάθε αντικείμενο εντός του τομέα. Στην πραγματικότητα, η πολιτική λογαριασμού είναι πολιτική υπολογιστή. Αυτό σημαίνει ότι το τμήμα διαμόρφωσης χρήστη του GPO μπορεί να απενεργοποιηθεί. Η προεπιλεγμένη πολιτική ελεγκτών τομέα πρέπει επίσης να τροποποιηθεί.

Περιοχή	Ρύθμιση	Προτεινόμενο	Σχόλια
Account Policies/ Kerberos Policy	Enforce user logon restrictions	Enabled (default)	Αυτό διασφαλίζει ότι οι χρήστες έχουν το δικαίωμα πρόσβασης σε τοπικούς πόρους ή σε πόρους δικτύου πριν τους δώσουν ένα εισιτήριο Kerberos.
	Maximum lifetime for service ticket	Six hundred minutes (default)	Αυτό δηλώνει τη διάρκεια του εισιτηρίου περιόδου σύνδεσης που χρησιμοποιείται για την έναρξη σύνδεσης με διακομιστή. Πρέπει να ανανεωθεί όταν λήξει.
	Maximum lifetime for user ticket	Ten hours (default)	Αυτό πρέπει να είναι μεγαλύτερο ή ίσο με την προηγούμενη ρύθμιση. Πρέπει να ανανεωθεί όταν λήξει.
	Maximum lifetime for user ticket renewal	Seven days (default)	Αυτό αναφέρει λεπτομερώς τη διάρκεια του εισιτηρίου εκχώρησης ενός χρήστη. Ο χρήστης πρέπει να συνδεθεί ξανά μόλις λήξει αυτό το εισιτήριο.
	Maximum tolerance for computer clock synchronization	Five minutes (default)	Το Kerberos χρησιμοποιεί time stamps για να παραχωρήσει εισιτήρια. Όλοι οι υπολογιστές ενός τομέα συγχρονίζονται μέσω των ελεγκτών τομέα.
Restricted Groups	*Domain*/Enterprise Admins	Individuals only	Αξιόπιστα άτομα θα πρέπει να είναι μέλη αυτής της ομάδας.
	Domain/Domain Admins	Individuals only	Αξιόπιστα άτομα θα πρέπει να είναι μέλη αυτής της ομάδας.
	Domain/ Administrators	Enterprise Admins Domain Admins	Αυτή η ομάδα πρέπει να περιέχει μόνο αξιόπιστες ομάδες.

Πίνακας 6.8

Local Domain Controller Policies

Συγκεκριμένες πολιτικές πρέπει να εφαρμόζονται στους ελεγκτές τομέα μόλις δημιουργηθούν. Η διαδικασία προώθησης DC θα ασφαλίσει αυτόματα διαφορετικές πτυχές του τοπικού συστήματος και θα δημιουργήσει το πρότυπο DC Security.inf, αλλά στις περισσότερες περιπτώσεις απαιτείται πρόσθετη τοπική ασφάλεια. Όποιο πρότυπο και αν χρησιμοποιούμε, πρέπει να βεβαιωθούμε ότι έχετε ασφαλίσει τις ακόλουθες περιοχές:

- Εστίαση στον έλεγχο ταυτότητας Kerberos αντί για NTLM, ακόμη και στην έκδοση 2 NTLM
- Χρησιμοποιήούμε την υπογραφή δεδομένων για ερωτήματα Lightweight Directory Access Protocol (LDAP)
- Καταργούμε την υποστήριξη πελατών χαμηλού επιπέδου
- Ασφαλίζουμε το αρχείο αποθήκευσης NTDS.DIT

Member Server Baseline Policy

Μια άλλη πολιτική ασφαλείας που είναι καθολική για μια ομάδα αντικειμένων είναι η πολιτική βάσης διακομιστή-μέλους. Αυτή η πολιτική περιλαμβάνει μια ποικιλία ρυθμίσεων που εφαρμόζονται σε όλους τους διακομιστές. Βρίσκεται Virtual Service Offerings OU, και επειδή είναι το γονικό OU για όλους τους διακομιστές μελών, εφαρμόζεται σε όλους αυτούς. Εξαιτίας αυτού, κάθε συγκεκριμένος ρόλος διακομιστή GPO περιλαμβάνει μόνο επαυξητικές ρυθμίσεις ασφαλείας, καθώς και τις ρυθμίσεις που απαιτεί για να λειτουργεί σωστά ο ρόλος του. Για παράδειγμα, για να παρέχουμε πρόσθετη ασφάλεια, μπορείτε να συμπεριλάβετε τη ρύθμιση Αποτροπή εγκατάστασης IIS (Prevent IIS Installation), από το Computer Configuration → Policies → Administrative Templates → Windows Components → Internet Information Services, σε αυτό το πρότυπο βάσης. Με αυτόν τον τρόπο, κανείς δεν θα μπορεί να εγκαταστήσει IIS σε κανέναν από τους διακομιστές μελών. Στη συνέχεια, μπορούμε να απενεργοποιήσουμε αυτήν τη ρύθμιση στο στοιχειώδες GPO που εφαρμόζετε σε Application Servers και Dedicated Web Servers OU.

Έλεγχος πρόσβασης διακομιστή Web

Ένας άλλος τομέας όπου απαιτείται έλεγχος ταυτότητας είναι στον διακομιστή Web. Οι υπηρεσίες IIS παρέχουν διάφορους τύπους ελέγχου ταυτότητας, από ανώνυμη σύνδεση έως πλήρη έλεγχο ταυτότητας βάσει πιστοποιητικών. Ο Πίνακας 6.9 παραθέτει τις λειτουργίες ελέγχου ταυτότητας που είναι διαθέσιμες στο IIS 7.

Βασικά, πρέπει να καθορίσουμε ποια λειτουργία ελέγχου ταυτότητας λειτουργεί καλύτερα για εμάς και για τις απαιτήσεις διακομιστή Web. Οι εσωτερικές και εξωτερικές λύσεις θα είναι διαφορετικές και θα υπάρχουν επίσης διαφορές μεταξύ των λύσεων που εφαρμόζουμε σε κάθε δίκτυο.

Ο έλεγχος ταυτότητας IIS ορίζεται στην κονσόλα IIS κάτω από το web site's home location στην ενότητα authentication module. Από προεπιλογή, είναι ενεργοποιημένη μόνο η ανώνυμη λειτουργία ελέγχου ταυτότητας. Τροποποιούμε τις ρυθμίσεις για κάθε λειτουργία ελέγχου ταυτότητας που χρειαζόμαστε. Επιλέγουμε και εφαρμόζουμε την κατάλληλη λειτουργία ελέγχου ταυτότητας για κάθε ιστότοπο.

Mode	Ασφάλεια	Περιορισμοί
Anonymous	Καμία	
Basic	Χαμηλή	Χρήση μόνο με SSL
Digest	Μέτρια	
ASP.NET Impersonation	Υψηλή	
Windows Authentication	Υψηλή	
Forms Authentication	Πολύ Υψηλή	
ADDS Client Certificate Authentication	Πολύ Υψηλή	Τα WS08 παρέχουν αυτόματη εγγραφή και αυτόματη ανανέωση για τα πιστοποιητικά

Πίνακας 6.9

Αυθεντικοποίηση .NET Framework

Δεδομένου ότι το .NET Framework χρησιμοποιεί υπηρεσίες Web, τα μοντέλα ελέγχου ταυτότητας βασίζονται σε μεγάλο βαθμό στις υπηρεσίες IIS, αλλά υπάρχουν ορισμένες βασικές λειτουργίες εντός του ίδιου του .NET Framework. Παρέχει ασφάλεια βάσει ρόλων (RBS). Το RBS στο .NET Framework μπορεί να βασίζεται σε τρεις διαφορετικούς τύπους ελέγχου ταυτότητας: Έλεγχος ταυτότητας βάσει φορμών (δημιουργεί cookie), έλεγχο ταυτότητας IIS και έλεγχο ταυτότητας Windows. Το πρώτο πρέπει να προγραμματιστεί εντός της υπηρεσίας Web. Η δεύτερη και η τρίτη μέθοδος διαχειρίζονται από λειτουργίες δικτύου.

Ο ευκολότερος τρόπος για έλεγχο ταυτότητας χρηστών και εξουσιοδότηση πρόσβασης σε πόρους Web εντός του intranet είναι η ανάθεση ρόλων σε αυτούς. Οι ρόλοι είναι ομάδες που έχουν διαφορετικά επίπεδα πρόσβασης σε κάθε εφαρμογή. Αυτές οι ομάδες είναι συγκεκριμένες για τις εφαρμογές, αλλά μπορούν να αντιστοιχιστούν στα Active Directory Domain Services. Τα Authorization stores πρέπει να δημιουργηθούν πριν από την ομαδική ανάθεση. Αυτό μπορεί να γίνει μέσω της κονσόλας Authorization Manager, η οποία ξεκινά εκτελώντας την εντολή AZMAN.MSC. Το Authorization Manager είναι επίσης ένα συμπληρωματικό πρόγραμμα που μπορεί να προστεθεί σε οποιαδήποτε προσαρμοσμένη κονσόλα MMC. Οι προγραμματιστές πρέπει να δημιουργήσουν το αρχικό store και να το συνδέσουν με μια εφαρμογή και έπειτα οι διαχειριστές μπορούν να εκχωρήσουν χρήστες και ομάδες σε αυτό. Το store μπορεί να βρίσκεται στις Active Directory Domain Services, αλλά ο προγραμματιστής πρέπει να έχει δικαιώματα δημιουργίας store εντός του ADDS για να το πράξει. Αυτό είναι ένα μοντέλο ασφαλείας που είναι πολύ ισχυρό και απαιτεί λιγότερη διαχείριση από τα προηγούμενα σχήματα εξουσιοδότησης εφαρμογών. Βεβαιωνόμαστε ότι οι προγραμματιστές μας προσπαθούν να χρησιμοποιήσουν αυτήν την προσέγγιση κατά τη δημιουργία υπηρεσιών Web για εσωτερική χρήση.

Access Audition and Monitoring

Η τελική πτυχή του Layer 4 είναι το audition. Είναι σημαντικό να παρακολουθούμε τη χρήση πόρων και να παρακολουθούμε αρχεία καταγραφής για να διασφαλίζουμε ότι οι χρήστες έχουν τα κατάλληλα δικαιώματα πρόσβασης και ότι κανένας χρήστης δεν προσπαθεί να κάνει κατάχρηση των δικαιωμάτων του. Το audition είναι μια διαδικασία δύο βημάτων. Πρώτον, πρέπει να ενεργοποιήσουμε την πολιτική ελέγχου για ένα συμβάν. Στη συνέχεια, για συγκεκριμένους τύπους αντικειμένων, πρέπει να ενεργοποιήσουμε τον έλεγχο για το αντικείμενο που θέλουμε να παρακολουθήσουμε και να προσδιορίσουμε ποιος θέλουμε να παρακολουθείτε. Τα WS08 μάς επιτρέπουν να ελέγχουμε διάφορους τύπους συμβάντων:

- Συμβάντα σύνδεσης λογαριασμού
- Διαχείριση λογαριασμών
- Πρόσβαση στην υπηρεσία καταλόγου
- Συμβάντα σύνδεσης
- Πρόσβαση αντικειμένων
- Αλλαγή πολιτικής

- Χρήση προνομίων
- Παρακολούθηση διαδικασίας
- Συμβάντα συστήματος

Η ενεργοποίηση της πολιτικής ελέγχου μπορεί να έχει σημαντικό αντίκτυπο στο δίκτυό μας. Τα ελεγμένα αντικείμενα και τα συμβάντα επιβραδύνουν το σύστημα, επομένως είναι σημαντικό να ελέγχουμε μόνο τα συμβάντα ή τα αντικείμενα που θεωρούμε κρίσιμα στο δίκτυό μας.

Για να ορίσουμε την πολιτική ελέγχου, μεταβαίνουμε στο κατάλληλο GPO και επιλέγουμε Computer Configuration → Policies → Windows Settings → Security Settings → Audit Policy. Κάνουμε διπλό κλικ στο συμβάν που θέλουμε να ελέγξουμε και τροποποιούμε την πολιτική. Μπορούμε να ελέγξουμε την επιτυχία ή την αποτυχία ενός συμβάντος ή και των δύο. Ο έλεγχος αποτυγχάνει μόνο εάν υποπτευόμαστε κακόβουλη δραστηριότητα στο δίκτυό μας. Αυτό θα μειώσει τον αριθμό των συμβάντων που δημιουργούνται από τον έλεγχο.

Εάν θέλουμε να ελέγξουμε την πρόσβαση σε αντικείμενα, όπως η πρόσβαση σε ένα αρχείο σε έναν διακομιστή, πρέπει στη συνέχεια να ενεργοποιήσουμε τον έλεγχο αυτού του αντικειμένου και να προσδιορίσουμε ποιος θέλουμε να ελέγχετε. Για να το κάνουμε αυτό, πρέπει να δούμε τις ιδιότητες ασφαλείας του αντικειμένου και να χρησιμοποιήσουμε το κουμπί Advanced.

Διαχείριση δικαιωμάτων πληροφοριών

Ένα άλλο επίπεδο προστασίας που μπορούμε να εφαρμόσουμε είναι η διαχείριση δικαιωμάτων πληροφοριών. Αυτό εκτελείται μέσω του Active Directory Rights Management Services (ADRMS). Αυτό προστατεύει τις πληροφορίες που δημιουργούμε συνδέοντας τα πιστοποιητικά PKI στη δομή του εγγράφου. Η υποδομή ADRMS βασίζεται στον ρόλο του διακομιστή ADRMS, σε μια βάση δεδομένων, σε αυτήν την περίπτωση στην εσωτερική βάση δεδομένων των Windows, και σε έναν πελάτη. Είναι καλή ιδέα να εφαρμόσουμε το ADRMS μαζί με το Active Directory Certificate Services, καθώς πρέπει να βασιζόμαστε σε πιστοποιητικά για να λειτουργήσει το ADRMS. Φυσικά, μπορούμε επίσης να βασιστούμε σε εξωτερικά πιστοποιητικά για το σκοπό αυτό.

Το ADRMS θα προστατεύσει τις πληροφορίες με τον ακόλουθο τρόπο:

- Έχει σχεδιαστεί για ενσωμάτωση τόσο σε προσαρμοσμένες όσο και σε εμπορικές εφαρμογές, όπως το Microsoft Office. Αυτό το επίπεδο προστασίας μας επιτρέπει να καθορίσουμε ποιος μπορεί να ανοίξει, να τροποποιήσει, να εκτυπώσει, να προωθήσει ή να χειριστεί με άλλο τρόπο πληροφορίες που περιέχονται σε μορφή εγγράφου. Τα έγγραφα μπορούν να είναι παρουσιάσεις, μηνύματα ηλεκτρονικού ταχυδρομείου, κείμενο, υπολογιστικά φύλλα και ούτω καθεξής.
- Η προστασία ADRMS διαρκεί επειδή η προστασία βρίσκεται στο επίπεδο του εγγράφου και παραμένει ακόμη και αν το έγγραφο είναι πέρα από τα όρια του δικτύου μας.
- Το ADRMS είναι επίσης επεκτάσιμο και μπορεί να ενσωματωθεί σε άλλους μηχανισμούς προστασίας εγγράφων τρίτων.

- Το ADRMS μπορεί να συνδυαστεί με τις υπηρεσίες Active Directory Federation Services για τη δημιουργία μιας πλήρους δομής ομόσπονδης ταυτότητας που υποστηρίζει επίσης τη διαχείριση δικαιωμάτων.

Βασικά, το ADRMS εφαρμόζει μια υποδομή που μας επιτρέπει να εκδίδουμε άδειες σε χρήστες, ώστε να προστατεύουν περαιτέρω τις πληροφορίες που δημιουργούν. Είναι μια καλή προσθήκη σε κάθε οργανισμό που απαιτεί πλήρη προστασία εγγράφων ανά πάσα στιγμή.

Επίπεδο 5 - Εξωτερική πρόσβαση

Το Επίπεδο 5 εστιάζει στο περιμετρικό δίκτυο και στην προστασία του εσωτερικού μας δικτύου από εξωτερικές επιρροές. Στον σημερινό συνδεδεμένο κόσμο, είναι αδύνατο να δημιουργηθούν εσωτερικά δίκτυα που είναι πλήρως αποσυνδεδεμένα από τον εξωτερικό κόσμο. Εξαιτίας αυτού, πρέπει να ασφαλίσουμε το εσωτερικό δίκτυο όσο το δυνατόν περισσότερο, στην πραγματικότητα, δημιουργώντας ένα εμπόδιο που πρέπει να διασχίσει κανείς πριν εισέλθει. Αυτό το εμπόδιο μπορεί να λάβει πολλές διαφορετικές μορφές, αλλά στην περίπτωση του παράλληλου δικτύου VSO, αυτό σημαίνει τη δημιουργία, ή μάλλον, τη συνεχιζόμενη χρήση του περιμετρικού μας περιβάλλοντος. Αυτό το περιβάλλον ονομάζεται συχνά αποστρατικοποιημένη ζώνη (demilitarized zone ή DMZ).

Τα περιμετρικά δίκτυα μπορούν να περιέχουν οποιονδήποτε αριθμό στοιχείων. Μπορούν να περιοριστούν σε μια σειρά τείχους προστασίας που προστατεύουν το εσωτερικό μας δίκτυο ή μπορούν να περιλαμβάνουν και να περιέχουν τους διακομιστές μας στο Διαδίκτυο, καθώς και τις υπηρεσίες extranet. Εάν συμβαίνει αυτό, αυτό το δίκτυο θα είναι αρκετά περίπλοκο και θα περιλαμβάνει άμυνα σε κάθε στρώμα του Castle Defense System.

Όσον αφορά τις ομάδες πόρων και τις VSO, θα πρέπει να προστατεύσουμε τα συστήματα στα ακόλουθα επίπεδα:

- Οι ομάδες πόρων δεν διαθέτουν περιμετρικό δίκτυο επειδή δεν αλληλεπιδρούν με τους χρήστες και δεν παρέχουν υπηρεσίες σχετικές με τον χρήστη. Ωστόσο, αλληλεπιδρούν με απομακρυσμένους διαχειριστές. Για αυτό το επίπεδο αλληλεπίδρασης, πρέπει να εργαστούμε είτε με SSTP είτε με εικονικές ιδιωτικές συνδέσεις δικτύου IPSec. Θα χρειαστούμε επίσης υποδομή δημόσιου κλειδιού για την υποστήριξη SSTP και έξυπνων καρτών. Θα πρέπει επίσης να διασφαλίσουμε ότι οποιοσδήποτε απομακρυσμένος ιστότοπος θα χρησιμοποιεί IPSec για επικοινωνίες μεταξύ διακομιστών. Μπορούμε επίσης να προσδιορίσουμε ότι πρέπει να εφαρμόσουμε το Network Access Protection για να διασφαλίσουμε ότι οποιοδήποτε σύστημα που συνδέεται με την ομάδα πόρων είναι πάντα ενημερωμένο όσον αφορά τις ενημερώσεις κώδικα ασφαλείας και την προστασία από κακόβουλο λογισμικό.
- Τα Virtual service offerings έχουν περιμετρικό δίκτυο και, επομένως, χρειάζονται προστασία σε πολλά επίπεδα. Τα περιμετρικά δίκτυα για VSO μπορούν να περιλαμβάνουν πλήθος υπηρεσιών, αλλά τις περισσότερες φορές περιλαμβάνουν: α) Απομακρυσμένες συνδέσεις για τελικούς χρήστες που ενεργούν έξω από τις εγκαταστάσεις μας.

β) Federation services για συνεργαζόμενους οργανισμούς.
γ) Network Access Protection για οποιοδήποτε σύστημα θέλει να συνδεθεί στο δίκτυο.
δ) Υποδομές δημόσιου κλειδιού για την προστασία των εφαρμογών που διαθέτουμε στην περίμετρο καθώς και για την υποστήριξη έξυπνων καρτών

Το επίπεδο υλοποίησης είναι πιο ολοκληρωμένο στα VSO από ό, τι στο σύνολο πόρων, καθώς οι ομάδες πόρων αλληλεπιδρούν μόνο με διαχειριστές.

Ασφάλεια διακομιστών με το Windows Server Firewall with Advanced Security

Ένα από τα πρώτα εργαλεία με τα οποία πρέπει να εργαστούμε, όπως με όλους τους διακομιστές σε οποιαδήποτε ζώνη του δικτύου μας, είναι το Windows Server Firewall with Advanced Security (WSFAS).Το τείχος προστασίας των Windows είναι πλέον ενσωματωμένο σε κάθε έκδοση των Windows και εγκαθίσταται από προεπιλογή. Στην πραγματικότητα, από προεπιλογή, όταν εγκαθιστάμε τα WS08, το τείχος προστασίας έχει ρυθμιστεί να απαγορεύει κάθε απομακρυσμένη πρόσβαση. Στη συνέχεια, καθώς διαμορφώνουμε ρόλους για τον διακομιστή μας, τροποποιούμε την προεπιλεγμένη πολιτική τείχους προστασίας για να ανοίξουμε και να ελέγξουμε συγκεκριμένες θύρες δικτύου.

Η διαφορά μεταξύ του βασικού τείχους προστασίας και του WSFAS είναι ότι το τελευταίο συνδυάζει ένα τείχος προστασίας με διαχείριση IPSec σε ένα εργαλείο για την παροχή ολοκληρωμένης διαχείρισης ασφαλών επικοινωνιών. Αυτό σημαίνει ότι χρησιμοποιούμε το WSFAS για τη διαχείριση όχι μόνο εσωτερικών και εξωτερικών επικοινωνιών διακομιστή, αλλά και εικονικών ιδιωτικών συνδέσεων δικτύου.

Στα περισσότερα περιμετρικά δίκτυα, το WSFAS δεν αρκεί από μόνο του. Οι περισσότεροι οργανισμοί θα περιλαμβάνουν επίσης είτε τεχνολογίες προστασίας βάσει υλικού είτε εργαλεία κρατικής επιθεώρησης που βασίζονται σε λογισμικό. Είναι επίσης καλή πρακτική να εφαρμόζουμε κάποια μορφή ανίχνευσης εισβολής στην περίμετρο.

Windows Server Secure Sockets Tunneling Protocol

Παραδοσιακά, οι εικονικές ιδιωτικές συνδέσεις δικτύου στα δίκτυα Windows βασίστηκαν στο πρωτόκολλο IPSec, το οποίο παρέχει μια σύνδεση από άκρο σε άκρο στο επίπεδο δικτύωσης. Ωστόσο, τα IPSec VPN δεν μπορούν να λειτουργήσουν σε κάθε περίπτωση. Για παράδειγμα, όταν χρησιμοποιούμε συσκευές μετάφρασης διευθύνσεων δικτύου ή ακόμη και διακομιστές μεσολάβησης Web, η σύνδεση IPSec VPN θα αποκλείεται στην πύλη. Επιπλέον, τα IPSec VPN είναι πιο περίπλοκα στην εφαρμογή και απαιτούν να έχουμε κάποιο βαθμό ελέγχου στο τελικό σημείο ή στο σύστημα πελάτη που κάνει τη σύνδεση από τον εξωτερικό κόσμο και αυτό συχνά δεν συμβαίνει.

Αυτός είναι ένας λόγος για τον οποίο η Microsoft έχει εφαρμόσει το πρωτόκολλο Secure Sockets Tunneling Protocol. Το SSTP βασίζεται στο HTTP μέσω του Secure Sockets Layer (HTTPS) για τη δημιουργία συνδέσεων VPN μέσω της θύρας 443. Υποστηρίζει προστασία πρόσβασης δικτύου καθώς και IPv6. Όταν δημιουργούμε ένα SSTP VPN, ο υπολογιστής-πελάτης δημιουργεί μία σύνδεση με τον εσωτερικό διακομιστή και όλη η κίνηση ταξιδεύει μέσω αυτής της σύνδεσης. Δεν μπορούμε, ωστόσο, να το

χρησιμοποιήσουμε για να δημιουργήσουμε συνδέσεις site-to-site. Το SSTP βασίζεται σε πιστοποιητικά PKI για τη δημιουργία συνδέσεων. Οι διακομιστές που φιλοξενούν συνδέσεις SSTP πρέπει να έχουν εγκατεστημένα πιστοποιητικά που να περιλαμβάνουν τον έλεγχο ταυτότητας διακομιστή ή την ιδιότητα All-Purpose Enhanced Key Usage για την αποδοχή συνδέσεων SSTP. Αυτός είναι ένας ακόμη λόγος για τον οποίο είναι τόσο σημαντικό να δημιουργήσουμε μια σωστή δομή PKI μέσω ADCS στο δίκτυό μας. Τα SSTP VPN αποτελούν μέρος του ρόλου του διακομιστή Network Policy and Access Services και πρέπει να διαχειρίζονται μέσω του κόμβου της υπηρεσίας δρομολόγησης και απομακρυσμένης πρόσβασης.

Υποδομή δημόσιου κλειδιού

Οι υλοποιήσεις PKI μπορεί να είναι αρκετά περίπλοκες, ειδικά αν πρέπει να τις χρησιμοποιήσουμε για να αλληλεπιδράσουμε με πελάτες και προμηθευτές εκτός του εσωτερικού μας δικτύου. Το κύριο ζήτημα σε αυτό το επίπεδο είναι το θέμα της αρχής: Είμαστε εμείς που λέμε ότι είμαστε και μπορούν να είναι αξιόπιστα τα πιστοποιητικά μας; Σε αυτήν την περίπτωση, θα πρέπει να βασιστούμε σε μια αρχή τρίτου μέρους που ειδικεύεται σε αυτόν τον τομέα για να μας εγγυηθεί και να υποδείξει ότι τα πιστοποιητικά μας μπορούν και πρέπει να είναι αξιόπιστα. Για άλλη μια φορά, τα WS08 μπορούν να παίξουν σημαντικό ρόλο στη μείωση του κόστους PKI σε αυτές τις περιπτώσεις. Δεδομένου ότι περιλαμβάνουν όλες τις δυνατότητες που απαιτούνται για την εφαρμογή μιας υπηρεσίας PKI μέσω του Active Directory Certificate Services, το μόνο που χρειάζεται να κάνουμε είναι να αποκτήσουμε το πιστοποιητικό διακομιστή ρίζας από μια εξωτερική πηγή. Αυτό το πιστοποιητικό θα ενσωματωθεί έπειτα σε κάθε πιστοποιητικό που εκδίδεται από την υποδομή μας. Θα αποδείξει στους πελάτες, τους συνεργάτες και τους προμηθευτές μας ότι είμαστε αυτοί που λέμε ότι είμαστε και δεν θα χρειαστεί να εφαρμόσουμε μια ακριβή λύση PKI τρίτων.

Ωστόσο, δεν χρειαζόμαστε αυτόν τον τύπο πιστοποιητικού για τους σκοπούς του εσωτερικού δικτύου, καθώς ελέγχουμε όλα τα συστήματα εντός του δικτύου και δεν χρειάζεται να αποδείξουμε τον εαυτό μας ή τον οργανισμό μας σε αυτά. Οι υπηρεσίες ADCS υποστηρίζουν διάφορους τύπους καταστάσεων ασφαλείας.

Μπορούμε να τα χρησιμοποιήσετε για:

- Ασφαλείς υπηρεσίες Web, διακομιστές και εφαρμογές
- Ασφαλής και ψηφιακή υπογραφή e-mail
- Υποστήριξη EFS
- Κωδικός υπογραφής
- Υποστήριξη σύνδεσης έξυπνης κάρτας
- Υποστήριξη εικονικής ιδιωτικής δικτύωσης
- Υποστήριξη ελέγχου ταυτότητας απομακρυσμένης πρόσβασης
- Υποστηρίξη της αυθεντικοποίησης των συνδέσμων αναπαραγωγής υπηρεσιών του Active Directory Domain Services μέσω SMTP
- Υποστήριξη ελέγχου ταυτότητας ασύρματου δικτύου

Τα WS08 παρέχουν δύο τύπους αρχών έκδοσης πιστοποιητικών (CAs): αυτόνομη και εταιρική. Το τελευταίο παρέχει πλήρη ενσωμάτωση με ADDS. Το πλεονέκτημα των

εταιρικών CAs είναι ότι επειδή τα πιστοποιητικά τους είναι ενσωματωμένα στον κατάλογο, μπορούν να παρέχουν υπηρεσίες αυτόματης εγγραφής και αυτόματης ανανέωσης. Αυτός είναι ο λόγος για τον οποίο η υπηρεσία PKI που εφαρμόζετε στο εσωτερικό δίκτυο πρέπει να βασίζεται σε εταιρικές CAs.

Οι βέλτιστες πρακτικές PKI απαιτούν πολύ υψηλά επίπεδα φυσικής προστασίας για τις αρχές πιστοποιητικών ρίζας. Αυτό συμβαίνει επειδή η ρίζα CA είναι ο πυρήνας CA για ολόκληρη την ιεραρχία PKI. Εάν καταστραφεί για κάποιο λόγο, ολόκληρη η υποδομή του δημόσιου κλειδιού μας θα καταστραφεί. Επομένως, είναι σημαντικό να καταργήσουμε τη ρίζα CA από τη λειτουργία μόλις εκδοθούν τα πιστοποιητικά της. Δεδομένου ότι θα καταργήσουμε αυτόν τον διακομιστή από τη λειτουργία, είναι λογικό να τον δημιουργήσουμε ως αυτόνομο CA (η αφαίρεση μιας εταιρικής CA από το δίκτυο θα προκαλέσει σφάλματα στο ADDS).

Οι βέλτιστες πρακτικές PKI απαιτούν επίσης διάφορα επίπεδα ιεραρχίας. Στην πραγματικότητα, σε περιβάλλοντα PKI που πρέπει να αλληλεπιδρούν με το κοινό, είναι λογικό να προστατεύονται τα δύο πρώτα επίπεδα της υποδομής και να αφαιρούνται και τα δύο από το δίκτυο. Αλλά σε ένα εσωτερικό περιβάλλον PKI, ειδικά σε αυτό που θα χρησιμοποιείται κυρίως για υπογραφή κώδικα, κρυπτογράφηση, σύνδεση έξυπνης κάρτας και συνδέσεις VPN, δύο επίπεδα είναι επαρκή. Οι δευτερεύουσες CAs πρέπει να είναι εταιρικές CAs, έτσι ώστε να μπορούν να ενσωματωθούν στο ADDS. Για να προσθέσουμε περαιτέρω προστασία στην δευτερεύουσα CAs, δεν την εγκαθιστούμε σε έναν ελεγκτή τομέα. Αυτό θα μειώσει τον αριθμό των υπηρεσιών στον διακομιστή. Ακόμα κι αν το περιβάλλον PKI μας θα είναι εσωτερικό, θα πρέπει να εστιάσουμε σε ένα σωστό σχεδιασμό PKI. Αυτό σημαίνει εφαρμογή μιας διαδικασίας επτά βημάτων:

1. Ανατρέχουμε στις πληροφορίες WS08 PKI και εξοικειωνόμαστε με βασικές έννοιες.
2. Ορίζουμε τις απαιτήσεις του πιστοποιητικού μας. Προσδιορίζουμε όλες τις χρήσεις για εσωτερικά πιστοποιητικά, τα καταχωρούμε και ορίζουμε πώς πρέπει να αποδοθούν.
3. Δημιουργούμε την αρχιτεκτονική μας PKI. Πόσα επίπεδα αρχών έκδοσης πιστοποιητικών θα χρειαστούμε; Πώς θα διαχειριστούμε τις CAs εκτός σύνδεσης; Πόσες CAs απαιτούνται;
4. Δημιουργούμε ή τροποποιούμε τους τύπους πιστοποιητικών που χρειαζόμαστε. Προσδιορίζουμε εάν πρέπει να χρησιμοποιήσουμε πρότυπα. Τα πρότυπα είναι η προτιμώμενη μέθοδος απόδοσης πιστοποιητικών.
5. Διαμορφώνουμε τη διάρκεια του πιστοποιητικού. Η διάρκεια επηρεάζει ολόκληρη την υποδομή. Οι ρίζες CAs πρέπει να έχουν πιστοποιητικά που διαρκούν περισσότερο από τις δευτερεύουσες CAs.
6. Προσδιορίζουμε πώς θα διαχειριστούμε και θα διανείμουμε λίστες ανάκλησης πιστοποιητικών, καθώς και ποιους ρόλους ADCS θέλουμε να συμπεριλάβουμε στην υποδομή μας. Αυτό μπορεί να περιλαμβάνει εγγραφή στο Διαδίκτυο και διαδικτυακούς ανταποκριτές εκτός από CAs.
7. Προσδιορίζουμε το σχέδιο λειτουργίας σας για την υποδομή πιστοποιητικών στον οργανισμό μας. Ποιος θα διαχειριστεί τα πιστοποιητικά; Ποιος μπορεί να τα παρέχει στους χρήστες; Εάν χρησιμοποιούνται έξυπνες κάρτες, πώς αποδίδονται;

Εξετάζουμε κάθε βήμα προτού αναπτύξουμε το ADCS. Αυτό δεν είναι ένα μέρος όπου μπορούμε να κάνουμε πολλά λάθη. Ελέγχουμε διεξοδικά κάθε στοιχείο της αρχιτεκτονικής μας ADCS πριν προχωρήσουμε στην υλοποίησή του στο εσωτερικό μας δίκτυο. Τέλος, ακριβώς όπως όταν δημιουργήσαμε την πολιτική ασφαλείας μας για να ορίσουμε πώς προστατεύουμε το περιβάλλον μας, θα πρέπει να δημιουργήσουμε μια πολιτική πιστοποίησης και να την κοινοποιήσουμε στο προσωπικό μας.

Active Directory Federation Services

Παλιότερα, όταν οι οργανισμοί ήθελαν να αλληλεπιδρούν μεταξύ τους, έπρεπε να μοιραστούν πολύ ευαίσθητες πληροφορίες, συχνά μέσω της εφαρμογής εξωτερικών καταλόγων ADDS. Το πρόβλημα με αυτό είναι ότι κάθε ευαίσθητο store πληροφοριών, όπως ένας κατάλογος, που είναι εκτεθειμένος σε εξωτερικούς πόρους μπορεί να παραβιαστεί εάν ο κακόβουλος εισβολέας είναι αρκετά καταρτισμένος.

Τα WS08 περιλαμβάνουν μια σειρά εργαλείων που αποφεύγουν την ανάγκη εφαρμογής τεχνολογιών ADDS σε περιμετρικά δίκτυα. Για παράδειγμα, εάν σκοπεύουμε να παρέχουμε μόνο πρόσβαση σε μια εξωτερική εφαρμογή, μπορούμε πάντα να βασιζόμαστε σε ADLDS για να το κάνουμε. Το ADLDS παρέχει πολλές από τις δυνατότητες του ADDS χωρίς να εκθέτει πολύ ευαίσθητες πληροφορίες.

Ένας καλύτερος τρόπος παροχής ενοποίησης μεταξύ οργανισμών που θέλουν να μοιραστούν εφαρμογές είναι μέσω της υπηρεσίας Active Directory Federation Services. Το ADFS παρέχει μια απλή, κρυπτογραφημένη διαδικασία ομοσπονδίας ταυτότητας και υποστηρίζει μία σύνδεση στο Web. Επιπλέον, το ADFS μπορεί να ενσωματωθεί στο ADRMS για την παροχή εκτεταμένων υπηρεσιών διαχείρισης δικαιωμάτων πληροφοριών. Η διαδικασία ADFS είναι απλή:

1. Ένας πελάτης θέλει να αποκτήσει πρόσβαση σε μια εφαρμογή Web.
2. Ο διακομιστής Web επαληθεύει με έναν διακομιστή συνένωσης πόρων (RFS) για να διαπιστώσει εάν έχει παραχωρηθεί πρόσβαση στον πελάτη. Επειδή το αίτημα πρέπει να διασχίσει ένα τείχος προστασίας, ο διακομιστής Web επικοινωνεί πρώτα με έναν Resource Federation Proxy Server, ο οποίος στη συνέχεια έρχεται σε επαφή με το πραγματικό RFS.
3. Το RFS ελέγχει με έναν Account Federation Server (AFS), για άλλη μια φορά μέσω διακομιστή μεσολάβησης, για να δει ποια δικαιώματα πρόσβασης έχει ο χρήστης. Το AFS συνδέεται άμεσα με το εσωτερικό ADDS του οργανισμού και αποκτά δικαιώματα πρόσβασης από τον κατάλογο.
4. Το AFS αποκρίνεται στον διακομιστή Web με τα δικαιώματα πρόσβασης του πελάτη.
5. Ο διακομιστής Web παρέχει πρόσβαση στην εφαρμογή.

Η διαδικασία είναι απλή, αλλά η εφαρμογή του ADFS είναι πιο περίπλοκη. Το πλεονέκτημα είναι ότι μέσω του ADFS, κάθε συνεργαζόμενος οργανισμός μπορεί να βασίζεται στους δικούς του εσωτερικούς καταλόγους ADDS για να παρέχει στους χρήστες πρόσβαση σε εξωτερικές εφαρμογές. Αυτό καθιστά τη διαχείριση της πρόσβασης πολύ πιο απλή.

Network Access Protection

Μια άλλη πολύ ισχυρή λειτουργία των WS08 είναι το Network Access Protection. Το NAP ομαδοποιεί μια σειρά τεχνολογιών για την προστασία των δικτύων μέσω της επικύρωσης των διαμορφώσεων πελατών πριν από τη δημιουργία σύνδεσης με εσωτερικούς πόρους του δικτύου. Αυτό σημαίνει ότι οι πελάτες που δεν συμμορφώνονται με συγκεκριμένες πολιτικές υγείας (για παράδειγμα έχοντας ενημερωμένες υπογραφές προστασίας από ιούς, ενημερωμένες ενημερώσεις λογισμικού ή ενημερωμένα service pack) βρίσκονται σε καραντίνα σε μία ζώνη περιορισμένων πόρων του δικτύου, και όταν επικυρώσουν ότι είναι ενημερωμένοι, παρέχεται μια πλήρως λειτουργική σύνδεση δικτύου. Αυτό το επίπεδο προστασίας είναι χρήσιμο τόσο για ομάδες πόρων όσο και για VSO.

Το NAP παρέχει καραντίνες ή περιορισμένη εφαρμογή πρόσβασης για τις ακόλουθες τεχνολογίες:

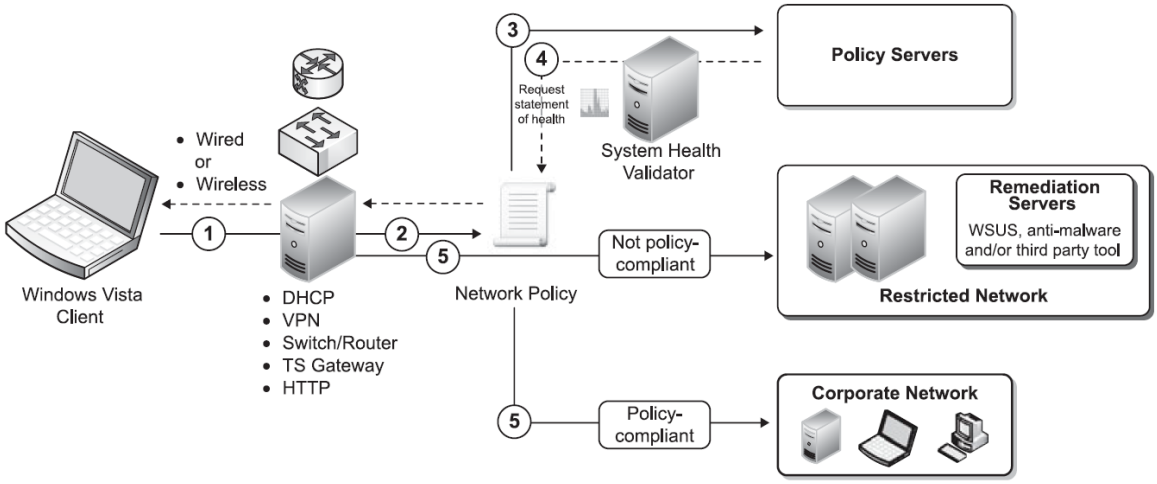
• Συνδέσεις IPSec
• Ενσύρματες (IEEE 802.3) συνδέσεις
• Ασύρματες (IEEE 802.11) συνδέσεις
• Συνδέσεις DHCP
• Εικονικά ιδιωτικά δίκτυα (Virtual private networks)
• Συνδέσεις τερματικών υπηρεσιών
• Host Credential Authorization Protocol (HCAP) που βασίζονται σε HTTP

Το NAP βασίζεται σε έναν διακομιστή επικύρωσης υγείας για να προσδιορίσει την κατάσταση υγείας των συσκευών που ζητούν συνδέσεις. Τα συστήματα NAP περιλαμβάνουν διακομιστές αποκατάστασης, διακομιστές επιβολής, διακομιστές υγείας και συστήματα διαχείρισης πολιτικής. Βασικά, οποιαδήποτε σύνδεση με το δίκτυο μπορεί να προστατευτεί, αρκεί ο πελάτης να υποστηρίζει αυτό το επίπεδο προστασίας. Όταν θέλουμε καθορίζουμε το επίπεδο προστασίας που θέλουμε να εφαρμόσουμε. Μόλις τεθεί σε εφαρμογή, τα αιτήματά σύνδεσης θα περνούν πάντα μέσω του Network Policy Server, όπως φαίνεται στην εικόνα 6.64, και θα λειτουργεί ως εξής:

1. Ο πελάτης θα ξεκινήσει ένα αίτημα σύνδεσης χρησιμοποιώντας είτε ενσύρματη είτε ασύρματη σύνδεση.
2. Ο πάροχος σύνδεσης (HTTP, DHCP, VPN, Switch, Router ή TS Gateway) θα επαληθεύσει με την Πολιτική δικτύου για να δει τι πρέπει να κάνει με το αίτημα σύνδεσης.
3. Οι Network Policy Servers θα παρέχουν στον πάροχο την κατάλληλη πολιτική. Η πολιτική θα πρέπει να ζητήσει επικύρωση υγείας του πελάτη.
4. Οι επικυρωτές υγείας συστήματος θα καθορίσουν την κατάσταση υγείας του πελάτη και θα τον επιστρέψουν στον πάροχο ζητώντας μια δήλωση υγείας από τον πελάτη.
5. Με βάση την κατάσταση υγείας του πελάτη, θα συμβεί μία από τις δύο ενέργειες:
    - Εάν ο πελάτης δεν θεωρείται υγιής, τότε θα κατευθυνθεί προς ένα περιορισμένο δίκτυο. Το περιορισμένο δίκτυο θα βάλει σε καραντίνα το σύστημα έως ότου τεθεί σε υγιή κατάσταση. Το περιορισμένο δίκτυο συνεπώς θα περιλαμβάνει μόνο πρόσβαση σε διακομιστές αποκατάστασης (Windows Server Update Services, Anti-malware ή / και άλλο εργαλείο

διαχείρισης διαμόρφωσης). Μόλις ενημερωθεί ο πελάτης, η κατάσταση υγείας του ενημερώνεται έτσι ώστε ο πάροχος να μπορεί να του δώσει πλήρη πρόσβαση στο δίκτυο.

- Εάν ο πελάτης κριθεί υγιής ή ενημερωθεί σε κατάσταση όπου θεωρείται υγιής, του επιτρέπεται η πλήρης πρόσβαση στο δίκτυο.



Εικόνα 6.64

6.5. IIS Web Servers

Οι διακομιστές Web, είτε είναι dedicated είτε όχι, βασίζονται στις υπηρεσίες Microsoft Internet Information Services (IIS). Το IIS έχει θεωρηθεί ως το πιο αδύναμο σημείο των Windows στο παρελθόν. Σε παλαιότερες εκδόσεις των Windows, εγκαθίστονταν από προεπιλογή και συχνά δεν ήταν διαχειριζόμενο με τον τρόπο που θα έπρεπε. Αυτό δεν είναι πλέον πρόβλημα με τα WS08, καθώς δεν υπάρχει προεπιλεγμένος ρόλος διακομιστή. Εάν εγκαταστήσουμε έναν ρόλο διακομιστή, το κάνουμε συνειδητά και, ως εκ τούτου, πρέπει να γνωρίζουμε ότι αυτό θα απαιτήσει διαχείριση σε κάποιο βαθμό.

Πολλά χαρακτηριστικά του IIS έχουν τροποποιηθεί στα Windows Server 2008:

- Το IIS 7 έχει πλέον χωριστεί σε λειτουργικές μονάδες που εγκαθιστάτε και ενεργοποιούνται όπως απαιτείται. Για παράδειγμα, εάν χρειαζόμαστε Server Side Includes (SSI) στον διακομιστή Web, τότε πρέπει να εγκαταστήσουμε το στοιχείο SSI για να το εκτελέσουμε. Το IIS περιλαμβάνει πλέον περισσότερα από 30 στοιχεία που μπορούμε να εγκαταστήσουμε και να διαμορφώσουμε ανάλογα με τις ανάγκες μας.
- Το IIS Manager, η κονσόλα διαχείρισης του IIS, έχει κάθε στοιχείο ξεκάθαρο και εύκολο στην πρόσβαση. Περιλαμβάνει χαρακτηριστικά και προβολή περιεχομένου. Η προβολή περιεχομένου παρέχει μια διεπαφή παρόμοια με τις προηγούμενες εκδόσεις του IIS. Η προβολή δυνατοτήτων μας παρέχει πρόσβαση σε διεπαφές διαχείρισης για καθένα από τα εγκατεστημένα στοιχεία.
- Ο τρόπος εκτέλεσης για τον IIS είναι εντελώς διαφορετικός στα WS08. Κάθε εφαρμογή που εκτελείται στο IIS 7 εκτελείται στο δικό της περιβάλλον εκτέλεσης ή σε μια ομάδα εφαρμογών και είναι πλήρως απομονωμένη από άλλες εφαρμογές. Εάν μια εφαρμογή θέλει να εκτελέσει παράνομες λειτουργίες, δεν μπορεί να επηρεάσει άλλες εφαρμογές που εκτελούνται στον ίδιο διακομιστή. Οι υπηρεσίες IIS μπορούν επίσης να επανεκκινήσουν αυτόματα εφαρμογές μετά τη διακοπή λειτουργίας, περιορίζοντας τη ζημιά που μπορεί να έχει μια επίθεση denial-of-service σε κάθε εφαρμογή. Η απομόνωση εφαρμογών εμφανίζεται αυτόματα στο IIS 7 κάθε φορά που προστίθεται μια νέα εφαρμογή στο διακομιστή Web.
- Η έκδοση Web των WS08 περιλαμβάνει μόνο έναν ρόλο: Web Services (IIS) που δεν είναι εγκατεστημένο από προεπιλογή. Αυτή η έκδοση του WS08 είναι μια ειδική έκδοση που έχει σχεδιαστεί για να παρέχει εναλλακτική λύση χαμηλού κόστους σε διακομιστές Web που δεν είναι Windows. Χρησιμοποιεί τις ίδιες προσεγγίσεις με τις υπηρεσίες IIS για διαχείριση και παρακολούθηση διακομιστών που εκτελούν αυτήν την έκδοση.
- Προηγουμένως, οι υπηρεσίες IIS θα εγκαθιστούσαν μια ολόκληρη σειρά στοιχείων, επειδή η δομή του ήταν μονολιθική. Αυτό αύξησε την επιφάνεια επίθεσης. Φυσικά, είχαμε τον έλεγχο κατά πόσον τα στοιχεία ήταν ενεργοποιημένα ή όχι, αλλά αφού εγκαταστάθηκαν, θα μπορούσαν να προσφερθούν σε κακόβουλη χρήση. Το IIS 7 δεν απαιτεί ενεργοποίηση στοιχείων. Εάν επιλέξουμε να εγκαταστήσουμε το στοιχείο, ενεργοποιείται. Εάν δεν είναι εγκατεστημένο, δεν μπορεί να ενεργοποιηθεί κακόβουλα ή ακούσια.

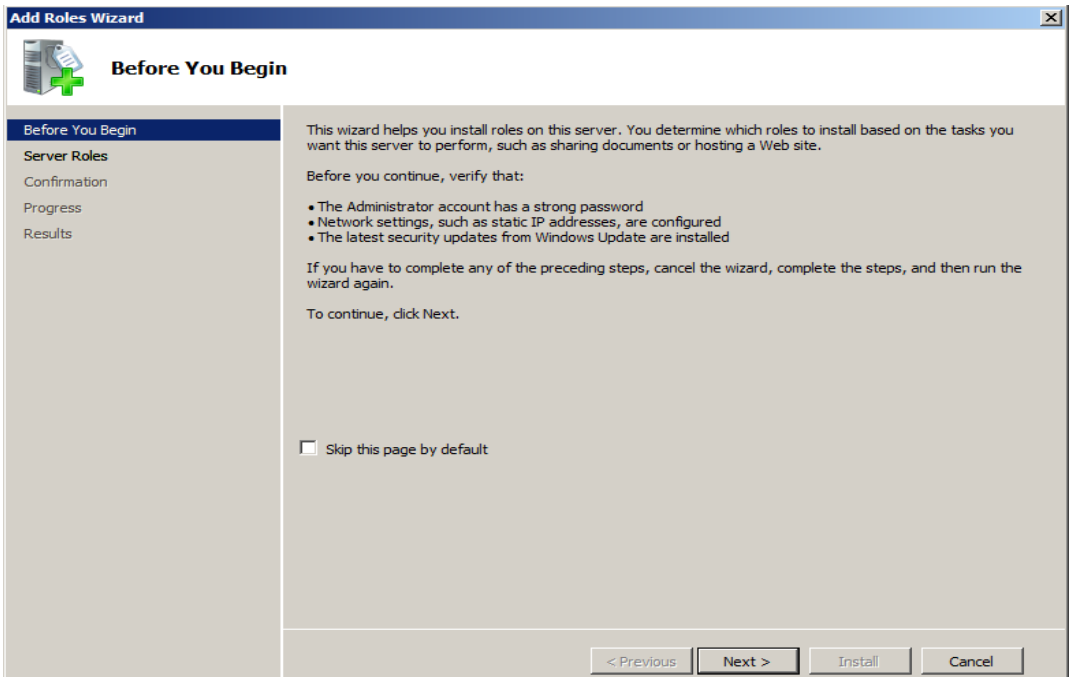
- Οι υπηρεσίες IIS δεν απαιτούνται πλέον στους περισσότερους διακομιστές μας. Επιπλέον, δεν πρέπει να τοποθετούμε τις υπηρεσίες IIS σε κανέναν από τους ελεγκτές τομέα μας εάν είναι δυνατόν. Μπορεί να υπάρχουν ορισμένες περιπτώσεις όπου δεν έχετε καμία επιλογή σε αυτό το θέμα (για παράδειγμα, στην περίπτωση διακομιστών πολλαπλών χρήσεων).

6.5.1. Εγκατάσταση Application ή Dedicated Web Server Role

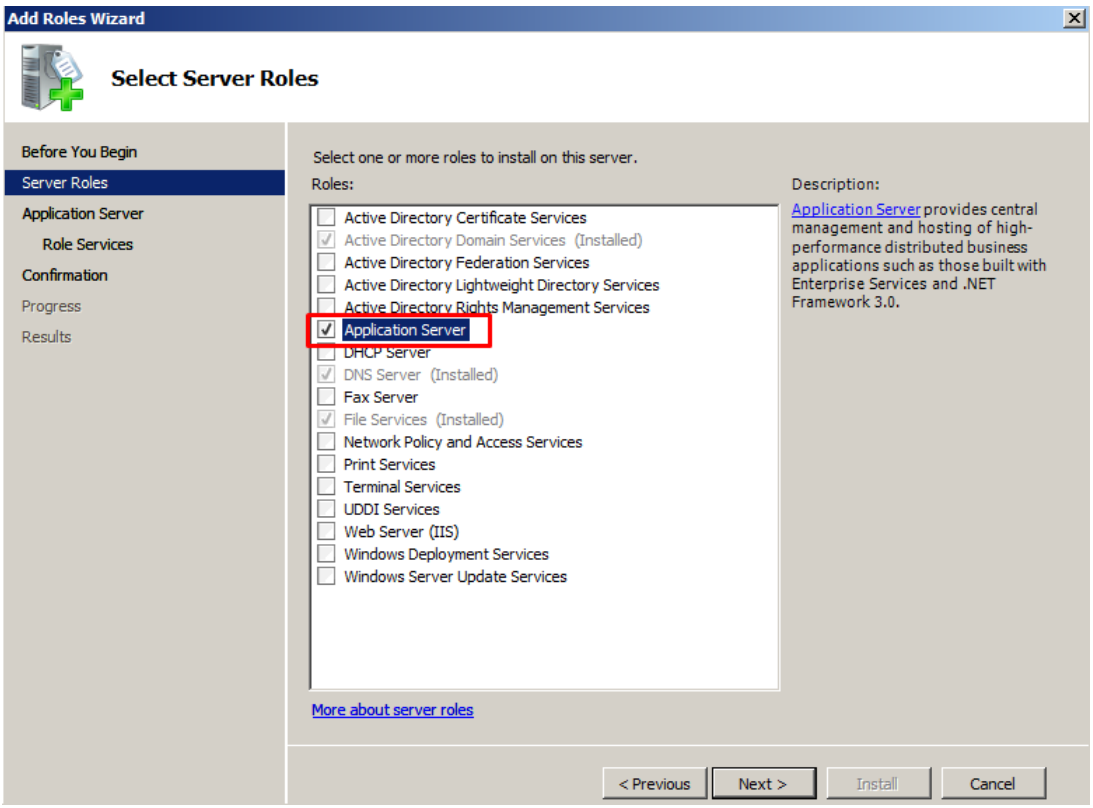
Ο ρόλος διακομιστή Application και ο ρόλος διακομιστή Dedicated Web είναι παρόμοιοι επειδή και οι δύο μπορούν να βασίζονται στο IIS για να παρέχουν μια πλατφόρμα για την εκτέλεση εφαρμογών. Η κύρια διαφορά είναι ότι ο ρόλος του Dedicated Web server βασίζεται στην έκδοση Web του Windows Server 2008. Ο ρόλος του Application server βασίζεται στις άλλες τρεις εκδόσεις. Υπάρχουν πολλές εργασίες που πρέπει να εκτελέσουμε κατά την προετοιμασία των υπηρεσιών IIS Web ή εφαρμογών:

- Όλα ξεκινούν με την προσθήκη του ρόλου στον Server Manager. Κάνουμε δεξί κλικ στους ρόλους στο Server Manager και επιλέγουμε Add Roles.
- Στην έκδοση Web, ο ρόλος ονομάζεται Web Server (IIS) και στις άλλες τρεις εκδόσεις, μπορούμε να επιλέξουμε απλά τον ρόλο του Web Server (IIS) ή μπορούμε να επιλέξουμε τον ρόλο του Application server, ο οποίος θα μας επιτρέψει να συμπεριλάβουμε τον ρόλο Web server. Για λόγους απλότητας, η εγκατάσταση του ρόλου Application server καλύπτεται εδώ.
- Χρησιμοποιούμε τις τιμές στον Πίνακα 6.11 για την εγκατάσταση ρόλων διακομιστή Web.

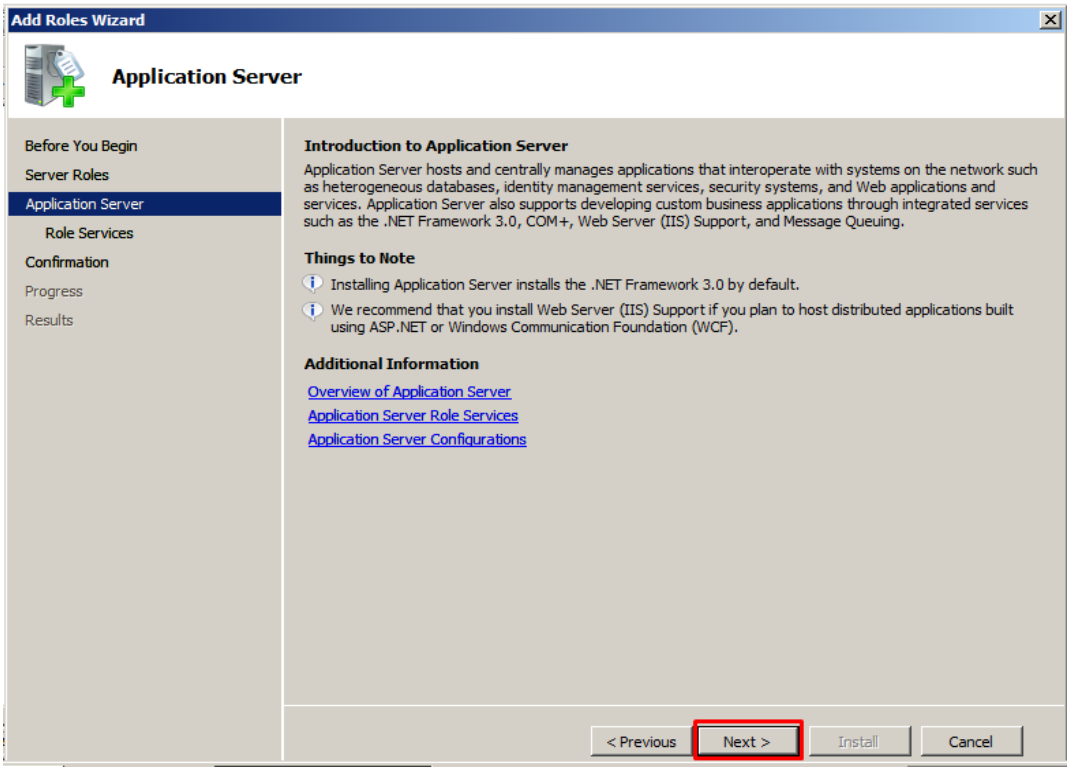
Η διαδικασία μιας τυπικής εγκατάστασης παρουσιάζετε στις παρακάτω εικόνες:



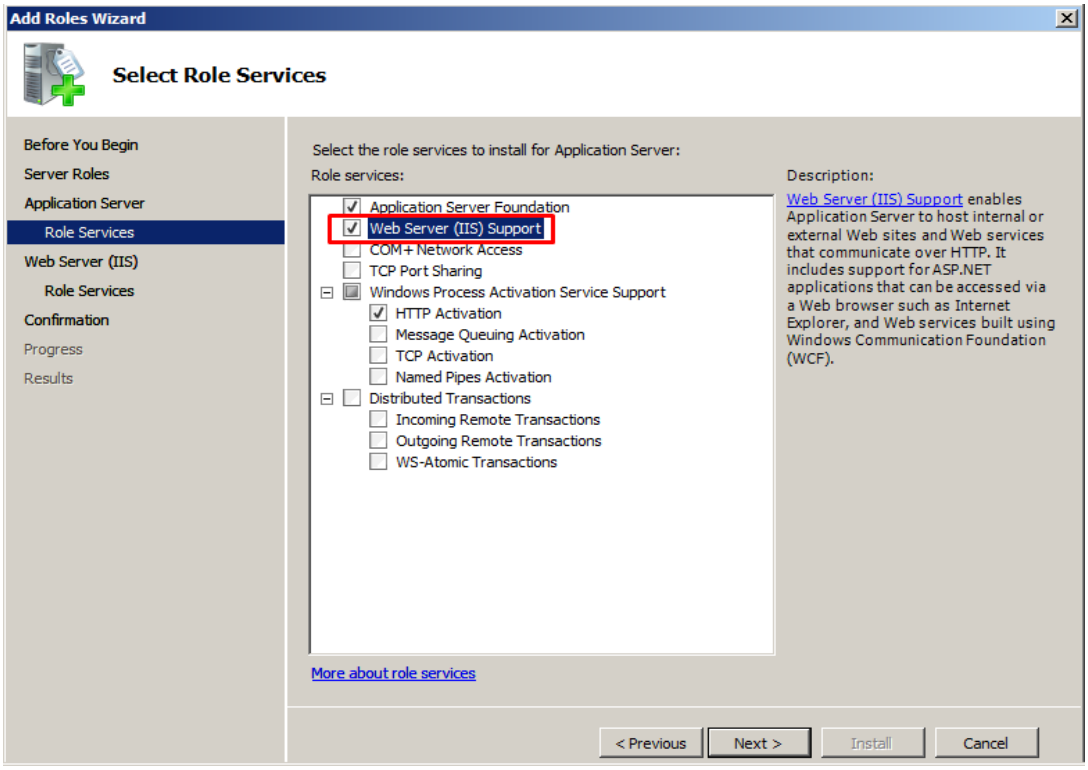
Εικόνα 6.64



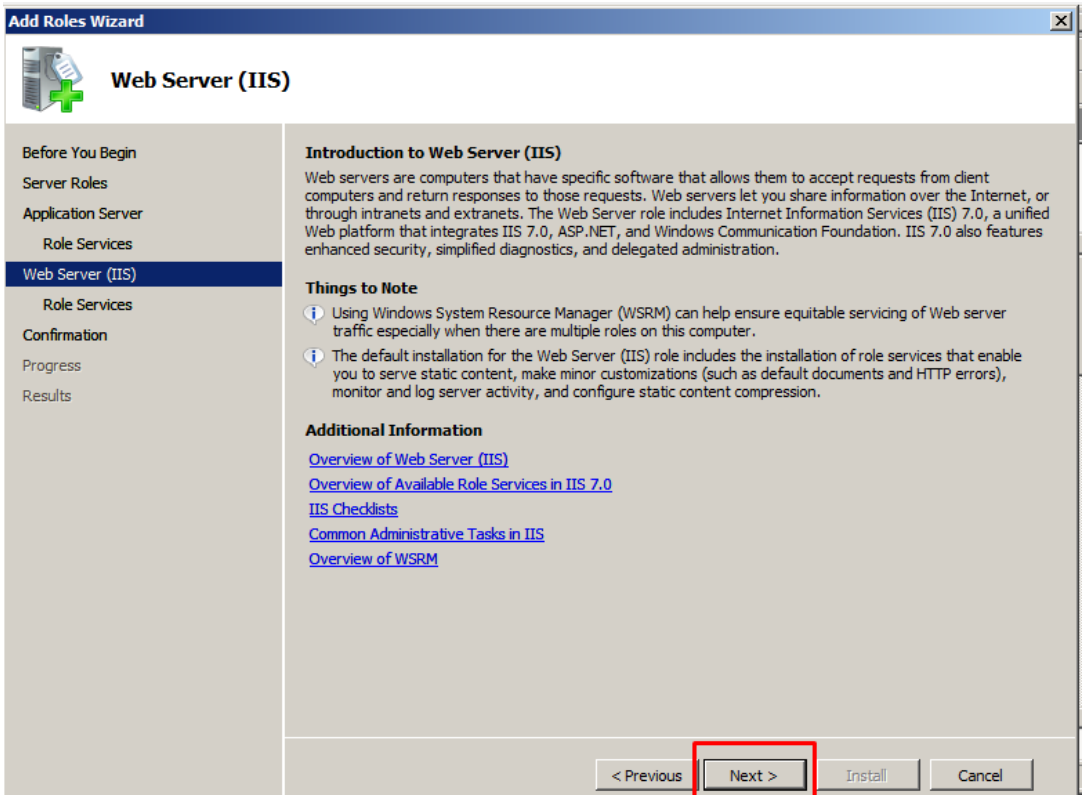
Εικόνα 6.65



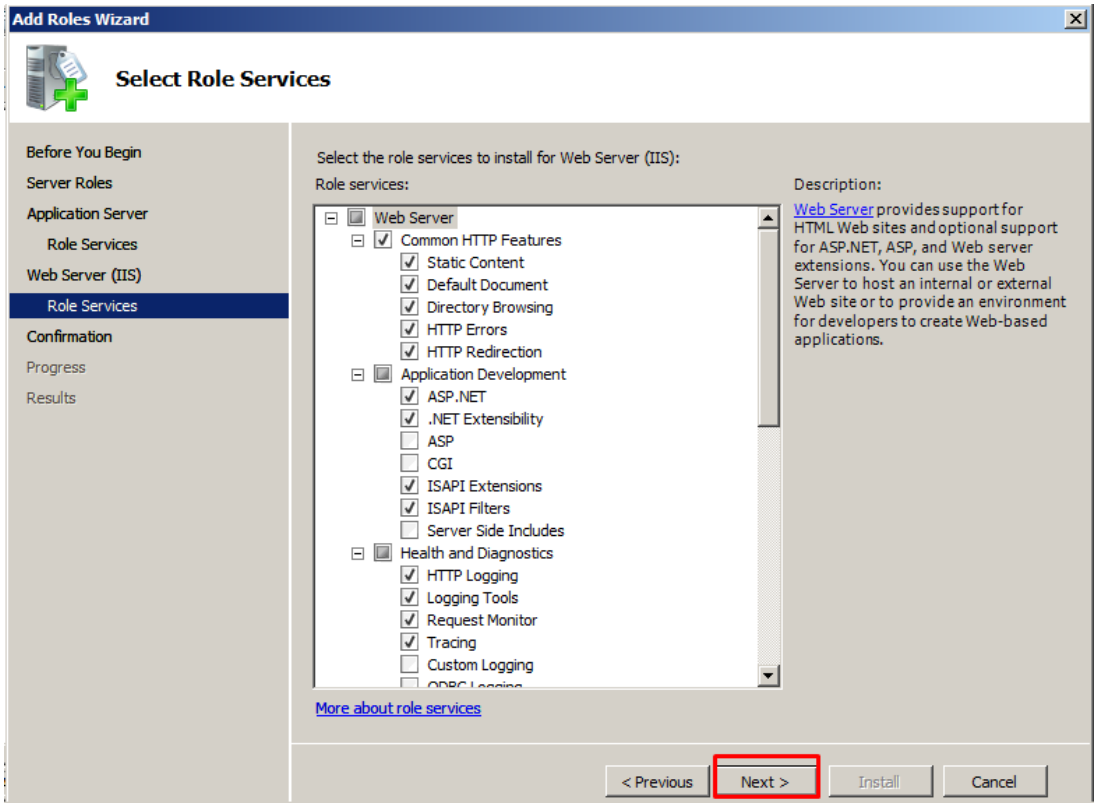
Εικόνα 6.66



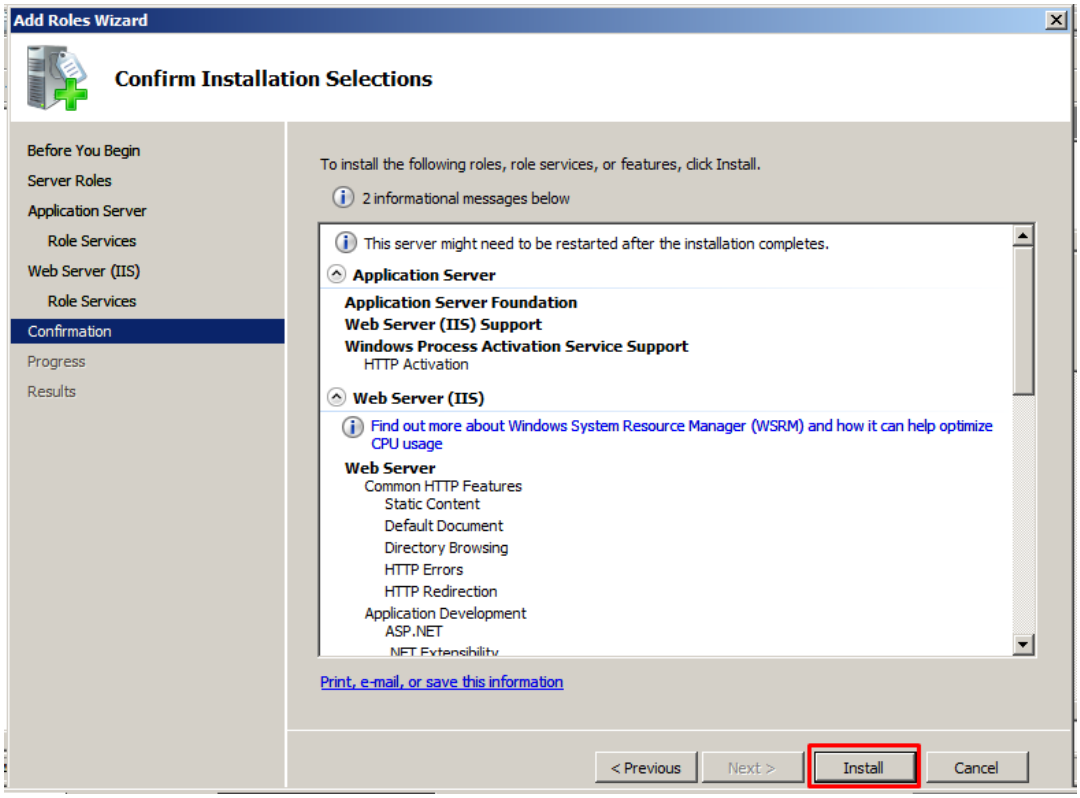
Εικόνα 6.67



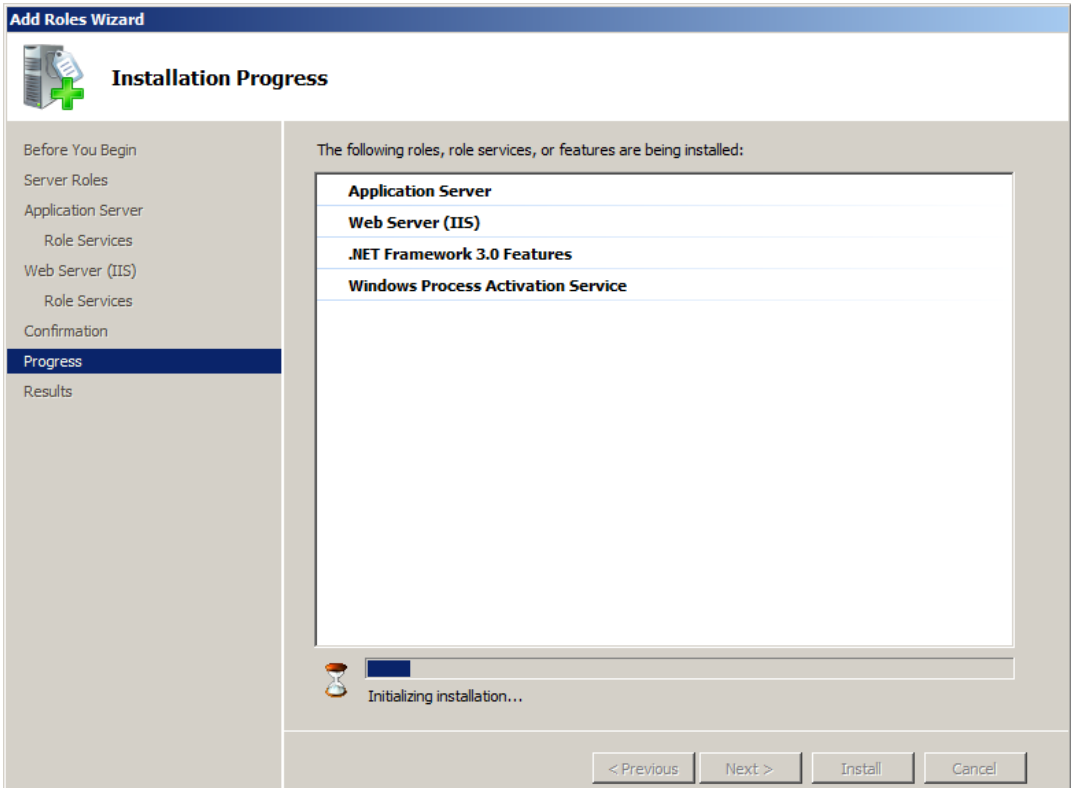
Εικόνα 6.68



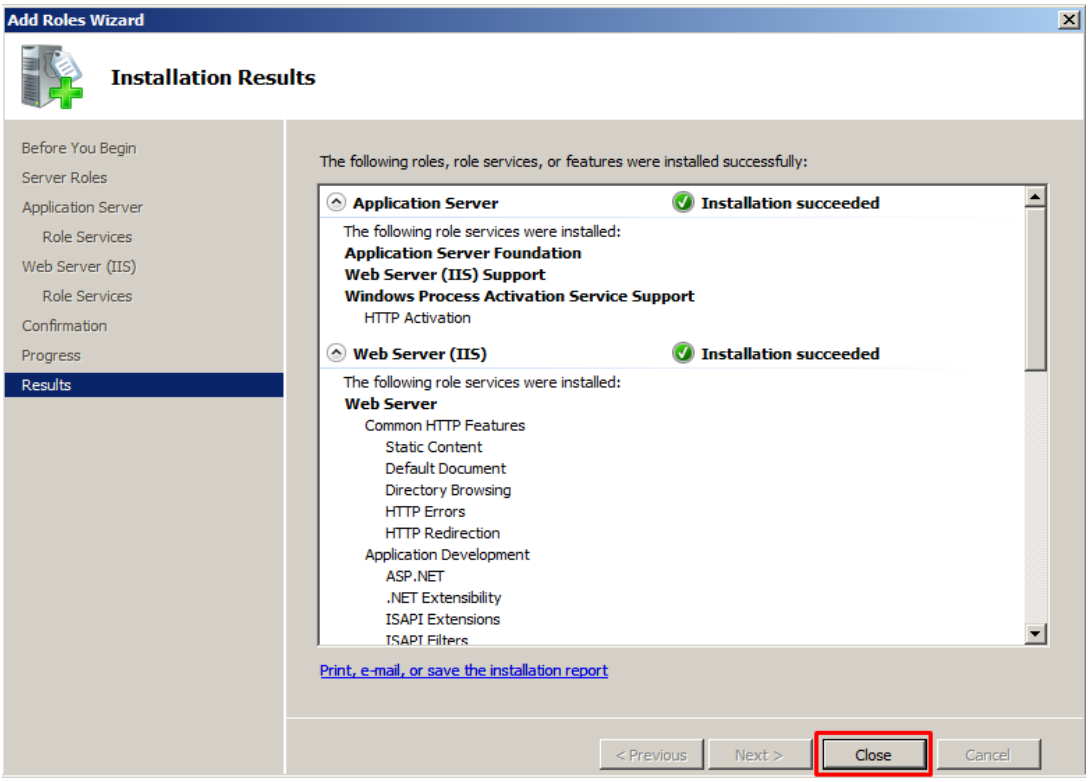
Εικόνα 6.69



Εικόνα 6.70



Εικόνα 6.71



Εικόνα 6.72

Μόλις εγκατασταθεί, θα διαχειριστούμε το IIS μέσω της κονσόλας διαχείρισης του IIS. Αυτή η κονσόλα περιλαμβάνει δύο προβολές:

1. Την προβολή λειτουργιών και
2. Την προβολή περιεχομένου

Η προβολή λειτουργιών χρησιμοποιείται για την πρόσβαση στα στοιχεία που κάνουν τις υπηρεσίες IIS και web sites να τρέχουν. Η προβολή περιεχομένου χρησιμοποιείται για την προβολή των αρχείων που αποτελούν έναν ιστότοπο. Θα πρέπει να αλλάξουμε από τη μία προβολή στην άλλη για να μπορέσουμε να τροποποιήσουμε τις ρυθμίσεις οποιουδήποτε στοιχείου. Αν θέλουμε να τροποποιήσετε τις ιδιότητες των Windows των αντικειμένων που επιλέγουμε, πρέπει να το κάνουμε στην προβολή περιεχομένου.

Το IIS λαμβάνει τη δομή διαμόρφωσης από το ASP.NET και περιλαμβάνει αρχεία διαμόρφωσης που βασίζονται σε XML. Οι προεπιλεγμένες πληροφορίες διαμόρφωσης περιλαμβάνονται σε ένα αρχείο που ονομάζεται applicationHost.config. Αυτό το αρχείο περιέχει ρυθμίσεις διαμόρφωσης σε επίπεδο διακομιστή.

Add Application Server Role Wizard Page	**Τιμή**
Select Server Role	Επιλέγουμε Application Server. Ο ρόλος Web Server (IIS) θα είναι διαθέσιμος καθώς εκτελούμε τις επιλογές για τον κύριο ρόλο του διακομιστή. Στην έκδοση Web, επιλέγουμε το ρόλο Web Server (IIS)
Add Roles Wizard Dialog Box	Όταν επιλέγουμε το ρόλο Application server, ο Server Manager μας προειδοποιεί για τις εξαρτήσεις του. Σε αυτήν την περίπτωση, χρειαζόμαστε επίσης την Windows Process Activation Service μαζί με τα τρία υποστοιχεία της.
Application Server	Ελέγχουμε τις πληροφορίες σχετικά με αυτόν τον ρόλο, εάν απαιτείται, προτού προχωρήσουμε.
Role Services	Διάφορες υπηρεσίες είναι διαθέσιμες για αυτόν τον ρόλο: - Το Application Server Foundation επιλέγεται από προεπιλογή. - Επιλέγουμε Web Server (IIS) Support για να συμπεριλάβουμε την εγκατάσταση διακομιστή Web στον διακομιστή εφαρμογών. Οι απαιτούμενες υπηρεσίες και δυνατότητες θα επιλεγούν αυτόματα. - Προσθέτουμε τις απαιτούμενες υπηρεσίες ρόλου. Αυτό περιλαμβάνει επίσης το .NET Framework έκδοση 3. - Προσθέτουμε πρόσβαση στο δίκτυο COM + για να υποστηρίξουμε την απομακρυσμένη εφαρμογή COM + ή εταιρικών υπηρεσιών. - Προσθέτουμε την κοινή χρήση θύρας Transmission Control Protocol (TCP) για να υποστηρίξουμε την απομόνωση της εφαρμογής, ακόμα και αν μοιράζονται την ίδια θύρα TCP, για παράδειγμα, τη θύρα 80. - Στο Windows Process Activation Service Support η ενεργοποίηση HTTP είναι επιλεγμένη από προεπιλογή. Προσθέτουμε τα Message Queuing Activation, TCP Activation, και Named Pipes Activation με βάση τις απαιτήσεις των εφαρμογών που πρέπει να υποστηρίξουμε. Θα απαιτηθούν πρόσθετες δυνατότητες για την υποστήριξη αυτών των μεθόδων ενεργοποίησης. - Προσθέτουμε Distributed Transactions εάν η εφαρμογή μας θα βρίσκεται σε πολλούς διακομιστές και θα αλληλεπιδρά με πολλές πηγές πληροφοριών.
Server Authentication Certificate	Εάν έχουμε επιλέξει τη μέθοδο WS-Atomic Transactions για την υποστήριξη Distributed Transactions, τότε ο Server Manager θα θέλει να επιλέξουμε και να εγκαταστήσουμε ένα πιστοποιητικό PKI

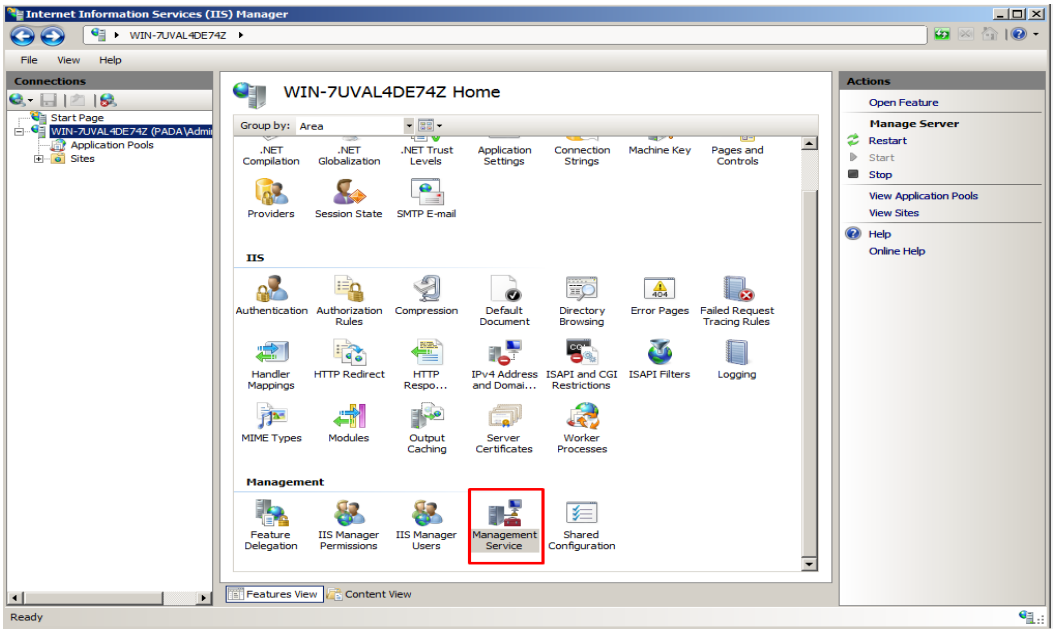
	για έλεγχο ταυτότητας αυτού του διακομιστή σε άλλους. Υπάρχουν τρεις επιλογές: - Επιλέγουμε ένα υπάρχον πιστοποιητικό - Δημιουργούμε ένα αυτοϋπογεγραμμένο πιστοποιητικό - Επιλέγουμε ένα πιστοποιητικό αργότερα Συνιστάται η πρώτη ή τρίτη επιλογή. Εάν είναι δυνατόν, θα πρέπει να επιλέξουμε ένα πιστοποιητικό από μια εξωτερική αρχή έκδοσης πιστοποιητικών (CA), επειδή θα εμπιστευτεί αυτόματα τους πελάτες στο δίκτυό μας. Εάν επιλέξουμε ένα αυτοϋπογεγραμμένο πιστοποιητικό, θα πρέπει να το εγκαταστήσουμε μη αυτόματα σε κάθε πελάτη που αλληλοεπιδρά με αυτόν τον διακομιστή IIS.
Web Server (IIS)	Ελέγχουμε τις πληροφορίες σχετικά με αυτόν τον ρόλο, εάν απαιτείται, προτού προχωρήσουμε.
IIS Role Services	Ορίζουμε τις επιλογές που πρέπει να εγκαταστήσετε για αυτόν τον ρόλο. Επιλέγουμε μόνο τις επιλογές που χρειαζόμαστε. Μπορούμε να προσθέσουμε ή να καταργήσουμε υπηρεσίες ρόλου όταν απαιτείται.
Confirm Installation Selections	Εξετάζουμε τις επιλογές σας πριν συνεχίσουμε. Χρησιμοποιήσουμε το κουμπί Previous για να κάνουμε διορθώσεις, εάν απαιτείται. Κάνουμε κλικ στο Install όταν είμαστε έτοιμοι.
Installation Progress and Installation Results	Ελέγχουμε την πρόοδο της εγκατάστασης και κάνουμε κλικ στο Finish όταν τελειώσει.

Πίνακας 6.11

Στη συνέχεια, μια ιεραρχία αρχείων web.config αποθηκεύεται στον κατάλογο κάθε εφαρμογής και παρέχει περαιτέρω ρυθμίσεις διαμόρφωσης για εφαρμογές. Αν θέλουμε διαμορφώνουμε τις ρυθμίσεις μέσω των ενοτήτων στο IIS Manager και αυτές οι μονάδες πραγματοποιούν τις απαιτούμενες τροποποιήσεις στα αρχεία .config.

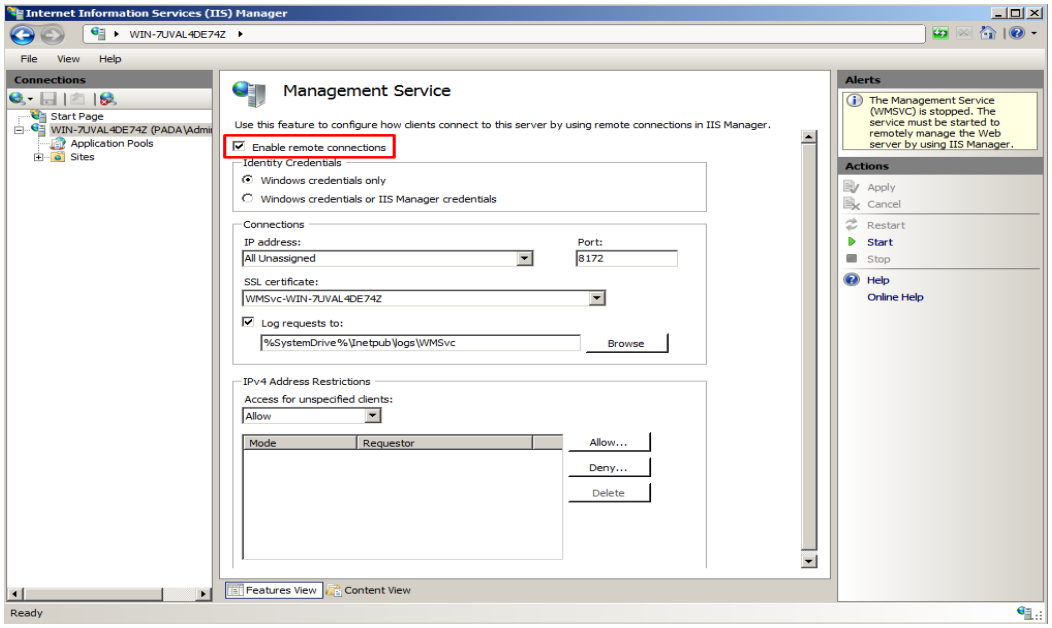
Ο IIS 7 περιλαμβάνει ένα εργαλείο γραμμής εντολών, APPCMD.EXE, το οποίο μας επιτρέπει να δημιουργήσουμε σενάριο (script) για οποιαδήποτε δραστηριότητα στο διακομιστή. Ο IIS Manager υποστηρίζει επίσης απομακρυσμένη διαχείριση μέσω κανονικών θυρών Hypertext Transfer Protocol Secure (HTTPS), όπως το 443. Αυτό ενεργοποιείται τροποποιώντας τις ρυθμίσεις Management Service settings στην ενότητα Management section του παραθύρου λεπτομερειών.

1. Κάνουμε διπλό κλικ στο εικονίδιο Management Service.



Εικόνα 6.73

2. Κάνουμε κλικ στην επιλογή Enable Remote Connections.

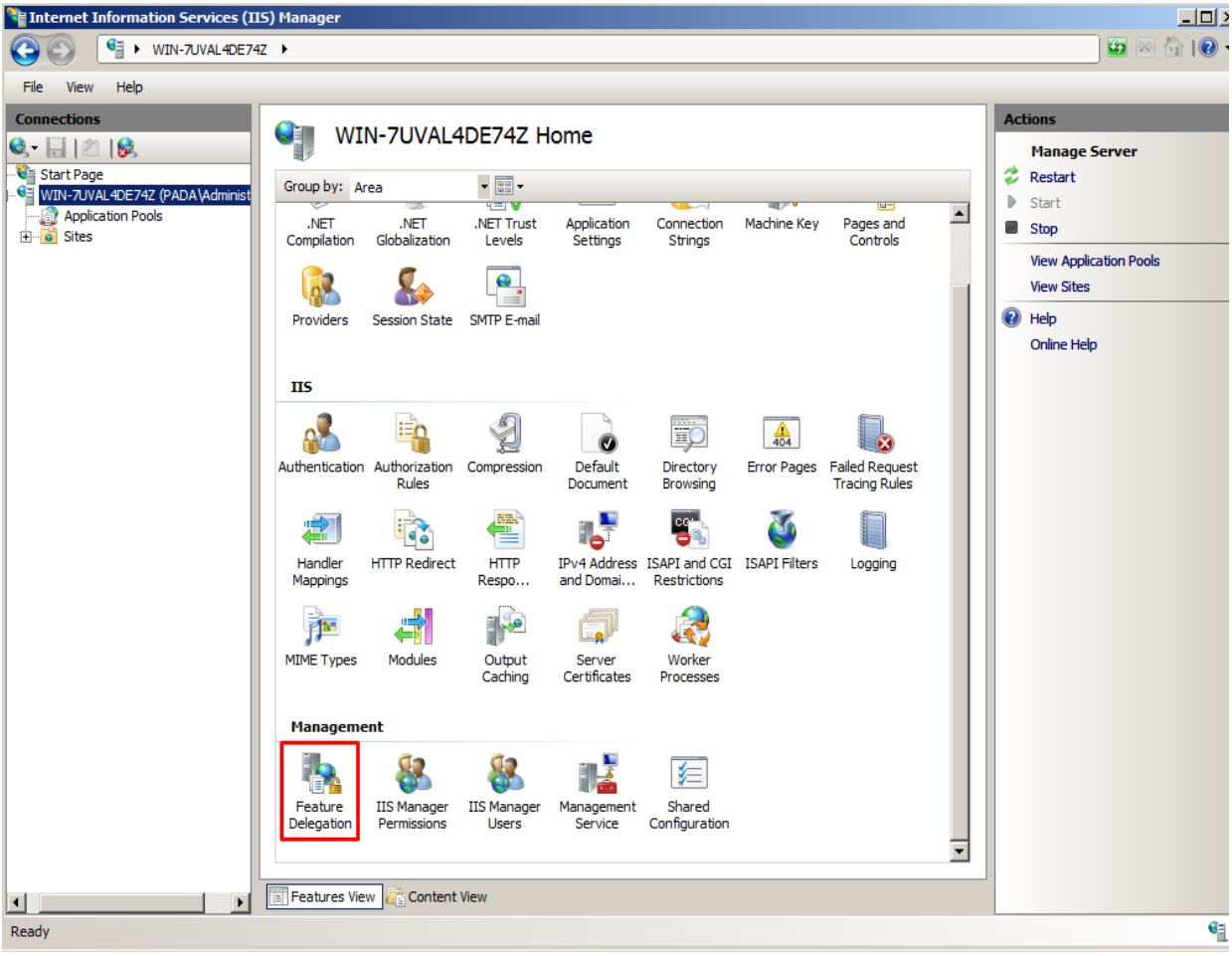


Εικόνα 6.74

3. Προσδιορίζουμε τη λειτουργία ελέγχου ταυτότητας.
4. Μεταβαίνουμε στο παράθυρο και κάνουμε κλικ στο Start για να ξεκινήσουμε την υπηρεσία.
5. Στη συνέχεια, κάνουμε κλικ στο κουμπί Apply στο παράθυρο ενεργειών για να ενεργοποιήσουμε την απομακρυσμένη διαχείριση. Κάνουμε κλικ στο όνομα διακομιστή στο δενδρικό παράθυρο για να επιστρέψουμε στην προβολή δυνατοτήτων.

Μπορούμε να αναθέσουμε οποιαδήποτε δραστηριότητα στην κονσόλα IIS 7. Αυτό πραγματοποιείται μέσω του εικονιδίου Feature Delegation στην ενότητα Management της προβολής δυνατοτήτων, όπως φαίνεται στην εικόνα 6.75.

Διάφορες ρυθμίσεις είναι διαθέσιμες στο παράθυρο ενεργειών: Read/Write, Read Only, Not Delegated, και Reset to Inherited. Ελέγχοντας καθεμία από αυτές τις ρυθμίσεις, μπορούμε να δημιουργήσουμε μια λεπτομερή στρατηγική ανάθεσης για τη διαχείριση των υπηρεσιών IIS. Αυτό είναι ιδανικό για να παρέχει στους διαχειριστές Web τη δυνατότητα διαχείρισης των δικών τους ιστότοπων, αλλά χωρίς τη δυνατότητα διαχείρισης των συνολικών ρυθμίσεων του διακομιστή IIS.



Εικόνα 6.75

6.6. Υπηρεσία DHCP

6.6.1. Κατανόηση των βασικών συστατικών ενός επιχειρηματικού δικτύου

Συχνά, ορισμένα από τα πιο σημαντικά στοιχεία ενός δικτύου παραβλέπονται επειδή κάνουν με συνέπεια τη δουλειά τους και διατηρούν χαμηλό προφίλ. Το Dynamic Host Configuration Protocol (DHCP) και το Windows Internet Naming Service (WINS) είναι δύο τέτοιες υπηρεσίες, που εκτελούν τις λειτουργίες τους και είναι ζωτικής σημασίας σε ένα περιβάλλον δικτύου. Γι' αυτές τις υπηρεσίες πρέπει να δοθεί ιδιαίτερη προσοχή στο σχεδιασμό, τη διαχείριση και τις λειτουργικές απαιτήσεις τους.

Βασικά στοιχεία ενός εταιρικού δικτύου

Παρόλο που ένα εταιρικό δίκτυο έχει πολλά λειτουργικά επίπεδα, παρακάτω επικεντρωνόμαστε σε τρία βασικά στοιχεία που είναι κρίσιμα για τη λειτουργικότητα ενός περιβάλλοντος των Windows 2008. Αυτές οι τρεις πτυχές - διεύθυνση δικτύου, ανάλυση ονόματος και ενοποίηση καταλόγου - παρέχουν τη λειτουργικότητα σε επίπεδο βάσης που αναμένεται από οποιοδήποτε σύγχρονο εταιρικό δίκτυο και παρέχουν τη ραχοκοκαλιά για την υποδομή των Windows 2008.

Η σημασία της διεύθυνσης δικτύου

Η πρώτη κρίσιμη συνιστώσα ενός δικτύου είναι να απευθύνεται ή να επιτρέπει στους πελάτες να αναλαμβάνουν μια λογική θέση σε ένα δίκτυο, έτσι ώστε πακέτα πληροφοριών να μπορούν να προωθούνται από και προς τους πελάτες. Αυτό το στοιχείο πραγματοποιήθηκε ιστορικά από ιδιόκτητα πρωτόκολλα δικτύου, ένα για κάθε λειτουργικό σύστημα δικτύου (NOS). Αυτό έδωσε στους σχεδιαστές της NOS μεγάλη ευελιξία στην προσαρμογή των στοιχείων επικοινωνίας του δικτύου τους στις συγκεκριμένες ανάγκες σχεδίασής τους, αλλά κατέστησε δύσκολη την ανταλλαγή πληροφοριών μεταξύ των δικτύων.

Το Transmission Control Protocol/Internet Protocol (TCP / IP) σχεδιάστηκε για να λειτουργεί μεταξύ διαφορετικών ποικιλιών δικτύων, επιτρέποντάς τους να μιλούν μια κοινή γλώσσα. Η άνοδος αυτού του πρωτοκόλλου συνέπεσε με την ευρεία υιοθέτηση του ίδιου του Διαδικτύου, και αυτή η δημοτικότητα και η πανταχού παρούσα χρήση αυτού του πρωτοκόλλου οδήγησαν τη Microsoft να το επιλέξει ως το τυπικό πρωτόκολλο για τα Windows 2000. Τα Windows 2008 συνεχίζουν να χρησιμοποιούν το TCP / IP ως το προεπιλεγμένο πρωτόκολλο δικτύου.

Το TCP / IP απαιτεί κάθε κόμβος ενός δικτύου να αντιμετωπίζεται από μια μοναδική διεύθυνση IP, όπως 10.23.151.20. Κάθε διεύθυνση IP πρέπει να αντιστοιχιστεί σε κάθε κόμβο ενός δικτύου, είτε χειροκίνητα είτε με αυτόματες μεθόδους. Το στοιχείο αυτόματης διεύθυνσης είναι το μέρος όπου λαμβάνει δράση η υπηρεσία DHCP η οποία παρέχει την αυτοματοποίηση της διεύθυνσης TCP / IP στα Windows 2008 και καθιστά τη διαχείριση ενός δικτύου πιο εύκολη.

Ανάλυση ονόματος (Name Resolution)

Η δεύτερη κρίσιμη πτυχή στα δίκτυα είναι η ανάλυση ονόματος. Επειδή οι άνθρωποι κατανοούν την έννοια των ονομάτων καλύτερα από ό, τι κάνουν τις διευθύνσεις IP, προκύπτει η ανάγκη να μεταφραστούν αυτά τα σύνολα αριθμών σε κοινά ονόματα.

Τα Windows 2008 υποστηρίζουν δύο τύπους ανάλυσης ονομάτων. Ο πρώτος τύπος, το σύστημα ονομάτων τομέα (DNS), μεταφράζει πλήρως αναγνωρισμένα ονόματα τομέα (FQDN) σε διευθύνσεις IP, κάτι που τους επιτρέπει να απευθύνονται σε μια δομή Active Directory ή Internet DNS. Αυτός ο τύπος ανάλυσης ονόματος είναι ο προεπιλεγμένος (και απαιτούμενος) τύπος στα Windows Server 2008. Ο δεύτερος τύπος ανάλυσης ονομάτων, αντιστοίχιση παλαιών ονομάτων Microsoft NetBIOS σε διευθύνσεις IP, παρέχεται από το WINS.

Ενοποίηση καταλόγου

Η τελική σημαντική υπηρεσία που παρέχεται από ένα λειτουργικό εταιρικό δίκτυο είναι η δυνατότητα τοποθέτησης και αναζήτησης καταλόγου. Έχοντας έναν κεντρικό κατάλογο που ελέγχει την πρόσβαση σε πόρους και παρέχει κεντρική διαχείριση είναι μια ζωτικής σημασίας λειτουργία στα σύγχρονα δίκτυα. Οι υπηρεσίες τομέα Active Directory είναι η υπηρεσία καταλόγου που παρέχεται με τα Windows Server 2008 και είναι ενσωματωμένη σε πολλά από τα στοιχεία του λειτουργικού συστήματος. Οι διακομιστές που χειρίζονται αιτήματα σύνδεσης και αλλαγές κωδικού πρόσβασης και περιέχουν πληροφορίες καταλόγου είναι οι ελεγκτές τομέα και ελεγκτές τομέα παγκόσμιου καταλόγου. Στη συνέχεια, ο ελεγκτής τομέα και η καθολική τοποθέτηση καταλόγου είναι ένα κρίσιμο κομμάτι του περιβάλλοντος των Windows Server 2008. Πρέπει να ληφθούν ειδικά θέματα σχετικά με αυτό ιδέα επειδή η πρόσβαση στην αναζήτηση καταλόγου και η εγγραφή είναι το κλειδί για τη λειτουργικότητα του πελάτη σε δίκτυο.

6.6.2. Εξερεύνηση του Dynamic Host Configuration Protocol (DHCP)

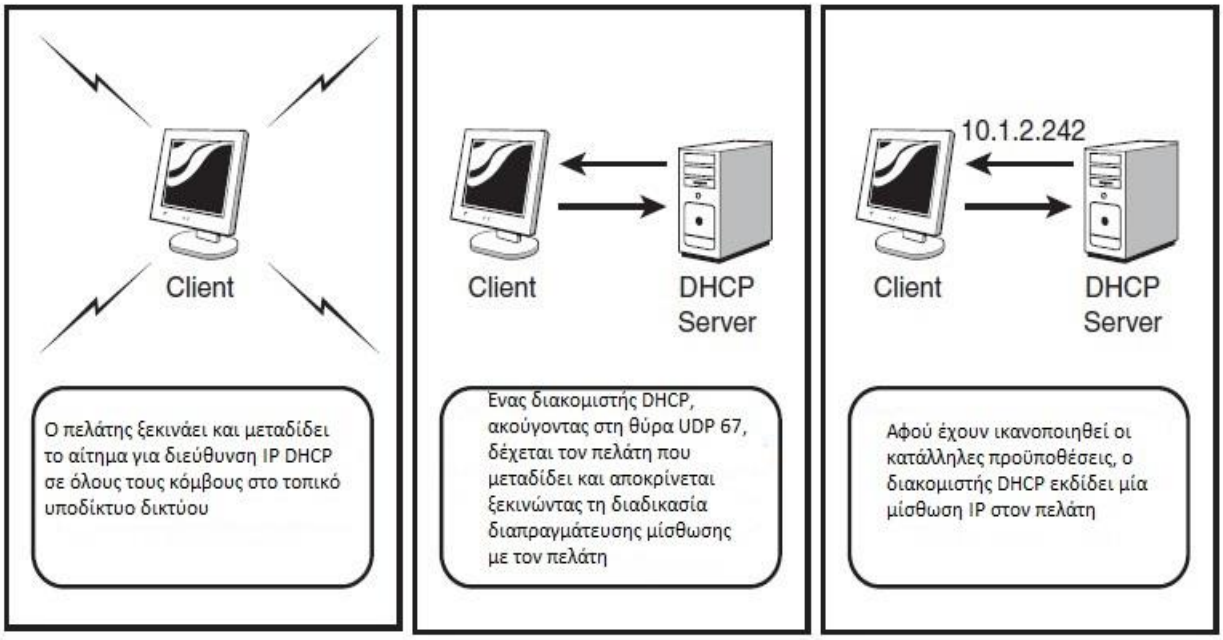
Οι καθημερινές λειτουργίες του TCP/IP μπορεί να είναι περίπλοκες, καθώς οι πελάτες πρέπει να μπορούν να λαμβάνουν και να ενημερώνουν τακτικά τις πληροφορίες δικτύου τους για να συμβαδίζουν με τις αλλαγές στο δίκτυό τους. Κάθε αντικείμενο σε περιβάλλον TCP/IP απαιτεί μια μοναδική διεύθυνση που ορίζει την τοποθεσία και παρέχει ένα μέσο δρομολόγησης πακέτων δικτύου από τόπο σε τόπο. Αυτή η διεύθυνση ή διεύθυνση IP, πρέπει να εκχωρηθεί σε κάθε πελάτη σε ένα δίκτυο για να επιτρέπεται στους πελάτες να επικοινωνούν χρησιμοποιώντας TCP/IP. Στο παρελθόν, πολλές διευθύνσεις IP διανεμήθηκαν μη αυτόματα σε νέους πελάτες που προστέθηκαν σε ένα δίκτυο. Αυτό απαιτούσε μεγάλο διαχειριστικό κόστος για να διατηρηθεί, και συχνά είχε προβλήματα στη διαμόρφωση που μπορεί να έχουν προκληθεί από απλά τυπογραφικά λάθη ως αποτέλεσμα βασικών ανθρώπινων λαθών.

Στη συνέχεια αναζητήθηκε μια αυτόματη μέθοδος διανομής διευθύνσεων IP σε πελάτες όπου τα διοικητικά πλεονεκτήματα ενός τέτοιου συστήματος ήταν προφανή. Η αναζήτηση ενός τέτοιου συστήματος οδήγησε στους προκατόχους του DHCP: RARP και BOOTP.
Η ανάγκη για δυναμική κατανομή διευθύνσεων IP σε πελάτες αντιμετωπίστηκε πρώτα από το πρωτόκολλο ανάλυσης αντίστροφης διεύθυνσης (Reverse Address Resolution Protocol - RARP). Το RARP απλώς εκχωρούσε μια διεύθυνση IP σε ένα πελάτη αφού ο

πελάτης το ζητούσε μέσω εκπομπής δικτύου. Αυτό το πρωτόκολλο γρήγορα ανακαλύφθηκε ότι ήταν αναποτελεσματικό, επειδή χρησιμοποιούνταν σε ένα μόνο δίκτυο, το οποίο μπορούσε να εκχωρήσει μόνο διευθύνσεις IP και όχι μάσκες υποδικτύου, πύλες ή άλλες σημαντικές πληροφορίες για TCP / IP.
Ο διάδοχος του RARP ήταν το Bootstrap Protocol (BOOTP), το οποίο βελτίωσε τη δυναμική εκχώρηση διευθύνσεων IP επιτρέποντας τη δρομολόγηση μέσω διαφορετικών δικτύων και χρησιμοποίησε μία έννοια που ονομάζεται μαγικό cookie, ένα τμήμα 64-byte του πακέτου BOOTP που περιείχε πληροφορίες διαμόρφωσης όπως μάσκα υποδικτύου, ονομασίες διακομιστή DNS και ούτω καθεξής. Αυτό το πρωτόκολλο ήταν μια δραστική βελτίωση σε σχέση με το RARP, αλλά ήταν ακόμη περιορισμένο σε μερικές λειτουργικές περιοχές - δηλαδή, το γεγονός ότι η βάση δεδομένων δεν ήταν δυναμική και αποθηκεύονταν σε στατικό αρχείο κειμένου, το οποίο περιόριζε τη χρηστικότητά του.

Το DHCP αναπτύχθηκε ως βελτίωση του BOOTP. Στην πραγματικότητα, ένα πακέτο DHCP είναι σχεδόν πανομοιότυπο με ένα πακέτο BOOTP, εκτός από την τροποποίηση του μαγικού τμήματος cookie του πακέτου, το οποίο επεκτάθηκε σε μέγεθος για να φιλοξενήσει πρόσθετες επιλογές όπως DNS διακομιστής, διακομιστής WINS και ούτω καθεξής.

Η διαδικασία DHCP είναι απλή. Ένας πελάτης ξεκινά και αποστέλλεται ένα αίτημα μετάδοσης σε όλους τους κόμβους ενός υποδικτύου για το οποίο απαιτείται μια δυναμική διεύθυνση IP. Αυτή η μετάδοση συμβαίνει στη θύρα UDP 68. Ο διακομιστής, ο οποίος ακούει αυτές τις εκπομπές στη θύρα UDP 67, ανταποκρίνεται στο αίτημα του πελάτη εκδίδοντας μια διεύθυνση IP σε ένα προκαθορισμένο εύρος, όπως φαίνεται στην εικόνα 6.76.



Εικόνα 6.76

Εκτός από μια διεύθυνση IP, όλες οι επιλογές που ορίζονται στο πεδίο του διακομιστή εκδίδονται σε ένα πελάτη. Αυτό περιλαμβάνει διακομιστές DNS, διακομιστές WINS, πύλες, μάσκες υποδικτύου και πολλές άλλες ρυθμίσεις. Εάν αυτές οι επιλογές εκδίδονται

αυτόματα, η πιθανότητα σφαλμάτων μειώνεται και ολόκληρη η εκχώρηση διεύθυνσης IP γίνεται αυτοματοποιημένη, μειώνοντας τα διαχειριστικά γενικά έξοδα.

Το τμήμα διακομιστή του DHCP αποτελεί μόνο το μισό μέρος της εξίσωσης σε μια συναλλαγή DHCP. ο Το αίτημα για διεύθυνση IP προέρχεται από μια συγκεκριμένη διεπαφή γνωστή ως πελάτης DHCP. Ο πελάτης είναι εγκατεστημένος με TCP / IP στα Windows 2000 και σε υψηλότερους πελάτες και μπορεί να εγκατασταθεί ως ένα πρόσθετο στοιχείο σε πελάτες χαμηλού επιπέδου. Ο πελάτης DHCP χειρίζεται τις επικοινωνίες με το DHCP Υπηρεσία διακομιστή, όσον αφορά τον χειρισμό αιτημάτων IP και ενημερώσεων. Κάθε επανάληψη του πρόγραμμα-πελάτης των Windows περιλαμβάνει διαφορετικό πρόγραμμα-πελάτη DHCP και υπάρχουν μικρές παραλλαγές στη λειτουργικότητα κάθε πελάτη. Ωστόσο, η συνολική λειτουργία (υποβολή αίτησης και λήψη μιας IP διεύθυνσης από έναν διακομιστή DHCP) παραμένει η ίδια σε κάθε πελάτη των Windows.

Η υπηρεσία Client / Server έχει ενημερωθεί σε υπολογιστές-πελάτες των Windows 2000 και σε υψηλότερες εκδόσεις, επιτρέποντας την αυτόματη εκχώρηση μιας διεύθυνση IP εάν δεν υπάρχει διαθέσιμος διακομιστής. Αυτό επιτυγχάνεται μέσω μιας διαδικασίας που ονομάζεται Αυτόματη ιδιωτική διεύθυνση IP (Automatic Private IP Addressing -APIPA). Οι πελάτες APIPA εκχωρούν αυτόματα σε μια διεύθυνση IP στο εύρος 169.254.0.0/16 σε αυτήν την περίπτωση, κάτι που τους επιτρέπει να υπάρχει βασική συνδεσιμότητα TCP / IP σε μικρά δίκτυα.

Το APIPA μπορεί να είναι προβληματικό σε μεγαλύτερα δίκτυα επειδή αναγκάζει τους πελάτες να αναθέσουν στον εαυτό τους διευθύνσεις σε ένα εύρος που κανονικά δεν είναι μέρος υποδικτύου τοπικής εταιρείας. Εάν ένας DHCP διακομιστής είναι εκτός λειτουργίας, οι πελάτες που προσπαθούν να ανανεώσουν μια μίσθωση με τον διακομιστή θα αποτύχουν και εκχωρούν αυτόματα μια διεύθυνση APIPA. Όταν ο διακομιστής επανέλθει στο διαδίκτυο, δεν θα εγγράψουν αμέσως τον εαυτό τους και θα αποκοπούν αποτελεσματικά από το δίκτυο. Στη συνέχεια, η Microsoft παρέχει ένα κλειδί μητρώου που θα απενεργοποιήσει το APIPA σε αυτή την περίπτωση. Το κλειδί που θα δημιουργηθεί είναι:

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<AdapterName>\ _IPAutoconfigurationEnabled: REG_DWORD = 0

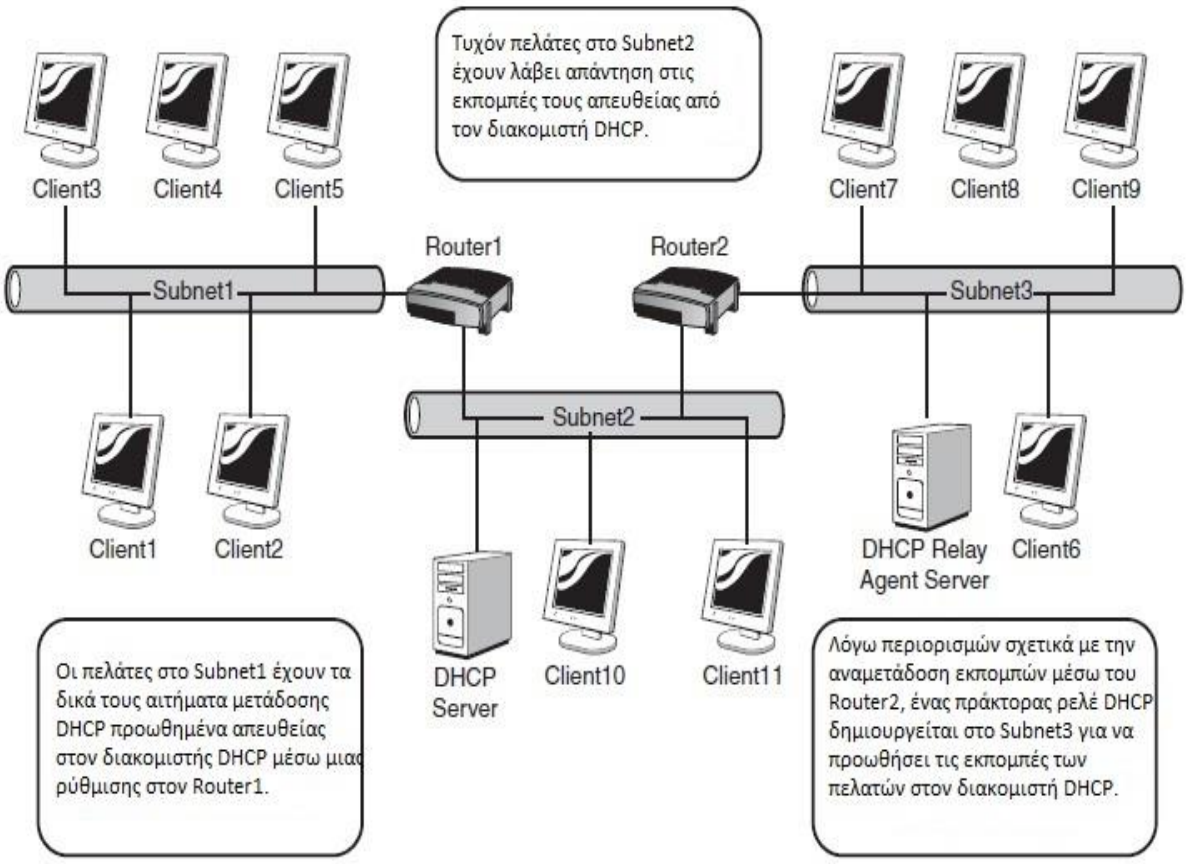
Μπορούμε να δημιουργήσουμε αυτό το κλειδί ακολουθώντας αυτά τα βήματα στον πελάτη:

1. Ανοίγουμε τον Επεξεργαστή Μητρώου (επιλέγουμε Έναρξη, Εκτέλεση και, στη συνέχεια, πληκτρολογούμε regedit).
2. Θα πρέπει να μεταβούμε στο HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\Tcpip\Parameters_Interfaces\<AdapterName>(όπου το AdapterName είναι η δεκαεξαδική αναπαράσταση του εν λόγω προσαρμογέα δικτύου).
3. Κάνουμε δεξί κλικ στο πλήκτρο <AdapterName> και επιλέγουμε νέα, τιμή DWORD.
4. Πληκτρολογούμε IPAutoconfigurationEnabled για να μετονομάσουμε την τιμή DWORD.
5. Κάνουμε διπλό κλικ στη νέα τιμή και βεβαιωνόμαστε ότι το 0 έχει εισαχθεί ως δεδομένα τιμής.

6. Κάνουμε κλικ στο OK και κλείνουμε τον Επεξεργαστή Μητρώου.

Για να επιβεβαιώσουμε ότι το APIPA είναι απενεργοποιημένο, ένας διαχειριστής θα πρέπει να εκτελέσει την εντολή IPCONFIG /ALL από τη γραμμή εντολών και, στη συνέχεια, μπορεί να ελέγξει ότι έχει οριστεί στην επιλογή Autoconfiguration Enabled το NO.

Επειδή οι πελάτες DHCP χρησιμοποιούν εκπομπές δικτύου για να αναζητήσουν διακομιστές DHCP, είναι σημαντικό ότι αυτή η κίνηση πρέπει να δρομολογείται σωστά σε ένα δίκτυο με πολλά υποδίκτυα. Αυτό σημαίνει ότι πρέπει να υπάρχει κάποιου είδους παράγοντας για την ανίχνευση πακέτων εκπομπής DHCP και την προώθησή τους στον κατάλληλο διακομιστή DHCP, εάν βρίσκεται σε άλλο δίκτυο. Οι δρομολογητές Cisco, για παράδειγμα, λαμβάνουν τη μορφή καταχώρησης ip-helper στη διαμόρφωση του δρομολογητή που καθορίζει τη διεύθυνση IP προορισμού για τα πακέτα εκπομπής προς προώθηση. Εάν αυτός ο τύπος διαμόρφωσης δρομολογητή δεν χρησιμοποιείται, ένας διακομιστής Windows που εκτελεί τη δρομολόγηση και η υπηρεσία απομακρυσμένης πρόσβασης πρέπει να ρυθμιστούν ως πράκτορας ρελέ DHCP, όπως φαίνεται στην εικόνα 6.77.



Εικόνα 6.77

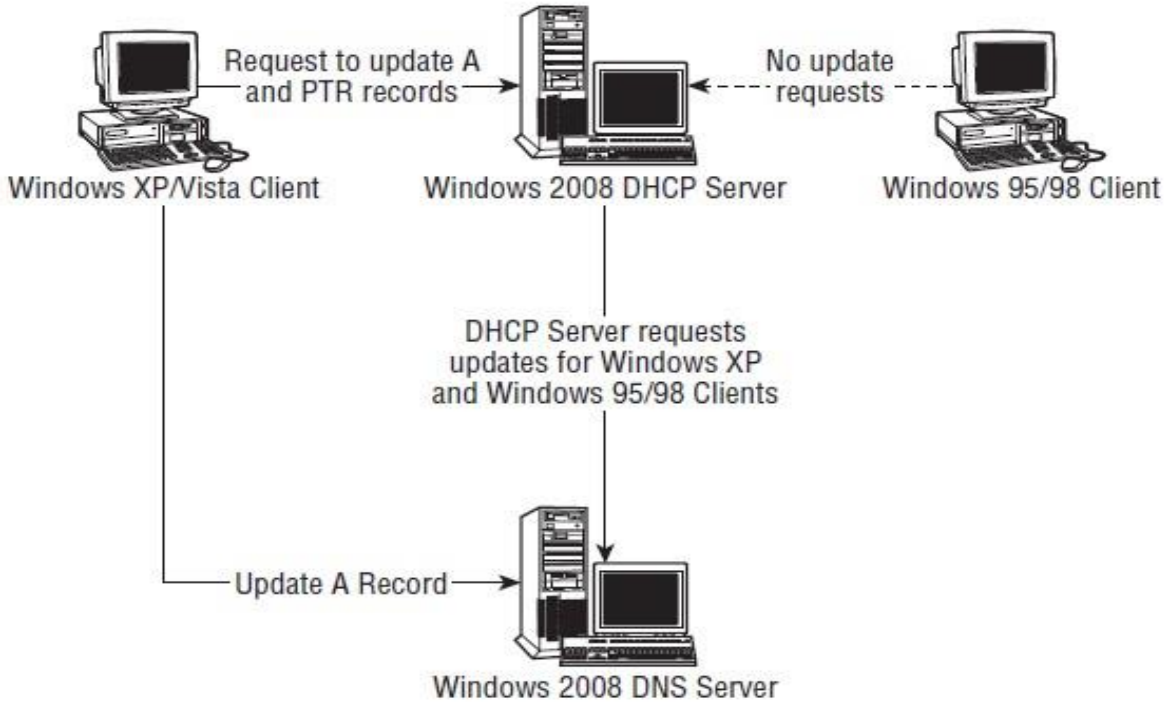
6.6.3. Η υπηρεσία DHCP Windows Server

Τα Windows Server 2008 περιλαμβάνουν μια ενσωματωμένη υπηρεσία DHCP που προσφέρουν εξαιρετική λειτουργικότητα για κατανομή και διαχείριση διευθύνσεων. Η υπηρεσία διακομιστή DHCP βασίζεται σε βιομηχανικά πρότυπα (Request for Comments - RFC) που ορίζονται από την Ομάδα Μηχανικής του Διαδικτύου (Internet Engineering Task Force - IETF). Η τήρηση αυτών των προτύπων διασφαλίζει ότι η υπηρεσία DHCP θα φιλοξενήσει όχι μόνο Windows πελάτες, αλλά και άλλους πελάτες, συμπεριλαμβανομένων των Unix, Macintosh και ούτω καθεξής. Όπως και με άλλες υπηρεσίες, η διαχείριση του DHCP σε διακομιστή των Windows πραγματοποιείται μέσω της διαχείρισης της Microsoft Κονσόλα (MMC). Το συμπληρωματικό πρόγραμμα DHCP της κονσόλας επιτρέπει τη δημιουργία πεδίων DHCP (μια σειρά διευθύνσεων και αντίστοιχων ιδιοτήτων), εκχώρηση καθολικών ιδιοτήτων, προβολή τρεχόντων αναθέσεων και εκτέλεση όλων των άλλων εργασιών διαχείρισης DHCP. Εκτός από την υποστήριξη των προτύπων IETF, η υπηρεσία DHCP των Windows Server 2008 επεκτείνει τη λειτουργικότητα του τυπικού DHCP περιλαμβάνοντας καταγραφή, παρακολούθηση και άλλες δυνατότητες λόγω της ενοποίησης του DHCP με το λειτουργικό σύστημα Windows Server 2008. Εκτός από τις πολύ ισχυρές δυνατότητες που έχουν προστεθεί σε προηγούμενες εκδόσεις του λειτουργικού συστήματος που βελτιώνουν τη χρησιμότητα του DHCP, διαχείριση και ενοποίηση με άλλες υπηρεσίες, όπως DNS, τα Windows Server 2008 περιλαμβάνουν το πρωτόκολλο Dynamic Host Configuration Protocol για υποστήριξη IPv6 (DHCPv6).

Υποστήριξη για δυναμικό DNS

Το DHCP παρέχει δυναμική εκχώρηση διεύθυνσης και επομένως μπορεί να δυσκολευτεί η συντήρηση ακριβής αντιστοίχισης ονόματος προς διεύθυνση σε διακομιστές DNS. Μόλις ένας κόμβος αλλάξει τη διεύθυνσή του, οι εγγραφές στη βάση δεδομένων DNS καθίστανται άκυρες. Το Windows Server 2008 DHCP ενσωματώνεται στο DNS επιτρέποντας στον διακομιστή DHCP και στους πελάτες να ζητούν ενημερώσεις στη βάση δεδομένων DNS όταν αλλάζουν διευθύνσεις ή ονόματα κεντρικών υπολογιστών. Αυτή η δυνατότητα επιτρέπει στη βάση δεδομένων DNS να παραμένει ενημερωμένη ακόμη και για πελάτες με δυναμικά εκχωρημένες διευθύνσεις IP. Το Dynamic DNS (DDNS) λειτουργεί μέσω ενός μηχανισμού πελάτη-διακομιστή. Τα Windows Server και οι υπολογιστές-πελάτες DHCP των Windows XP/Vista υποστηρίζουν DDNS και μπορούν να ζητήσουν απευθείας από τον διακομιστή Windows DNS Server 2008 να ενημερώνει τις εγγραφές πόρων κεντρικού υπολογιστή (ονομάζονται επίσης εγγραφές A) όταν οι διευθύνσεις IP των πελατών ή τα ονόματα κεντρικών υπολογιστών αλλάζουν. Οι διακομιστές Windows Server 2008 μπορούν επίσης να υποβάλουν αιτήματα για λογαριασμό πελατών, παρόλο που ένας διακομιστής DHCP μπορεί να ζητήσει ενημέρωση εγγραφών και στους δύο πελάτες κεντρικού υπολογιστή και δείκτη (PTR). Οι εγγραφές κεντρικού υπολογιστή χρησιμοποιούνται για αντιστοίχιση κεντρικού υπολογιστή σε διεύθυνση και οι εγγραφές δείκτη χρησιμοποιούνται για αντίστροφη αναζήτηση. Ένας διακομιστής DHCP των Windows Server 2008 μπορεί επίσης να λειτουργήσει ως διακομιστής μεσολάβησης για μη Windows 2000/XP/Vista πελάτες DHCP εκτελώντας δυναμικές ενημερώσεις DNS. Για παράδειγμα, ένας Windows Server 2008 DHCP διακομιστής μπορεί να εκτελεί ενημερώσεις για προγράμματα-πελάτες των Windows

95/98 και Windows NT, οι οποίες δεν υποστηρίζουν δυναμικό DNS και δεν είναι σε θέση να υποβάλουν αιτήματα είτε στον διακομιστή DHCP είτε στον DNS διακομιστή για να ενημερώσει τις εγγραφές πόρων τους. Η εικόνα 6.78 απεικονίζει τον τρόπο αλληλεπίδρασης DHCP και DNS.



Εικόνα 6.78

Κατηγορίες προμηθευτών και χρηστών

Οι τάξεις προμηθευτών επιτρέπουν τον ορισμό ενός συνόλου ρυθμίσεων DHCP για έναν συγκεκριμένο εξοπλισμό προμηθευτή και εφαρμογή αυτών των ρυθμίσεων σε οποιονδήποτε κόμβο εμπίπτει σε αυτήν την κατηγορία. Οι τάξεις χρηστών επιτρέπουν την υλοποίηση των ίδιων χαρακτηριστικών, ορίζοντας τις ρυθμίσεις DHCP για εφαρμογή σε μια συγκεκριμένη ομάδα κόμβων. Οι κατηγορίες προμηθευτών και χρηστών προσφέρουν βελτιωμένη ευελιξία στην εκχώρηση προσαρμοσμένων ρυθμίσεων σε μεμονωμένους κόμβους ή ομάδες κόμβους χωρίς να επηρεάζουν άλλους στο ίδιο δίκτυο. Μέσω ενός προμηθευτή ή κατηγορίας χρηστών, ένας κόμβος μπορεί να ζητήσει ένα προσαρμοσμένο σύνολο ρυθμίσεων DHCP που ταιριάζει στη διαμόρφωσή του. Για παράδειγμα, μπορεί να πραγματοποιηθεί εκχώρηση μικρότερης διάρκειας μίσθωσης σε φορητούς υπολογιστές, επειδή εγκαταλείπουν το δίκτυο πιο συχνά. Μπορεί να οριστεί μια κατηγορία χρηστών που ονομάζεται Notebook και να εκχωρηθεί σε αυτήν μια μικρότερη περίοδο μίσθωσης. Ο πελάτης, ο οποίος παρουσιάζει την κατηγορία χρηστών στο διακομιστή, λαμβάνει τη συντομότερη μίσθωση με βάση αυτήν την κατηγορία χρηστών.

Κατανομή διευθύνσεων πολλαπλής διανομής

Οι διευθύνσεις πολλαπλής διανομής επιτρέπουν τη μετάδοση κίνησης IP σε μια ομάδα κόμβων. Χρησιμοποιείται συνήθως στη διάσκεψη ήχου ή βίντεο. Μια τυπική διεύθυνση IP είναι επίσης γνωστή ως unicast διεύθυνση επειδή η κυκλοφορία μεταδίδεται σε μία μόνο διεύθυνση. Ωστόσο, μια διεύθυνση πολλαπλής διανομής μας επιτρέπει να στείλουμε σε μια ομάδα υπολογιστών τα ίδια πακέτα δεδομένων με μία μόνο μετάδοση, αντί χρήση πολλαπλών εκπομπών σε μια ομάδα διευθύνσεων unicast. Η χρήση πολλαπλών διανομής επιτρέπει σε μια ομάδα υπολογιστών να λαμβάνουν τα ίδια δεδομένα χωρίς να αντιγράφουν τα πακέτα, μειώνοντας έτσι την κυκλοφορία πακέτων.

Εντοπισμός μη εξουσιοδοτημένου διακομιστή DHCP

Οι μη εξουσιοδοτημένοι διακομιστές DHCP μπορούν να προκαλέσουν πραγματικά προβλήματα σε ένα δίκτυο εκχωρώντας εσφαλμένα ή αντικρουόμενες πληροφορίες διαμόρφωσης σε πελάτες. Για παράδειγμα, διαχειριστής ή power user ενδέχεται να εγκαταστήσει και να ξεκινήσει έναν διακομιστή DHCP, αγνοώντας ότι υπάρχει ήδη ένας ή περισσότεροι διακομιστές DHCP στο δίκτυο.

Η υπηρεσία καταλόγου Active Directory (AD) αποθηκεύει μια λίστα εξουσιοδοτημένων διακομιστών DHCP. Όταν ένας Windows Server που εκτελεί την υπηρεσία διακομιστή DHCP 2008 σε έναν τομέα ξεκινά, προσπαθεί να προσδιορίσει εάν αναφέρεται ως εξουσιοδοτημένος διακομιστής στο AD. Εάν δεν μπορεί να συνδεθεί με το AD ή δεν βρίσκεται στον κατάλογο AD ως εξουσιοδοτημένος διακομιστής, υποθέτει ότι είναι μη εξουσιοδοτημένος και η υπηρεσία δεν δέχεται DHCP αιτήματα πελατών. Εάν ο διακομιστής βρεθεί εξουσιοδοτημένος, αρχίζει να επεξεργάζεται αιτήματα πελατών.

Οι διακομιστές DHCP που ανήκουν σε μια ομάδας εργασίας (αυτόνομοι διακομιστές που δεν ανήκουν σε τομέα) συμπεριφέρονται κάπως διαφορετικά. Όταν ξεκινά ένας διακομιστής DHCP ομάδας εργασίας, μεταδίδει ένα μήνυμα *dhcpinform*. Οι διακομιστές DHCP που βασίζονται σε τομέα στο δίκτυο αποκρίνονται με μήνυμα dhcpack και παρέχουν το όνομα του τομέα καταλόγου στον οποίο αποτελούν μέρος. Εάν ο διακομιστής DHCP της ομάδας εργασίας λάβει μηνύματα dhcpack από διακομιστές DHCP τομέα, ο διακομιστής ομάδας εργασίας υποθέτει ότι δεν είναι εξουσιοδοτημένος και δεν εξυπηρετεί αιτήματα πελατών. Εάν ένας διακομιστής DHCP ομάδας εργασίας δεν εντοπίζει άλλους διακομιστές ή ανιχνεύει μόνο άλλους διακομιστές DHCP ομάδας εργασίας, ξεκινά την επεξεργασία αιτημάτων πελάτη. Επομένως, οι διακομιστές DHCP της ομάδας εργασίας δεν θα λειτουργούν σε ένα δίκτυο όπου υπάρχουν διακομιστές DHCP που βασίζονται σε τομέα ενεργό, αλλά μπορούν να συνυπάρχουν με άλλους διακομιστές DHCP ομάδας εργασίας.

Αυτόματη διαμόρφωση πελάτη

Οι υπολογιστές-πελάτες Windows 200X, XP και Vista DHCP επιχειρούν να εντοπίσουν έναν διακομιστή DHCP κατά την εκκίνηση και να ανανεώσουν τυχόν μη ληγμένες μισθώσεις (η μίσθωση είναι μια διεύθυνση IP και τα σχετικά δεδομένα που εκχωρούνται από ένα διακομιστή DHCP). Εάν δεν βρεθεί διακομιστής DHCP, ο πελάτης κάνει ping την προεπιλεγμένη πύλη που ορίζεται από τη μίσθωση. Εάν το ping πετύχει, ο πελάτης

συνεχίζει να χρησιμοποιεί τη μίσθωση και προσπαθεί αυτόματα να ανανεώσει τη μίσθωση όταν λήξει ο μισός χρόνος μίσθωσης.

Εάν ο υπολογιστής-πελάτης δεν είναι σε θέση να εντοπίσει έναν διακομιστή DHCP και το ping στη προεπιλεγμένη πύλη αποτυγχάνει, τότε ο πελάτης υποθέτει ότι βρίσκεται σε δίκτυο χωρίς υπηρεσίες DHCP, εκχωρεί αυτόματα μία διεύθυνση IP και συνεχίζει τον έλεγχο για διακομιστή DHCP κάθε πέντε λεπτά. Ο πελάτης εκχωρεί μια διεύθυνση στο υποδίκτυο 169.254.0.0/16 (κλάση B, μάσκα υποδικτύου 255.255.0.0), αλλά πριν την εκχώρηση, ο πελάτης ελέγχει για να επιβεβαιώσει ότι η διεύθυνση είναι έγκυρη και δεν έρχεται σε διένεξη με άλλους κόμβους.

Η αυτόματη εκχώρηση διεύθυνσης είναι μια χρήσιμη λειτουργία, ιδιαίτερα για μικρά δίκτυα, όπως ένα οικιακό δίκτυο, χωρίς διακομιστή DHCP. Επιτρέπει στους χρήστες να μετακινούνται μεταξύ δικτύων με τα ίδια χαρακτηριστικά, διευκολύνοντας και εξαλείφοντας την ανάγκη αναδιάρθρωσης των συστημάτων τους. Για παράδειγμα, ένας χρήστης μπορεί να μετακινήσει το notebook από το γραφείο στο σπίτι έχοντας μια έγκυρη διεύθυνση στο τρέχον δίκτυο χωρίς να πρέπει να επαναδιαμορφώσει το TCP/IP κάθε φορά.

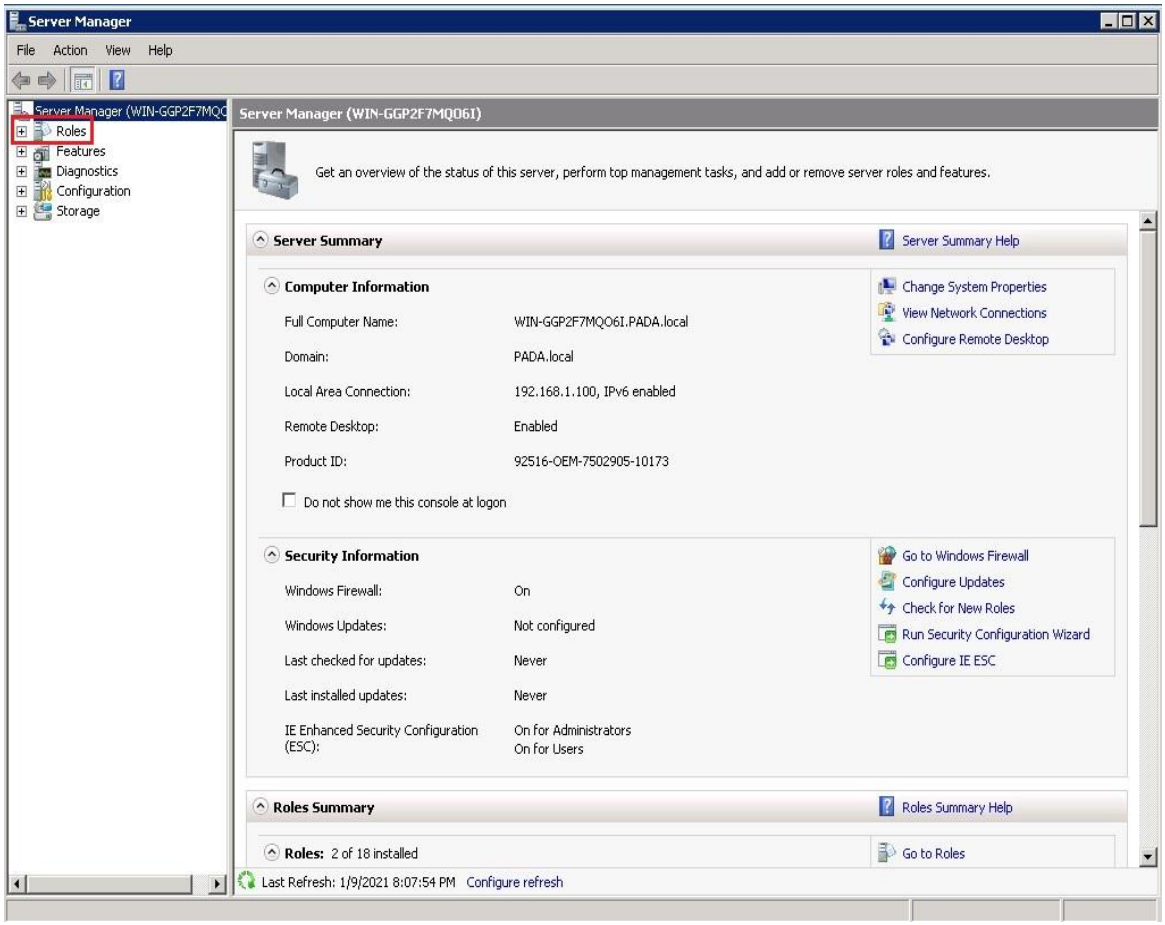
Παρακολούθηση και υποβολή αναφορών

Η υπηρεσία DHCP εκτελεί τη δική της παρακολούθηση και καταγραφή συμβάντων στο αρχείο καταγραφής συστήματος, το οποίο ο χρήστης μπορεί να προβάλει μέσω της κονσόλα Event Viewer. Το DHCP παρέχει επίσης πρόσθετη παρακολούθηση και στατιστική αναφορά. Για παράδειγμα, μπορούμε να ρυθμίσουμε το DHCP ώστε να δημιουργεί ειδοποιήσεις όταν το ποσοστό των διαθέσιμες διευθύνσεων σε ένα δεδομένο εύρος πέφτουν κάτω από ένα καθορισμένο επίπεδο.

6.6.4. Εγκατάσταση DHCP και δημιουργία νέων scope

Η εγκατάσταση DHCP είναι σχετικά μια απλή διαδικασία. Στα Windows 2008, η εγκατάσταση έχει βελτιωθεί ακόμη περισσότερο μέσω της χρήσης του οδηγού προσθήκης ρόλων στον διακομιστή. Αυτός ο οδηγός εγκαθιστά την υπηρεσία διακομιστή DHCP και καλεί αυτόματα τον οδηγό νέας εμβέλειας, το οποίο μπορεί να χρησιμοποιηθεί για τη δημιουργία και τη διαμόρφωση πεδίων DHCP. Προκειμένου να δημιουργήσουμε ένα Windows 2008 σύστημα ως διακομιστή DHCP, θα πρέπει να ακολουθήσουμε τα παρακάτω βήματα:

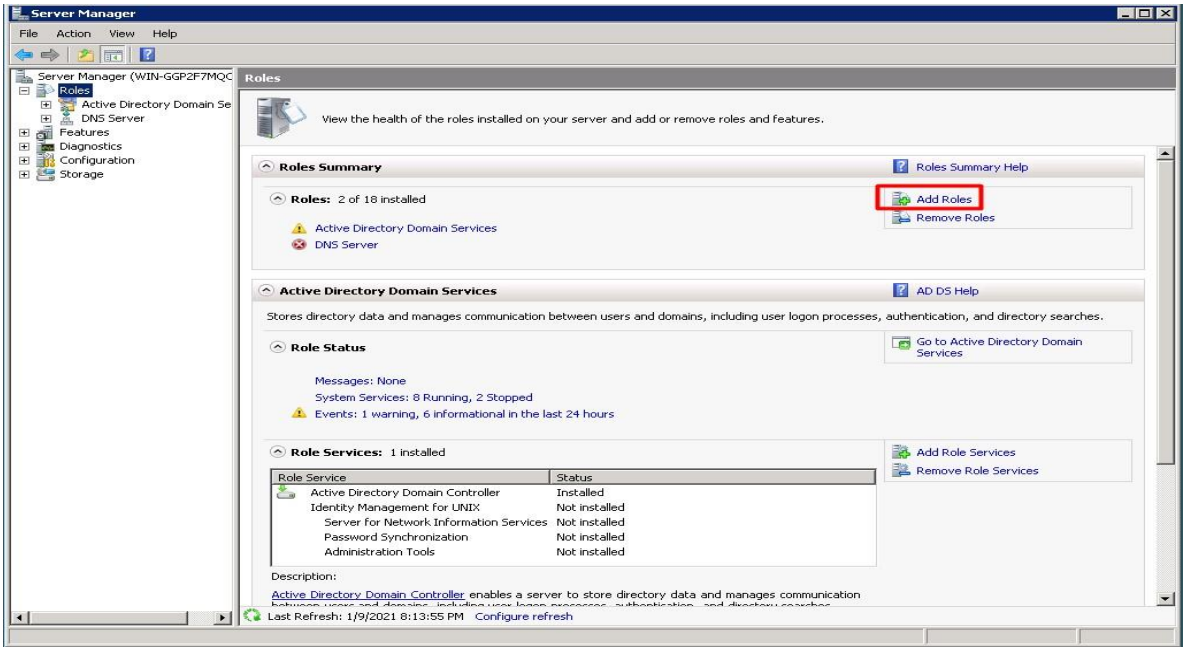
1. Επιλέγουμε Έναρξη, Όλα τα προγράμματα, Εργαλεία διαχείρισης, Διαχείριση διακομιστή. Εάν ζητηθεί, κάνουμε κλικ στο Συνεχίστε για να επιβεβαιώσουμε την ενέργεια. Στην εικόνα 6.79 φαίνεται η Διαχείριση διακομιστή.



Εικόνα 6.79

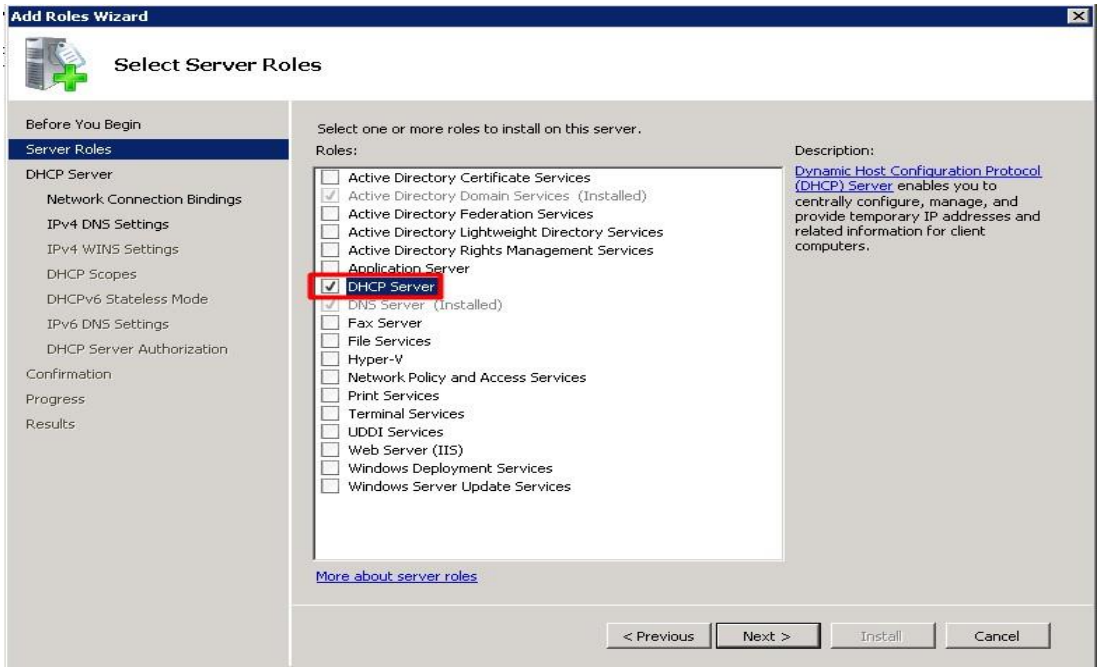
2. Στο παράθυρο διαλόγου Διαχείριση διακομιστή, κάνουμε κλικ στην επιλογή Ρόλοι (Roles) στο αριστερό παράθυρο για να εμφανίσουμε συνοπτικές πληροφορίες για τους ρόλους τους οποίους έχουμε ήδη εγκαταστήσει στο δεξιό τμήμα του παραθύρου. Στη συνέχεια, κάνουμε κλικ στην επιλογή Προσθήκη ρόλων (Add Roles) στο δεξιό τμήμα του παραθύρου για να εκκινήσουμε τον Οδηγό Προσθήκη

ρόλων. Αφού διαβάσουμε τις πληροφορίες πριν ξεκινήσουμε, κάνουμε κλικ στο Δίπλα στη Συνέχεια. Στην εικόνα 6.80 φαίνεται το πλαίσιο διαλόγου.



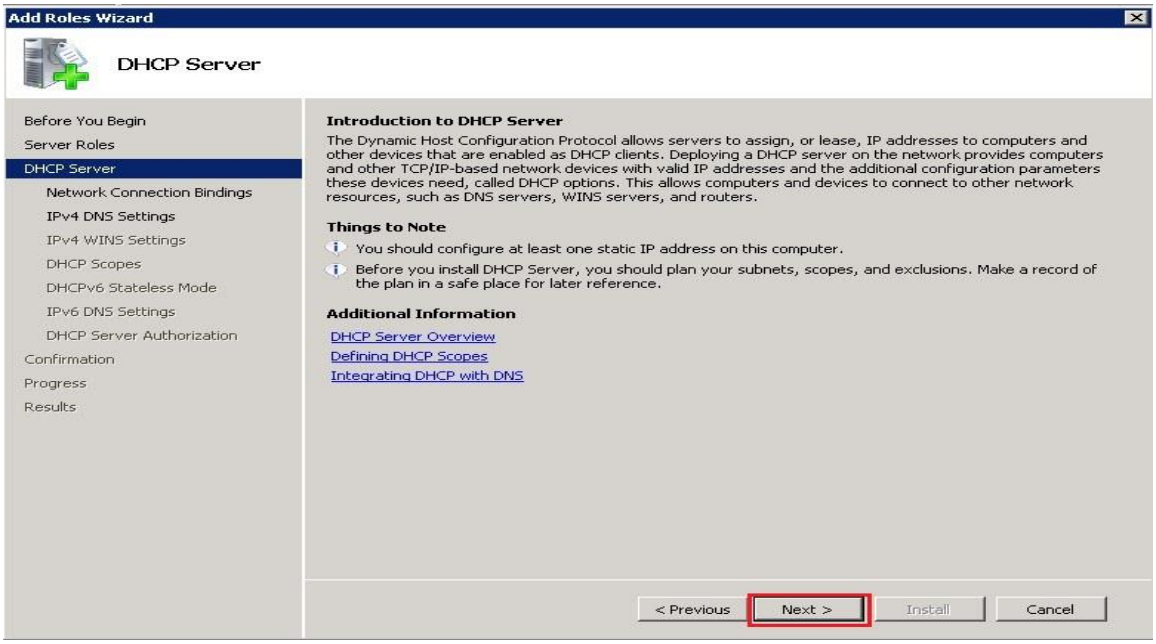
Εικόνα 6.80

3. Στο παράθυρο διαλόγου που μας εμφανίζεται, στην επιλογή ρόλων διακομιστή, επιλέγουμε το πλαίσιο ελέγχου δίπλα στον διακομιστή DHCP και στη συνέχεια κάνουμε κλικ στο Επόμενο για να συνεχίσουμε, όπως φαίνεται στην εικόνα 6.81.



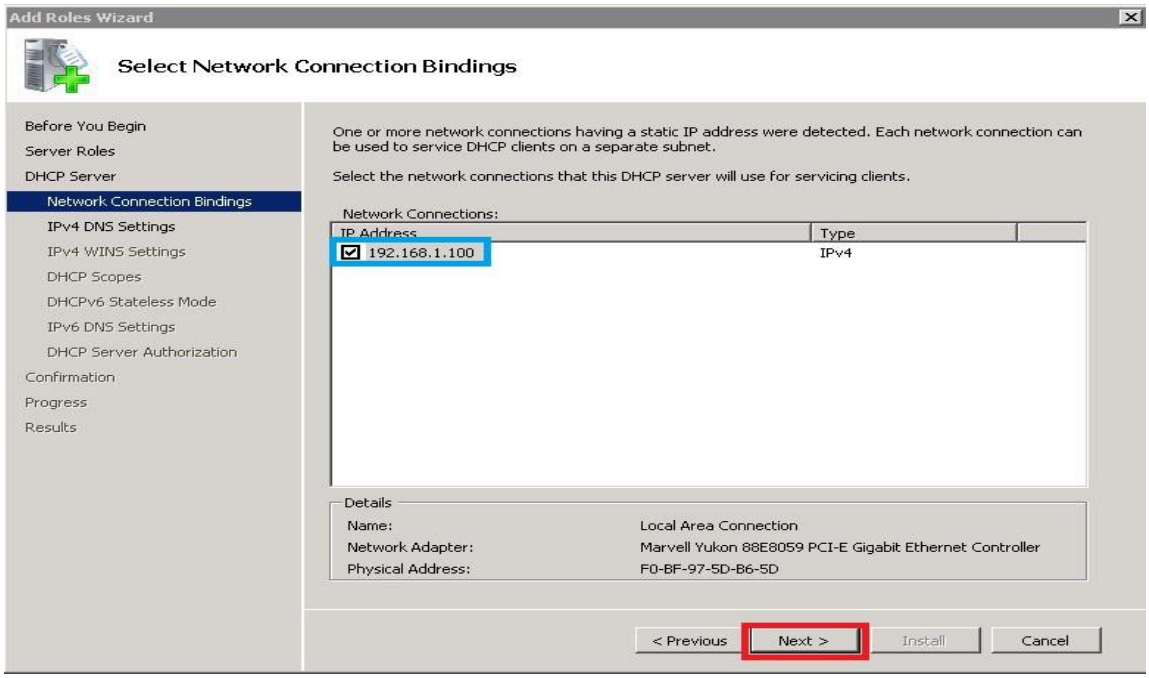
Εικόνα 6.81

4. Στη συνέχεια μας εμφανίζεται μια σύντομη εισαγωγή στο DHCP με τις βασικές απαιτήσεις προεγκατάστασης. Αφού διαβάσουμε τις πληροφορίες, κάνουμε κλικ στο Επόμενο (Next), όπως φαίνεται στην εικόνα 6.82.



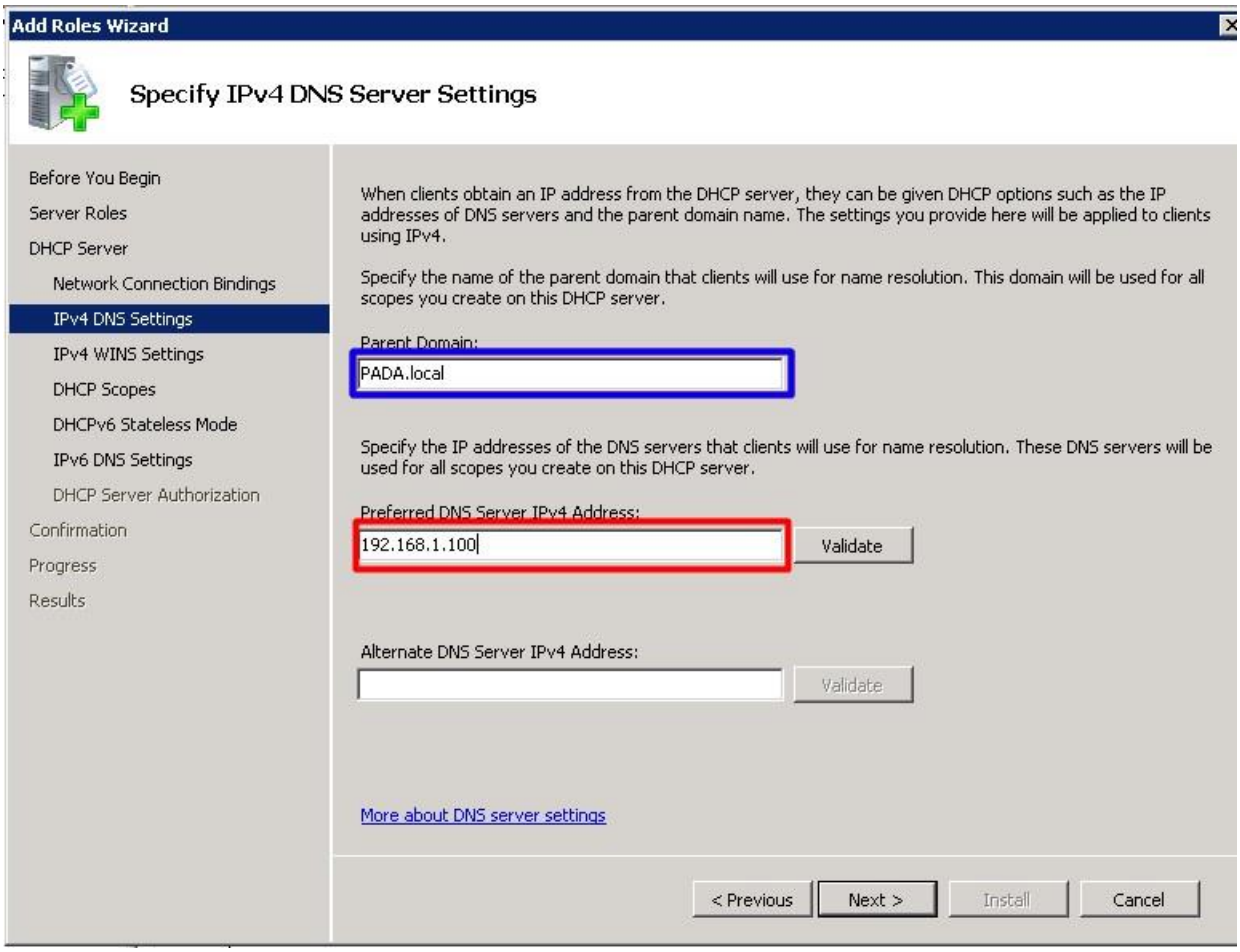
Εικόνα 6.82

5. Επαληθεύουμε σε ποιο δίκτυο επιθυμούμε να εφαρμοστεί ο DHCP server και στη συνέχεια κάνουμε κλικ στο Επόμενο (Next), όπως φαίνεται στην εικόνα 6.83.



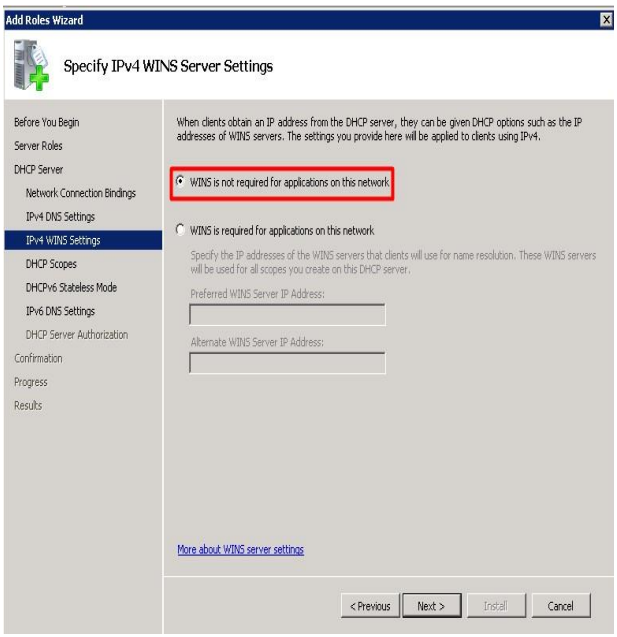
Εικόνα 6.83

6. Σε αυτό το σημείο, ο "Οδηγός προσθήκης ρόλων" εμφανίζει τις ρυθμίσεις διακομιστή DNS για τον καθορισμό IPv4. Εισάγουμε το όνομα του γονικού τομέα που θα χρησιμοποιούν οι πελάτες για την επίλυση ονομάτων, όπως φαίνεται στο μπλε πλαίσιο. Στη συνέχεια εισάγουμε το όνομα της προτιμώμενης διεύθυνσης IP διακομιστή DNS IPv4 και εάν χρειάζεται, η εναλλακτική Διεύθυνση IP διακομιστή DNS και κάνουμε κλικ στο Επόμενο για να συνεχίσουμε. Οι παραπάνω ενέργειες φαίνονται στην εικόνα 6.84.

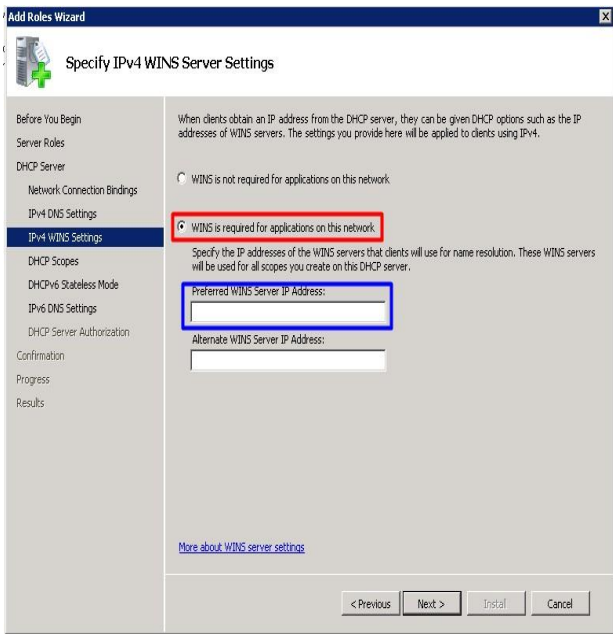


Εικόνα 6.84

7. Στο επόμενο παράθυρο διαλόγου μας εμφανίζεται ο καθορισμός ρυθμίσεων διακομιστή WINS όπου και κάνουμε κλικ στο κουμπί επιλογής για ένδειξη εάν απαιτείται WINS στο δίκτυο. Εάν απαιτείται, καθορίζουμε τις διευθύνσεις IP για τον κύριο και, εάν χρειαστεί, τον εναλλακτικό διακομιστή. Κάνουμε κλικ στο Επόμενο για να συνεχίσουμε, όπως φαίνεται στις εικόνες 6.85 και 6.86.

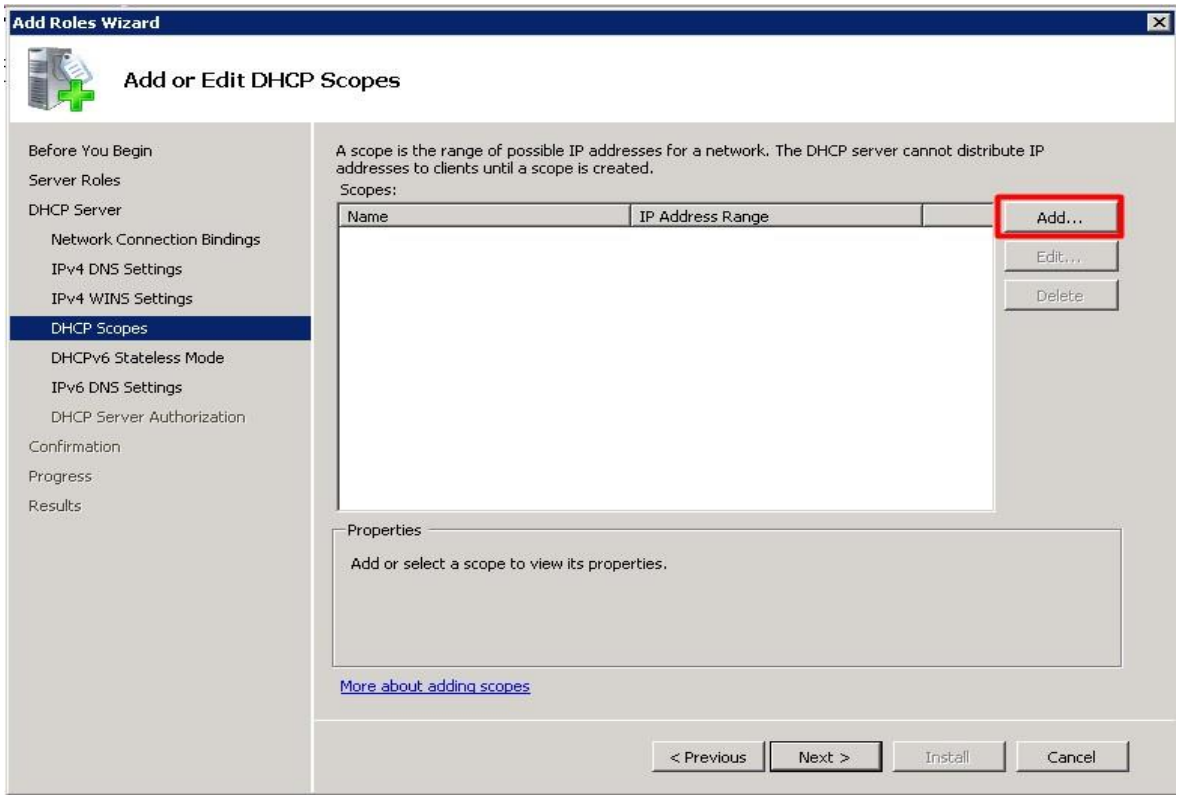


Εικόνα 6.85



Εικόνα 6.86

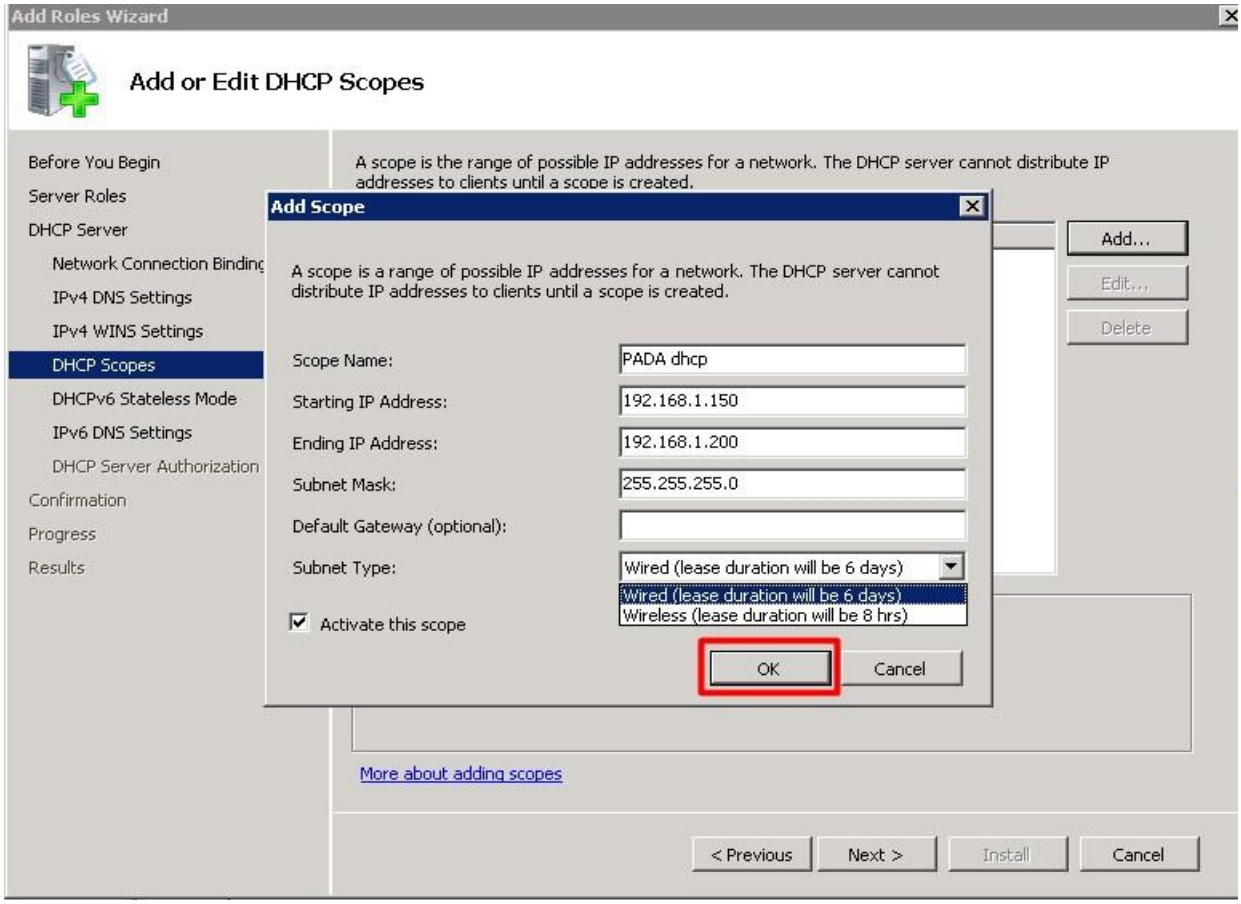
8. Στο παράθυρο διαλόγου Προσθήκη ή Επεξεργασία πεδίων DHCP, κάνουμε κλικ στην επιλογή Προσθήκη όπως φαίνεται στην εικόνα 6.87.



Εικόνα 6.87

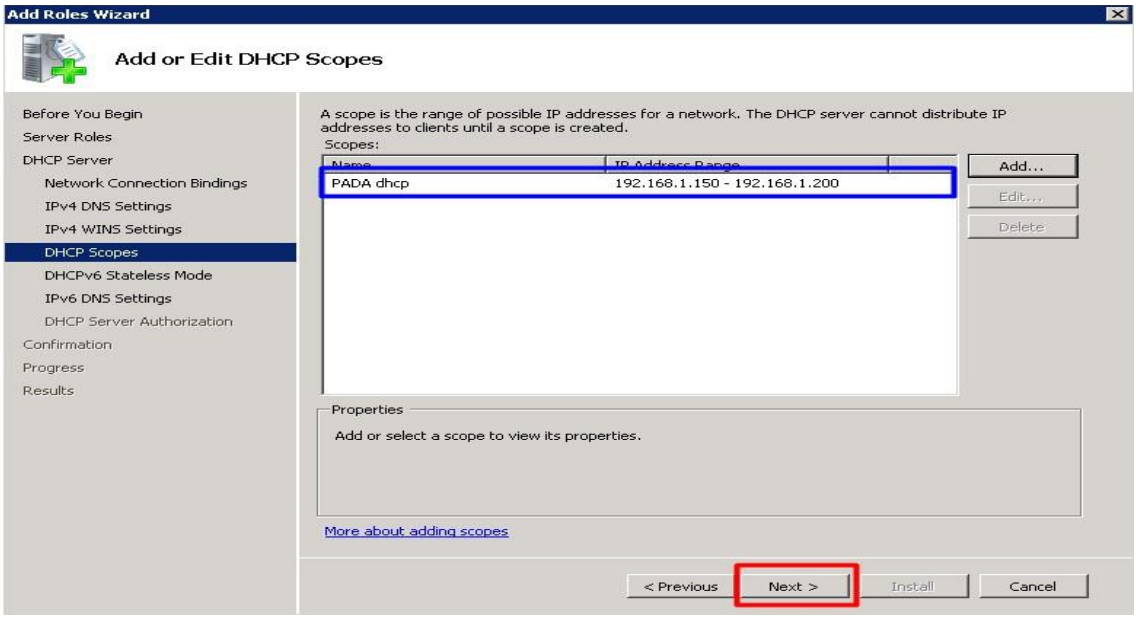
9. Στο αναδυόμενο παράθυρο που μας εμφανίζεται παρουσιάζονται οι παρακάτω επιλογές:
    - **Scope Name**: Αυτό είναι το φιλικό όνομα που εμφανίζεται στην κονσόλα DHCP για scope που επιθυμούμε να δημιουργήσουμε.
    - **Starting IP address**: Σε αυτό το πεδίο καθορίζουμε τη διεύθυνση έναρξης του εύρους των διευθύνσεων IP που θέλουμε να γίνει εκχώρηση σε αυτό το scope.
    - **Ending IP address**: Σε αυτό το πεδίο καθορίζουμε την τελική διεύθυνση του εύρους των διευθύνσεων IP που θέλουμε να γίνει εκχώρηση σε αυτό το scope.
    - **Subnet Mask**: Σε αυτό το πεδίο καθορίζουμε τη μάσκα υποδικτύου για το εύρος διευθύνσεων που θα εκχωρηθούν σε αυτό το scope.
    - **Default Gateway**: Σε αυτό το πεδίο εκχωρούμε την IP διεύθυνση του Gateway, το οποίο είναι προαιρετικό πεδίο.
    - **Subnet Type**: Σε αυτό το πεδίο επιλέγουμε τον τύπο που επιθυμούμε. Έχουμε δύο επιλογές:
        - Ενσύρματο με διάρκεια μίσθωσης 6 ημερών
        - Ασύρματο με διάρκεια μίσθωσης 8 ωρών

Οι παραπάνω ενέργειες φαίνονται στην εικόνα 6.88.



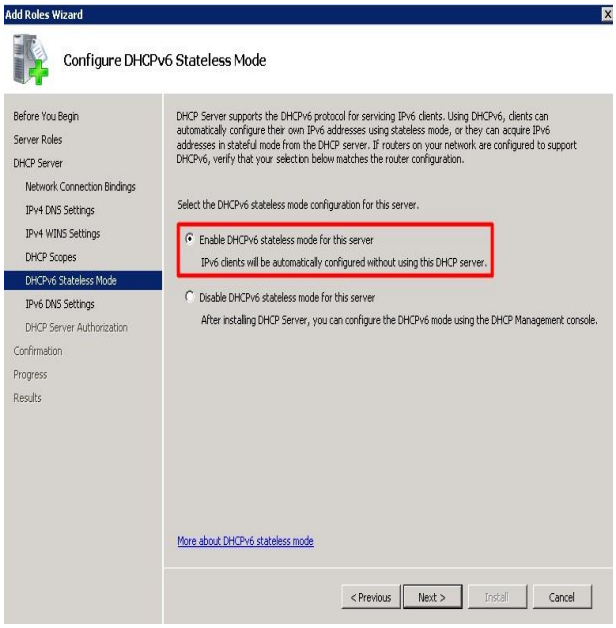
Εικόνα 6.88

10. Αφού έχουμε υλοποιήσει τις ρυθμίσεις που επιθυμούμε επιλέγουμε OK και μας επαναφέρει στο προηγούμενο παράθυρο διαλόγου. Αφού έχουμε ελέγξει ότι είναι το επιθυμητό scope κάνουμε κλικ στο Επόμενο (Next), όπως φαίνεται στην εικόνα 6.89.

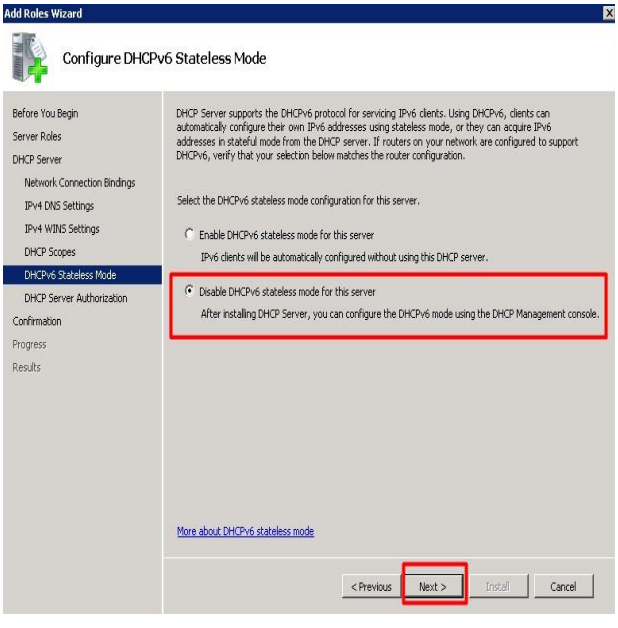


Εικόνα 6.89

11. Στο επόμενο παράθυρο διαλόγου μας εμφανίζει αν θέλουμε να κάνουμε ρυθμίσεις IPv6 για το scope που επιθυμούμε. Εμείς επιλέγουμε ότι δεν επιθυμούμε και κάνουμε κλικ Επόμενο. Οι δύο επιλογές φαίνονται στις εικόνες 6.90 και 6.91.

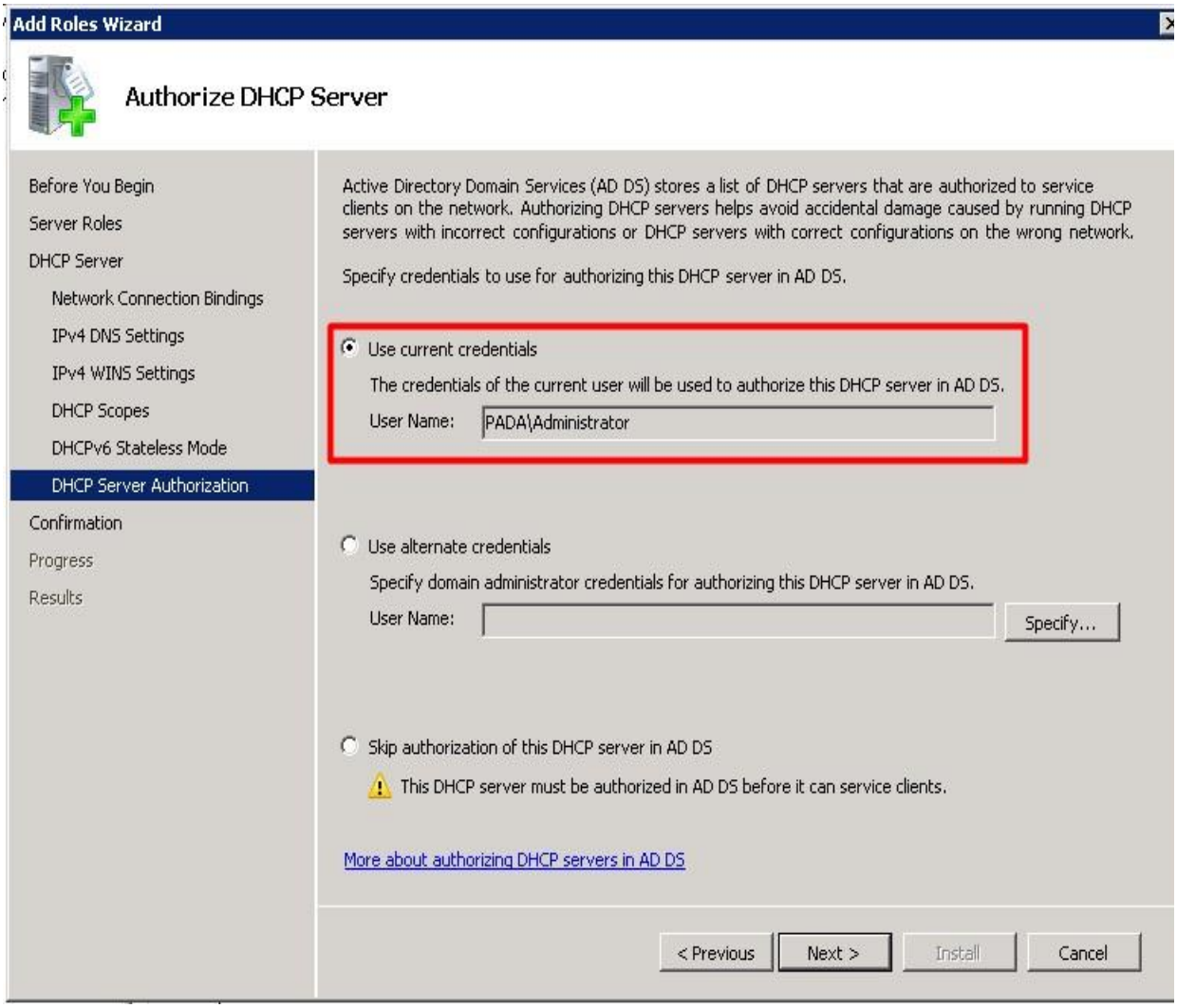


Εικόνα 6.90



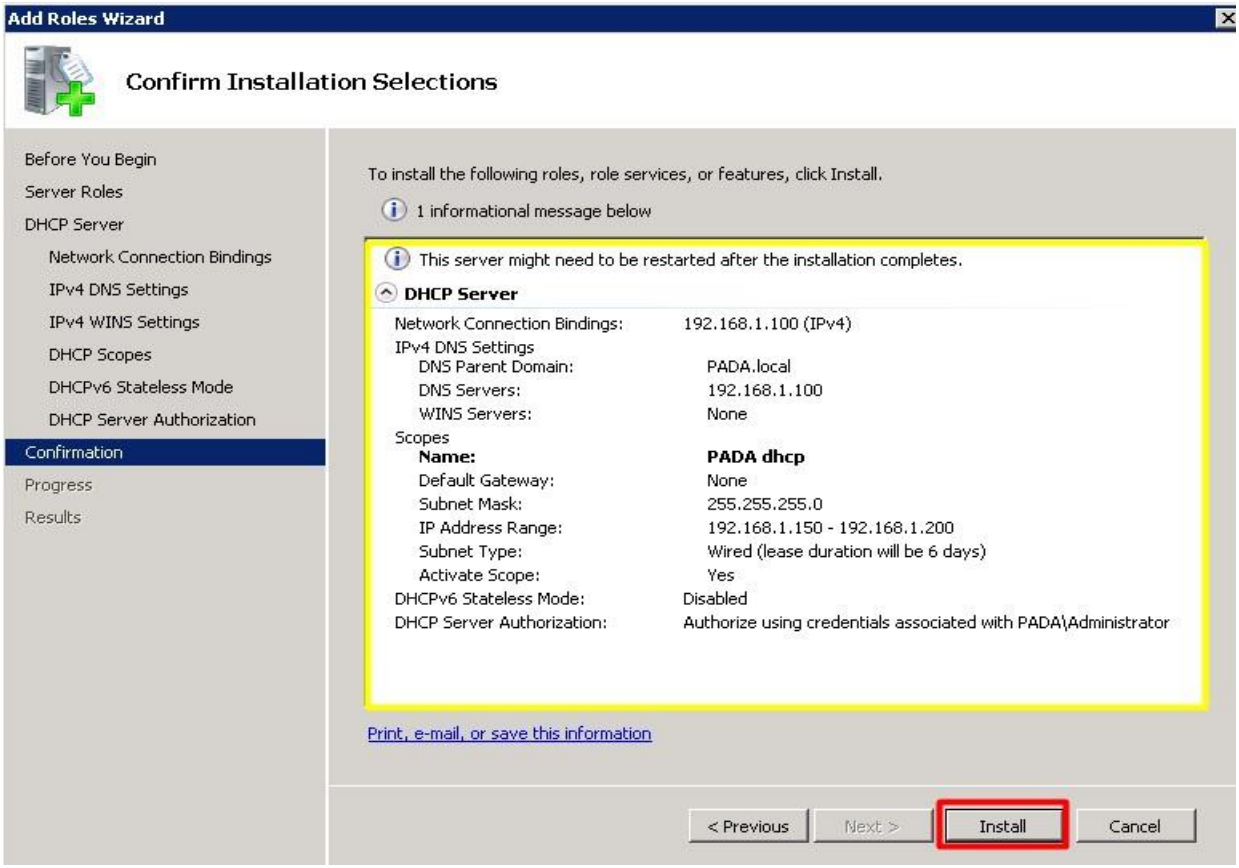
Εικόνα 6.91

12. Εάν ρυθμίζουμε το DHCP σε διακομιστή μέλους, πρέπει να εξουσιοδοτήσουμε το DHCP διακομιστή για λειτουργία στον τομέα. Στο παράθυρο διαλόγου που φαίνεται στην εικόνα 6.92 εξουσιοδότηση διακομιστή DHCP, επιλέγουμε εάν θα χρησιμοποιήσουμε τα τρέχοντα ή εναλλακτικά διαπιστευτήρια που χρησιμοποιούνται για την εξουσιοδότηση του DHCP διακομιστή στον τομέα.



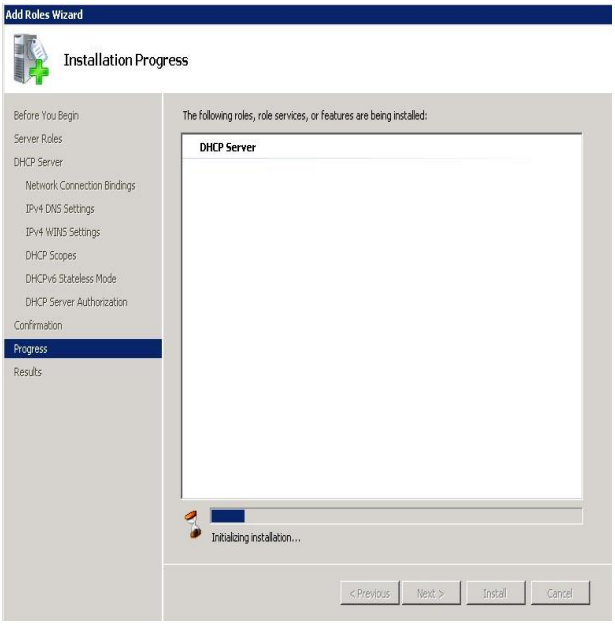
Εικόνα 6.92

13. Στη συνέχεια στο παράθυρο διαλόγου που μας εμφανίζεται, όπως φαίνεται στην εικόνα 6.93, γίνεται μια προεπισκόπηση των ρυθμίσεων που έχουμε επιλέξει για τον διακομιστή DHCP προκειμένου να επιβεβαιώσουμε ότι όλα είναι όπως τα επιθυμούμε. Αφού τα έχουμε ελέγξει κάνουμε κλικ εγκατάσταση για να εγκατασταθεί ο ρόλος μας.

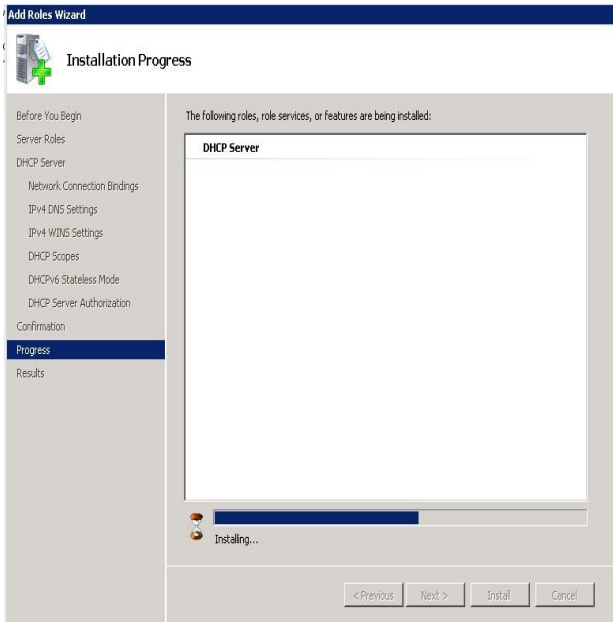


Εικόνα 6.93

14. Στις εικόνες 6.94 και 6.95 φαίνεται η πρόοδος εγκατάστασης.

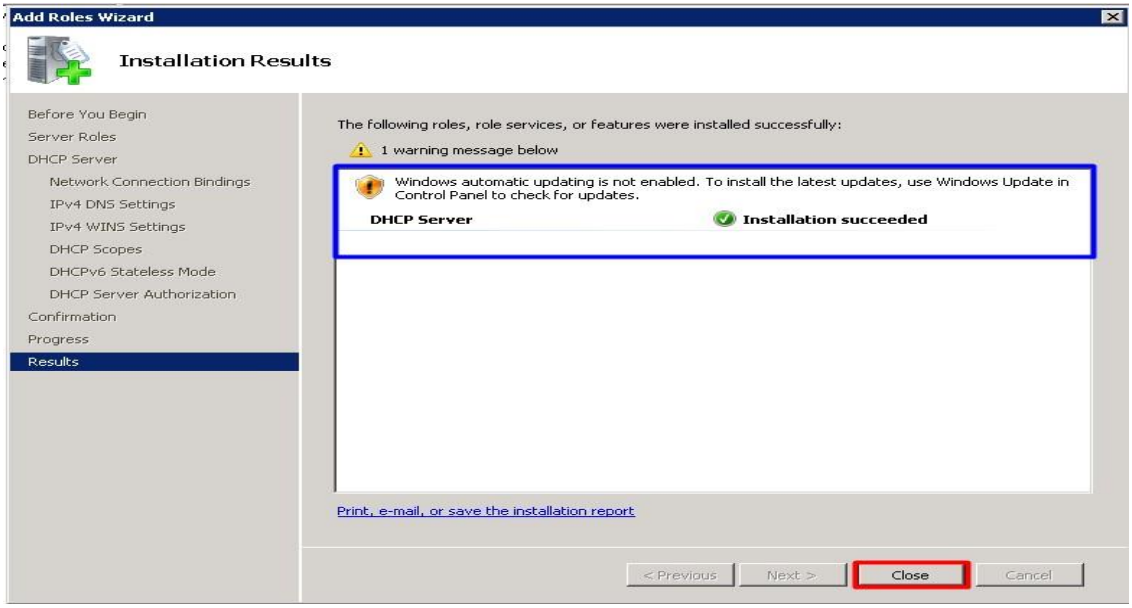


Εικόνα 6.94



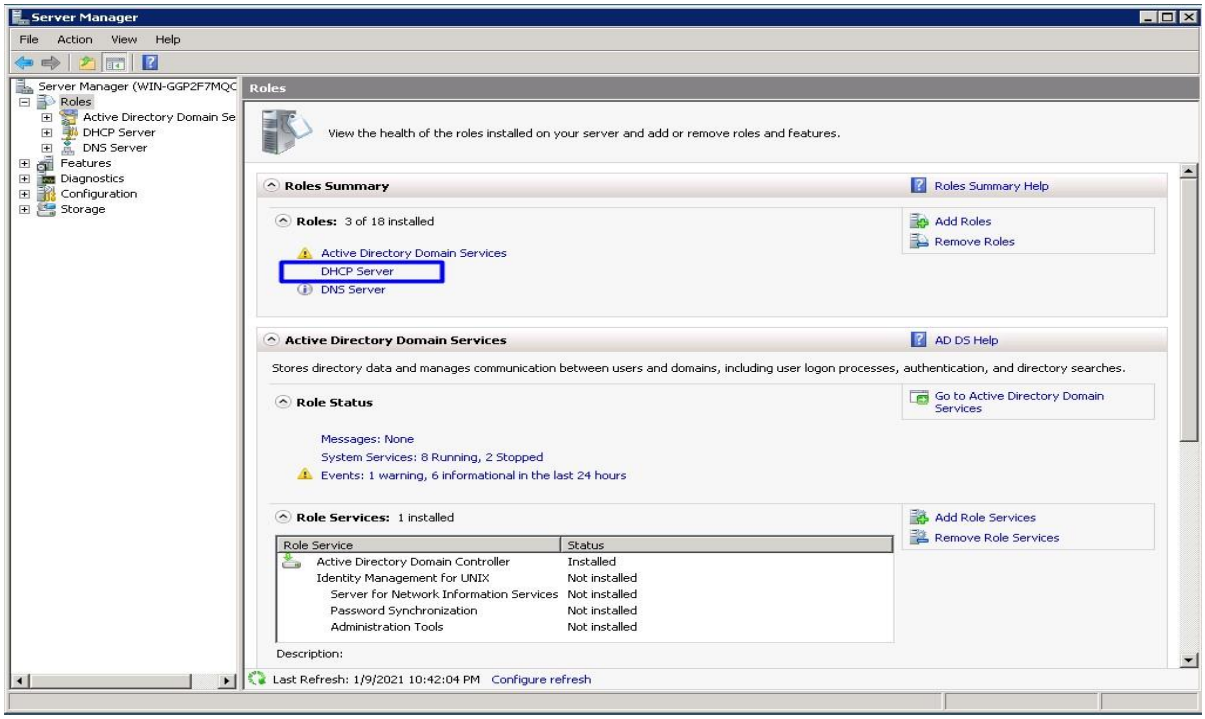
Εικόνα 6.95

15. Στην εικόνα 6.96 φαίνεται η επιτυχής εγκατάσταση του DHCP διακομιστή με την προβολή του ανάλογου μηνύματος.



Εικόνα 6.96

16. Στην εικόνα 6.97 στη Διαχείριση του διακομιστή μπορούμε πλέον να παρατηρήσουμε ότι ο νέος ρόλος έχει εγκατασταθεί και βρίσκεται ήδη σε λειτουργία.



Εικόνα 6.97

6.7. Τεχνολογίες ανοχής σφαλμάτων (Fault Tolerance Technologies)

6.7.1. Διαχείριση συστήματος αρχείων και ανοχή σφαλμάτων (File System Management and Fault Tolerance)

Τα δίκτυα υπολογιστών δημιουργήθηκαν για κοινή χρήση δεδομένων. Η πιο γνωστή μορφή ανταλλαγής δεδομένων σε δίκτυα υπολογιστών έχει να κάνει με την πρόσβαση σε αρχεία και φακέλους που είναι αποθηκευμένοι σε συστήματα δικτύων ή σε κεντρικούς διακομιστές αρχείων, όπως Windows Server 2008 διακομιστές αρχείων. Καθώς οι ανάγκες αποθήκευσης δεδομένων και οι υπηρεσίες υπολογιστών έχουν εξελιχθεί τα τελευταία 20 περίπου χρόνια, πολλές διαφορετικές μέθοδοι γίνονται διαθέσιμοι για παρουσίαση, πρόσβαση, ασφάλεια και διαχείριση δεδομένων. Για παράδειγμα, η πρόσβαση στα δεδομένα γίνεται μέσω διαδικτύου μέσω του προγράμματος περιήγησης με πρόσβαση σε δεδομένα που είναι αποθηκευμένα σε εξωτερικό χώρο όπως μονάδες USB, δισκέτες, CD και DVD, αλλά και με πρόσβαση σε δεδομένα που είναι αποθηκευμένα σε οποιονδήποτε από τους διαφορετικούς τύπους πολυμέσων διαθέσιμα σε πολλά διαφορετικά λειτουργικά συστήματα και συστήματα αρχείων.

Σύστημα αρχείων Windows Server 2008

Όταν ένας νέος δίσκος προστίθεται σε ένα σύστημα Windows Server 2008, πρέπει να διαμορφωθεί επιλέγοντας τι είδους δίσκος, τύπος τόμου και τύπος μορφής τόμου θα χρησιμοποιηθεί. Τα Windows 2008 επιτρέπουν στους διαχειριστές να μορφοποιήσουν τους τόμους δίσκων των Windows επιλέγοντας μία από τις δύο επιλογές, τη μορφή πίνακα κατανομής αρχείων (FAT) ή τη μορφή συστήματος αρχείων NT (NTFS). Η διαμόρφωσε σε FAT αναφέρεται σε διαμερίσματα παλαιού τύπου που χρησιμοποιούνται από παλαιότερα λειτουργικά συστήματα και μονάδες δισκέτας. Τα δεδομένα που αποθηκεύονται σε διαμερίσματα FAT δεν είναι ασφαλή και δεν παρέχουν πολλές δυνατότητες. Η διαμόρφωση σε NTFS είναι διαθέσιμη από τα Windows NT 3.51 και παρέχουν στους διαχειριστές τη δυνατότητα προστασίας αρχείων και φακέλων, καθώς και τη δυνατότητα αξιοποίησης πολλών υπηρεσιών που παρέχονται με τα Windows Server 2008. Το NTFS επιτρέπει πολλές δυνατότητες που μπορούν να αξιοποιηθούν για να παρέχουν ένα εξαιρετικά αξιόπιστο, επεκτάσιμο, ασφαλές και διαχειρίσιμο σύστημα αρχείων.

Τα βασικά χαρακτηριστικά των διαμερισμάτων με μορφοποίηση NTFS περιλαμβάνουν υποστήριξη για μεγάλους όγκους, ρύθμιση παραμέτρων αδειών ή περιορισμός της πρόσβασης σε σύνολα δεδομένων, συμπίεση ή κρυπτογράφηση δεδομένων και διαμόρφωση ποσοστώσεων αποθήκευσης ανά χρήστη σε ολόκληρα διαμερίσματα ή και συγκεκριμένους φακέλους. Ως βέλτιστη πρακτική, συνιστάται σε όλα τα διαμερίσματα που δημιουργούνται σε συστήματα Windows 2008 να διαμορφώνονται χρησιμοποιώντας το σύστημα αρχείων NT (NTFS).

Οι υπηρεσίες ποσοστώσεων συστήματος αρχείων επιτρέπουν στους διαχειριστές να ρυθμίζουν συγκεκριμένα τα όρια αποθήκευσης σε σύνολα δεδομένων που είναι αποθηκευμένα σε volumes του διακομιστή. Αυτό μπορεί να χρησιμοποιηθεί για να αποτρέψει τους χρήστες από να γεμίζουν μια μονάδα δίσκου διακομιστή. Επίσης, οι ποσοστώσεις μπορούν να χρησιμοποιηθούν σε σενάρια φιλοξενίας όπου το ενιαίο σύστημα αποθήκευσης μοιράζεται μεταξύ τμημάτων ή οργανισμών και ο αποθηκευτικός χώρος είναι κατανέμεται βάσει συνδρομών ή εταιρικών προτύπων. Τα Windows 2008 περιλαμβάνουν επίσης τη δυνατότητα διαχείρισης ποσοστώσεων σε επίπεδο όγκου, αλλά μπορεί να διαμορφωθεί για να ενεργοποιεί και να επιβάλλει ποσοστώσεις σε

επίπεδο φακέλου σε οποιοδήποτε συγκεκριμένο τόμο χρησιμοποιώντας την υπηρεσία διαχείρισης πόρων διακομιστή αρχείων.
Οι τόμοι NTFS επιτρέπουν στους διαχειριστές να ενεργοποιούν τη συμπίεση δεδομένων σε έναν ολόκληρο τόμο και να επιτρέπουν σε όλους τους χρήστες να συμπιέζουν δεδομένα σε φακέλους ή / και αρχεία. Η συμπίεση δεδομένων μειώνει το απαιτούμενος αποθηκευτικός χώρος για δεδομένα. Η συμπίεση δεδομένων, ωστόσο, έχει κάποιους περιορισμούς, όπως το επιπρόσθετο φορτίο που ανατίθεται στο σύστημα κατά την ανάγνωση, εγγραφή και συμπίεση και λειτουργίες αποσυμπίεσης. . Δεν είναι δυνατή η κρυπτογράφηση συμπιεσμένων δεδομένων. Οι διαχειριστές συστήματος μπορούν να διαμορφώσουν έναν ολόκληρο τόμο που θα συμπιεστεί ή οι τελικοί χρήστες μπορούν επιλέξουν να συμπιέσουν έναν συγκεκριμένο φάκελο, αρχείο ή ένα σύνολο αρχείων στα οποία έχουν πρόσβαση.
Οι τόμοι NTFS υποστηρίζουν τη δυνατότητα των χρηστών και των διαχειριστών να κρυπτογραφούν το σύνολο ενός τόμου, ένα φάκελο ή ένα μόνο αρχείο. Αυτό παρέχει υψηλότερο επίπεδο ασφάλειας για τα δεδομένα. Εάν ο δίσκος, σταθμός εργασίας ή διακομιστής, στον οποίο είναι αποθηκευμένα κρυπτογραφημένα δεδομένα, κλαπεί ή χαθεί, δεν είναι δυνατή η πρόσβαση στα δεδομένα λόγω του ότι είναι κρυπτογραφημένα.
Ο έλεγχος αρχείων επιτρέπει στους διαχειριστές να καθορίσουν τους τύπους αρχείων που μπορούν να αποθηκευτούν. Με ενεργοποιημένο ένα πρότυπο ελέγχου αρχείου, όλες οι λειτουργίες εγγραφής ή αποθήκευσης παρακολουθούνται και ελέγχονται και μόνο τα αρχεία που περνούν από την πολιτική ελέγχου του αρχείου επιτρέπεται να αποθηκευτούν στον συγκεκριμένο τόμο ή φάκελο.
Καθώς οι ανάγκες των υπηρεσιών αρχείων ενός οργανισμού αλλάζουν, είναι μια πρόκληση για τους διαχειριστές να σχεδιάσουν ένα σχέδιο μετεγκατάστασης για να υποστηρίξουν τις νέες απαιτήσεις. Σε πολλές περιπτώσεις όταν οι διακομιστές αρχείων χρειάζονται επιπλέον χώρο ή πρέπει να αντικατασταθούν, απαιτείται χρόνος για την μετεγκατάσταση, προγραμματισμένες διακοπές λειτουργίας και, μερικές φορές, επιπτώσεις στον χρήστη.
Ως αποτέλεσμα της προσπάθειας απλοποίησης της διαδικασίας διαχείρισης του διακομιστή αρχείων και της μείωσης του αντίκτυπου στους τελικούς χρήστες, στα Windows Server 2008 ενσωματώθηκε η υπηρεσία κατανεμημένων συστημάτων αρχείων (DFS). Το DFS παρέχει πρόσβαση σε δεδομένα αρχείων από έναν μόνο χώρο ονομάτων που μπορεί να χρησιμοποιηθεί για την αναπαράσταση ενός μεμονωμένου διακομιστή ή ενός αριθμού διακομιστών που αποθηκεύουν διαφορετικά σύνολα ή επαναλαμβανόμενα σύνολα των ίδιων δεδομένων. Οι χρήστες και οι διαχειριστές μπορούν και οι δύο να επωφεληθούν από το DFS επειδή χρειάζεται να θυμούνται μόνο έναν μεμονωμένο διακομιστή ή όνομα τομέα για τον εντοπισμό όλων των απαραίτητων κοινόχρηστων αρχείων.

Τύποι δίσκων Windows Server 2008

Τα Windows 2008 επιτρέπουν στους διαχειριστές να καθορίσουν τον τρόπο παρουσίασης και χρήσης δίσκων του συστήματος. Ανάλογα με τον τύπο και το μέγεθος ενός δίσκου, οι διαχειριστές μπορούν να καθορίσουν ποιο συγκεκριμένο τύπο δίσκου και τόμους θα πρέπει να εξετάσουν για την ανάπτυξη των συστημάτων τους. Οι δίσκοι των Windows μπορούν να οριστούν ως βασικοί ή δυναμικοί δίσκοι. Επιπλέον, αυτοί οι ίδιοι δίσκοι μπορεί να οριστούν ως δίσκος Master Boot Record (MBR) ή GUID Partition Table (GPT). Οι βασικοί δίσκοι υποστηρίζουν μόνο απλούς τόμους, ενώ οι δυναμικοί δίσκοι επιτρέπουν λογικούς τόμους να δημιουργηθούν σε πολλούς φυσικούς δίσκους. Η επιλογή

μεταξύ δίσκων MBR και GPT εξαρτάται σχετικά με το μέγεθος του δίσκου καθώς και την κατανόηση πόσων κατατμήσεων θα χρειαστούμε κατά τη δημιουργία του δίσκου. Οι τύποι των δίσκων είναι:

- **Δίσκοι Master Boot Record:** Οι δίσκοι Master Boot Record (MBR) χρησιμοποιούν την παραδοσιακή διαμόρφωση δίσκου. Η διαμόρφωση του δίσκου, συμπεριλαμβανομένης της διαμόρφωσης διαμερισμάτων και της διάταξης δίσκου, αποθηκεύεται στον πρώτο τομέα του δίσκου στο MBR. Παραδοσιακά, εάν το MBR καταστραφεί ή μετακινηθεί σε ένα διαφορετικό μέρος του δίσκου, τα δεδομένα γίνονται απρόσιτα. Οι δίσκοι MBR έχουν περιορισμό μέχρι τρία κύρια διαμερίσματα και ένα μόνο εκτεταμένο διαμέρισμα που μπορεί να περιέχει πολλές λογικές μονάδες δίσκου. Η επιλογή δημιουργίας δίσκου MBR θα πρέπει να παρέχει στους διαχειριστές περισσότερους συμβατούς δίσκους που μπορούν εύκολα να τοποθετηθούν ή να διαχειριστούν μεταξύ διαφορετικών λειτουργιών από πλατφόρμες συστήματος και εργαλεία διαχείρισης δίσκων τρίτων.
- **GUID Partition Table (GPT) Disks:** Οι δίσκοι GPT παρουσιάστηκαν για πρώτη φορά στα Windows με το Windows Server 2003 Service Pack 1. Συνιστώνται δίσκοι GPT για δίσκους μεγέθους άνω των 2 TB. Οι δίσκοι GPT μπορούν να υποστηρίξουν απεριόριστο αριθμό πρωτογενών διαμερισμάτων και αυτό μπορεί να είναι πολύ χρήσιμο όταν οι διαχειριστές αξιοποιούν μεγάλες σειρές εξωτερικών δίσκων και πρέπει να τμηματοποιούν δεδομένα για ασφάλεια, φιλοξενία ή κατανεμημένη διαχείριση και πρόσβαση. Οι δίσκοι GPT αναγνωρίζονται μόνο από τα Windows Server 2003 SP1 και νεότερα λειτουργικά συστήματα Windows.
- **Βασικός δίσκος:** Ο δίσκος των Windows ορίζεται ως βασικός ή δυναμικός δίσκος ανεξάρτητα από το αν ο δίσκος είναι MBR ή δίσκος GPT. Ένας βασικός δίσκος υποστηρίζει μόνο απλούς τόμους ή τόμους που υπάρχουν σε ένα μονό δίσκο και διαμέρισμα. Οι βασικοί δίσκοι δεν περιέχουν ανοχή σφαλμάτων που διαχειρίζεται το λειτουργικό σύστημα, αλλά μπορούν να είναι ανεκτικοί σε σφάλματα εάν διαχειρίζεται ο δίσκος που παρουσιάζεται στα Windows από έναν εξωτερικό ελεγκτή δίσκου και έχει διαμορφωθεί σε μια σειρά δίσκων ανεκτών σε σφάλματα. Οι βασικοί δίσκοι μετακινούνται ευκολότερα σε διαφορετικά λειτουργικά συστήματα και συνήθως οι περισσότεροι είναι συμβατοί με το σύστημα αρχείων των Windows και εργαλεία διαχείρισης τρίτων. Οι βασικοί δίσκοι υποστηρίζουν επίσης την εκκίνηση σε διαφορετικά λειτουργικά συστήματα που είναι αποθηκευμένα σε ξεχωριστά χωρίσματα.
- **Δυναμικός δίσκος:** Οι δυναμικοί δίσκοι επεκτείνουν τη λειτουργικότητα των Windows κατά τη διαχείριση πολλαπλών δίσκων χρησιμοποιώντας Windows 2008. Οι διαχειριστές των Windows μπορούν να διαμορφώσουν δυναμικούς δίσκους για να φιλοξενήσουν τόμους που εκτείνονται σε πολλά διαμερίσματα και δίσκους σε ένα μόνο σύστημα. Αυτό επιτρέπει στους διαχειριστές να δημιουργούν τόμους ανεκτούς σε σφάλματα και καλύτερες αποδόσεις. Σε ορισμένες αναπτύξεις διακομιστή, απαιτούνται δυναμικοί δίσκοι ανοχής σφαλμάτων στις προτεινόμενες προδιαγραφές συστήματος. Σε αυτές τις περιπτώσεις, μπορούν να χρησιμοποιηθούν δυναμικοί δίσκοι με τόμους ανεκτούς σε σφάλματα ή τόμους που μπορούν να διαβάζουν και να γράφουν δεδομένα σε πολλούς φυσικούς δίσκους για μεγαλύτερη απόδοση και μεγαλύτερη αξιοπιστία. Η διαχείριση των δυναμικών δίσκων γίνεται από το λειτουργικό σύστημα χρησιμοποιώντας την υπηρεσία εικονικού δίσκου (VDS).

Το κατανεμημένο σύστημα αρχείων (DFS)

Για να βελτιωθεί η αξιοπιστία και η διαθεσιμότητα των κοινόχρηστων αρχείων σε ένα εταιρικό δίκτυο, η Microsoft έχει αναπτύξει το κατανεμημένο σύστημα αρχείων (DFS). Το DFS βελτιώνει τη διαθεσιμότητα κοινής χρήσης αρχείων παρέχοντας έναν ενιαίο χώρο ονομάτων για πρόσβαση σε κοινόχρηστους φακέλους που φιλοξενούνται σε έναν ή περισσότερους διακομιστές. Ένας χρήστης πρέπει να θυμάται μόνο έναν διακομιστή ή ένα όνομα τομέα και αφού έχει συνδεθεί να μοιράζεται έναν κοινόχρηστο φάκελο DFS.
Το DFS έχει πολλά οφέλη και δυνατότητες που μπορούν να απλοποιήσουν την πρόσβαση και τη διαχείριση δεδομένων από την προοπτική του διαχειριστή όσο και του τελικού χρήστη. Το DFS παρέχει τρεις κύριες λειτουργίες:

- *Ενοποιημένος χώρος ονομάτων (Unified namespace)*: Τα δεδομένα DFS βρίσκονται κάτω από ένα μόνο όνομα διακομιστή ή ένα όνομα τομέα.
- *Απόλυση δεδομένων (Data redundancy)*: Το DFS μπορεί να παρέχει πρόσβαση σε ένα κοινόχρηστο στοιχείο που φιλοξενείται σε πολλαπλούς διακομιστές. Αυτό επιτρέπει στους πελάτες να παραπέμπουν ή να αποτύχουν σε διαφορετικό διακομιστή εάν δεν είναι δυνατή η επικοινωνία με τον κύριο διακομιστή.
- *Αυτοματοποιημένη αναπαραγωγή δεδομένων (Automated data replication)*:Το DFS μπορεί να ρυθμιστεί ώστε να χρησιμοποιεί την ενσωματωμένη υπηρεσία File Replication Service (FRS) ή το Distributed File System Replication (DFSR), και μπορεί να ρυθμιστεί ώστε να συγχρονίζει αυτόματα φακέλους μεταξύ διακομιστών DFS έτσι ώστε να παρέχει πλεονασμό δεδομένων ή κεντρική αποθήκευση δεδομένων.

Το DFS μπορεί να χρησιμοποιηθεί με διαφορετικούς τρόπους, αλλά απαιτεί πάντα τη δημιουργία ενός DFS χώρου ονομάτων (namespace). Ένας χώρος ονομάτων DFS μπορεί να είναι το όνομα ενός μεμονωμένου διακομιστή και κοινόχρηστου φακέλου ή του DNS και το όνομα NetBIOS ενός τομέα Active Directory και του κοινόχρηστου φακέλου. Ο χώρος ονομάτων επιτρέπει στις συνδέσεις να ανακατευθύνονται αυτόματα σε διαφορετικούς διακομιστές χωρίς να το γνωρίζει ο χρήστης. Υπάρχουν δύο τύποι χώρων ονομάτων:

- *Αυτόνομος χώρος ονομάτων DFS*: Ένας αυτόνομος χώρος ονομάτων DFS χρησιμοποιεί το όνομα του διακομιστή που φιλοξενεί τον χώρο ονομάτων DFS. Οι αυτόνομοι χώροι ονομάτων DFS πρέπει να χρησιμοποιούνται όταν πρέπει να απλοποιηθεί η πρόσβαση στο σύστημα αρχείων και η ποσότητα των δεδομένων υπερβαίνει τη χωρητικότητα ενός μόνο διακομιστή. Επίσης, εάν δεν έχει ενεργοποιηθεί ο τομέας Active Directory, υποστηρίζεται ένας αυτόνομος χώρος ονομάτων DFS. Όταν δημιουργείται ο αυτόνομος χώρος ονομάτων DFS σε διακομιστή των Windows 2008 που είναι μέλος ενός Active Τομέας καταλόγου, μπορεί να ρυθμιστεί η αναπαραγωγή DFS.
- *Χώρος ονομάτων DFS βάσει τομέα*: Ένας χώρος ονομάτων DFS που βασίζεται σε τομέα χρησιμοποιεί το όνομα του τομέα Active Directory στο οποίο ο DFS διακομιστής είναι μέλος του. Ένας χώρος ονομάτων DFS που βασίζεται σε τομέα δημιουργείται κατά την ανάπτυξη ενός τομέα Active Directory στη θέση του \\ domain \ SYSVOL για την αναπαραγωγή των Group Policies Domain.

6.7.2. Ανοχή σφαλμάτων σε επίπεδο συστήματος (System-Level Fault Tolerance)

Δημιουργία Fault-Tolerant συστημάτων Windows Server 2008

Η δημιουργία ανεκτικών συστημάτων Windows 2008 με χρήση των ενσωματωμένων τεχνολογιών συμπλέγματος πραγματοποιείται μετά από προσεκτικό σχεδιασμό και διαμόρφωση υλικού και λογισμικού διακομιστή, προγραμματισμού και διαμόρφωση των συσκευών δικτύου που συνδέουν το διακομιστή στο δίκτυο και παρέχουν αξιόπιστη ισχύς για τον διακομιστή. Η αγορά υψηλής ποιότητας διακομιστή και υλικού δικτύου είναι καλή αρχή για την οικοδόμηση ενός ανεκτικού συστήματος, αλλά η σωστή διαμόρφωση αυτού του υλικού είναι εξίσου σημαντικό. Η παροχή σε αυτόν τον εξοπλισμό αξιόπιστου UPS και πιθανώς πηγών τροφοδοσίας που υποστηρίζονται από γεννήτρια μπορούν να προσθέσουν ανοχή σφαλμάτων στο διακομιστή καθώς και στην υποδομή δικτύωσης. Ο σωστός συντονισμός των λειτουργικών συστημάτων διακομιστή για τον εξορθολογισμό της απόδοσης για τους επιθυμητούς ρόλους, υπηρεσίες ρόλου, δυνατότητες και εφαρμογές βοηθά στη βελτίωση της διαθεσιμότητας και της σταθερότητας του διακομιστή. Πολλοί οργανισμοί δεν μπορούν να αντέξουν οικονομικά για την εφαρμογή περιττών πηγών ενέργειας ή γεννητριών για την τροφοδοσία γραφείων, κέντρων δεδομένων, και δωμάτια διακομιστών. Για αυτούς τους οργανισμούς, η καλύτερη προσέγγιση για την παροχή αξιόπιστης ισχύος στον υπολογιστή και την υποδομή δικτύου είναι η ανάπτυξη αδιάλειπτων τροφοδοτικών (UPS) με ισχύ και μπαταρία. Με ένα UPS, τροφοδοτείται κανονικά από τις μπαταρίες, οι οποίες φορτίζονται συνεχώς από τη γραμμή ισχύος. Όταν η γραμμή ισχύος αποτύχει, το UPS παρέχει άφθονο χρόνο στους τελικούς χρήστες να αποθηκεύσουν τα δεδομένα τους στον διακομιστή και στη συνέχεια να απενεργοποιήσουν τον διακομιστή ή τη συσκευή δικτύου χωρίς κίνδυνο πρόκλησης ζημιάς στο υλικό ή αλλοίωσης των δεδομένων. Οι κατασκευαστές UPS παρέχουν συνήθως λογισμικό που μπορεί να στέλνει ειδοποιήσεις δικτύου, να εκτελεί δέσμες ενεργειών ή ακόμη και τερματισμό των διακομιστών αυτόματα όταν τα όρια ισχύος είναι κάτω από ένα όριο που εμείς έχουμε θέσει. Φυσικά, εάν τα δεδομένα των τελικών χρηστών είναι σημαντικά, κάθε σταθμός εργασίας τελικού χρήστη και τα switches του δικτύου που συνδέουν αυτούς τους σταθμούς εργασίας με την υποδομή του υπολογιστή και του δικτύου θα πρέπει επίσης να προστατεύονται με UPS που μπορούν να παρέχουν τουλάχιστον 5 έως 10 λεπτά παροχής ισχύος για την δημιουργία αντιγράφων ασφαλείας.

Σχεδιασμός δικτύων IP ανεκτικών σε σφάλματα

Ο σχεδιασμός δικτύου μπορεί επίσης να ενσωματωθεί στην ανοχή σφαλμάτων δημιουργώντας δευτερεύοντες (backup) διαδρομές δικτύου και με τη χρήση τεχνολογιών που μπορούν να ομαδοποιήσουν τις συσκευές με σκοπό την εξισορρόπηση φορτίου (load balancing) και την αστοχία συσκευών (failover devices). Η εξισορρόπηση φορτίου είναι η διαδικασία διάδοσης αιτημάτων σε πολλαπλές συσκευές για να διατηρηθεί το φορτίο μεμονωμένων συσκευών σε αποδεκτό επίπεδο. Το failover είναι η διαδικασία μετακίνησης υπηρεσιών που προσφέρονται από τη μία συσκευή στην άλλη μετά από αστοχία της συσκευής, για συνέχιση της διαθεσιμότητας.

Τα κοινά σενάρια για τη δημιουργία δικτύων IP ανεκτικών σε σφάλματα μπορούν να περιλαμβάνουν τα ακόλουθα:

- ✓ Απόκτηση πολλαπλών συνδέσεων δικτύου μεταξύ του κέντρου δεδομένων και του Διαδίκτυο: Αυτό περιλαμβάνει τη χρήση διαφορετικών παρόχων υπηρεσιών Διαδικτύου και κάθε μία από τις συνδέσεις δεν είναι συνδεδεμένη στο ίδιο σημείο

σύνδεσης καθώς αυτό γίνεται το μοναδικό σημείο αποτυχίας εάν χτυπηθεί από αυτοκίνητο, φορτηγό ή αποκοπεί από τις επικοινωνίες.

- ✓ Ανάπτυξη πολλαπλών και περιττών τειχών προστασίας, εικονικών ιδιωτικών δικτύων (VPN), και δρομολογητών δικτύου που θα μετακινούνται μεταξύ τους: Αυτό συνήθως περιλαμβάνει λογισμικό ή διαμορφώσεις υλικού που επιτρέπουν σε κάθε συσκευή να επικοινωνούν με άλλες συσκευές για τον εντοπισμό αστοχιών. Αυτές οι συσκευές, όταν αναπτύσσονται σε περιττές διαμορφώσεις, μπορεί να αξιοποιηθούν σε μια ενεργή / παθητική διαμόρφωση όπου μόνο η κύρια συσκευή χρησιμοποιείται και η δευτερεύουσα συσκευή συνδέεται μόνο όταν αποτύχει η κύρια. Εναλλακτικά, σε πολλές περιπτώσεις αυτές οι συσκευές μπορούν να χρησιμοποιηθούν σε active / active διαμόρφωση που διασκορπίζει ή κατανέμει το φορτίο και τα αιτήματα σε κάθε συσκευή και όταν μία συσκευή αποτυγχάνει, η υπόλοιπη συσκευή χειρίζεται ολόκληρο το φορτίο.
- ✓ Ανάπτυξη κρίσιμων διακομιστών με πολλαπλούς προσαρμογείς δικτύου συνδεδεμένους για διαχωρισμό των switches του δικτύου - Αυτό επιτρέπει σε έναν διακομιστή να είναι συνδεδεμένος και διαθέσιμος σε διαφορετικά swithes σε περίπτωση που μία κάρτα δικτύου στο διακομιστή αποτύχει ή εάν ολόκληρο το switch του δικτύου ή το blade αποτυγχάνουν.
- ✓ Ανάπτυξη συσκευών NLB βάσει υλικού - Πολλά switches δικτύου, δρομολογητές και ορισμένες συσκευές που έχουν δημιουργηθεί μόνο για το σκοπό αυτό μπορούν να παρέχουν κάποια, αν όχι όλες, λειτουργικότητα που περιλαμβάνεται στα Windows 2008 NLB. Αυτή, φυσικά, μπορεί να είναι η καλύτερη επιλογή για εξισορρόπηση φορτίου σε επίπεδο δικτύου όταν οι οργανισμοί αναπτύσσουν και υποστηρίζουν συστήματα εκτός από τα Windows 2008 και όταν πρέπει επίσης να υπάρχει ισορροπία μεταξύ των συσκευών του δικτύου, όπως τείχη προστασίας και συσκευές VPN.
- ✓ Ανάπτυξη διακομιστών με πολλαπλούς προσαρμογείς δικτύου χρησιμοποιώντας λογισμικό ομαδοποίησης δικτύου από τρίτους - Αυτή η διαμόρφωση χρησιμοποιεί εγκατεστημένο και διαμορφωμένο λογισμικό τρίτου μέρους σε διακομιστή για τη δημιουργία ενός νέου εικονικού προσαρμογέα δικτύου που χρησιμοποιείται για την πρόσβαση στο σύστημα διακομιστή μέσω ενός ή και των δύο φυσικών προσαρμογέων δικτύου στον διακομιστή. Τα Windows 2008 υποστηρίζουν ομαδοποιημένους προσαρμογείς δικτύου όσο τα προγράμματα οδήγησης και το λογισμικό είναι πιστοποιημένα ότι λειτουργούν με τα Windows 2008.

Σχεδιασμός δίσκων διακομιστή με ανοχή σφαλμάτων

Τα συστήματα Windows 2008 που θα χρησιμοποιηθούν για συμπλέγματα NLB ή failover αναπτύσσονται συνήθως με τοπικό χώρο αποθήκευσης δίσκου. Οι τοπικοί δίσκοι αποθηκεύουν συνήθως τα αρχεία του λειτουργικού συστήματος όπως και τα απαραίτητα αρχεία υπηρεσίας ή εφαρμογής. Κάθε σύστημα που θα συμμετέχει σε ένα σύμπλεγμα θα πρέπει να έχει τους τοπικούς δίσκους και τόμους διαμορφωμένους ακριβώς το ίδιο, συμπεριλαμβανομένης της αντιστοίχισης γραμμάτων της μονάδας δίσκου και σημείων προσάρτησης. Όταν χρησιμοποιούνται τοπικοί δίσκοι για την παροχή της λειτουργίας συστήματος, αρχείων πυρήνα και εφαρμογών ή υπηρεσιών, οι τοπικοί δίσκοι πρέπει να αναπτυχθούν χρησιμοποιώντας πλεονάζουσες, ανεκτικές σε βλάβες διαμορφώσεις. Υπάρχουν κυρίως δύο διαφορετικοί τρόποι για να προσθέσετε ανοχή σφαλμάτων στους τοπικούς δίσκους σε Windows Σύστημα 2008. Η πρώτη είναι η δημιουργία περιττών συστοιχιών φθηνών δίσκων (RAID) χρησιμοποιώντας βοηθητικά προγράμματα

διαμόρφωσης ελεγκτή (επίσης γνωστά ως RAID σε επίπεδο υλικού) και το δεύτερο είναι δημιουργία δίσκων RAID χρησιμοποιώντας δυναμικούς δίσκους χρησιμοποιώντας την κονσόλα διαχείρισης δίσκων από εντός του λειτουργικού συστήματος (γνωστό ως RAID σε επίπεδο λογισμικού). Χρησιμοποιώντας δύο ή περισσότερους δίσκους, μπορούν να διαμορφωθούν διαφορετικές συστοιχίες επιπέδου RAID ώστε να παρέχουν ανοχή σφαλμάτων που μπορεί να αντέξει σε αστοχίες δίσκου και εξακολουθεί να παρέχει αδιάλειπτη πρόσβαση στο δίσκο. Η υλοποίηση RAID επιπέδου υλικού που έχει διαμορφωθεί, αποθηκευτεί και διαχειρίζεται από το δίσκο από τους controllers του συστήματος προτιμάται από το RAID επιπέδου λογισμικού που μπορεί να διαμορφωθεί στα Windows 2008. Η διαχείριση των Windows 2008 με δυναμικό δίσκο και οι τόμοι RAID-5 διαχειρίζονται από το σύστημα και προσθέτουν λίγο φορτίο στο σύστημα. Επιπλέον, ένας άλλος καλός λόγος για την παροχή σκληρού επιπέδου RAID είναι ότι η διαμόρφωση των δίσκων δεν εξαρτάται από το λειτουργικό σύστημα, γεγονός που δίνει στους διαχειριστές μεγαλύτερη ευελιξία όσον αφορά την ανάκτηση συστημάτων διακομιστή και εκτέλεση αναβαθμίσεων. Ως βέλτιστη πρακτική, τα Windows 2008 μπορούν να αναπτυχθούν με αποθηκευμένους δίσκους λειτουργικού συστήματος σε RAID-1, ή κατοπτρισμένοι, δίσκοι και παρουσιάζονται στο λειτουργικό σύστημα ως τόμος "C". Ο δεύτερος τόμος στο σύστημα μπορεί να χρησιμοποιηθεί για την αποθήκευση δεδομένων και αρχείων εφαρμογής και, όταν είναι δυνατόν, αυτά τα δεδομένα θα πρέπει να τοποθετούνται σε διαφορετικούς περιττούς δίσκους ή τουλάχιστον σε ξεχωριστούς τόμους που δεν επηρεάζουν τον διαθέσιμο χώρο στον όγκο του λειτουργικού συστήματος.

6.8. Εικονικές μηχανές και Hyper-V (Virtual Machines and Hyper-V)

Η τεχνολογία VM επιτρέπει ένα τμήμα της CPU και της μνήμη ενός μηχανήματος να αφιερωθεί σε μια διαδικασία που μιμείται ένα φυσικό περιβάλλον μηχανών. Αυτό το περιβάλλον είναι πλήρες με το δικό του εικονικό BIOS, δικά του γραφικά και προσαρμογέα δικτύου. Αυτό ονομάζεται εικονική μηχανή (VM). Επιπλέον, τα εικονικά αρχεία σκληρού δίσκου (VHD) συνδέονται με VM, τα οποία είναι πραγματικά αρχεία στο σύστημα αρχείων του κεντρικού υπολογιστή. Αυτά τα αρχεία περιέχουν ένα πλήρες δικό τους σύστημα αρχείων, με ιεραρχία φακέλων και αρχείων, σαν ένα αρχείο ZIP ή CAB. Όταν συνδυάζουμε την εκχωρημένη μνήμη και τους πόρους CPU, μαζί με το εικονικό BIOS, δίκτυο, μονάδες CD και συνδέσμους προς VHD, έχουμε ένα πλήρες περιβάλλον υπολογιστή. Στη συνέχεια, μπορούμε να ξεκινήσουμε αυτό το εικονικό περιβάλλον και κάνουμε ότι επιθυμούμε όπως με ένα κανονικό φυσικό υπολογιστή, εγκατάσταση OS (τα οποία στη συνέχεια μπορούν να εκτελούν εφαρμογές) και να επικοινωνούν μέσω δικτύου.

Εικόνα 6.98

Μπορούμε να κάνουμε τα ίδια ακριβώς πράγματα όπως σε ένα λειτουργικό ενός φυσικού υπολογιστή. Στην εικόνα 6.98 φαίνεται ένα παράδειγμα ενός εικονικού διακομιστή: Ο διακομιστής εκτελεί Windows Server 2008, ο οποίος έχει δύο καθορισμένα VM. Κάθε μηχάνημα διαθέτει τη δική του ποσότητα μνήμης, πόρους CPU και σκληρό δίσκο που συνδέεται με ένα αρχείο VHD στο τοπικό σύστημα αρχείων.

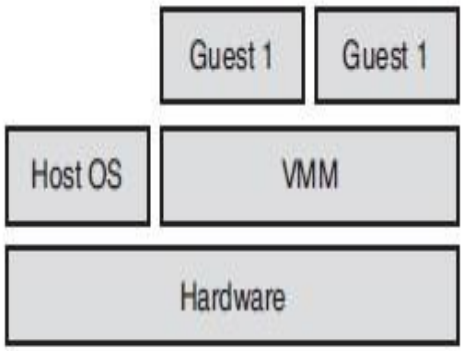
Οι μόνοι περιορισμοί είναι οι δυνατότητες των εικονικών στοιχείων που εμφανίζονται από το VM, όπως περιορισμένο γραφικό υλικό και περιορισμοί στη πιθανή απόδοση των αρχείων VHD. Ωστόσο, ορισμένες λύσεις επιτρέπουν στα VM να συνδέονται με πραγματικούς φυσικούς σκληρούς δίσκους, αφαιρώντας αυτήν την επιπλοκή απόδοσης. Υπάρχουν επίσης περιορισμοί σε διάφορες εφαρμογές λύσεων VM που δεν επιτρέπουν την πρόσβαση σε συσκευές USB και άλλους τύπους υλικού, όπως κάρτες ινών.

6.8.1. Τεχνολογίες εικονικοποίησης

Υπάρχουν πολλές τεχνολογίες για τη διευκόλυνση της διαδικασίας εικονικοποίησης. Αυτές οι τεχνολογίες δημιουργούν ένα ολόκληρο περιβάλλον υπολογιστή μέσα σε από μια διαδικασία που επιτρέπει την εκτέλεση πολλαπλών λειτουργικών συστημάτων σε ένα σύνολο υλικού. Ως εκ τούτου, η τεχνολογία της εικονικοποίηση πρέπει να μοιράζεται την πρόσβαση στην CPU, τους προσαρμογείς δικτύου και την πρόσβαση σε οποιοδήποτε άλλο υλικό, προσπαθώντας ταυτόχρονα να ελαχιστοποιήσει τα γενικά έξοδα για τη μείωση της απόδοσης των εικονικών περιβαλλόντων.

Hosted Virtual Machine Manager (VMM)

Όπως αναφέρθηκε προηγουμένως, πολλές τεχνολογίες χρησιμοποιούνται για εικονικοποίηση. Ας ξεκινήσουμε με λύσεις όπως Virtual PC και Virtual Server, που είναι γνωστά ως Υβριδικά ή Hosted Virtual Machine Managers (VMMs). Το VMM και το κεντρικό λειτουργικό σύστημα λειτουργούν και τα δύο σε λειτουργία πυρήνα, οπότε έχουν ίση πρόσβαση στους πόρους της CPU. Τα λειτουργικά συστήματα επισκεπτών εκτελούνται πάνω από το VMM, όπως φαίνεται στην εικόνα 6.99.



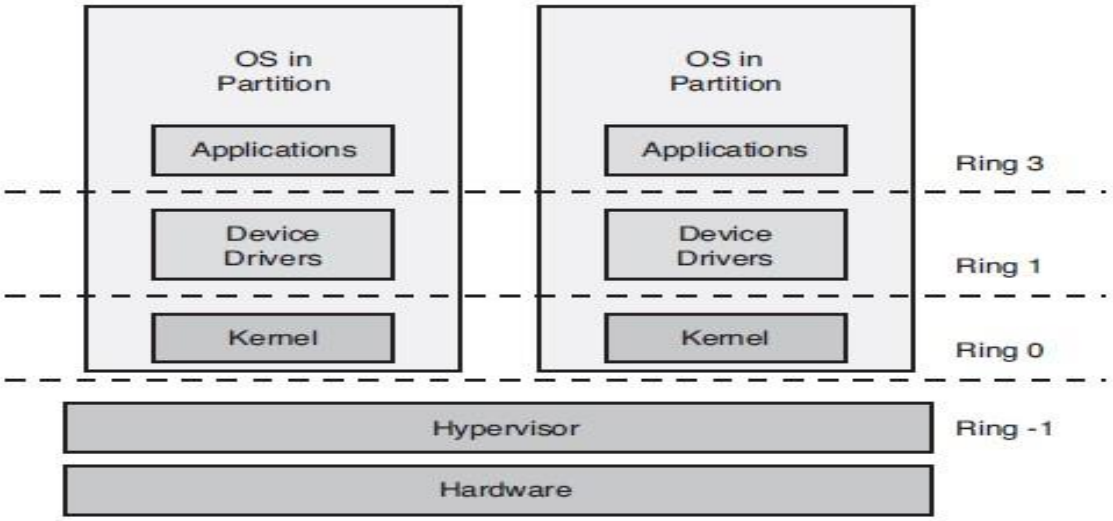
Εικόνα 6.99

Το VMM εξακολουθεί να λειτουργεί εντός του κεντρικού λειτουργικού συστήματος. Ωστόσο, εμφανίζονται δίπλα το ένα στο άλλο επειδή τρέχουν σε λειτουργία πυρήνα, όπως δηλώνεται και με το λειτουργικό σύστημα του κεντρικού υπολογιστή. Η διαδικασία για ένα VMM, όπως το Virtual PC, χρησιμοποιεί πολλούς πόρους από το kernel time. Ωστόσο, θα πρέπει ακόμη να ζητήσει από το κεντρικό λειτουργικό σύστημα να πάρει τους κύκλους ρολογιού επειδή το κεντρικό λειτουργικό σύστημα ελέγχει τον επεξεργαστή. Το VMM μπορεί να δώσει τους κύκλους ρολογιού του λειτουργικού συστήματος όποτε αυτό απαιτηθεί, οπότε η απόδοση είναι πολύ μικρότερη από ό, τι αν λειτουργούσε το λειτουργικό σύστημα απευθείας στο δικό του υλικό.

Hypervisor Virtualization

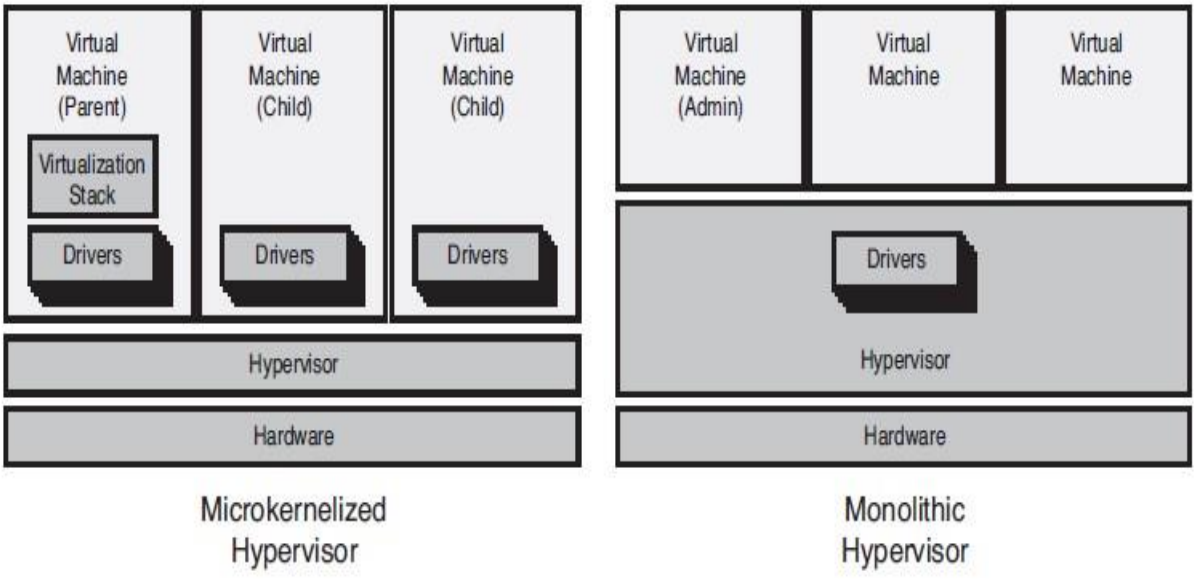
Ο νέος τύπος τεχνολογίας εικονικοποίησης είναι γνωστός ως τύπος 1 VMM ή Hypervisor Virtualization. Το VMM κάθεται απευθείας στο υλικό ως λεπτό επίπεδο υπεύθυνο για την απομόνωση ξεχωριστών περιβαλλόντων, γνωστών ως διαμερισμάτων, και για την εκτέλεση λειτουργικών συστημάτων. Διαιρεί επίσης τη μνήμη, τους κύκλους της CPU και άλλους πόρους υλικού μεταξύ των διαμερισμάτων που εκτελούνται πάνω από τον επόπτη. Αυτή η διαίρεση, η οποία θα περιλαμβάνει το «κύριο» λειτουργικό σύστημα (όπως τα Windows Server 2008), είναι δύσκολη επειδή ένα εγκατεστημένο λειτουργικό σύστημα αναμένει άμεση πρόσβαση στον επεξεργαστή στο δακτύλιο 0 στο kernel του επεξεργαστή. Για να υποστηριχθεί ένα επίπεδο από κάτω στο λειτουργικό σύστημα, ο επεξεργαστής πρέπει να υποστηρίζει τον αρνητικό δακτύλιο 1 (-1), το οποίο παρέχεται μόνο σε συγκεκριμένους επεξεργαστές 64-bit που υποστηρίζουν την εκτέλεση εικονικοποίησης, δηλαδή AMD-V ή Intel-VT. Επιπλέον, το υλικό για Data Execution Protection (DEP) πρέπει να είναι ενεργοποιημένο μέσω του BIOS (Intel XD bit ή bit AMD NX, ανάλογα με τον επεξεργαστή). Ο Hypervisor μπορεί στη συνέχεια να τρέξει τον δακτύλιο -1 στον επεξεργαστή κάτω από τον κανονικό δακτύλιο 0. Εδώ ο πυρήνας των λειτουργικών συστημάτων είναι εγκατεστημένος στα διαμερίσματα στον δακτύλιο πρόσβασης 0 του Hypervisor όπως και άλλοι δακτύλιοι του επεξεργαστή που χρησιμοποιούνται κανονικά. Τα προγράμματα οδήγησης συσκευών λειτουργούν στον δακτύλιο 1 και οι εφαρμογές εκτελούνται στον δακτύλιο 3 σε κανονική λειτουργία χρήστη. Αυτό είναι σημαντικό στο hypervisor: Τα VM λειτουργούν το ίδιο με ένα κανονικό

λειτουργικό σύστημα εγκατεστημένο στο υλικό με άμεση πρόσβαση στο δακτύλιο 0, δίνοντας απόδοση ισοδύναμη με την εκτέλεση στο φυσικό υλικό, όπως φαίνεται και στην εικόνα 6.100.



Εικόνα 6.100

Υπάρχουν δύο τύποι hypervisor: μονολιθικοί και μικρο-πυρήνες (microkernelized), όπως φαίνεται στην εικόνα 6.101.



Εικόνα 6.101

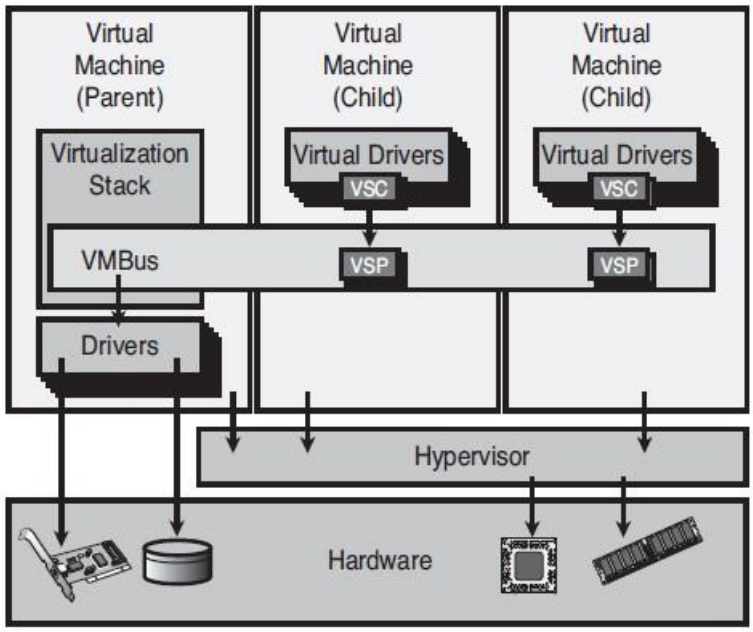
Η τεχνολογία Hyper-V, η οποία χρησιμοποιείται από την εικονικοποίηση των Windows Server 2008, είναι ένας microkernelized hypervisor. Ο διακομιστής ESX του VMware χρησιμοποιεί έναν μονολιθικός hypervisor. Στον μονολιθικό hypervisor, τους οδηγούς που

είναι υπεύθυνοι για την επικοινωνία με το υλικό είναι εγκατεστημένοι στον πραγματικό επόπτη. Ο hypervisor είναι δίκαιος σύνθετος πυρήνας, στην πραγματικότητα είναι ένα μίνι-λειτουργικό σύστημα. Τα VM έχουν πρόσβαση στο υλικό μέσω εξειδικευμένων προγραμμάτων οδήγησης συσκευών, τα οποία αποδίδουν καλά επειδή τα VM μπορούν να πάνε απευθείας σε όλο το υλικό μέσω αυτών των προγραμμάτων οδήγησης. Φυσικά, υπάρχουν ζητήματα. Το πρώτο ζήτημα είναι ότι αυτά τα κοινόχρηστα προγράμματα οδήγησης είναι ειδικά γραμμένα για τον hypervisor Αυτό περιορίζει το υλικό που υποστηρίζεται από έναν μονολιθικό hypervisor και με αποτέλεσμα λύσεις εικονικοποίησης που χρησιμοποιούν μονολιθικό hypervisor συνήθως έχουν μια μικρή λίστα συμβατότητας υλικού. Αυτή η κοινόχρηστη βάση προγραμμάτων οδήγησης οδηγεί στις δύο κύριες ανησυχίες: ασφάλεια και σταθερότητα. Επειδή υπάρχει κοινόχρηστο πρόγραμμα οδήγησης για τα VM, εάν ένα πρόγραμμα οδήγησης κακόβουλου λογισμικού τοποθετηθεί στον hypervisor, όλα τα διαμερίσματα θα ήταν ευάλωτα σε επιθέσεις και κατασκοπεία. Επιπλέον, εάν το πρόγραμμα οδήγησης ενημερώνεται από τον hypervisor που έχει πρόβλημα, προκαλεί προβλήματα για όλα τα VM.
Λόγω αυτών των προβλημάτων, και ιδιαίτερα των περιορισμών υποστήριξης του υλικού, τα Windows Server 2008 χρησιμοποιούν τον μικροεπιχειρησιακό (microkernelized) hypervisor. Αυτή η προσέγγιση επιτρέπει στους drivers να υπάρχουν στα πραγματικά VM, που σημαίνει ότι τα υπάρχοντα προγράμματα οδήγησης για υλικό μπορούν να χρησιμοποιηθούν και το εύρος υποστηρίζεται από υλικό που εκτελεί Windows Server. Αυτό δίνει τη δυνατότητα ο επόπτης να παραμείνει κλειστός σε λογισμικά τρίτων, καθώς τίποτα δεν προστίθεται στον hypervisor.
Ο hypervisor καθορίζει την κατανομή των κύκλων CPU και της μνήμης RAM. Από τον hypervisor δεν καθορίζονται άλλοι τύποι συσκευών, όπως δίσκος και Ethernet, επειδή αυτό θα απαιτούσε από τον hypervisor να κατανοήσει πώς αυτοί οι τύποι συσκευών λειτουργούν. Με το Hyper-V, το πρώτο εγκατεστημένο λειτουργικό σύστημα (Windows Server 2008) λειτουργώντας ως γονικό διαμέρισμα, το οποίο κατέχει τους πόρους χωρίς CPU και μνήμη, εκτελώντας άμεση επικοινωνία με αυτούς τους πόρους για λογαριασμό του αλλά και άλλων θυγατρικών VM στο διακομιστή. Ο άλλος λόγος για τα διαμερίσματα παιδιά είναι ότι δεν μπορεί να έχουν άμεση πρόσβαση σε άλλους τύπους υλικού που σχετίζεται με μια εγγύηση ασφαλείας της Microsoft, η οποία δηλώνει ότι τα διαμερίσματα παιδιών δεν μπορούν να δουν, να διαχειριστούν, ή να αναλάβουν άλλα διαμερίσματα παιδιών ή να αποκτήσουν απευθείας πρόσβαση σε οποιοδήποτε υλικό. Η απομόνωση είναι μια βασική πτυχή για την εφαρμογή των εποπτικών αρχών των Windows. Εφαρμόζονται αυστηροί έλεγχοι που απαγορεύουν την κοινή χρήση εικονικών συσκευών μεταξύ θυγατρικών διαμερισμάτων ή κοινόχρηστη μνήμη και ούτε ένα διαμέρισμα παιδιού ούτε γονέα μπορεί να γράψει δεδομένα στον hypervisor.

Σκοπός ενός Γονικού Διαμερίσματος

Το γονικό διαμέρισμα φιλοξενεί μια στοίβα εικονικοποίησης που περιλαμβάνει διαχειριστικά στοιχεία που εκτελούνται σε κανονική λειτουργία χρήστη, γνωστή ως Εικονική Διαχείριση Μηχανής (VMM), η οποία περιέχει την υπηρεσία εικονικής μηχανής (VM Υπηρεσία). Αυτή η υπηρεσία VM διαχειρίζεται το Virtual Machine Worker Processes - μία για κάθε διαμέρισμα παιδί που εκτελείται - η οποία ελέγχει την κατάσταση του παιδικού διαμερίσματος, διακοπή, εκκίνηση και ούτω καθεξής. Χρειαζόμαστε το γονικό διαμέρισμα, μαζί με τον hypervisor, για να κάνουμε οτιδήποτε χρήσιμο, όπως δημιουργία χωρισμάτων παιδιών. Παρόλο που μπορούμε να εγκαταστήσουμε τον hypervisor από

μόνο του, δεν θα μπορεί να κάνει και πολλά πράγματα χωρίς το γονικό διαμέρισμα των Windows Server 2008.
Τα στοιχεία εκτελούνται επίσης σε λειτουργία πυρήνα, όπως το Bus Virtual Machine (VMBus). Αυτό φιλοξενεί έναν αριθμό παρόχων εικονικών υπηρεσιών (Virtual Service Provider - VSP) στο φυσικό υλικό, το οποίο αντιστοιχεί σε έναν αριθμό καταναλωτών εικονικών υπηρεσιών (Virtual Service Consumer - VSC) που εκτελούνται στα θυγατρικά διαμερίσματα. Για παράδειγμα, έχουμε ένα VSP και VSC για το δίκτυο, ένα ζεύγος για αποθήκευση και ούτω καθεξής. Όταν ένα παιδικό διαμέρισμα θέλει να αποκτήσει πρόσβαση σε πόρους υλικού που δεν είναι CPU ή μνήμη, το VSC του υποβάλλει ένα αίτημα στο VSP που φιλοξενείται στο VMBus στο γονικό διαμέρισμα. Αυτό εκτελεί την πραγματική επικοινωνία με το φυσικό υλικό, όπως φαίνεται στην εικόνα 6.102. Το VMBus δεν κοινοποιείται σε όλα τα θυγατρικά διαμερίσματα. Υπάρχει μία σύνδεση μεταξύ κάθε παιδιού και του γονέα, οπότε δεν υπάρχει επικοινωνία ή τα δεδομένα μπορούν να προβληθούν από άλλα θυγατρικά διαμερίσματα που εκτελούνται στον ίδιο εικονικό διακομιστή. Αυτό το VMBus φέρνει επιτυχία στην απόδοση επειδή αποτελεί το παιδί. Τα διαμερίσματα που θέλουν να έχουν πρόσβαση στο υλικό πρέπει να επικοινωνούν μέσω του VSC σε VSP. Αυτό γίνεται μέσω του VMBus που φιλοξενείται στο γονικό διαμέρισμα, που επικοινωνεί με το υλικό. Ωστόσο, αυτή η διαδρομή έχει γίνει όσο πιο σφιχτή γίνεται από τη Microsoft. Το πλεονέκτημα ενός μικρότερου, πιο ασφαλούς και πιο σταθερού hypervisor αξίζει τη μικρή επιτυχία απόδοσης, ειδικά όταν δεν χρειάζονται ειδικά προγράμματα οδήγησης συσκευών. Αυτό είναι ζωτικής σημασίας για το εύρος του διαθέσιμου υλικού για τα Windows Server.



Εικόνα 6.102

Εάν σκεφτούμε τι συμβαίνει για τα παιδικά διαμερίσματα τα οποία δεν καταλαβαίνουν το VMBus, έχουμε πολύ μεγαλύτερη επιτυχία. Για τα παιδικά διαχωριστικά αιτήματα, όπως λειτουργία δικτύου, το αίτημα πηγαίνει από τη λειτουργία χρήστη στο θυγατρικό διαμέρισμα, στη λειτουργία πυρήνα στο παιδί, στον πυρήνα στον γονέα (που φιλοξενεί τη εικονικοποιημένη συσκευή του παιδιού για το διαμέρισμα που βλέπει). Αυτό καταλήγει στο VM Worker Process σε λειτουργία γονέα στο χρήστη, η οποία στη συνέχεια υποβάλλει το πραγματικό αίτημα υλικού. Αυτή είναι μία αργή λειτουργία που απαιτεί εναλλαγή περιβάλλοντος χιλιάδες φορές. Το VMBus το αποφεύγει επειδή εκτελείται στον πυρήνα και επιτρέπει σχεδόν άμεση υλικό-επικοινωνία μέσω του VSC και του VSD. Επειδή αυτά είναι συνθετικά προγράμματα οδήγησης, οι μηχανές βλέπουν μια εικονική συσκευή δικτύου.

Το γονικό διαμέρισμα φιλοξενεί όλα τα στοιχεία υποστήριξης VM που δεν είναι μέρος του hypervisor. Εάν το γονικό διαμέρισμα επανεκκινήσει ή δεν είναι διαθέσιμο, κανένα από τα παιδικά διαμερίσματα δεν είναι διαθέσιμα.
Η στοίβα εικονικοποίησης εκθέτει επίσης μια διεπαφή διαχείρισης, η οποία χρησιμοποιείται όχι μόνο από το ενσωματωμένο εργαλείο διαχείρισης αλλά τεκμηριώνεται δημόσια μέσω της διεπαφής προγραμματισμού εφαρμογών (API). Αυτό επιτρέπει άλλη διαχείριση λύσεων για τη διαχείριση της εικονικοποίησης, όπως το System Center Virtual Machine Manager (SCVMM. Μια πλήρης διεπαφή WMI είναι επίσης διαθέσιμη για τη διαχείριση των στοιχείων εικονικοποίησης.

6.8.2. Hyper-V

Η ιστορία εικονικοποίησης ξεκίνησε με το στοιχείο Windows Server Virtualization (WSV) (επίσημα γνωστό ως Viridian) το οποίο απομονώθηκε από τον τυπικό κύκλο απελευθέρωσης του λειτουργικού συστήματος, και αντ 'αυτού υποσχέθηκε να είναι διαθέσιμο ως δωρεάν λήψη εντός 180 ημερών από τα Windows Server 2008 RTM ως ρόλο Hyper-V. Μία beta έκδοση του Hyper-V συμπεριλήφθηκε ως μέρος των μέσων ενημέρωσης RTM του 2008. Η τελική έκδοση του Hyper-V κυκλοφόρησε στις 26 Ιουνίου 2008. Διατίθεται από τη Microsoft ως ενημέρωση 950050 KB.
Το Hyper-V λειτουργεί μόνο σε πλατφόρμες 64 bit και ο επεξεργαστής πρέπει να υποστηρίζει εικονικοποίηση (για AMD επεξεργαστές θα πρέπει να έχει την τεχνολογία AMD-V, και για την Intel, την τεχνολογία Intel-VT). Το θετικό είναι ότι πλέον οι περισσότεροι νέοι επεξεργαστές υποστηρίζουν αυτές τις δυνατότητες, συμπεριλαμβανομένων των περισσότερων επιτραπέζιων και φορητών υπολογιστών. Επιπλέον, η προστασία εκτέλεσης των δεδομένα υλικού πρέπει να υποστηρίζεται και να ενεργοποιείται μέσω του BIOS που είναι γνωστό ως NX για επεξεργαστές AMD και XD για Intel.
Παρόλο που το κεντρικό λειτουργικό σύστημα πρέπει να είναι 64-bit, τα εικονικά λειτουργικά μπορούν να είναι 32-bit ή 64-bit. Επίσης, κάθε VM μπορεί να διαμορφωθεί με πολλούς επεξεργαστές (έως τέσσερις πυρήνες), εκτός από μνήμη έως 64 GB. Η πολλαπλή επεξεργασία υποστηρίζεται μόνο με Windows Server 2008 (32 και 64bit) και σε διαμερίσματα παιδιών Windows Vista SP1 (32 και 64bit). Για Windows Server 2003, 32-bit, υποστηρίζεται μόνο αμφίδρομο SMP. Για Windows Server 2003, 64-bit υποστηρίζονται δύο πυρήνες. Άλλες πλατφόρμες, όπως τα Windows 2000 SP24 και τα SUSE Linux Enterprise Server 10, υποστηρίζεται μόνο έναν πυρήνα. Δεν υπάρχουν γνωστά ζητήματα και υποστήριξη για άλλα λειτουργικά συστήματα με πολλαπλούς επεξεργαστές, τα οποία πιθανόν να έχουν προστεθεί σε νεότερες εκδόσεις με την πάροδο του χρόνου.
Από άποψη διαθεσιμότητας, υποστηρίζεται η ομαδοποίηση διακομιστών Hyper-V με τον νέο πόρο συμπλέγματος VM, ο οποίος επιτρέπει επίσης μία γρήγορη δυνατότητα μετεγκατάστασης για τη μετακίνηση VM μεταξύ φυσικών διακομιστών, συν τη δυνατότητα μετεγκατάστασης φυσικών κεντρικών υπολογιστών σε εικονικό περιβάλλον για την επίτευξη ενοποίησης σε έναν κεντρικό διακομιστή. Παρέχεται επίσης ένας πάροχος VM VSS για να επιτρέπει να παίρνονται τα στιγμιότυπα VM.
Η διαχείριση γίνεται κυρίως μέσω του συμπληρωματικού προγράμματος MMC 3.0. ωστόσο, υπάρχουν επίσης scriptable διεπαφές εκτός από το WMI. Με την απελευθέρωση των εργαλείων διαχείρισης απομακρυσμένου διακομιστή (RSAT) για το Windows Vista SP1, μπορούμε να εγκαταστήσουμε το συμπληρωματικό πρόγραμμα Hyper-V MMC σε ένα Vista box, το οποίο είναι διαθέσιμο για λήψη από τη Microsoft. Για να ενεργοποιήσουμε τη διαχείριση από τα Windows Vista, θα πρέπει να βεβαιωθούμε ότι οι

εξαιρέσεις ομάδας τείχους προστασίας Hyper-V και Hyper-V Clients είναι ενεργοποιημένες, οποίες είναι ενεργοποιημένες από προεπιλογή. Επιπλέον, στο μηχάνημα Vista, πρέπει να ενεργοποιήσουμε μια εξαίρεση DCOM στο τείχος προστασίας (πόρτα 135), που χρησιμοποιείται για το Hyper-V για την αποστολή πληροφοριών πίσω στο Hyper-V snapin. Η προσθήκη του κανόνα τείχους προστασίας σε ένα πρόγραμμα-πελάτη Vista διόρθωσε το πρόβλημα "Δεν είναι δυνατή η σύνδεση σε RPC ». Η εντολή για την επίλυση του προβλήματος φαίνεται παρακάτω:

netsh firewall add portopening protocol = tcp port = 135
name = DCOM_TCP135

Ένα καινούριο χαρακτηριστικό του Hyper-V είναι η πρόσβαση στο δίσκο που μεταβάλλεται, η οποία αλλάζει την εκτέλεση των λειτουργιών δίσκου. (Αυτός ήταν ένας περιοριστικός παράγοντας στη χρήση εικονικοποίησης.) Συνήθως στην εικονικοποίηση, οι σκληροί δίσκοι παρέχονται μέσω αρχείων VHD στο σύστημα αρχείων του κεντρικού συστήματος, τα οποία εξυπηρετούνται μέσω εικονικού χώρου αποθήκευσης στη στοίβα. Η πρόσβαση στο δίσκο διέλευσης επιτρέπει την παρουσίαση ενός ολόκληρου φυσικού δίσκου σε ένα παιδικό διαμέρισμα ως εικονική μονάδα δίσκου. Αυτό επιτρέπει την πρόσβαση σε όλους τους δίσκους απευθείας από τη στοίβα αποθήκευσης του παιδικού διαμερίσματος στον φυσικό δίσκο, παρακάμπτοντας την εικονική στοίβα αποθήκευσης και βελτιώνοντας την απόδοση.

Τα λειτουργικά συστήματα που υποστηρίζονται στα θυγατρικά διαμερίσματα χωρίζονται σε δύο τύποι: enlightened και nonenlightened. Τα παιδικά χωρίσματα επικοινωνούν με τον hypervisor με τεκμηριωμένες κλήσεις γνωστές ως υπερκλήσεις. Ένα λειτουργικό διαμέρισμα μπορεί να μάθει εάν εκτελείται σε έναν hypervisor (και ακόμη και την έκδοσή του) μέσω ενός hypercall εάν το λειτουργικό σύστημα γνωρίζει τον hypervisor (επίσης γνωστό ως enlightened guest OS). Λειτουργικά συστήματα όπως Windows Server 2008 και Windows Vista (με στοιχεία ενσωμάτωσης Hyper-V RC0) είναι πλήρως enlightened, ενώ Ο Windows Server 2003 είναι μερικώς enlightened. Κατανοεί δηλαδή μόνο εικονικοποίηση προγράμματος οδήγησης και όχι τον hypervisor σε επίπεδο πυρήνα. Ένα enlightened παιδικό διαμέρισμα κατανοεί ότι έχει έναν αριθμό VSC που χρησιμοποιούνται για πρόσβαση στο υλικό αποθήκευσης, δικτύου, βίντεο και τύπου εισαγωγής. Στη συνέχεια, το VSC επικοινωνεί με το VSP στο γονικό διαμέρισμα μέσω του VMBus, το οποίο εκτελεί την πραγματική άμεση φυσική επικοινωνία υλικού. Αυτά τα ζεύγη VSC-VSP είναι κοινά στον κόσμο των Windows, και οι κατασκευαστές υλικού θα τα παρέχουν στο μέλλον για πρόσθετη υποστήριξη υλικού. Εάν ένα λειτουργικό σύστημα δεν γνωρίζει ότι εκτελείται σε έναν hypervisor, δεν είναι enlightened και δεν έχει τη δυνατότητα να χρησιμοποιεί τα κανονικά ζεύγη VSC-VSP. Θα πρέπει να δει τις κανονικές προσομοιωμένες συσκευές μέσω ενός επιπέδου προσομοίωσης που είναι συνηθισμένο με λύσεις, όπως Virtual Server και Virtual H/Y. Αυτό προκύπτει σε ένα λειτουργικό σύστημα guest χαμηλότερης απόδοσης εξαιτίας της εικονικοποιημένης πλατφόρμα υλικού. Το guest λειτουργικό σύστημα επιχειρεί κανονική I/O πρόσβαση στο υλικό, το οποίο στη συνέχεια παγιδεύεται από τον hypervisor και περνά στη συνέχεια στο γονικό διαμέρισμα για χειρισμό. Μέσω αυτής της προσομοίωσης τα λειτουργικά συστήματα που δεν είναι enlightened υποστηρίζονται και να μπορούν να τρέχουν κάτω από το Hyper-V, αν και αυτή η απόδοση είναι πολύ λιγότερη από ό, τι με το μοντέλο VSC-VSP.

6.8.3. Λειτουργικά συστήματα HYPER-V και Guest Host

Η ακόλουθη λίστα περιλαμβάνει όλα τα τρέχοντα υποστηριζόμενα λειτουργικά συστήματα κεντρικού υπολογιστή 64-bit για Hyper-V:

- ❖ Windows Server 2008 Standard Edition
- ❖ Windows Server 2008 Enterprise Edition
- ❖ Windows Server 2008 Datacenter Edition
- ❖ Microsoft Hyper-V Server 2008

Υποστήριξη λειτουργικού συστήματος επισκεπτών Guest

Ο ακόλουθος πίνακας περιλαμβάνει όλα τα υποστηριζόμενα λειτουργικά συστήματα επισκεπτών x86 που μπορούν να χρησιμοποιηθούν με εκδόσεις Windows Server 2008 Standard, Enterprise και Datacenter, καθώς και Microsoft Διακομιστή Hyper-V 2008:

A/A	Λειτουργικό σύστημα	Εκδόσεις
1	Windows 2000 (support for one virtual processor)	• Windows 2000 Server with SP4 • Windows 2000 Advanced Server with SP4
2	Windows Server 2003 x86 (support for one or two virtual processors)	• Windows Server Web Edition with SP2 • Windows Server Standard Edition with SP2 • Windows Server Enterprise Edition with SP2 • Windows Server Datacenter Edition with SP2
3	Windows Server 2003 R2 x86 (support for one or two virtual processors)	• Windows Server Web Edition with SP2 • Windows Server Standard Edition with SP2 • Windows Server Enterprise Edition with SP2 • Windows Server Datacenter Edition with SP2
4	Windows Server 2003 x64 (support for one or two virtual processors)	• Windows Server Standard Edition with SP2 • Windows Server Enterprise Edition with SP2 • Windows Server Datacenter Edition with SP2
5	Windows Server 2003 R2 x64 (support for one or two virtual processors)	• Windows Server Standard Edition with SP2 • Windows Server Enterprise Edition with SP2 • Windows Server Datacenter Edition with SP2

6	Windows Server 2008 x86 (support for one, two, or four virtual processors)	• Windows Server 2008 Standard Edition • Windows Server 2008 Enterprise Edition • Windows Server 2008 Datacenter Edition • Windows Web Server 2008 Edition • Windows Server 2008 Standard Edition without Hyper-V • Windows Server 2008 Enterprise Edition without Hyper-V • Windows Server 2008 Datacenter Edition without Hyper-V
7	Windows Server 2008 x64 (support for one, two, or four virtual processors)	• Windows Server 2008 Standard Edition • Windows Server 2008 Enterprise Edition • Windows Server 2008 Datacenter Edition • Windows Web Server 2008 Edition • Windows Server 2008 Standard Edition without Hyper-V • Windows Server 2008 Enterprise Edition without Hyper-V • Windows Server 2008 Datacenter Edition without Hyper-V
8	Windows HPC Server 2008 (support for one, two or four virtual processors)	• Windows HPC Server 2008
9	Suse Linux Enterprise Server 10 x86 (support for one virtual processor)	• SUSE Linux Enterprise Server 10 with SP1 • SUSE Linux Enterprise Server 10 with SP2
10	Suse Linux Enterprise Server 10 x64 (support for one virtual processor)	• SUSE Linux Enterprise Server 10 with SP1 • SUSE Linux Enterprise Server 10 with SP2
11	Windows XP Professional x86	• Windows XP Professional with SP2 (support for one virtual processor) • Windows XP Professional with SP3 (support for one or two virtual processors)
12	Windows XP Professional x64	• Windows XP Professional with SP2 (support for one or two virtual processors)
13	Windows Vista x86 (support for one or two virtual processors)	• Windows Vista Business Edition with SP1 • Windows Vista Enterprise Edition with SP1 • Windows Vista Ultimate Edition with SP1
14	Windows Vista x64 (support for one or two virtual processors)	• Windows Vista Business Edition with SP1 • Windows Vista Enterprise Edition with SP1

		• Windows Vista Ultimate Edition with SP1

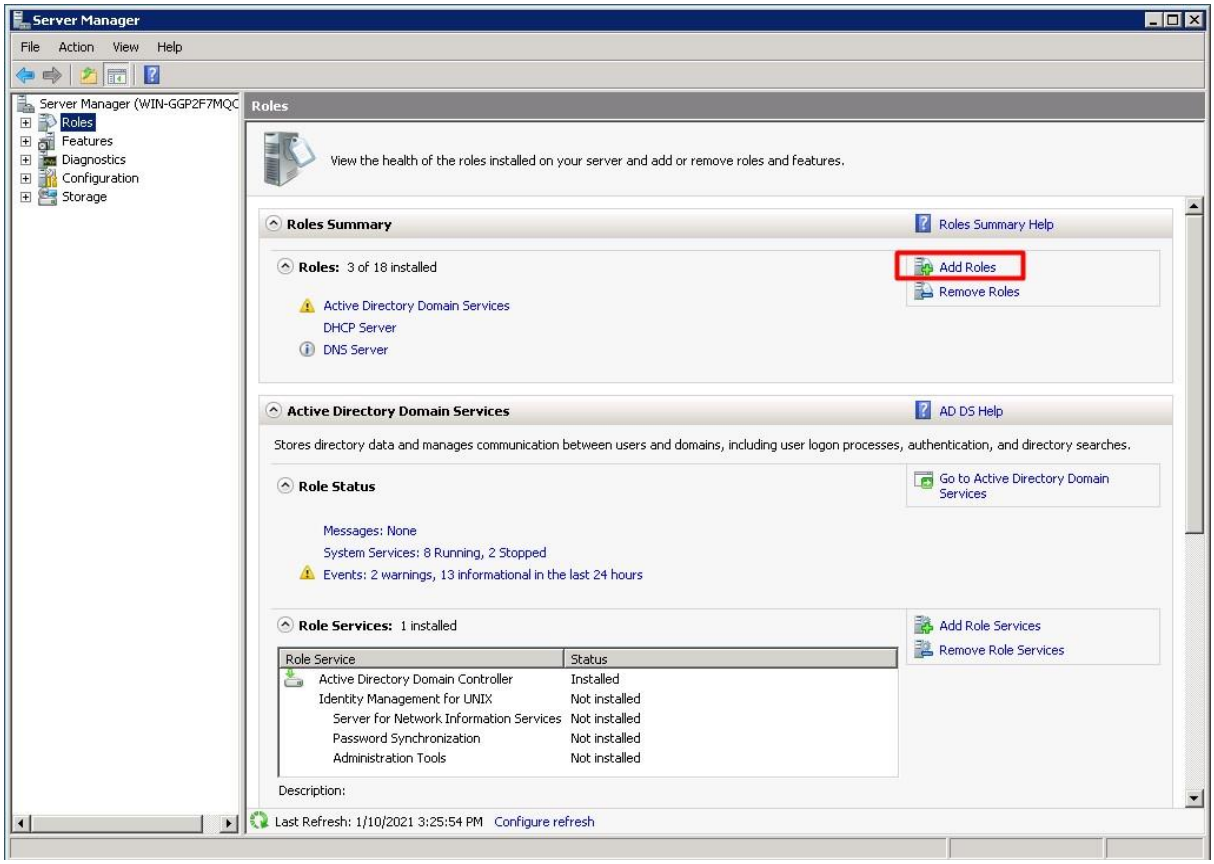
Πίνακας 6.12

6.8.4. Εγκατάσταση υπηρεσίας HYPER-V

Θα πρέπει πριν ξεκινήσουμε την εγκατάσταση της υπηρεσίας HYPER-V στον server μας να έχουμε βεβαιωθεί ότι έχουμε ενεργοποιήσει το "Virtualization Technology" και το "Execute Disable" στις ρυθμίσεις του BIOS του διακομιστή. Διαφορετικά, ακόμη και μετά την εγκατάσταση του ρόλου Hyper-V, δεν θα μπορούμε να ξεκινήσουμε να τον χρησιμοποιούμε και ενδέχεται να εμφανιστεί ένα από τα ακόλουθα σφάλματα:

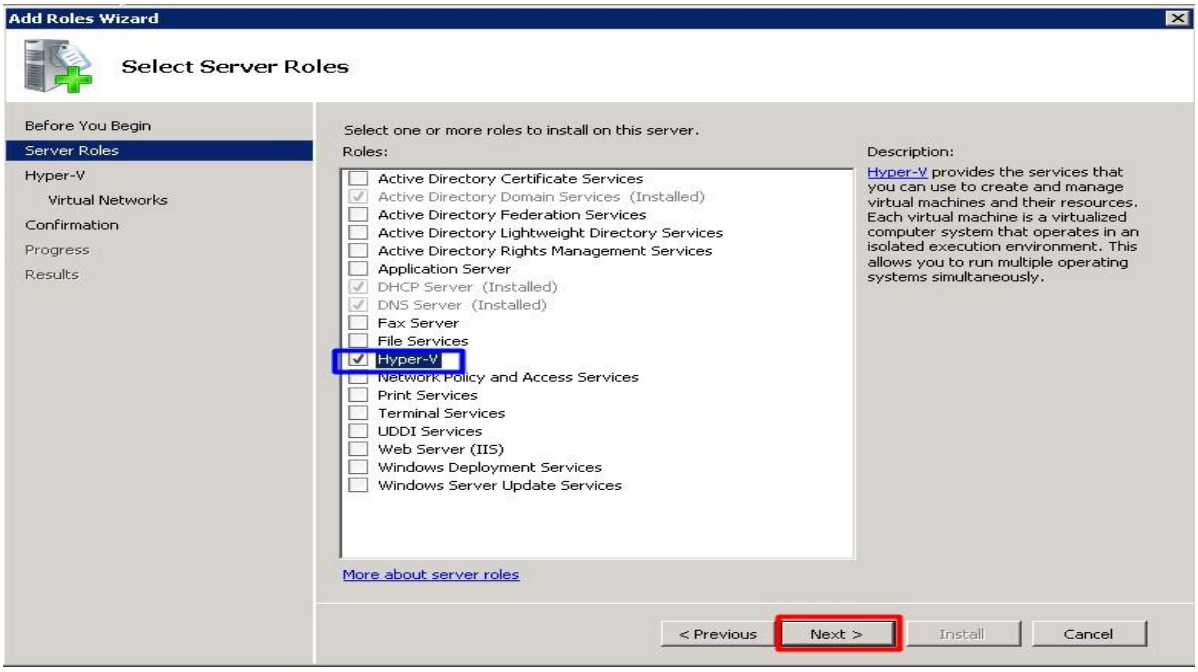
- Η εκκίνηση Hyper-V απέτυχε. Το VMX δεν υπάρχει ή δεν είναι ενεργοποιημένο στο BIOS.
- Η εκκίνηση Hyper-V απέτυχε. Τουλάχιστον ένας από τους επεξεργαστές στο σύστημα δεν φαίνεται να παρέχει πλατφόρμα εικονικοποίησης που υποστηρίζεται από το Hyper-V.

Προκειμένου να ξεκινήσει η εγκατάσταση της υπηρεσίας HYPER-V εκτελούμε, όπως και για όλες τις άλλες υπηρεσίες την Διαχείριση διακομιστή μέσα από Έναρξη, Όλα τα προγράμματα, Εργαλεία διαχείρισης, Διαχείριση διακομιστή. Στην εικόνα 6.103 φαίνεται η Διαχείριση διακομιστή.



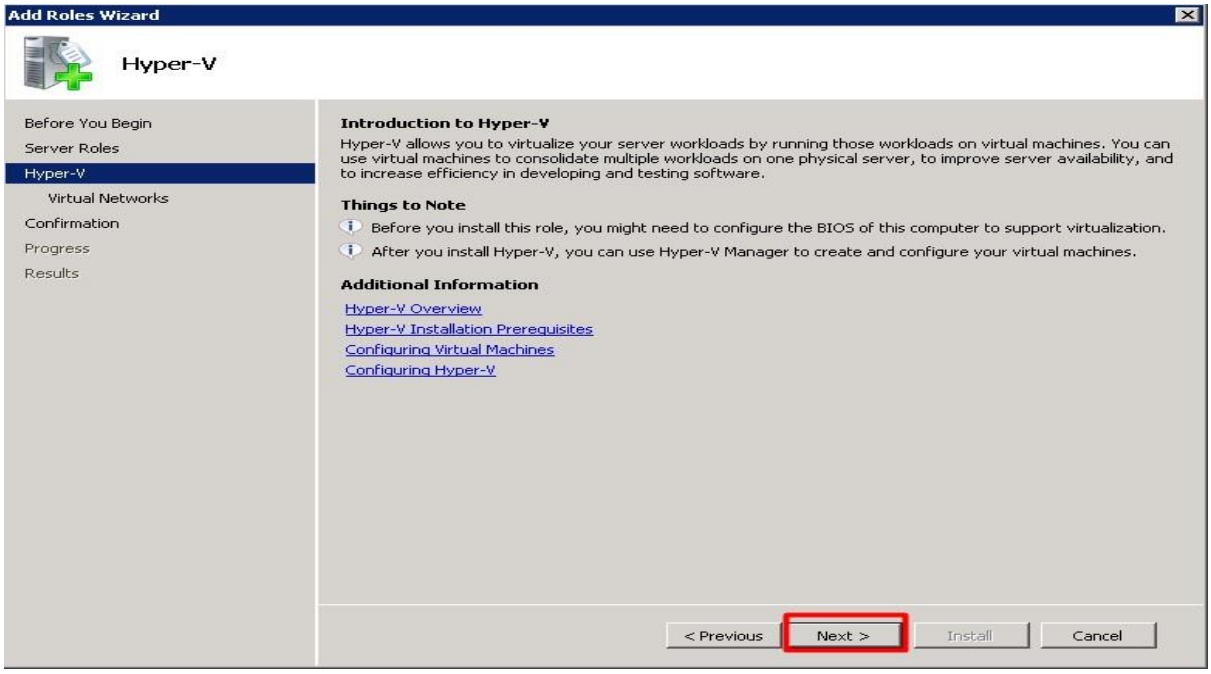
Εικόνα 6.103

Στη συνέχεια επιλέγουμε την υπηρεσία Hyper-V, όπως φαίνεται στην εικόνα 6.104, και κάνουμε κλικ στην επιλογή Επόμενο (Next).



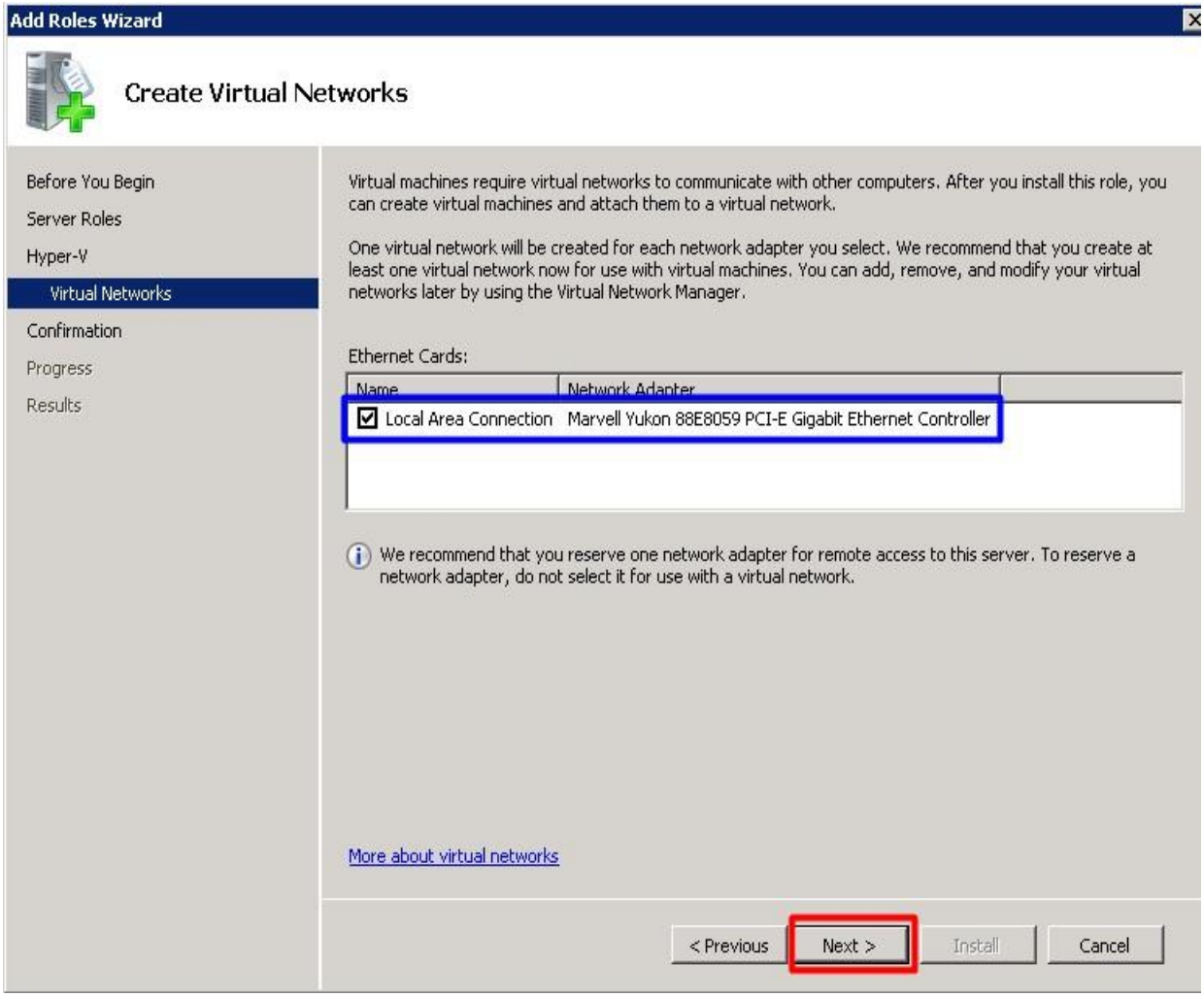
Εικόνα 6.104

Στη συνέχεια μας εμφανίζεται μια σύντομη εισαγωγή στο Hyper-V με τις βασικές απαιτήσεις προεγκατάστασης και αντίστοιχες πληροφορίες για την υπηρεσία. Αφού διαβάσουμε τις πληροφορίες, κάνουμε κλικ στο Επόμενο (Next), όπως φαίνεται στην εικόνα 6.105.



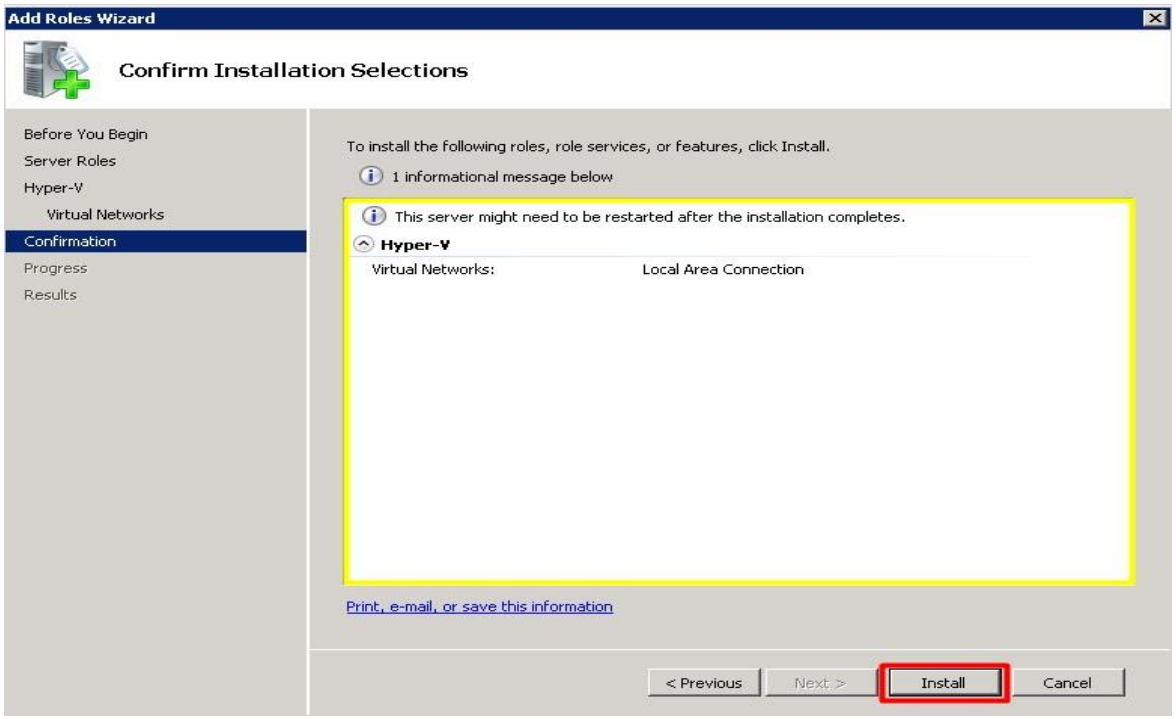
Εικόνα 6.105

Στο επόμενο παράθυρο διαλόγου που μας εμφανίζεται, Δημιουργία εικονικών δικτύων, επιλέγουμε τον προσαρμογέα (στην περίπτωση που έχουμε μόνο ένα) ή τους προσαρμογείς LAN που θέλουμε να έχουμε κοινή χρήση με τα guest μηχανήματα που θα εγκαταστήσουμε αργότερα. Κάνουμε κλικ στο Επόμενο για να συνεχίσουμε.



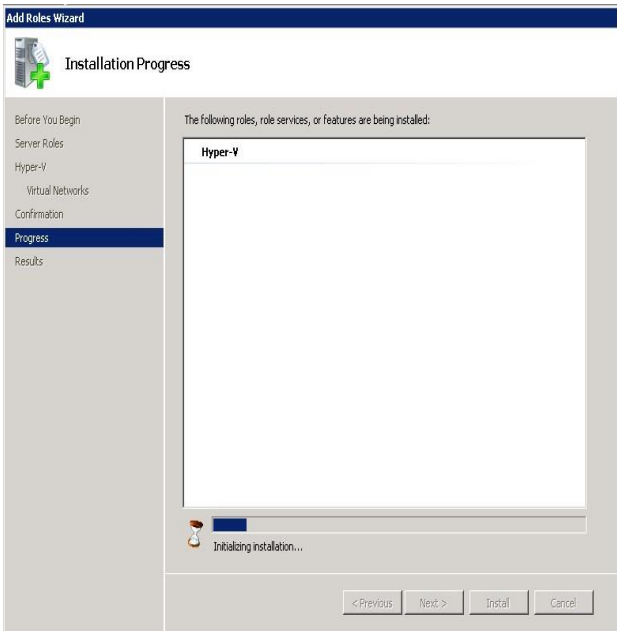
Εικόνα 6.106

Στη συνέχεια στο παράθυρο διαλόγου που μας εμφανίζεται, όπως φαίνεται στην εικόνα 6.107, γίνεται μια προεπισκόπηση των ρυθμίσεων που έχουμε επιλέξει για την υπηρεσία Hyper-V προκειμένου να επιβεβαιώσουμε ότι όλα είναι όπως τα επιθυμούμε. Αφού τα έχουμε ελέγξει κάνουμε κλικ εγκατάσταση για να εγκατασταθεί ο ρόλος μας.

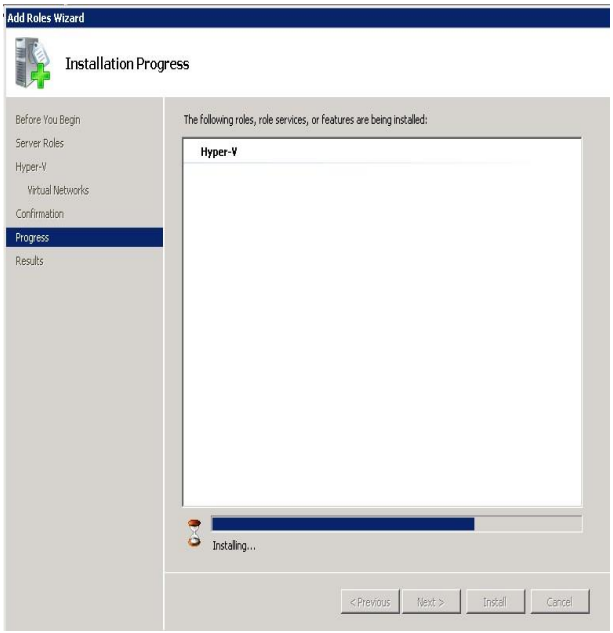


Εικόνα 6.107

Στις εικόνες 6.108 και 6.109 φαίνεται η πρόοδος εγκατάστασης.

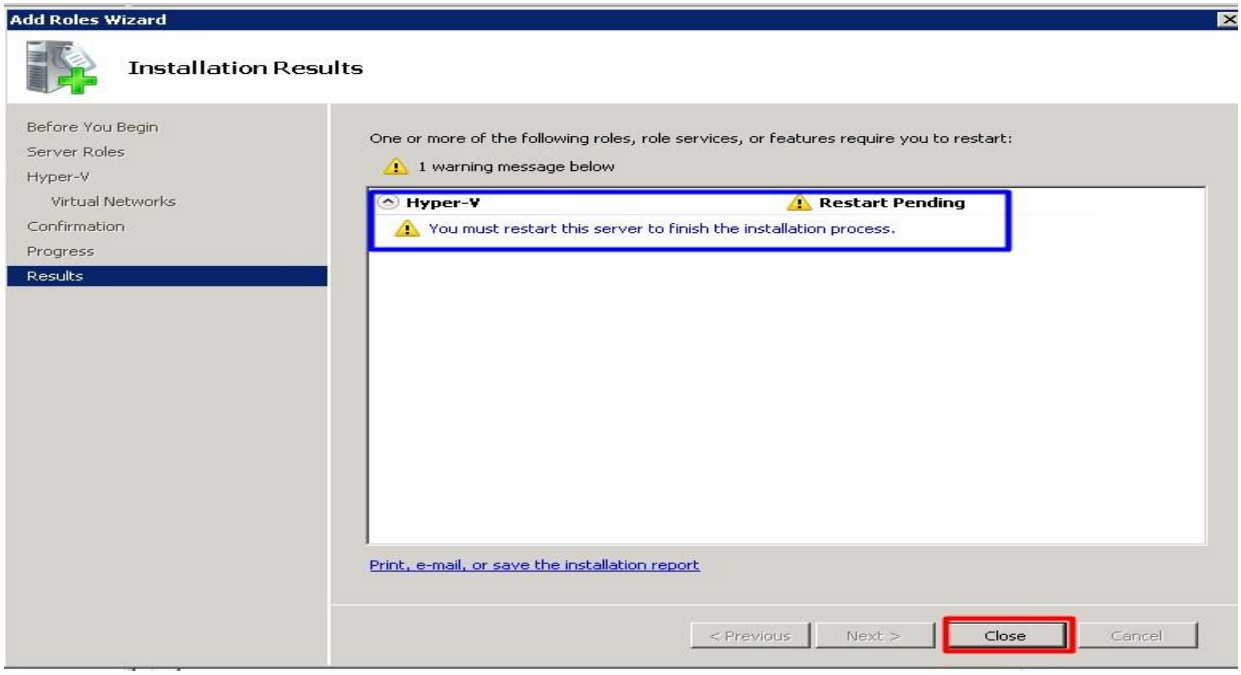


Εικόνα 6.108

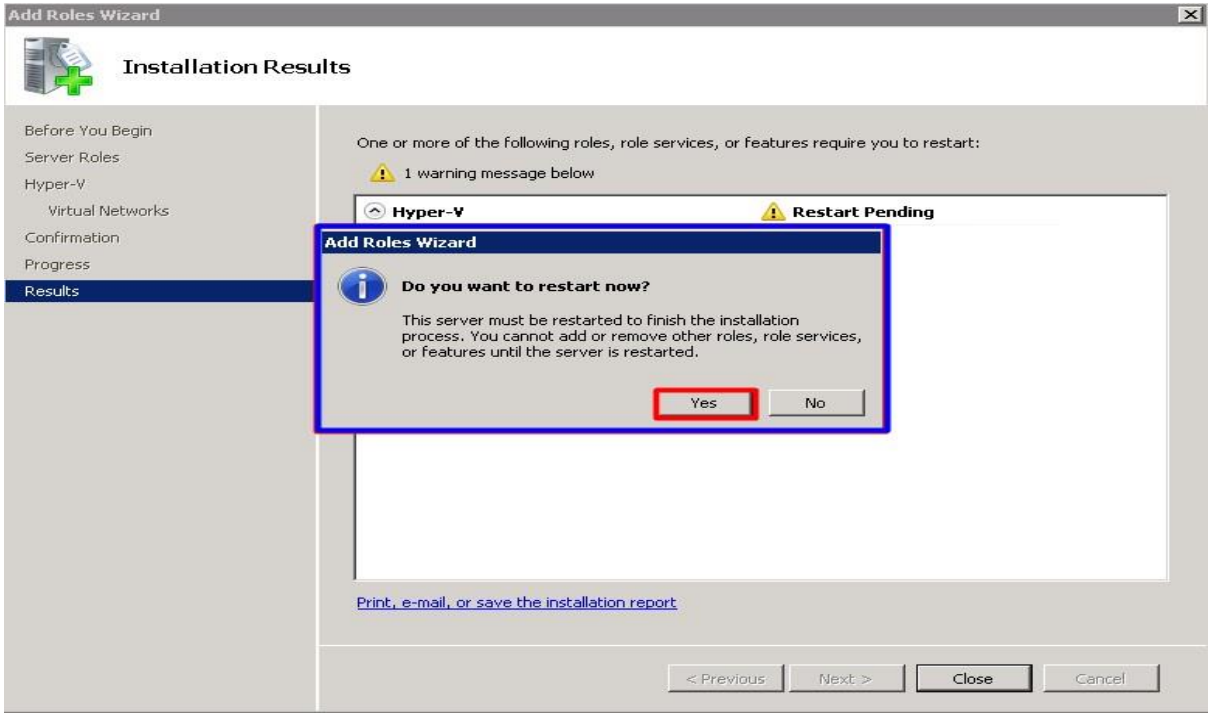


Εικόνα 6.109

Στην εικόνα 6.110 φαίνεται η επιτυχής εγκατάσταση της υπηρεσίας Hyper-V με την προβολή του ανάλογου μηνύματος. Προκειμένου να εφαρμοστούν οι ρυθμίσεις μας θα πρέπει να κάνουμε επανεκκίνηση στον διακομιστή μας όπως φαίνεται στην εικόνα 6.111.

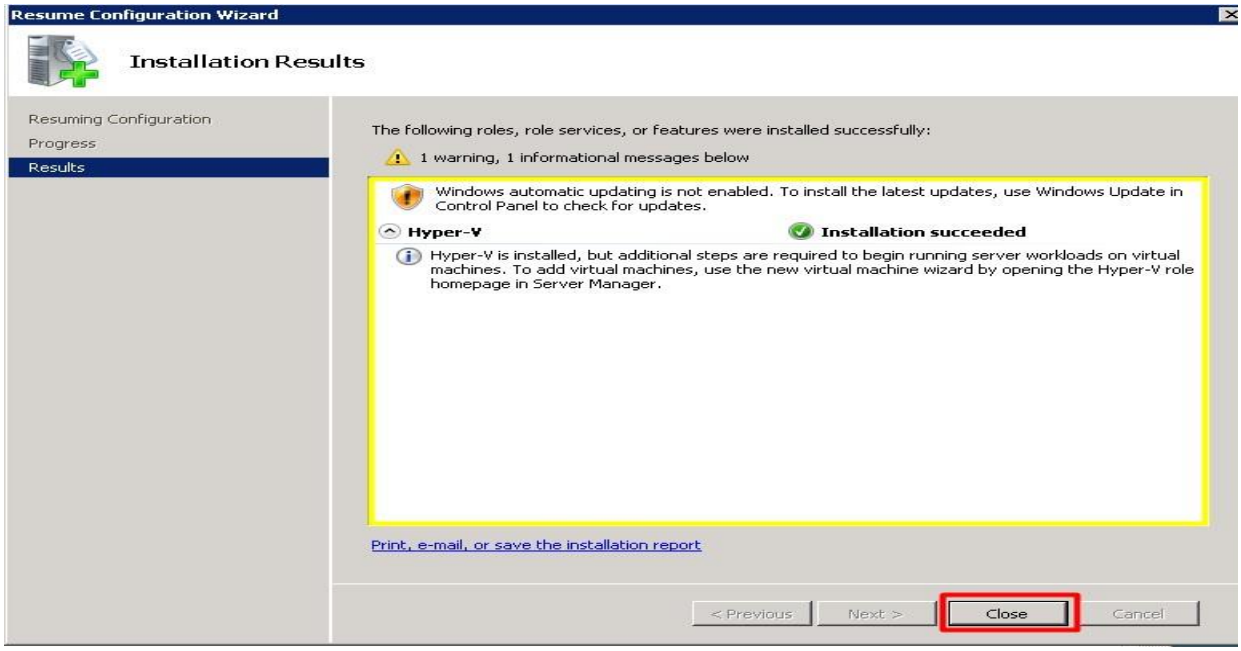


Εικόνα 6.110



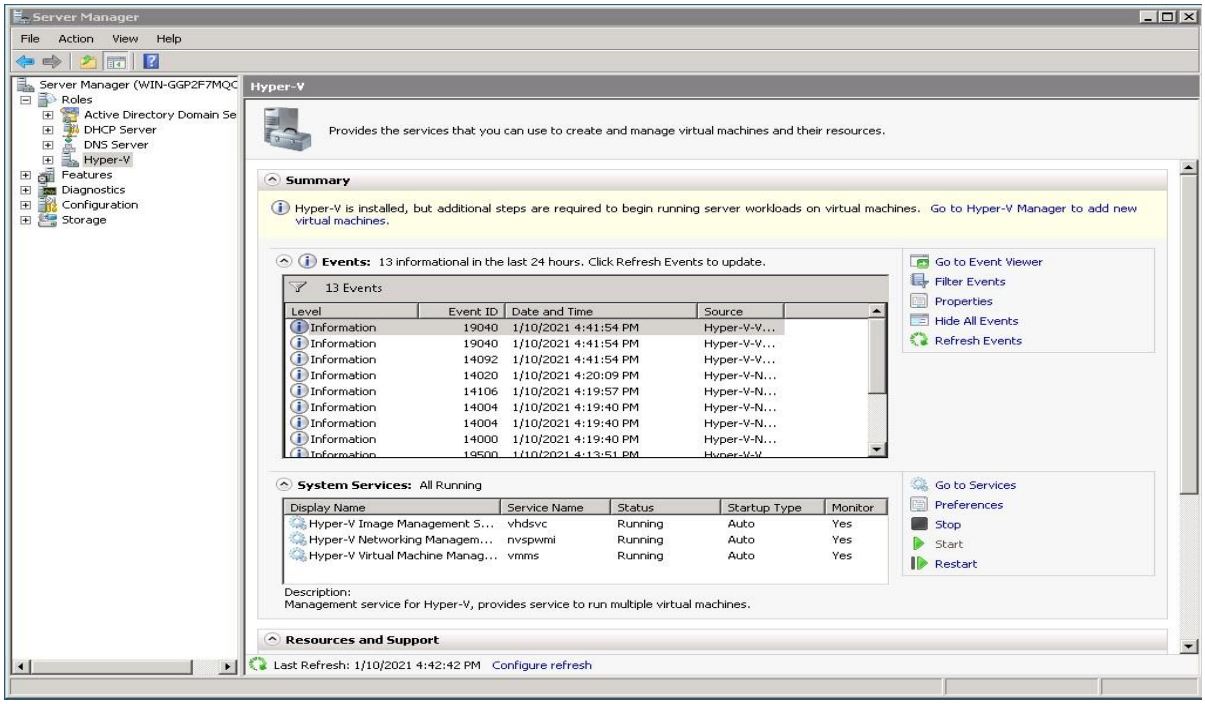
Εικόνα 6.111

Μετά και την επιτυχή επανεκκίνηση του συστήματός μας ο οδηγός προσθήκης ρόλων συνεχίζει την εγκατάσταση ρυθμίσεων έως ότου ολοκληρωθεί η εγκατάσταση με την προβολή του ανάλογου μηνύματος όπως φαίνεται στην εικόνα 6.112.



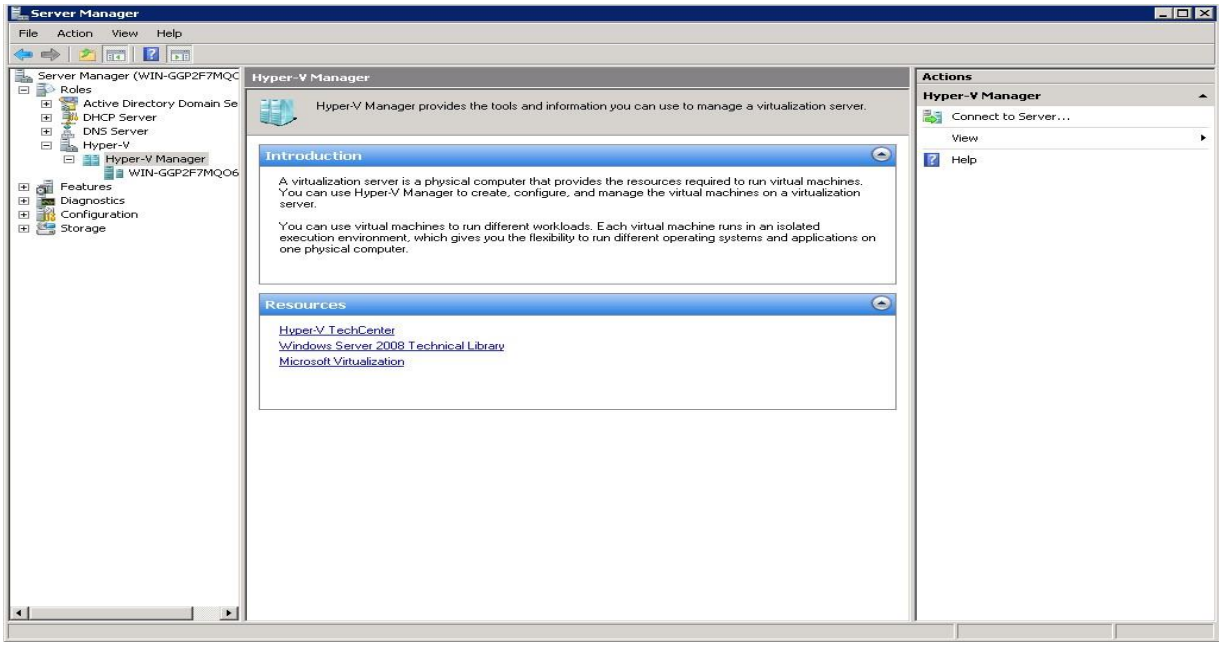
Εικόνα 6.112

Στην εικόνα 6.113 στη Διαχείριση του διακομιστή μας βλέπουμε ότι εγκαταστάθηκε η υπηρεσία Hyper-V.



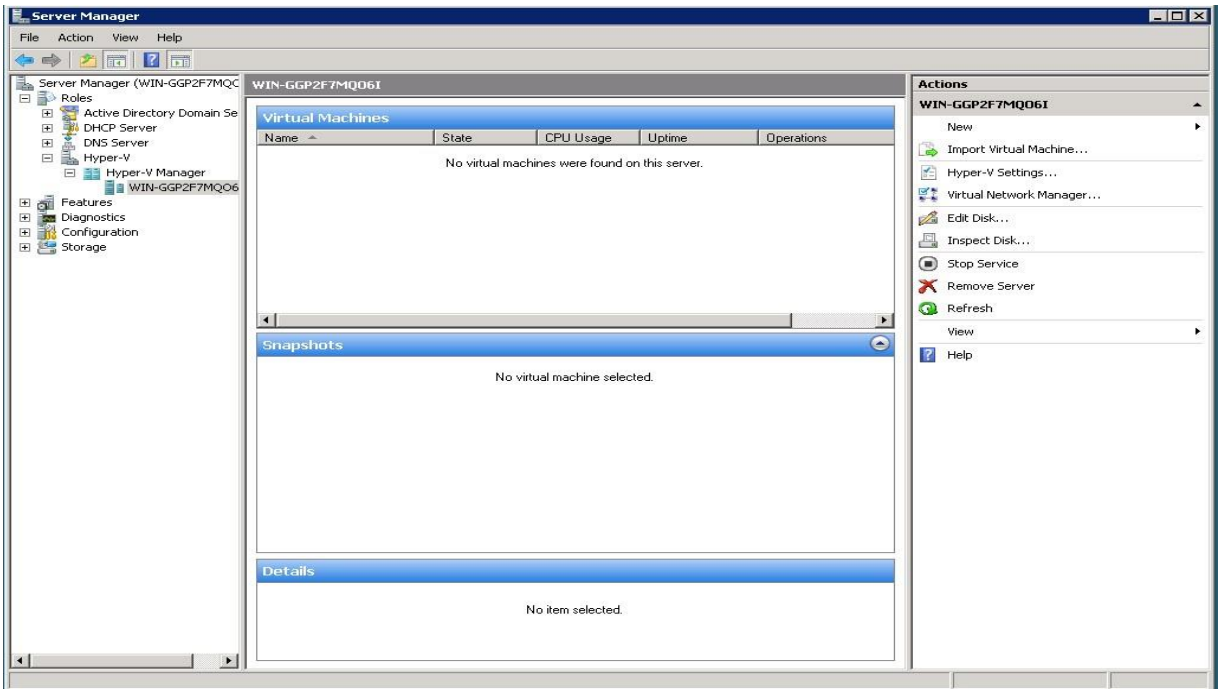
Εικόνα 6.113

Μέσα από την επιλογή Hyper-V Manager, όπως φαίνεται στην εικόνα 6.114, μπορούμε να συνδεθούμε για να δούμε τις ρυθμίσεις που έχουμε κάνει στην server μας.



Εικόνα 6.114

Στο παράθυρο διαλόγου που μας εμφανίζεται μπορούμε να εισάγουμε ένα Virtual Machine, να διαγράψουμε ένα VM, τροποποιήσουμε τις ρυθμίσεις στο Hyper-V και διάφορες άλλες επιλογές.



Εικόνα 6.115

6.9. File Server

Τα Windows Server 2008 έχουν βελτιώσει το ρόλο του συστήματος λειτουργίας του διακομιστή αρχείων με μερικές νέες δυνατότητες, όπως περιγράφεται παρακάτω:

- *Απομακρυσμένη κοινή χρήση εγγράφων*. Αυτή η δυνατότητα επιτρέπει την πρόσβαση σε αρχεία σε διακομιστές Web μέσω τυπικών κλήσεων συστήματος αρχείων μέσω του νέου πρωτοκόλλου Κατανεμημένης Συγγραφής και Εκδόσεων Ιστού (WebDAV). Αυτό είναι πολύ δημοφιλές για χρήση με κοινή χρήση εγγράφων και συστήματα ελέγχου εγγράφων όπως το SharePoint.
- *Βελτιωμένο κατανεμημένο σύστημα αρχείων*. Αν και η σύνδεση ή η αντιστοίχιση σε σημεία κοινής χρήσης που δημοσιεύονται στην υπηρεσία καταλόγου Active Directory είναι χρήσιμη, το DFS παρέχει τη μεγαλύτερη χρησιμότητα και αξία για μια εταιρεία με εκτεταμένη ή ευρέως διανεμημένη προβολή αρχείων.
- *Πίνακας διαμερισμάτων GUID*. Η υποστήριξη 64-bit στα Windows Server 2008 Enterprise Edition και το Datacenter Edition περιλαμβάνει το τεχνολογία διαμέρισης δίσκων που παρέχει μια εναλλακτική λύση στο Master Boot Record (MBR) που βρίσκεται σε όλα τα λειτουργικά συστήματα 32-bit. Αν και η νέα τεχνολογία είναι σε μεγάλο βαθμό κρυμμένη από τον χρήστη και ο διαχειριστής, βελτιώνει σημαντικά την αξιοπιστία και την απόδοση πάνω από αυτό του παλαιού MBR.

Τα περισσότερα δεδομένα δημιουργούνται και αποθηκεύονται σε συστήματα υπολογιστών, χρησιμοποιώντας το αρχείο και μεταφορές φακέλων που κληρονομήθηκαν από τον τρισδιάστατο κόσμο μας. Από την εμφάνιση δικτύων τοπικών και ευρέων περιοχών, και ιδίως του Διαδικτύου, τα αρχεία και οι φάκελοί μας είναι προσβάσιμοι σε οποιονδήποτε διαθέτει υπολογιστή και σύνδεση δικτύου, εκτός εάν τα ασφαλιστούν τα δεδομένα μας. Θα πρέπει να ασφαλίσουμε αυτά τα δεδομένα που περιέχονται σε αρχεία και φακέλους, ενώ ταυτόχρονα θα πρέπει να παρέχουμε ελεγχόμενη πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες. Το σύστημα αρχείων NT (NTFS) επιτρέπει να το κάνουμε αυτό στα ακόλουθα τρία επίπεδα πρόσβασης ασφαλείας:

- ✓ Κοινή χρήση
- ✓ Δικαιώματα φακέλων και δικαιώματα αρχείων (ονομάζονται δικαιώματα NTFS)
- ✓ Κρυπτογράφηση

Κοινή χρήση και προστασία των δεδομένων μας

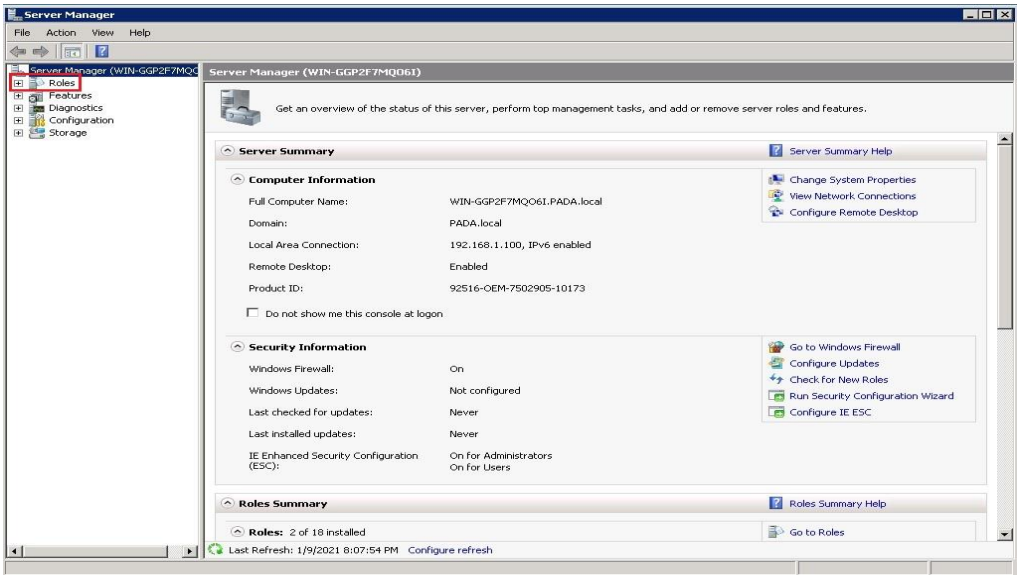
Τα Windows Server 2008, όπως συμβαίνει και σε όλες τις σύγχρονες λειτουργίες συστημάτων με γραφική διαχείριση ή διαχείριση γραμμής εντολών, μας επιτρέπει να διαχειριστούμε τα αρχεία και τους φακέλους μας με τον ίδιο τρόπο που διαχειριζόμαστε τα συστήματα κατάθεσης σε έντυπη μορφή: σε φακέλους και ντουλάπια αρχειοθέτησης.
Μία εταιρεία δεν κρύβει τα δεδομένα μακριά από το προσωπικό της που εργάζεται, επειδή είναι κοινόχρηστος πόρος και θέλει να τα γνωρίζει επειδή μπορεί να χρειαστούν τα δεδομένα αυτά για να κάνουν τη δουλειά τους.
Η ενεργοποίηση της κοινής χρήσης φακέλων για τους χρήστες και τις εφαρμογές πραγματοποιείται δημιουργώντας μια κοινή χρήση ή το γλωσσικό σύστημα mainframe, midrange και legacy, ένα sharepoint. Με την κατοχή των αρχείων και των φακέλων στο δικό τους μηχάνημα, αυτόματα έχουν πλήρη πρόσβαση και έλεγχο των φακέλων τους και

του περιεχομένου τους. Οι διαχειριστές κατέχουν όλους τους φακέλους που δημιουργούνται οπουδήποτε στο δίκτυο και μπορούν έτσι να τους μοιραστούν.
Ανάλογα με την κατάταξή των υπαλλήλων σε μια εταιρεία, το τμήμα για το οποίο εργάζονται και το έργο το οποίο κάνουν, μπορούν ή όχι να έχουν άδεια να διαβάσουν ένα αρχείο, να το ελέγξουν, να αλλάξουν το περιεχόμενό του ή να προσθέσουν δεδομένα σε αυτό. Ομοίως, κάποιος ως μέλος μιας ομάδας χρηστών ή με ατομική εξουσία, μπορεί να αποκτήσει πρόσβαση στο κοινόχρηστο NTFS, αλλά ορισμένα αρχεία μπορεί να μην έχει πρόσβαση ούτε καν να τα δει. Άλλοι φάκελοι μπορεί να είναι προσβάσιμοι μόνο για ανάγνωση - ενδέχεται να μην επιτρέπεται να αλλαχθούν, να διαγραφούν, να αντιγραφούν ή να μετακινηθούν.
Τα επίπεδα πρόσβασης που έχουμε στους φακέλους και τα αρχεία ονομάζονται δικαιώματα. Διαχειριστές, μέλη της ομάδας διαχείρισης (Διαχειριστής, Διαχειριστές τομέα ή ομάδες που έχουν ανατεθεί διαχειριστικά δικαιώματα), και οι κάτοχοι αντικειμένων (αυτοί που δημιουργούν τα αρχεία) μπορούν να εκχωρήσουν δικαιώματα και να ελέγχουν την πρόσβαση σε αυτά τα αντικείμενα όπως και μπορούν επίσης να κρυπτογραφήσουν τα αρχεία.

Εγκατάσταση File Server και δημιουργία φακέλου κοινής χρήσης

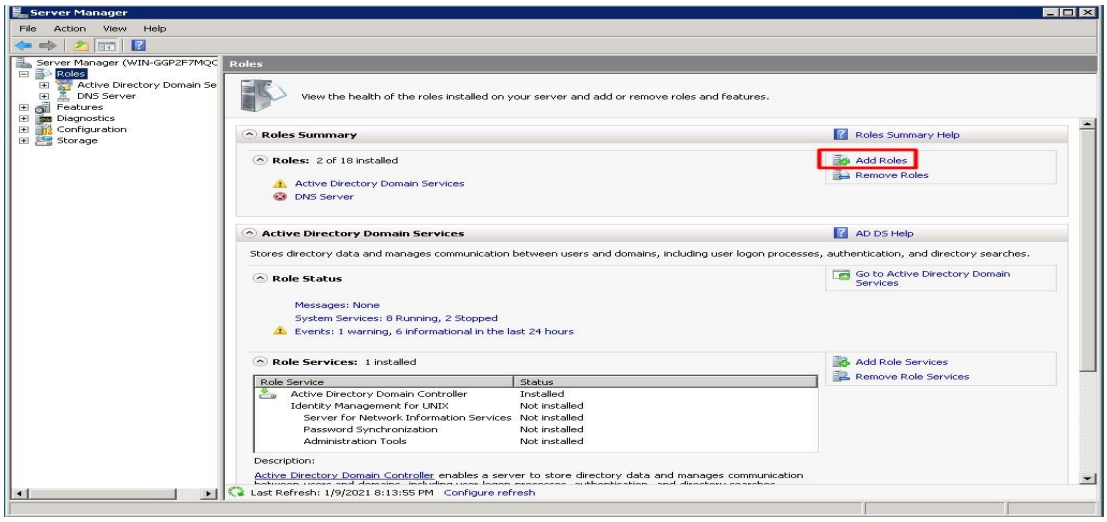
Η εγκατάσταση File Server είναι μια απλή διαδικασία. Στα Windows 2008, η εγκατάσταση έχει βελτιωθεί ακόμη περισσότερο μέσω της χρήσης του οδηγού προσθήκης ρόλων στον διακομιστή. Αυτός ο οδηγός εγκαθιστά την υπηρεσία διακομιστή File Server και καλεί αυτόματα τον οδηγό νέας προσθήκης φακέλου κοινής χρήσης στο group policy που επιθυμούμε. Προκειμένου να δημιουργήσουμε ένα Windows 2008 σύστημα ως διακομιστή File Server, θα πρέπει να ακολουθήσουμε τα παρακάτω βήματα:

17. Επιλέγουμε Έναρξη, Όλα τα προγράμματα, Εργαλεία διαχείρισης, Διαχείριση διακομιστή. Εάν ζητηθεί, κάνουμε κλικ στο Συνεχίστε για να επιβεβαιώσουμε την ενέργεια. Στην εικόνα 6.116 φαίνεται η Διαχείριση διακομιστή.



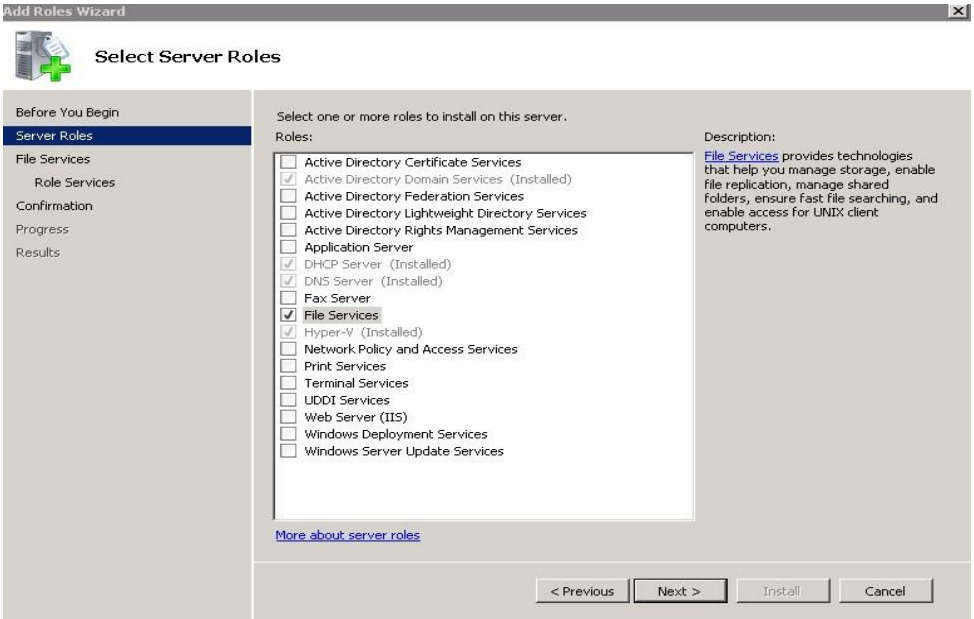
Εικόνα 6.116

18. Στο παράθυρο διαλόγου Διαχείριση διακομιστή, κάνουμε κλικ στην επιλογή Ρόλοι (Roles) στο αριστερό παράθυρο για να εμφανίσουμε συνοπτικές πληροφορίες για τους ρόλους τους οποίους έχουμε ήδη εγκαταστήσει στο δεξιό τμήμα του παραθύρου. Στη συνέχεια, κάνουμε κλικ στην επιλογή Προσθήκη ρόλων (Add Roles) στο δεξιό τμήμα του παραθύρου για να εκκινήσουμε τον Οδηγό Προσθήκη ρόλων. Αφού διαβάσουμε τις πληροφορίες πριν ξεκινήσουμε, κάνουμε κλικ στο Δίπλα στη Συνέχεια. Στην εικόνα 6.117 φαίνεται το πλαίσιο διαλόγου.



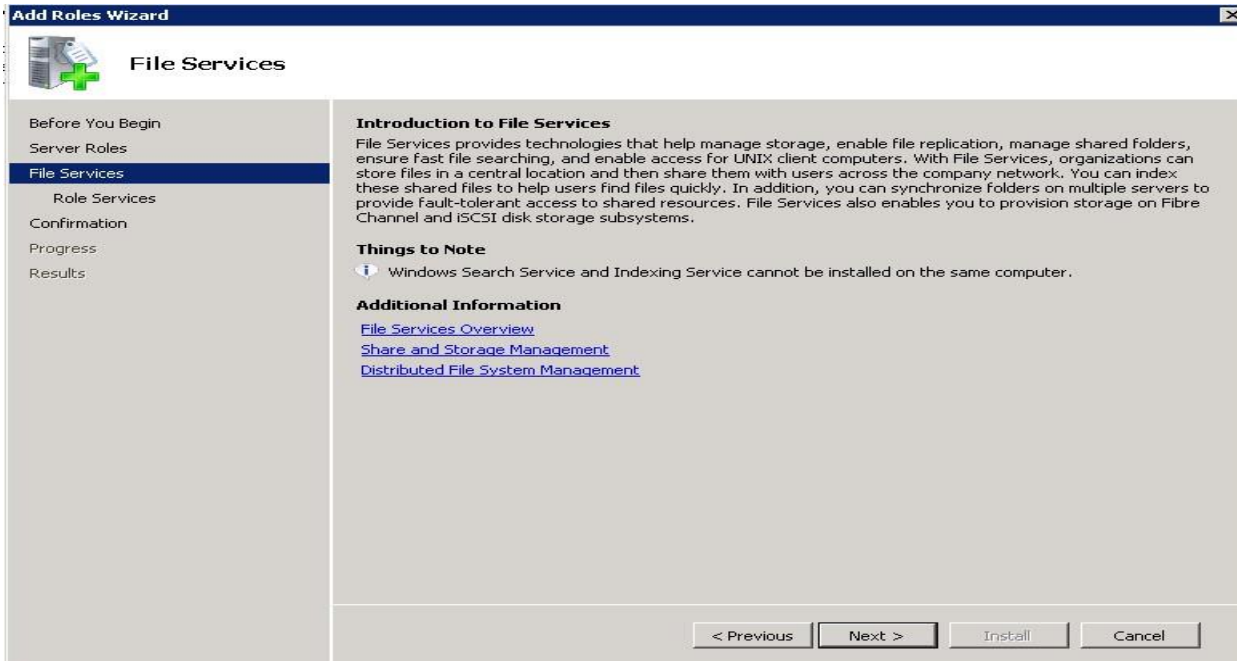
Εικόνα 6.117

19. Στο παράθυρο διαλόγου που μας εμφανίζεται, στην επιλογή ρόλων διακομιστή, επιλέγουμε το πλαίσιο ελέγχου δίπλα στον διακομιστή File Server και στη συνέχεια κάνουμε κλικ στο Επόμενο για να συνεχίσουμε, όπως φαίνεται στην εικόνα 6.118.



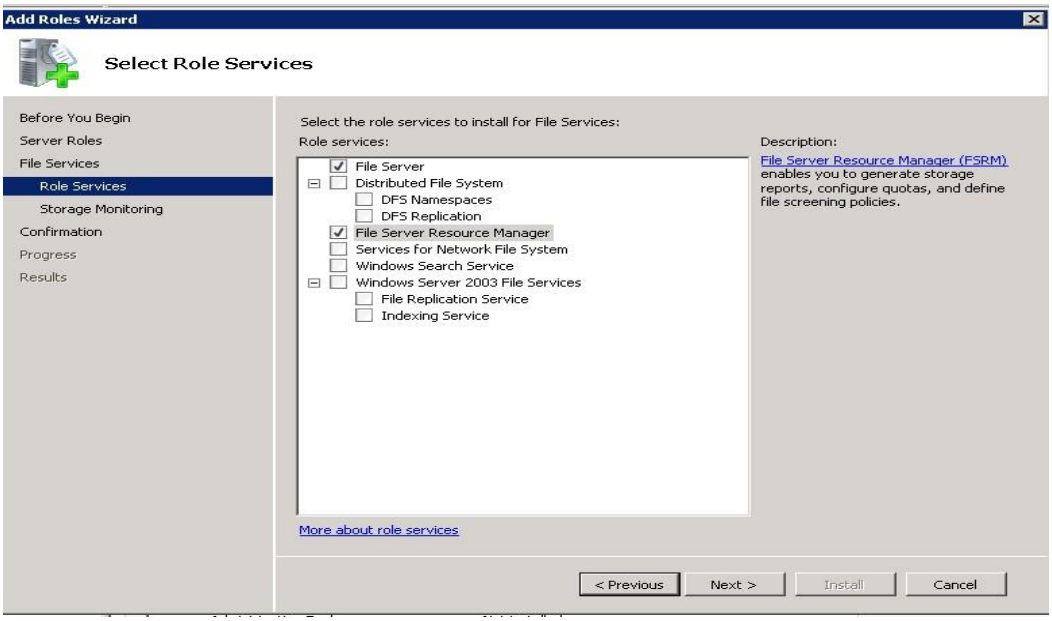
Εικόνα 6.118

20. Στη συνέχεια μας εμφανίζεται μια σύντομη εισαγωγή στο File Server με τις βασικές απαιτήσεις προεγκατάστασης. Αφού διαβάσουμε τις πληροφορίες, κάνουμε κλικ στο Επόμενο (Next), όπως φαίνεται στην εικόνα 6.119.



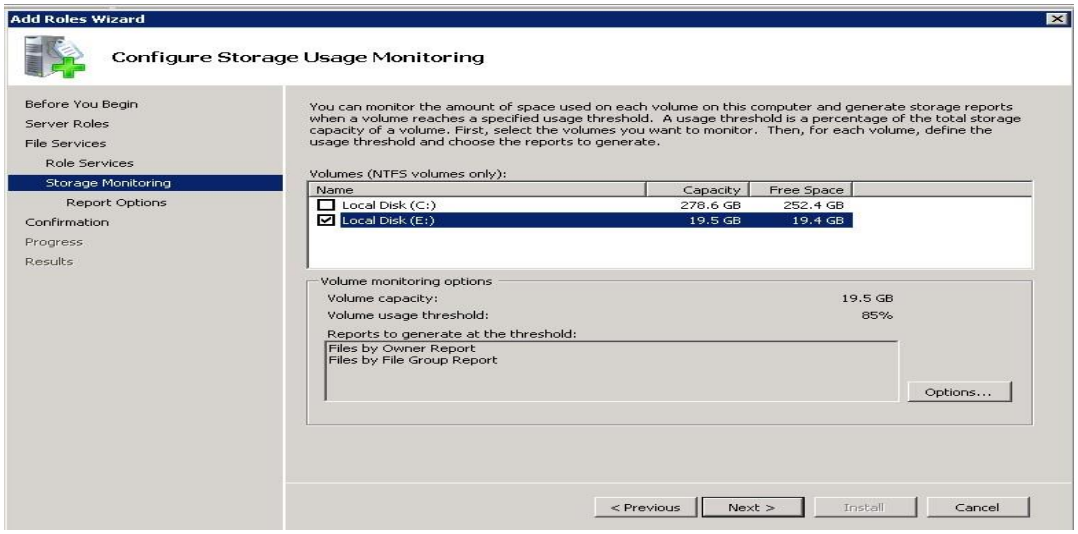
Εικόνα 6.119

21. Επιλέγουμε τις υπηρεσίες File Services που επιθυμούμε και στη συνέχεια κάνουμε κλικ στο Επόμενο (Next), όπως φαίνεται στην εικόνα 6.120. Εδώ επιλέγουμε και την υπηρεσία File Server Resource Manager όπου θα μας βοηθήσει στη συνέχεια με την κοινή χρήση αρχείων εντός του Domain μας.



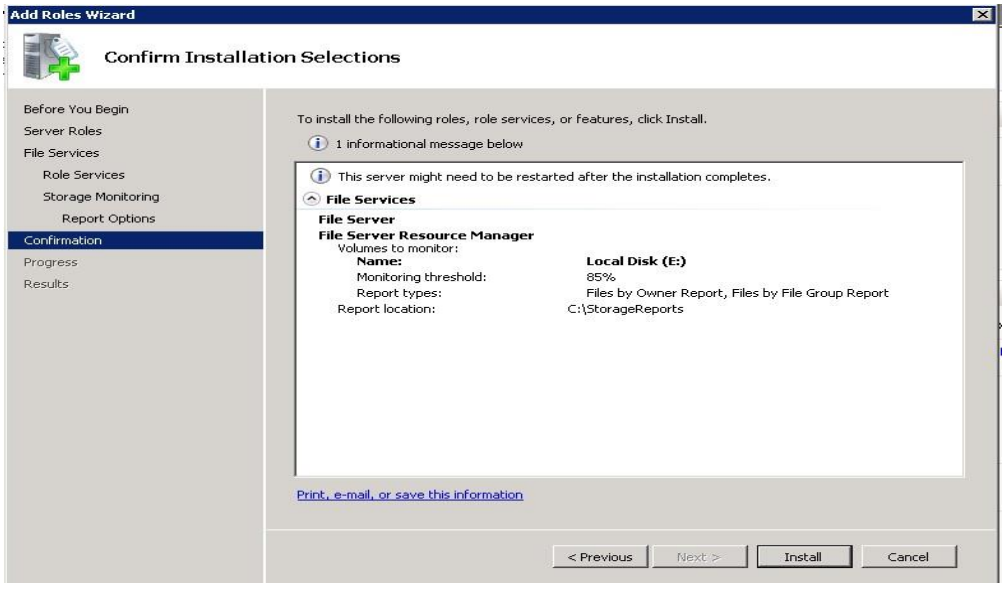
Εικόνα 6.120

22. Σε αυτό το σημείο, ο "Οδηγός προσθήκης ρόλων" εμφανίζει τις ρυθμίσεις διακομιστή σχετικά με τον καθορισμό της μονάδας δίσκου που επιθυμούμε να κάνουμε monitor από την υπηρεσία. Εδώ επιλέγουμε τον τοπικό δίσκο E: που είναι ο δεύτερος τοπικός δίσκος εκτός του συστήματος μας και κάνουμε κλικ στο Επόμενο για να συνεχίσουμε. Οι παραπάνω ενέργειες φαίνονται στην εικόνα 6.121.



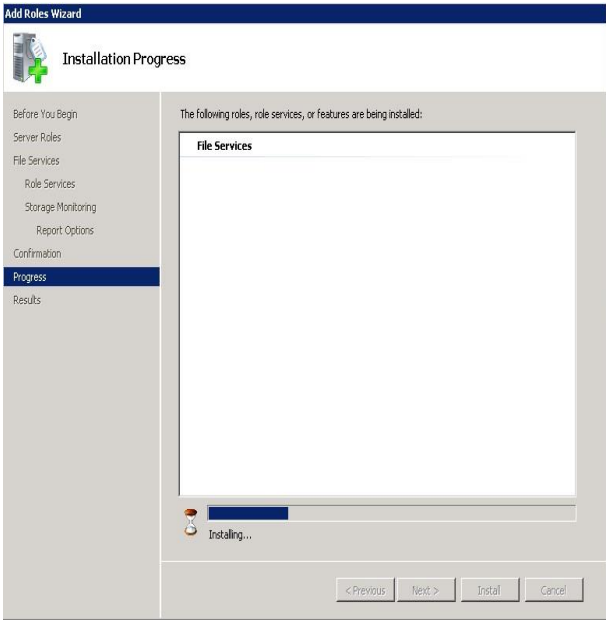
Εικόνα 6.121

23. Στη συνέχεια στο παράθυρο διαλόγου που μας εμφανίζεται, όπως φαίνεται στην εικόνα 6.122, γίνεται μια προεπισκόπηση των ρυθμίσεων που έχουμε επιλέξει για τον διακομιστή File Server προκειμένου να επιβεβαιώσουμε ότι όλα είναι όπως τα επιθυμούμε. Αφού τα έχουμε ελέγξει κάνουμε κλικ εγκατάσταση για να εγκατασταθεί ο ρόλος μας.

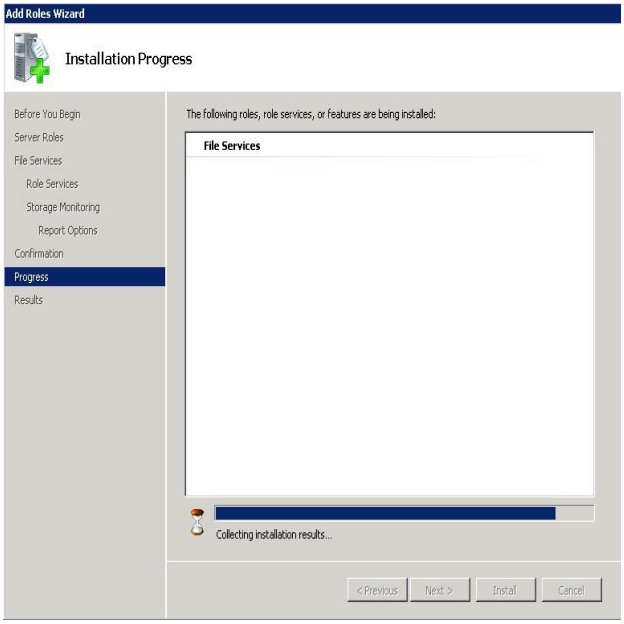


Εικόνα 6.122

24. Στις εικόνες 6.123 και 6.124 φαίνεται η πρόοδος εγκατάστασης.

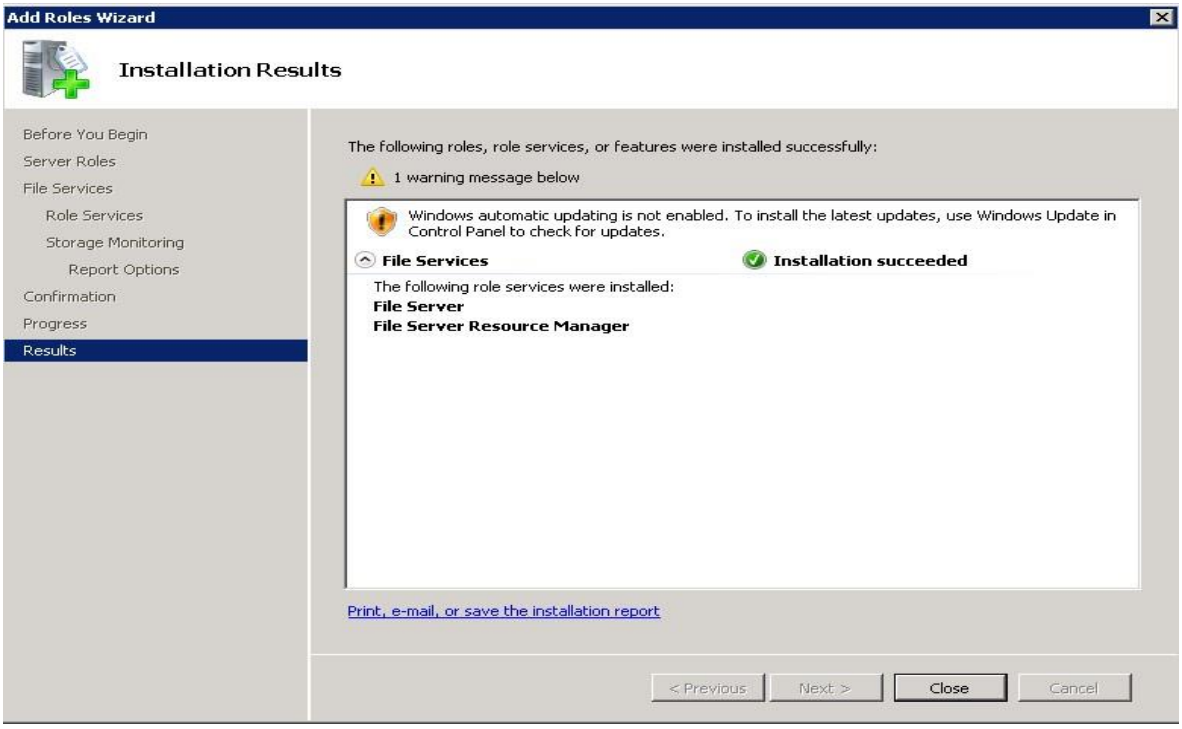


Εικόνα 6.123



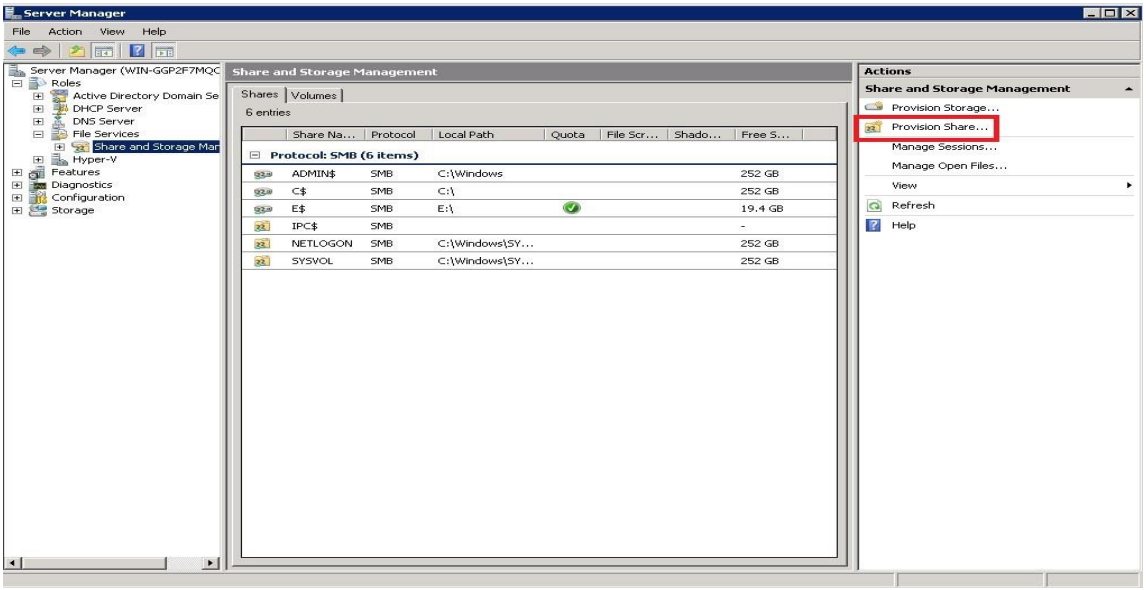
Εικόνα 6.124

25. Στην εικόνα 6.125 φαίνεται η επιτυχής εγκατάσταση του File Server διακομιστή με την προβολή του ανάλογου μηνύματος.



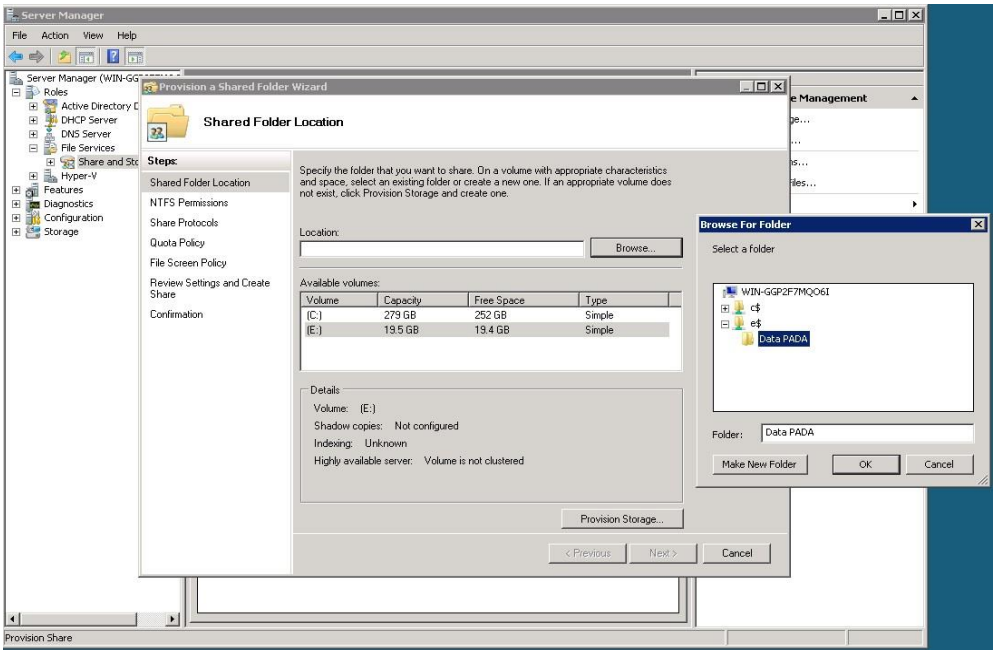
Εικόνα 6.125

26. Στη συνέχεια επιλέγουμε την υπηρεσία Share and Storage Management από τις υπηρεσίες του File Services προκειμένου να δημιουργήσουμε έναν κοινόχρηστο φάκελο όπου θα έχουν πρόσβαση μόνο όσοι έχουν δικαιώματα. Κάνουμε κλικ στο Provision Share, όπως φαίνεται στην εικόνα 6.126.



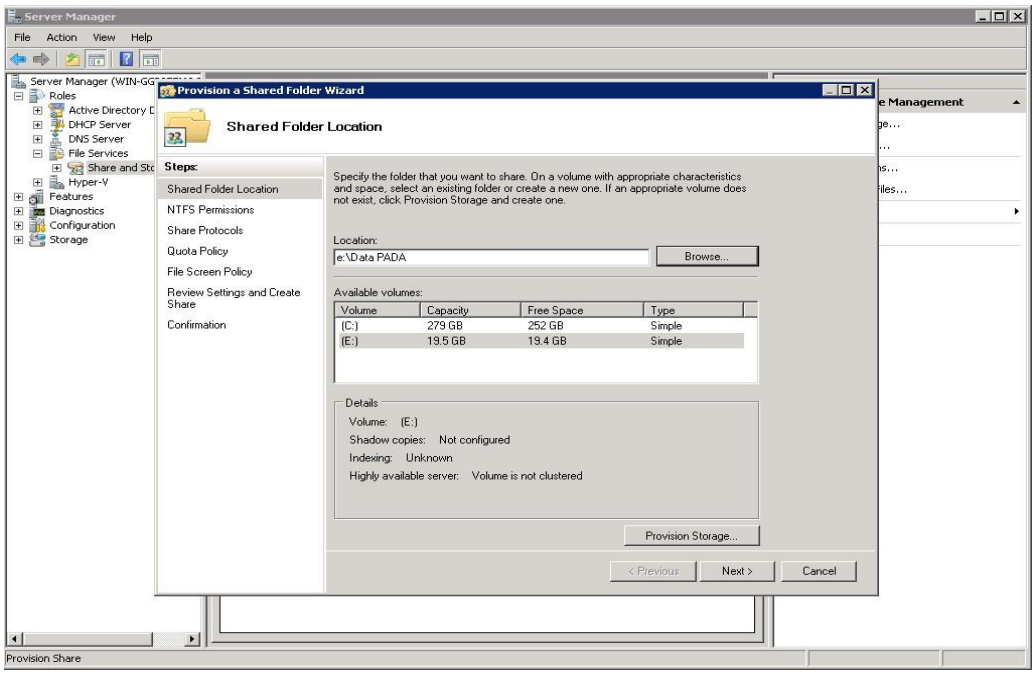
Εικόνα 6.126

27. Στο επόμενο παράθυρο διαλόγου επιλέγουμε το path για το οποίο θα κάνουμε τον φάκελο Data PADA που βρίσκεται στον τοπικό δίσκο E: και κάνουμε κλικ OK.



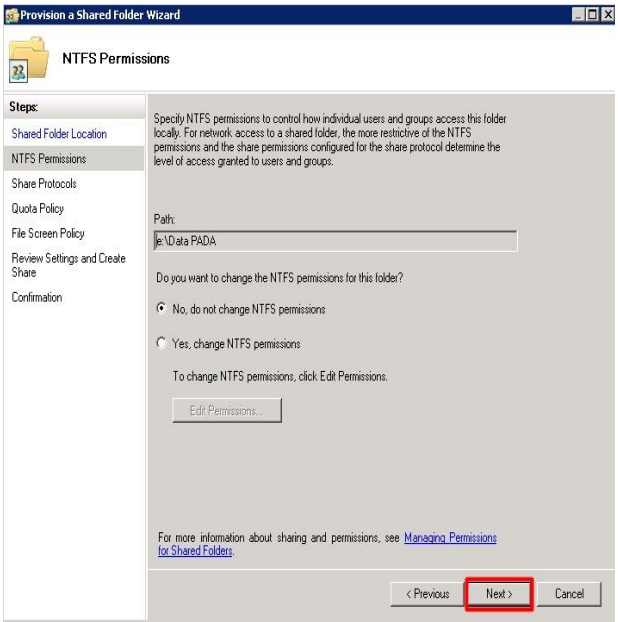
Εικόνα 6.127

28. Αφού τα έχουμε ελέγξει κάνουμε κλικ στο Επόμενο όπως φαίνεται στην εικόνα 6.128.

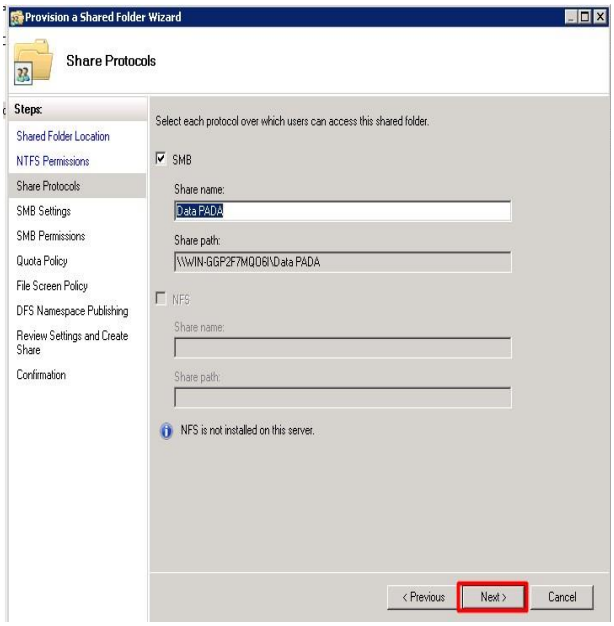


Εικόνα 6.128

29. Στις εικόνες 6.129 και 6.130 μπορούμε να αλλάξουμε τα δικαιώματα για το NTFS καθώς και το όνομα της κοινής χρήσης.

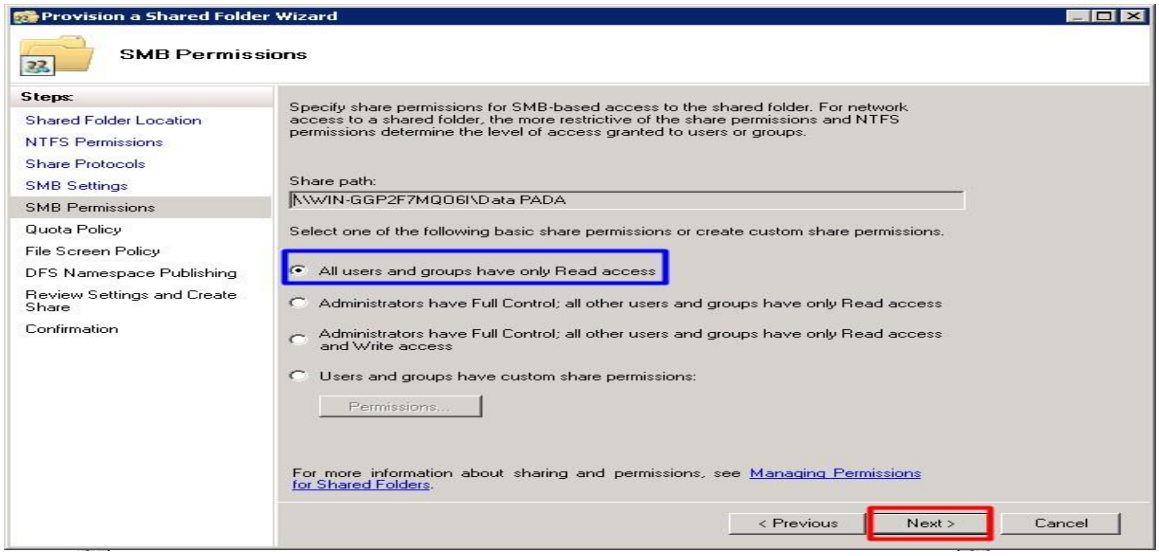


Εικόνα 6.129



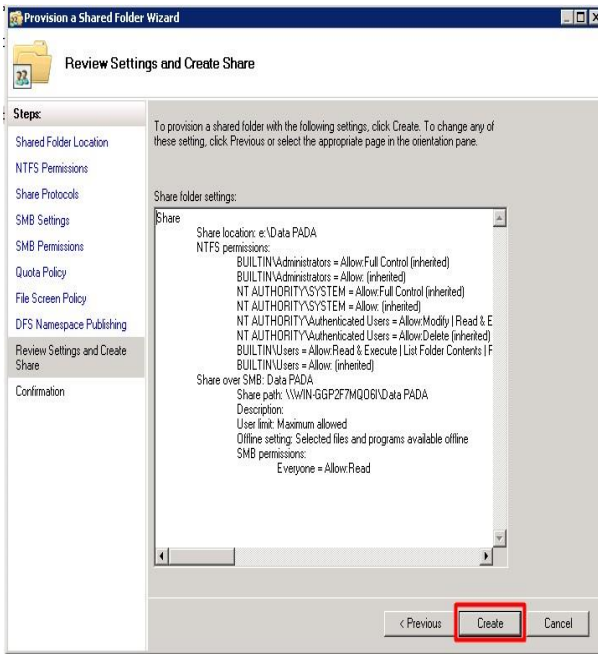
Εικόνα 6.130

30. Στην εικόνα 6.131 καθορίζουμε ποιος θα έχει πρόσβαση στην εν λόγω κοινή χρήση.

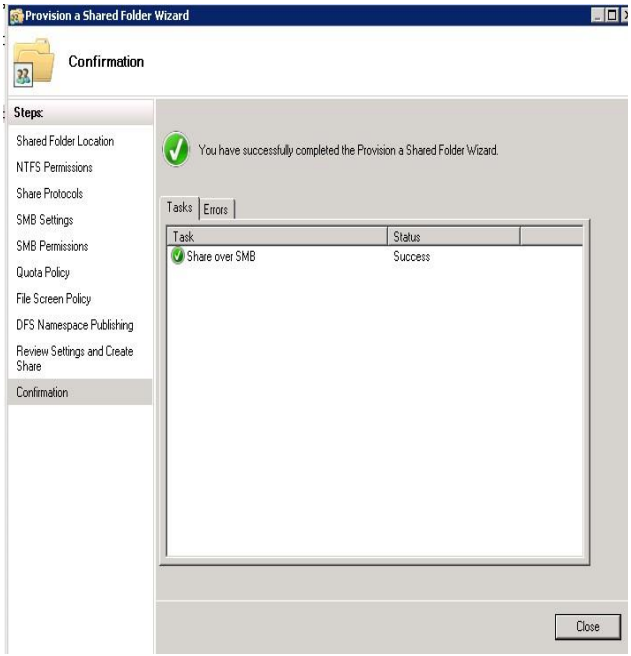


Εικόνα 6.131

31. Στις εικόνες 6.132 και 6.133 βλέπουμε μια προεπισκόπηση των ρυθμίσεων που έχουμε επιλέξει και αφού κάνουμε Δημιουργία βλέπουμε την επιτυχή εγκατάσταση των ρυθμίσεών μας.

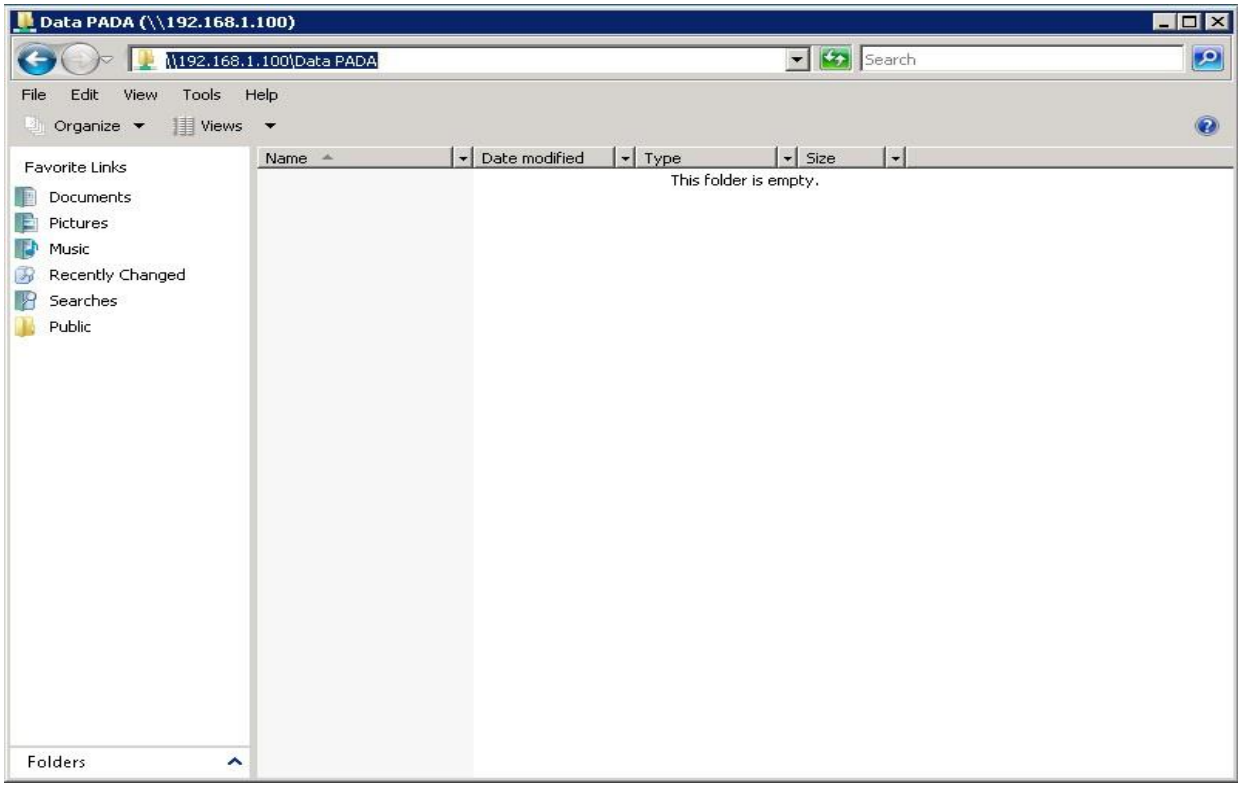


Εικόνα 6.132



Εικόνα 6.133

32. Στην εικόνα 6.134 ελέγχουμε ότι όλα πήγαν όπως επιθυμούμε κτυπώντας στον File Explorer το url του file path που έχουμε υλοποιήσει την κοινή χρήση.



Εικόνα 6.134

6.10. Windows Server 2008 ως διακομιστής e-mail και Microsoft Exchange

Ο Microsoft Exchange Server ενώνει τους χρήστες με γνώσεις ανά πάσα στιγμή, οπουδήποτε. Η ανταλλαγή (Exchange) είναι σχεδιασμένη για να καλύπτει τις ανάγκες ανταλλαγής μηνυμάτων και συνεργασίας μικρών οργανισμών, μεγάλων κατανεμημένων επιχειρήσεων καθώς και ενδιάμεσους οργανισμούς. Το Microsoft Exchange ενσωματώνεται στα Windows Server 2008.Παραθέτουμε μερικές από τις κύριες υπηρεσίες του Exchange Server στις ακόλουθες ενότητες.

Το Exchange είναι επίσης ενσωματωμένο στα IIS για την παροχή πρωτοκόλλων αλληλογραφίας υψηλής απόδοσης, πρωτοκόλλων SMTP, και πρωτόκολλα POP. Το Exchange παρέχει επίσης μια διεπαφή προγράμματος περιήγησης για πρόσβαση σε Microsoft client του Outlook Web Access. Ο Exchange Server υποστηρίζει SMTP, POP, LDAP, IMAP, HTTP, NNTP, S / MIME και X.509 έκδοση 3. Αυτή η ευελιξία επιτρέπει στον Exchange Server να ενεργεί ως πύλη ενός οργανισμού στο Διαδίκτυο. παρέχοντας δρομολόγηση υψηλής απόδοσης υπηρεσιών ηλεκτρονικού ταχυδρομείου. Το SMTP είναι, από προεπιλογή, το πρωτόκολλο μεταφοράς για τη δρομολόγηση όλης της κίνησης μηνυμάτων μεταξύ διακομιστών, σε μια τοποθεσία Exchange και μεταξύ ιστότοπων. Η χρήση του SMTP από έναν οργανισμό έχει ως αποτέλεσμα αυξημένη απόδοση και νέες ευκαιρίες για ένταξη στο Διαδίκτυο. Οι αλγόριθμοι μηνυμάτων του Exchange Server έχουν βελτιωθεί για την παροχή ανεκτικής παράδοσης μηνυμάτων και για την εξάλειψη μηνυμάτων που αναπηδούν, ακόμα και όταν πολλοί διακομιστές ή σύνδεσμοι δικτύου είναι εκτός λειτουργίας. Αυτό παρέχει αυξημένο εύρος ζώνης ανά μήνυμα και απόδοση. Η δρομολόγηση SMTP παρέχει στους πελάτες σημαντική ευελιξία
σχεδιάζοντας έναν αξιόπιστο κορμό μηνυμάτων υψηλής απόδοσης χρησιμοποιώντας τον Exchange Server.

Ο Exchange Server μπορεί να αυξήσει σημαντικά την απόδοση των e-mail, επειδή χρησιμοποιεί προγράμματα-πελάτες ηλεκτρονικού ταχυδρομείου για να αποθηκεύσει και να ανακτήσει περιεχόμενο πολλαπλών χρήσεων επεκτάσεων αλληλογραφίας Internet (MIME) απευθείας από τη βάση, χωρίς καμία μορφή μετατροπής περιεχομένου. Το λογισμικό πελάτη όπως το Outlook επιτρέπει τη ροή δεδομένων μέσα και έξω από τη βάση δεδομένων. Αυτή η διαδικασία βοηθάει πολύ την απόδοση.

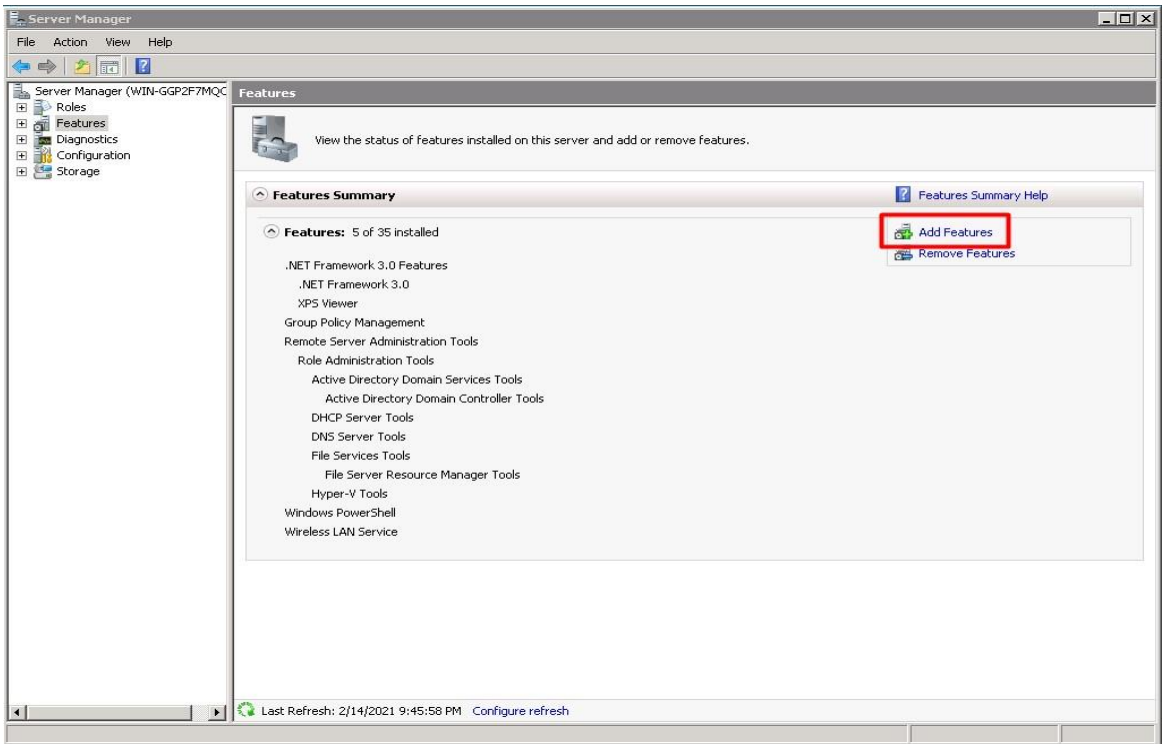
Όλες οι δυνατότητες που αναφέρθηκαν παρέχουν χαμηλό κόστος ιδιοκτησίας, κάτι που κάνει τον Microsoft Exchange Server να είναι ένα πολύτιμο στοιχείο για κάθε οργανισμό.

Το βοηθητικό πρόγραμμα των Windows Server 2008 για τη ρύθμιση παραμέτρων των υπηρεσιών SMTP είναι το Internet Information Services (IIS) 6.0 Manager Console, το οποίο μπορεί να εγκατασταθεί στο IIS 7 προσθέτοντας το IIS 6 Management Console της IIS 6 Compatability Role Service στο Web Server Role στο Διαχειριστής διακομιστή. Μετά την προσθήκη της υπηρεσίας ρόλου συμβατότητας IIS 6 εκτός από την προσθήκη της ίδιας της δυνατότητας SMTP, η κονσόλα διαχείρισης πληροφοριών Internet (IIS) 6.0 θα πρέπει να είναι ορατή στο φάκελο "Εργαλεία διαχείρισης" και θα πρέπει να απεικονίζει τον τοπικό διακομιστή SMTP.

Εγκατάσταση υπηρεσίας SMTP σε Windows Server 2008

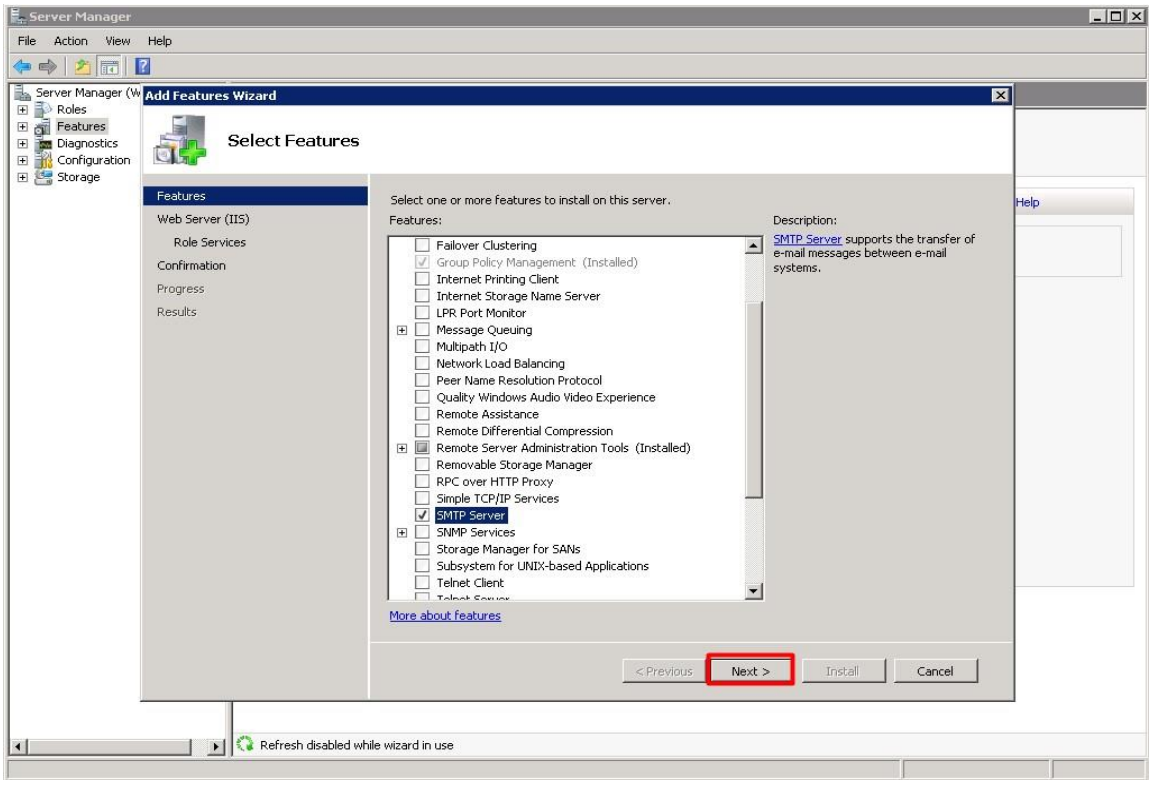
Η εγκατάσταση της υπηρεσίας SMTP πραγματοποιείται με την βοήθεια της προσθήκης νέων χαρακτηριστικών. Στα Windows 2008, η εγκατάσταση έχει βελτιωθεί ακόμη περισσότερο μέσω της χρήσης του οδηγού προσθήκης χαρακτηριστικών στον διακομιστή. Αυτός ο οδηγός εγκαθιστά την υπηρεσία SMTP και προσθέτει αυτόματα όλες τις απαραίτητες υπηρεσίες για την επιτυχή εγκατάσταση του SMTP. Προκειμένου να προσθέσουμε το χαρακτηριστικό του SMTP σε ένα λειτουργικό σύστημα Windows 2008, θα πρέπει να ακολουθήσουμε τα παρακάτω βήματα:

1. Επιλέγουμε Έναρξη, Όλα τα προγράμματα, Εργαλεία διαχείρισης, Διαχείριση διακομιστή. Εάν ζητηθεί, κάνουμε κλικ στο Συνεχίστε για να επιβεβαιώσουμε την ενέργεια. Στη συνέχεια κάνουμε κλικ στην επιλογή Προσθήκη χαρακτηριστικών όπως φαίνεται στην εικόνα 6.135.



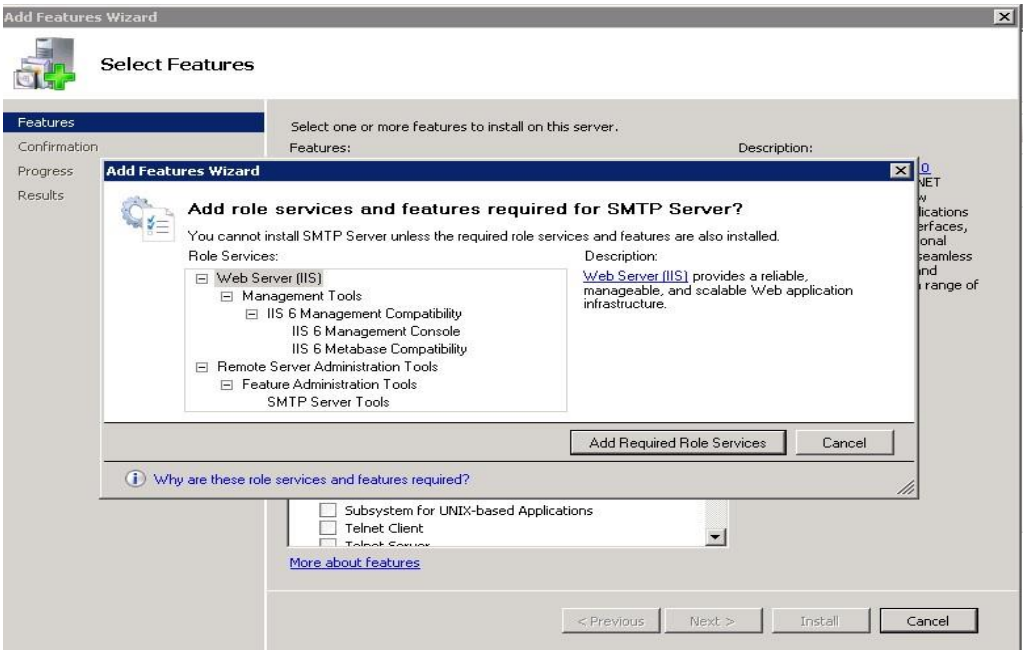
Εικόνα 6.135

2. Στο παράθυρο διαλόγου Διαχείριση διακομιστή, κάνουμε κλικ στην επιλογή SMTP και πατάμε συνέχεια όπως φαίνεται στην εικόνα 6.136.



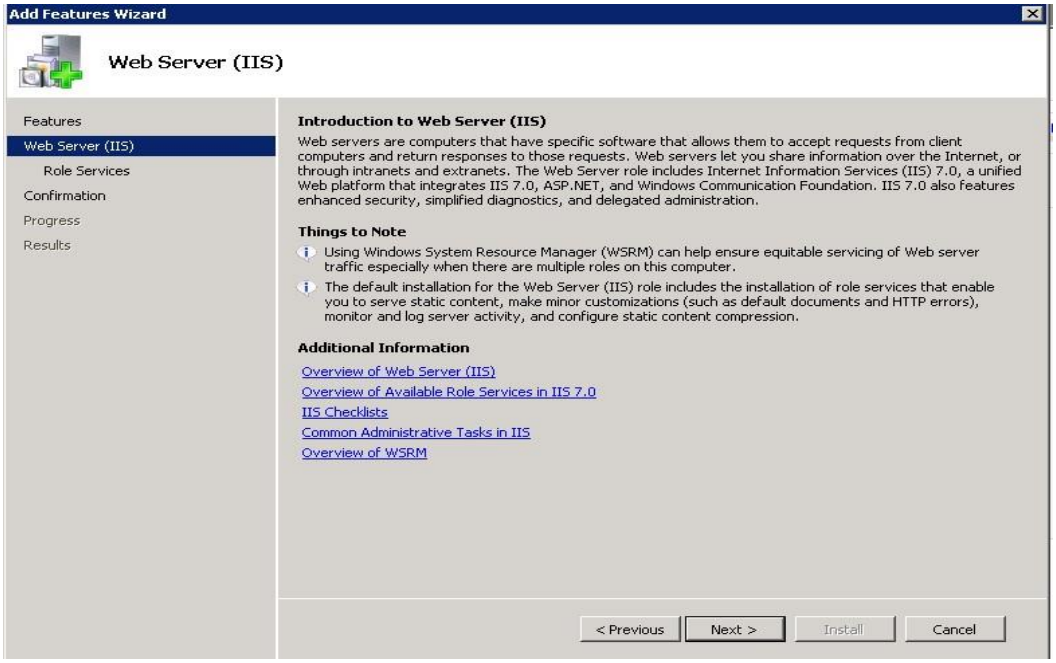
Εικόνα 6.136

3. Στο παράθυρο διαλόγου που μας εμφανίζεται, θα πρέπει να εγκαταστήσουμε υποχρεωτικά πρώτα τον IIS και τις υπηρεσίες του και μετά να γίνει η εγκατάσταση του επιπρόσθετου χαρακτηριστικού SMTP. Επιλέγουμε προσθήκη απαιτούμενων υπηρεσιών όπως φαίνεται στην εικόνα 6.137.



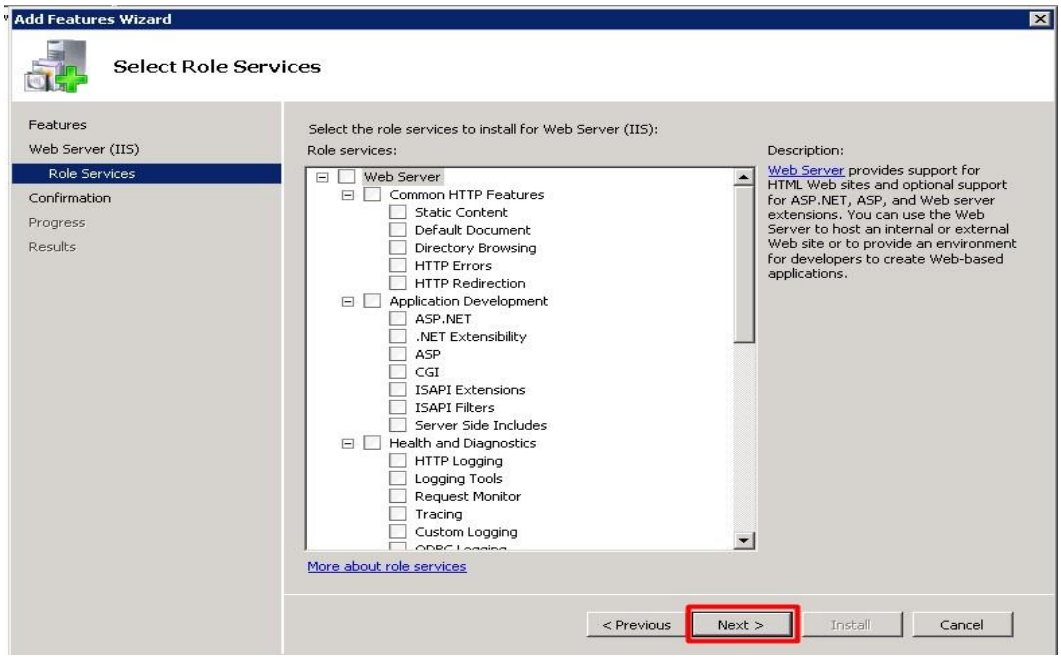
Εικόνα 6.137

4. Στη συνέχεια μας εμφανίζεται μια σύντομη εισαγωγή στον IIS με τις βασικές πληροφορίες εγκατάστασης. Αφού διαβάσουμε τις πληροφορίες, κάνουμε κλικ στο Επόμενο (Next), όπως φαίνεται στην εικόνα 6.138.



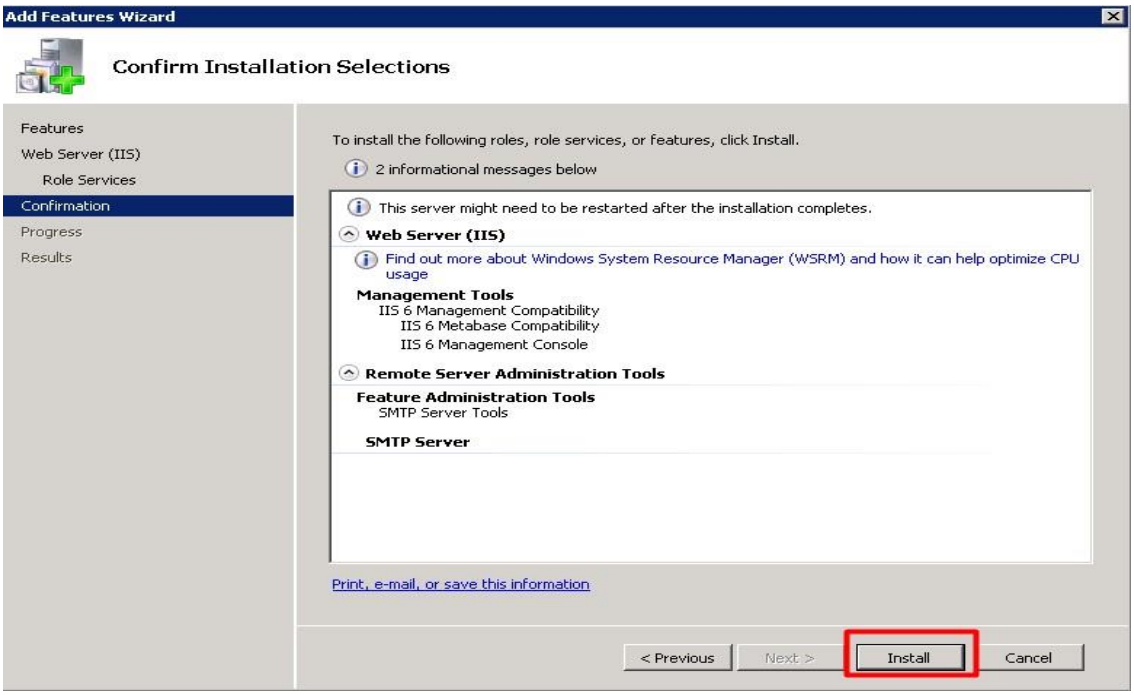
Εικόνα 6.138

5. Επιλέγουμε τις υπηρεσίες του IIS που επιθυμούμε να εγκατασταθούν και στη συνέχεια κάνουμε κλικ στο Επόμενο (Next), όπως φαίνεται στην εικόνα 6.139.



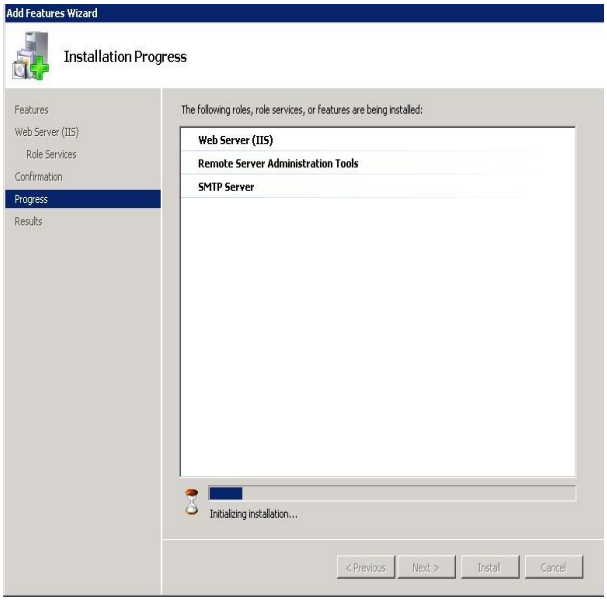
Εικόνα 6.139

6. Στη συνέχεια στο παράθυρο διαλόγου που μας εμφανίζεται, όπως φαίνεται στην εικόνα 6.140, γίνεται μια προεπισκόπηση των ρυθμίσεων που έχουμε επιλέξει για τον διακομιστή IIS προκειμένου να επιβεβαιώσουμε ότι όλα είναι όπως τα επιθυμούμε. Αφού τα έχουμε ελέγξει κάνουμε κλικ εγκατάσταση για να εγκατασταθεί η υπηρεσία μας.

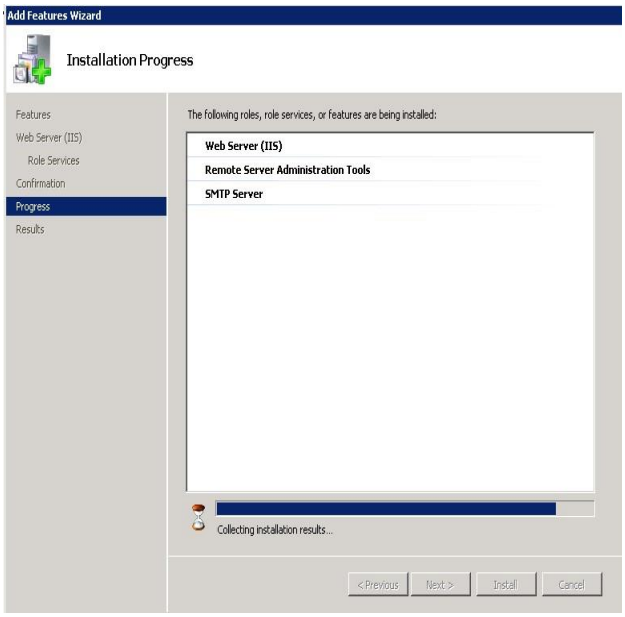


Εικόνα 6.140

7. Στις εικόνες 6.141 και 6.142 φαίνεται η πρόοδος εγκατάστασης

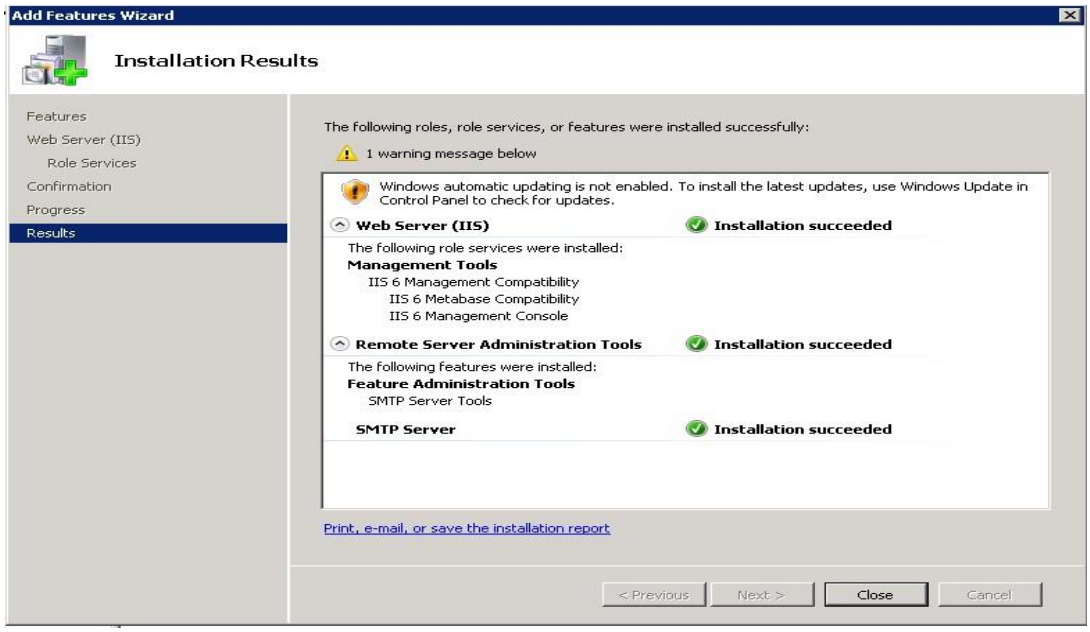


Εικόνα 6.141



Εικόνα 6.142

8. Στην εικόνα 6.143 φαίνεται η επιτυχής εγκατάσταση των υπηρεσιών IIS, Remote Server Administrator Tools και SMTP με την προβολή του ανάλογου μηνύματος.

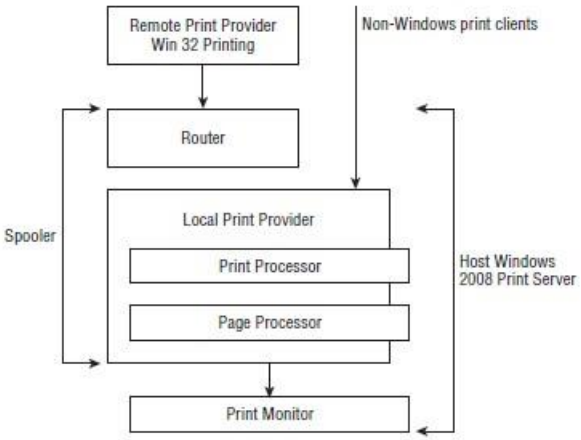


Εικόνα 6.143

6.11. Print Server

Στα Windows Server 2008, η Microsoft επέτρεψε στο διαχειριστή εκτύπωσης να ορίσει πολιτική και διαδικασίες για τη χρήση εκτυπωτών. Αυτό επιτυγχάνεται με την υπηρεσία Print Services. Η κονσόλα διαχείρισης εκτύπωσης (Print Management Console) στα Windows 2008 βοηθά τους οργανισμούς να διαχειρίζονται καλύτερα τη διαχείριση των εκτυπωτών σε εταιρική βάση. Πριν από την ύπαρξη της κονσόλας διαχείρισης εκτύπωσης, ο διαχειριστής δικτύου θα έπρεπε να πηγαίνει σε κάθε εκτυπωτή δικτύου ή διακομιστή εκτυπωτή ξεχωριστά για να τους διαχειριστεί. Για μια μεγάλη επιχείρηση με εκατοντάδες εκτυπωτές και δεκάδες διακομιστές εκτυπωτών, αυτό ήταν μια πολύ κουραστική εργασία για την επιλογή διακομιστών εκτύπωσης κάθε φορά που απαιτείται διαχείριση ενός εκτυπωτή. Επιπλέον, εάν ο διαχειριστής δεν θυμάται σε ποιον εκτυπωτή ή σε ποιον διακομιστή εκτύπωσης ήταν συνδεδεμένος, μπορεί να χρειαστεί χρόνος μέχρι να βρεθεί ο ανάλογος εκτυπωτής και ο διακομιστή εκτύπωσης που χρειάζονται διαχείριση.

Η κονσόλα διαχείρισης εκτύπωσης παρέχει μια μοναδική διεπαφή όπου μπορεί ένας διαχειριστής να ανοίξει την κονσόλα διαχείρισης εκτύπωσης και να δει όλους τους εκτυπωτές και τους διακομιστές εκτύπωσης σε μια επιχείρηση. Μπορεί χρησιμοποιήσει την κονσόλα για διαχείριση σφαλμάτων εκτύπωσης και να βοηθήσει τους χρήστες να συνδεθούν με εκτυπωτές που βρίσκονται πλησιέστερα ή σε απομακρυσμένες τοποθεσίες. Η κονσόλα επιτρέπει επίσης να ανακαλύψει και να εγκαταστήσει εκτυπωτές στα τοπικά υποδίκτυα, και μπορεί ακόμη και να εκτελέσει σενάρια εγκατάστασης. Επιπλέον, μπορεί να ομαδοποιήσει τους εκτυπωτές έτσι ώστε οι κεντρικοί διαχειριστές να μπορούν να ορίσουν υπευθύνους διαχειριστές όπου θα διαχειρίζονται αυτή την ομάδα εκτυπωτών. Για παράδειγμα, εάν ένας οργανισμός διαθέτει διαχειριστή για ένα συγκεκριμένο κτίριο, η διεπαφή διαχείρισης εκτύπωσης θα μπορούσε να φιλτράρει μόνο τη λίστα εκτυπωτών του συγκεκριμένου κτιρίου. Αυτό θα επέτρεπε στον διαχειριστή να βλέπει μόνο συγκεκριμένους εκτυπωτές για τους οποίους είναι υπεύθυνος, καθώς και να ενοποιεί πολλές ομάδες εκτυπωτών διακομιστών εκτύπωσης σε μία διεπαφή για διαχείριση.



Εικόνα 6.144

Το στοιχείο διαχείρισης εκτύπωσης πρέπει να εγκατασταθεί μόνο στο σύστημα στο οποίο διαχειρίζεται ο διαχειριστής, δεν χρειάζεται να εγκατασταθεί σε όλους τους διακομιστές εκτύπωσης ή σε όλα τα συστήματα μιας επιχείρησης. Η υπηρεσία εκτυπωτή, που απεικονίζεται εικόνα 6.144 , περιλαμβάνει διάφορα στοιχεία και έννοιες, οι οποίες περιγράφονται παρακάτω:

- Print routers: Οι δρομολογητές εκτύπωσης βρίσκονται μεταξύ της εφαρμογής πελάτη και του διακομιστή εκτύπωσης (ο οποίος μπορεί επίσης να βρίσκεται στο τοπικό μηχάνημα, εάν εκτυπώνεται στην παράλληλη ή σειριακή θύρα). Η πρώτη δουλειά του δρομολογητή είναι η δρομολόγηση εργασίες εκτύπωσης στους σωστούς διακομιστές και υπηρεσίες εκτύπωσης. Η δεύτερη δουλειά του δρομολογητή, μόλις ο στόχος ο διακομιστής βρέθηκε, είναι να βεβαιωθεί ότι ο πελάτης έχει το σωστό πρόγραμμα

οδήγησης για την εργασία. Ο δρομολογητής ελέγχει το πρόγραμμα οδήγησης του διακομιστή προορισμού με τον πελάτη και, εάν το πρόγραμμα οδήγησης του πελάτη είναι παλαιότερο ή απουσιάζει, ο δρομολογητής ενημερώνει το πρόγραμμα οδήγησης στον υπολογιστή-πελάτη.

- Printer drivers: Τα προγράμματα οδήγησης εκτυπωτή είναι τα πρώτα μεταβλητά στοιχεία που παρέχονται κατά τη ρύθμιση λογικών εκτυπωτών. Είναι τα στοιχεία του λογισμικού που αποστέλλονται στο λογισμικό του χρήστη για να του επιτρέψει να δημιουργήσει εργασίες εκτύπωσης ανάλογα με τις δυνατότητες των εκτυπωτών στόχου. Τα προγράμματα οδήγησης εκτυπωτή έχουν σχεδιαστεί για συγκεκριμένους εκτυπωτές ή οικογένειες εκτυπωτών. Τα προγράμματα οδήγησης εκτυπωτή εγκαθίστανται κατά την εγκατάσταση και τη διαμόρφωση λογικών συσκευών εκτύπωσης.

- Spooler (Ουρά): Η υπηρεσία spooler είναι μια μηχανή, μια συλλογή βιβλιοθηκών, που ελέγχει κάθε μία εργασία εκτύπωσης σε ένα μηχάνημα. Περιγράφεται καλύτερα ως στοίβα, ξεκινώντας από μια υπηρεσία δρομολογητή που μπορεί να κάνει λήψη εργασιών που παραδόθηκαν από διαδικασίες πελάτη. Είναι επίσης η υπηρεσία που ελέγχει τη διαχείριση, την εγκατάσταση του πελάτη και του διακομιστή και τη διαχείριση λογικών εκτυπωτών και πολλά άλλα. Η ουρά είναι υπό τον έλεγχο του διαχειριστή ελέγχου υπηρεσίας. Μπορεί να σταματήσει και να ξεκινήσει οποιαδήποτε στιγμή.

- Print Processor (Επεξεργαστής εκτύπωσης): Ο επεξεργαστής εκτύπωσης είναι το αρχείο .dll (όπως το Wntprint.dll) που βρίσκεται στο \system32\spool\prtprocs\w32x86 φάκελο. Αυτή η βιβλιοθήκη συναρτήσεων λαμβάνει τα δεδομένα εργασίας εκτύπωσης που αποστέλλονται από το spooler και το καθιστά σε δεδομένα που ο εκτυπωτής μπορεί να κατανοήσει.Οι περισσότερες εργασίες εκτύπωσης δεν απαιτούν παρέμβαση από τον επεξεργαστή εκτύπωσης, εκτός εάν υπάρχουν ιδιαίτερες απαιτήσεις εξόδου.

- Port (Θύρες): Ο όρος θύρα χρησιμοποιείται για να αναφέρεται στις συνδέσεις υλικού που επιτρέπουν τη ροή δεδομένων από τη μία συσκευή ή το μέσο στην άλλη. Χρήση διακομιστών εκτύπωσης και εξοπλισμού διεπαφής αντιπροσωπεύουν συνδέσεις δικτύου και καλωδίων. Στις θύρες εκχωρούνται διευθύνσεις δικτύου όπου βρίσκονται μεταξύ του εκτυπωτή και της υπηρεσίας ουράς.

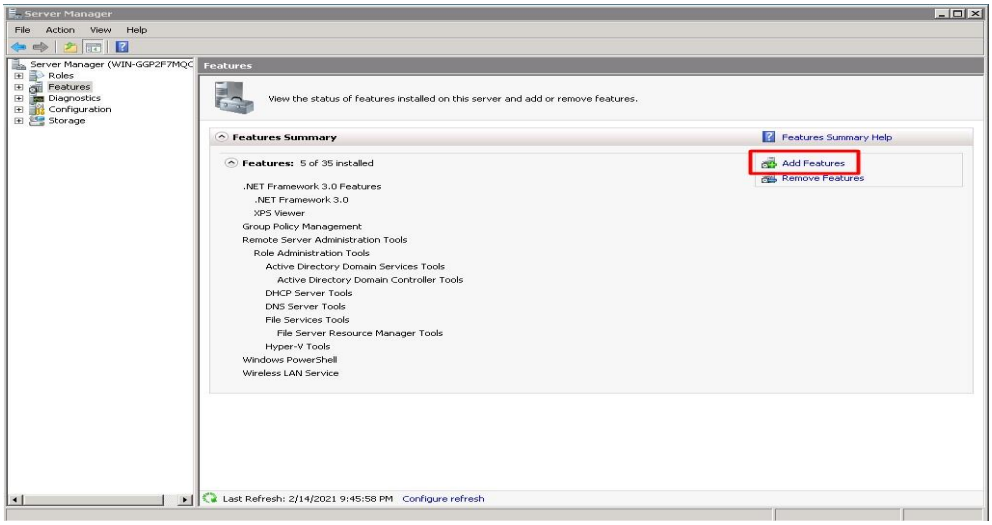
- Print monitors (Οθόνες εκτύπωσης): Τα Print monitors είναι ευαίσθητες συσκευές που ελέγχουν το διαδικασία μετάδοσης της εργασίας εκτύπωσης στις θύρες εισόδου/εξόδου στις συσκευές που διασυνδέονται με τη φυσικό εκτυπωτή. Ο Windows Server υποστηρίζει πολλές τυπικές οθόνες εκτύπωσης. Τα Print monitors εκτελούν οθόνες τις ακόλουθες εργασίες στην υπηρεσία εκτύπωσης:

- Ανοίγουν μια σύνδεση μεταξύ του επεξεργαστή εκτύπωσης και της θύρας. Η σύνδεση χρησιμοποιείται για τη μεταφορά των δεδομένων στις θύρες εισόδου/εξόδου του φυσικού εκτυπωτή ή της διεπαφής απομακρυσμένου εκτυπωτή.
- Παρακολουθούν την εργασία εκτύπωσης για μηνύματα σφάλματος, προόδου και ολοκλήρωσης.

Εγκατάσταση υπηρεσίας Print Server

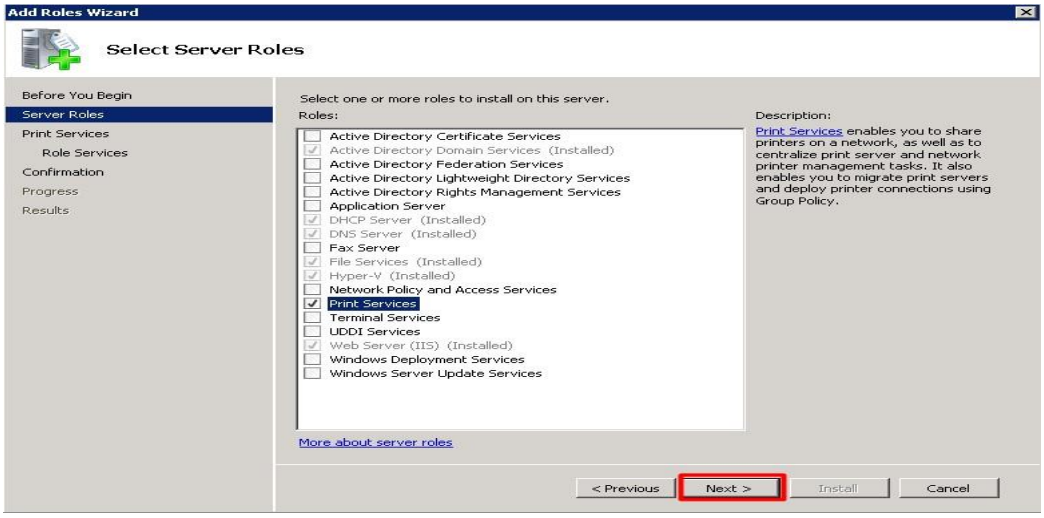
Η εγκατάσταση της υπηρεσίας Print Server πραγματοποιείται με την βοήθεια της προσθήκης νέων χαρακτηριστικών. Αυτός ο οδηγός εγκαθιστά την υπηρεσία Print Server και προσθέτει αυτόματα όλες τις απαραίτητες υπηρεσίες για την επιτυχή εγκατάσταση. Προκειμένου να προσθέσουμε την εν λόγω υπηρεσία σε ένα λειτουργικό σύστημα Windows 2008, θα πρέπει να ακολουθήσουμε τα παρακάτω βήματα:

1. Επιλέγουμε Έναρξη, Όλα τα προγράμματα, Εργαλεία διαχείρισης, Διαχείριση διακομιστή. Εάν ζητηθεί, κάνουμε κλικ στο Συνεχίστε για να επιβεβαιώσουμε την ενέργεια. Στη συνέχεια κάνουμε κλικ στην επιλογή Προσθήκη χαρακτηριστικών όπως φαίνεται στην εικόνα 6.145.



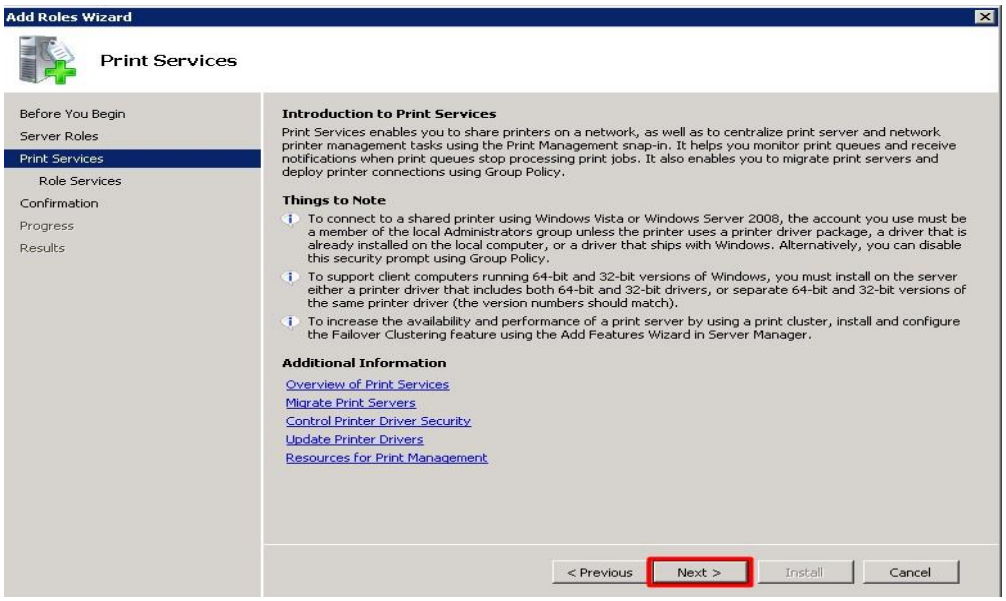
Εικόνα 6.145

2. Στο παράθυρο διαλόγου Διαχείριση διακομιστή, κάνουμε κλικ στην επιλογή Print Services και πατάμε συνέχεια όπως φαίνεται στην εικόνα 6.146.



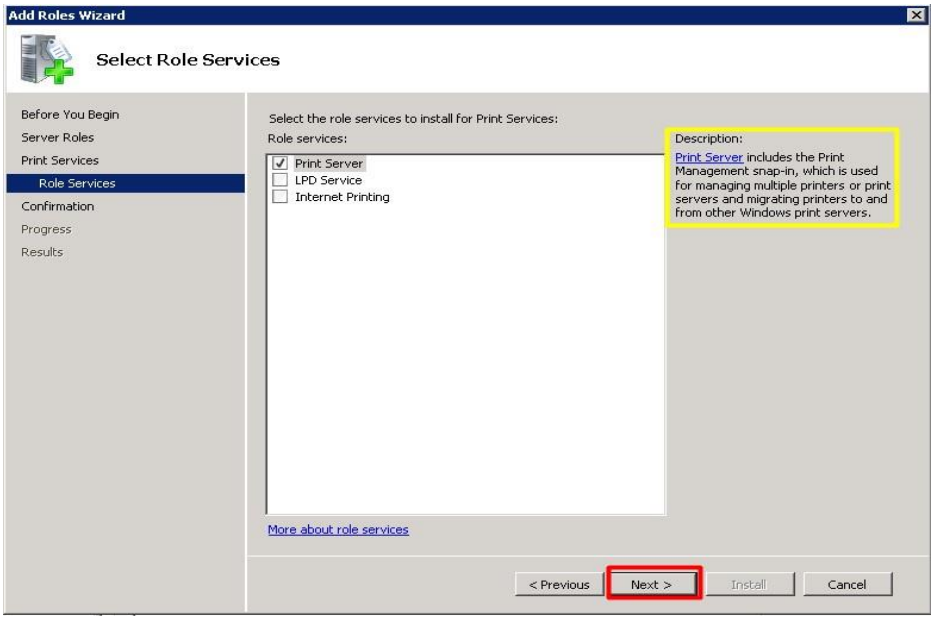
Εικόνα 6.146

3. Στη συνέχεια μας εμφανίζεται μια σύντομη εισαγωγή στην υπηρεσία Print Services με τις βασικές πληροφορίες εγκατάστασης. Αφού διαβάσουμε τις πληροφορίες, κάνουμε κλικ στο Επόμενο (Next), όπως φαίνεται στην εικόνα 6.147.



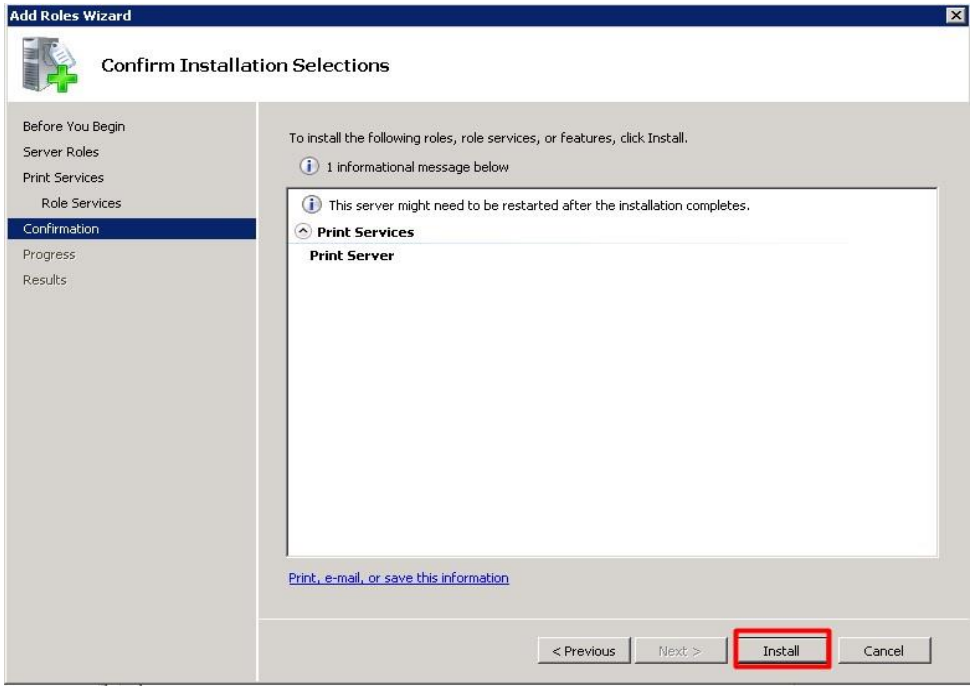
Εικόνα 6.147

4. Η υπηρεσία Print Server είναι ήδη επιλεγμένη από προηγούμενο βήμα, ωστόσο μας δίνεται η δυνατότητα να επιλέξουμε εγκατάσταση και στις υπηρεσίες LPD Service, Internet Printing. Στο κίτρινο πλαίσιο μας ενημερώνει ότι μαζί με την υπηρεσία Print Server θα εγκατασταθεί και η υπηρεσία Print Management. Στη συνέχεια κάνουμε κλικ στο Επόμενο (Next), όπως φαίνεται στην εικόνα 6.148.



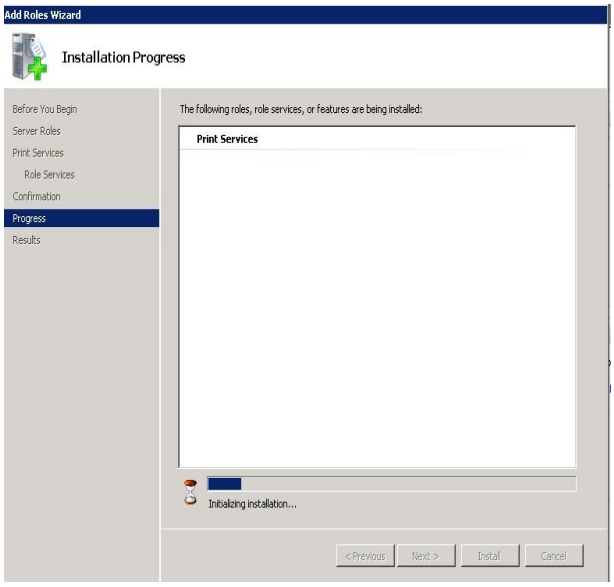
Εικόνα 6.148

5. Στη συνέχεια στο παράθυρο διαλόγου που μας εμφανίζεται, όπως φαίνεται στην εικόνα 6.149, γίνεται μια προεπισκόπηση των ρυθμίσεων που έχουμε επιλέξει για την υπηρεσία Print Server προκειμένου να επιβεβαιώσουμε ότι όλα είναι όπως τα επιθυμούμε. Αφού τα έχουμε ελέγξει κάνουμε κλικ εγκατάσταση για να εγκατασταθεί η υπηρεσία μας.

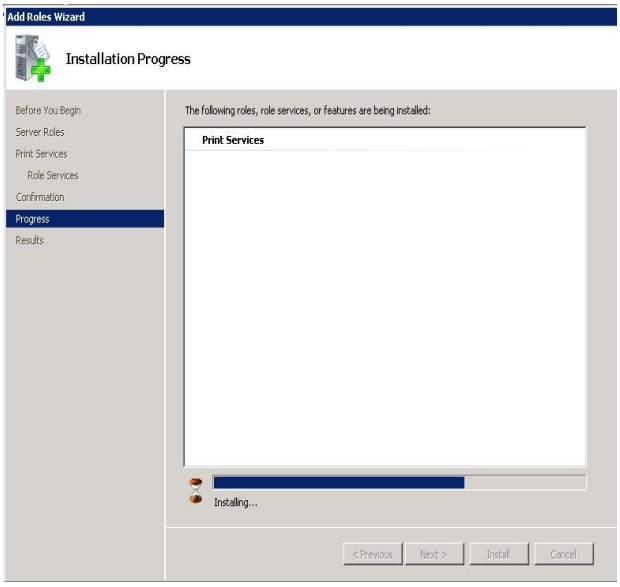


Εικόνα 6.149

6. Στις εικόνες 6.150 και 6.151 φαίνεται η πρόοδος εγκατάστασης

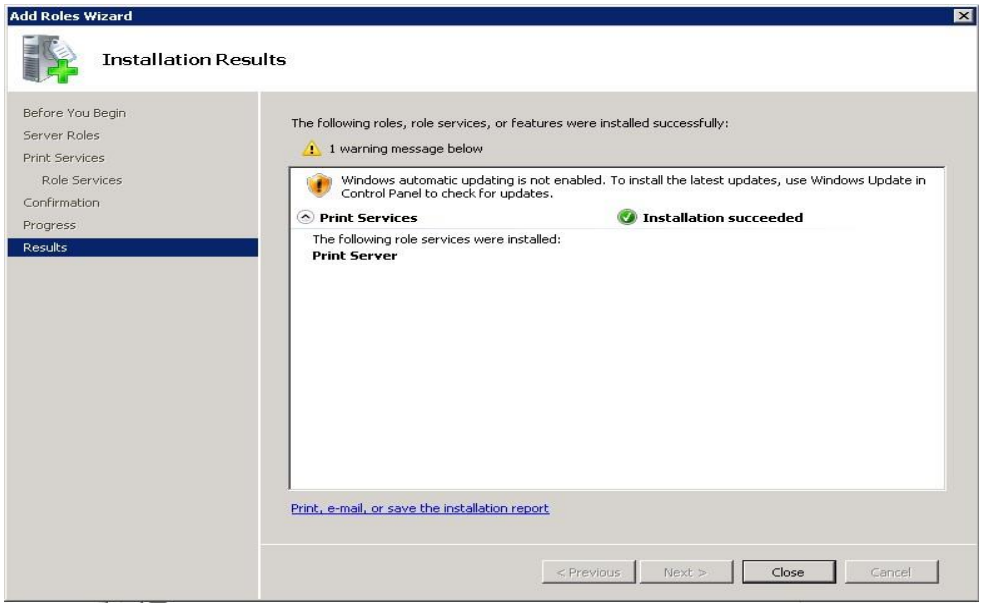


Εικόνα 6.150



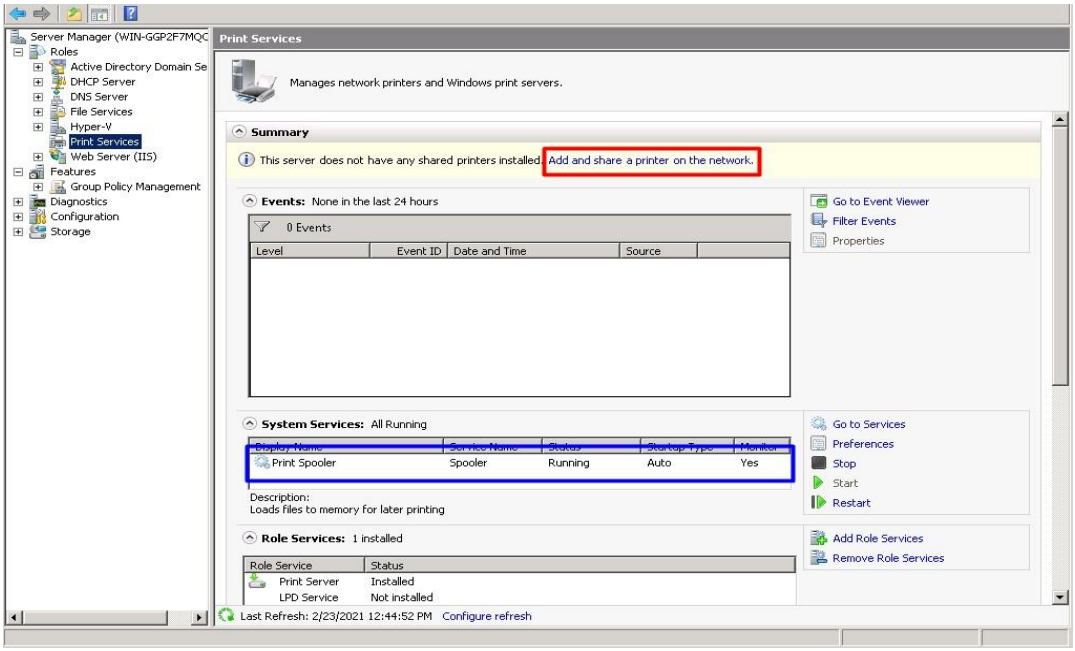
Εικόνα 6.151

7. Στην εικόνα 6.152 φαίνεται η επιτυχής εγκατάσταση της υπηρεσίας Print Server με την προβολή του ανάλογου μηνύματος.



Εικόνα 6.152

Μετά και την επιτυχή εγκατάσταση της υπηρεσίας θα πρέπει να ανοίξουμε το παράθυρο διαλόγου Διαχείρισης του Διακομιστή μας και να αρχίζουμε να προσθέτουμε τους εκτυπωτές μας όπως φαίνεται και στην εικόνα 6.153. Παρατηρούμε επίσης στο μπλε πλαίσιο ότι η υπηρεσία Print Spooler έχει αρχίσει ήδη και τρέχει.



Εικόνα 6.153

Βιβλιογραφία

Ruest Danielle and Ruest Nelson, 2008. *Microsoft Windows Server 2008: The Complete Reference*. USA: McGraw-Hill.

Morimoto Rand, Noel Michael, Droubi Omar, Mistry Ross and Amaris Chris, 2008. *Windows Server 2008 Unleashed*. Indianapolis USA: Sams Publishing.

Stallings William, 2019. *Computer Organization and Architecture Designing for Performance*. New York: Pearson Education.

Savill John, 2014. *he Complete Guide to Windows Server 2008*. USA: Addison-Wesley Professional.

Meloski Vladimir, Wright Byron, Martinez Santos and Bassett Doug, 2018. *Mastering Windows Server 2016*. Canada: SYBEX.

R. Shapiro Jeffrey, 2018. *Windows Server 2008 Bible 1st Edition*. Indianapolis, Indiana: Wiley.

Price John A., Price Brand, and Fenstermacher Scott, 2008. *Mastering Active Directory for Windows Server 2008.* Canada: SYBEX.

Carbone Janique and Larson Robert, 2009. *Windows Server 2008 Hyper V Resource Kit.* USA: Microsoft Press.

Hennessy John L. and Patterson David A., 2011. *Computer Architecture: A Quantitative Approach 5th Edition.* USA: Morgan Kaufmann.

Englander Irv, 2014. *The Architecture of Computer Hardware, Systems Software, and Networking: An Information Technology Approach, 5th Edition*. Indianapolis, Indiana: Wiley.

Chevance René, 2004. *Server Architectures Multiprocessors, Clusters, Parallel Systems, Web Servers, Storage Solutions 1th Edition*. USA: Digital Press.

Somogyi Stephen, 1994. *The Powerpc Macintosh: The Inside Story on the New Risc-Based Macintosh*. USA: Addison-Wesley.

McCabe John, 2016. *Introducing Windows Server 2016 Technical Preview*. USA: Microsoft Press.

Solihin Yan, 2015. *Fundamentals of Parallel Multicore Architecture*. New York: Chapman and Hall/CRC.

Holme Dan, Ruest Nelson, Ruest Danielle and Kellington Jason, 2011. *Configuring Windows Server 2008 Active Directory*. USA: Microsoft Press.

Krause Jordan, 2019. *Mastering Windows Server 2019: The complete guide for IT professionals to install and manage Windows Server 2019 and deploy new capabilities, 2nd Edition*. Birmingham UK: Packt Publishing .

Tulloch Mitch, 2013. *Introducing Windows Server 2012 R2*. USA: Microsoft Press.

Bartłomiej Romanski, Łukasz Heldt, Wojciech Kilian, Krzysztof Lichota and Cezary Dubnicki, 2011. *Anchor-Driven Subchunk Deduplication*. [online] Available at: https://www.researchgate.net/profile/Cezary_Dubnicki/publication/221351929_Anchor-

driven_subchunk_deduplication/links/0c9605320536b0aa70000000/Anchor-driven-subchunk-deduplication.pdf [Accessed 08 August 2020]

EDN, 2014. *LRDIMM vs RDIMM: Signal integrity, capacity, bandwidth*. [online] Available at: https://www.edn.com/lrdimm-vs-rdimm-signal-integrity-capacity-bandwidth/ [Accessed 10 October 2020]

Mostafa Rizk,AmerBaghdadi,MichelJezequel,YasserMohanna,Youssef Atat, 2018. *ImplementationofNISC-basedflexiblearchitecturefor MIMO MMSE-ICturbo-equalization*. [online] Available at: https://hal.archives-ouvertes.fr/hal-01864517 [Accessed 08 August 2020]

SADHNA K. MISHRA, ARVIND RAJAWAT, R.P. SINGH, 2010. *Processor Architecture Design Practices: survey & Issues*. [online] Available at: https://www.researchgate.net/publication/50281783_Processor_Architecture_Design_Practices_Survey_Issues [Accessed 17 September 2020]

Nicholas Economides and Evangelos Katsamakas, 2006. *Linux vs. Windows: A Comparison of Application and Platform Innovation Incentives for Open Source and Proprietary Software Platforms*. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=822894 [Accessed 17 September 2020]

britannica. *Dell Inc*. [online] Available at: https://www.britannica.com/topic/Dell-Inc [Accessed 10 October 2020]

britannica. *Hewlett-Packard Company*. [online] Available at: https://www.britannica.com/topic/Hewlett-Packard-Company [Accessed 10 October 2020]

britannica. *Intel*. [online] Available at: https://www.britannica.com/topic/Intel [Accessed 10 October 2021]

HP, 2019. *History of HP*. [online] Available at: https://store.hp.com/us/en/tech-takes/history-of-hp [Accessed 10 October 2020]

Microsoft, 2010. *Windows Server 2008 R2 SP1 Technical Overview*. [online] Available at: http://download.microsoft.com/download/8/B/9/8B953A85-06C6-4E88-8C27-3DC6F791C931/Windows_Server_2008_R2_SP1_RC_TDM_Whitepaper_final.pdf [Accessed 23 November 2020]

IBM, 2006. *Introduction to the New Mainframe: z/OS Basics*. [online] Available at: http://publibz.boulder.ibm.com/zoslib/pdf/zosbasic.pdf [Accessed 23 November 2020]

ionos, 2019. *Windows vs. Linux: a comparison*. [online] Available at: https://www.ionos.com/digitalguide/server/know-how/linux-vs-windows [Accessed 23 November 2020]

educba, 2020. *Linux vs Windows Server*. [online] Available at: https://www.educba.com/linux-vs-windows-server [Accessed 07 December 2020]

Bojana Dobran, 2021. *Windows Server vs Linux: The Ultimate Comparison*. [online] Available at: https://phoenixnap.com/blog/linux-vs-microsoft-windows-servers [Accessed 07 December 2020]

gthost, 2020. *Differences between Windows Server and a Linux server*. [online] Available at: https://gthost.com/blog/differences-between-windows-server-and-a-linux-server [Accessed 15 December 2020]

David Hayward. *A Brief History of Linux*. [online] Available at: https://bdmpublications.com/brief-history-linux [Accessed 15 December 2020]

Kathleen Juell, 2017. *A Brief History of Linux*. [online] Available at: https://www.digitalocean.com/community/tutorials/brief-history-of-linux [Accessed 15 December 2020]

javatpoint. *Linux History*. [online] Available at: https://www.javatpoint.com/linux-history [Accessed 18 December 2020]

distrowatch. [online] Available at: https://distrowatch.com/ [Accessed 22 December 2020]

Tom Walat, 2017. *Windows Server Core*. [online] Available at: https://searchwindowsserver.techtarget.com/definition/Server-Core [Accessed 06 January 2021]

Meike Chabowski, 2017. *The Mainframe versus the Server Farm – A Comparison*. [online] Available at: https://www.suse.com/c/mainframe-versus-server-farm-comparison/ [Accessed 06 January 2021]

Thomas E. Beach, 2016. *Computer Concepts and Terminology*. [online] Available at: http://www.unm.edu/~tbeach/terms/types.html [Accessed 10 January 2021]

paessler. *IT Explained: Server*. [online] Available at: https://www.paessler.com/it-explained/server [Accessed 10 January 2021]

Eric Reed, 2020. *History of IBM: Timeline and Facts*. [online] Available at: https://www.thestreet.com/personal-finance/history-of-ibm [Accessed 10 January 2021]

intel. [online] Available at: https://www.intel.com [Accessed 12 January 2021]

hp. [online] Available at: https://www8.hp.com/ [Accessed 12 January 2021]

ibm. [online] Available at: https://www.ibm.com/ [Accessed 12 January 2021]

dell. [online] Available at: https://www.dell.com/en-us?c=us&l=en [Accessed 12 January 2021]

supermicro. [online] Available at: https://www.supermicro.com/en/ [Accessed 17 January 2021]

ubuntu. [online] Available at: https://ubuntu.com/ [Accessed 17 January 2021]

Cliff Robinson, 2018. *New Gigabyte Marvell ThunderX2 32 Core Servers Available*. [online] Available at: https://www.servethehome.com/new-gigabyte-marvell-thunderx2-32-core-servers-available/ [Accessed 17 January 2021]

ukessays, 2015. *Numa And Uma And Shared Memory Multiprocessors Computer Science Essay*. [online] Available at: https://www.ukessays.com/essays/computer-science/numa-and-uma-and-shared-memory-multiprocessors-computer-science-essay.php [Accessed 17 January 2021]

Frank Denneman, 2016. *NUMA DEEP DIVE PART 1: FROM UMA TO NUMA*. [online] Available at: https://frankdenneman.nl/2016/07/07/numa-deep-dive-part-1-uma-numa/ [Accessed 22 January 2021]

David L Mulnix, 2019. *Intel® Xeon® Processor Scalable Family Technical Overview*. [online] Available at: https://software.intel.com/content/www/us/en/develop/articles/intel-xeon-processor-scalable-family-technical-overview.html [Accessed 22 January 2021]

Michael Westerfield, 2019. *Server Memory: RDIMM vs LRDIMM and When to Use Them*. [online] Available at: https://www.dasher.com/server-memory-rdimm-vs-lrdimm-and-when-to-use-them/ [Accessed 22 January 2021]

Doug Daniels, 2019. *Is RDIMM or LRDIMM Right for Your Design?*. [online] Available at: https://www.eeweb.com/is-rdimm-or-lrdimm-right-for-your-design/ [Accessed 22 January 2021]

Marc Rocque, 2015. *DDR4 RDIMM and LRDIMM Performance Comparison*. [online] Available at: https://www.microway.com/hpc-tech-tips/ddr4-rdimm-lrdimm-performance-comparison/ [Accessed 22 January 2021]

Yevgeniy Sverdlik, 2019. *Ampere Gears Up to Launch 7nm, 80-Core Arm Chip for Cloud Data Centers*. [online] Available at: https://www.datacenterknowledge.com/hardware/ampere-gears-launch-7nm-80-core-arm-chip-cloud-data-centers [Accessed 25 January 2021]

Andrei Frumusanu, 2020. *The Ampere Altra Review: 2x 80 Cores Arm Server Performance Monster*. [online] Available at: https://www.anandtech.com/show/16315/the-ampere-altra-review [Accessed 25 January 2021]

Dean Takahashi, 2020. *Ampere Altra is the first 80-core ARM-based server processor*. [online] Available at: https://venturebeat.com/2020/03/03/ampere-altra-is-the-first-80-core-arm-based-server-processor/ [Accessed 25 January 2021]

Roger Peene, 2020. *Ampere® Altra® - Industry's First 80-Core Server Processor Unveiled Brings New Level of Performance & Power Efficiency to Cloud Environments*. [online] Available at: https://amperecomputing.com/ampere-altra-industrys-first-80-core-server-processor-unveiled/ [Accessed 25 January 2021]

GigaByte. *Ampere Altra Server Solution*. [online] Available at: https://www.gigabyte.com/Industry-Solutions/5G-Data-Center/ampere-altra-server-solution [Accessed 28 January 2021]

Graeme Burton, 2020. *Microsoft is reportedly developing its own Arm server chips*. [online] Available at: https://www.datacenterdynamics.com/en/news/microsoft-reportedly-developing-its-own-arm-server-chips/ [Accessed 28 January 2021]

EDUCBA. *Difference Between Linux and Windows Server*. [online] Available at: https://www.educba.com/linux-vs-windows-server/ [Accessed 28 January 2021]