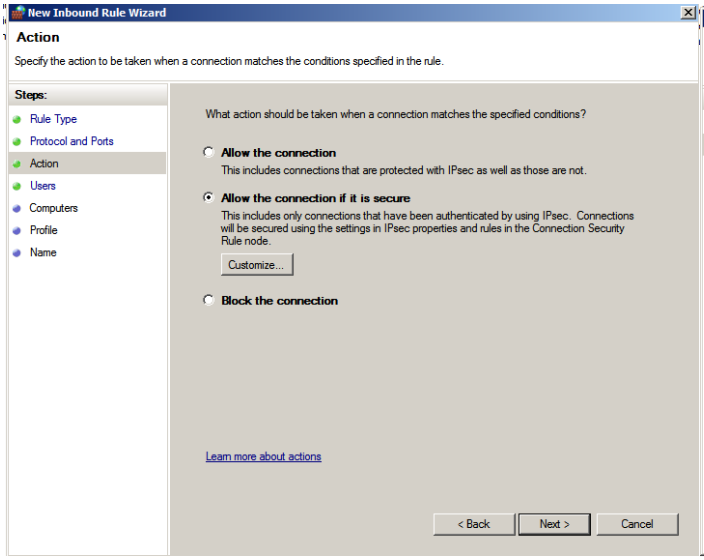
Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

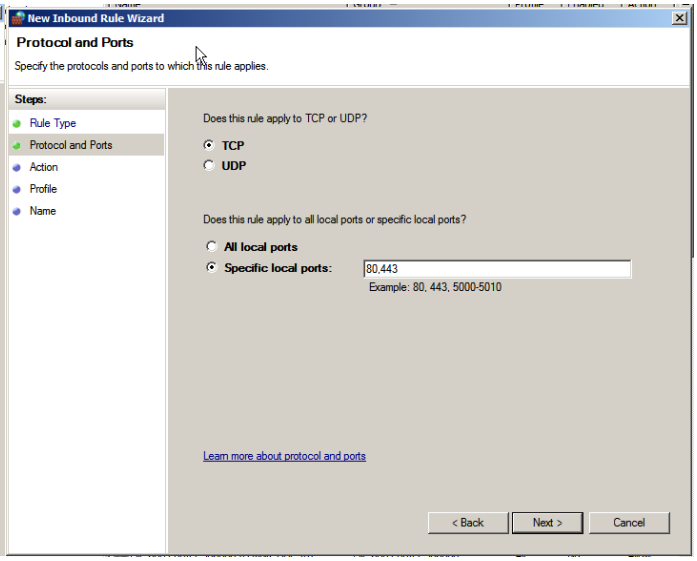
Αναφορά 1ης Εργαστηριακής Άσκησης
– Μέρος Δεύτερο –
Υλοποίηση Εξυπηρετητή Windows

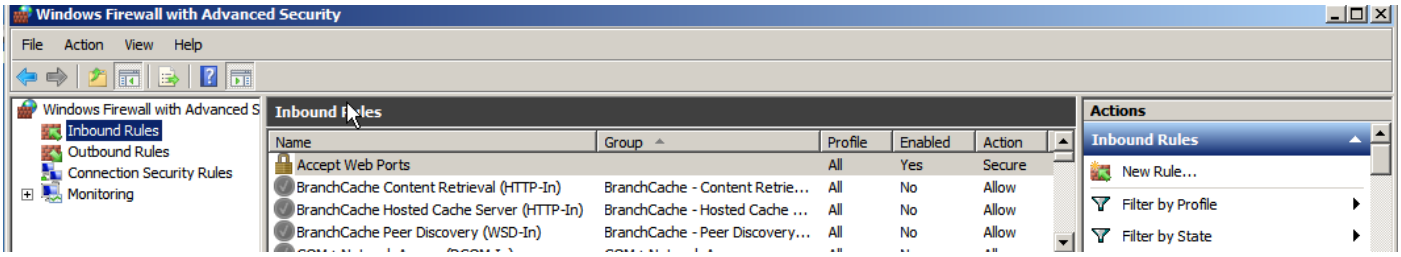
Αυλακιώτης Χρήστος – 321/2012015
Κατσιβέλης Κων/νος – 321/2011063
Φιωτάκης Γιώργος – 321/2013220

A1. Αρχικά δημιουργήσαμε ένα virtual machine και εγκαταστήσαμε το λειτουργικό Windows Server 2008 R2 Enterprise.

A2. Παραμετροποιήσαμε το τείχος προστασίας των Windows με Εξελιγμένη Ασφάλεια επιτρέποντας συνδέσεις στις θύρες 80(http) και 443 (https) που θα ενεργοποιήσουμε στην συνεχεία



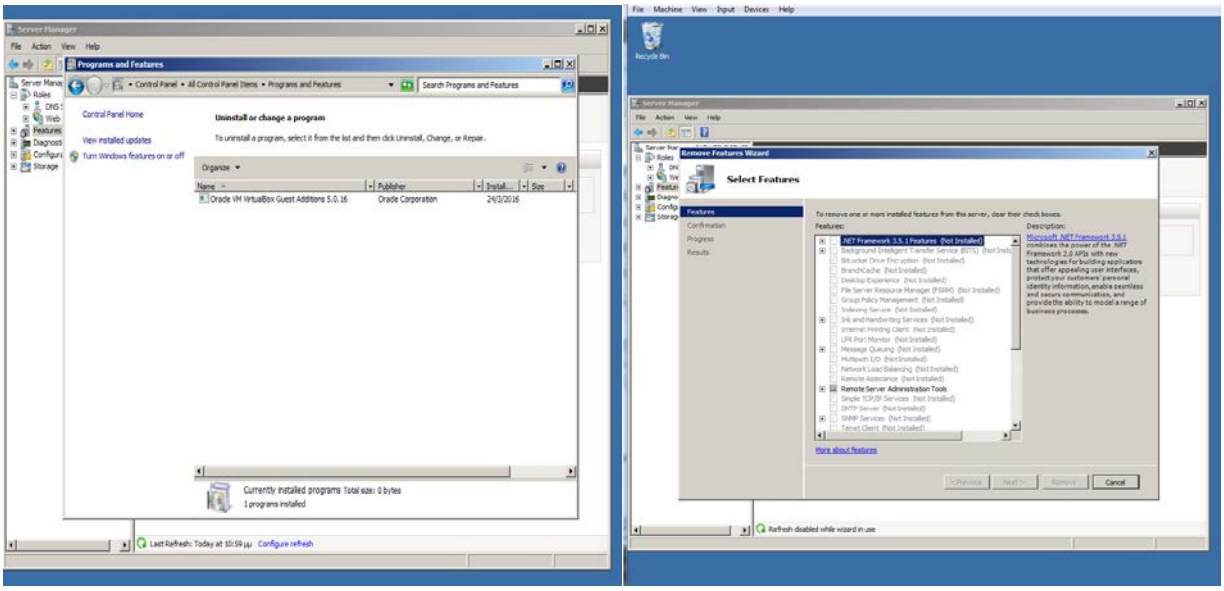




B1. Πήγαμε στα Services (start->administrative tools->services) και απενεργοποιήσαμε τις:

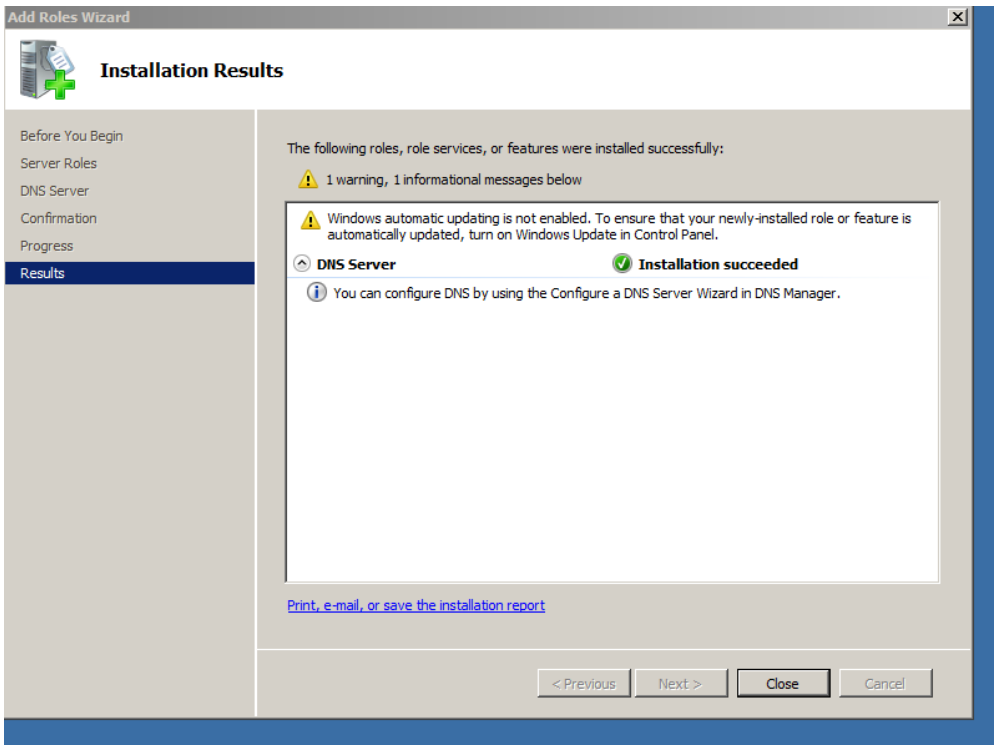
- Print Spooler, καθώς δε θα χρησιμοποιήσουμε εκτυπωτή
- Problem Reports and Solutions Control Panel Support, καθώς δεν μας ενδιαφέρουν τα Problem Reports
- Remote Procedure Call (RPC) Locator, γιατί δε θέλουμε να χρησιμοποιήσουμε Remote Procedures
- RPC Endpoint Mapper <<
- Remote Registry, καθώς δε θέλουμε να γίνονται αλλαγές στο Registry από remote users
- Smart Card καθώς δε κάνουμε χρήση smart cards
- Smart Card Removal Policy καθώς δε κάνουμε χρήση smart cards
- Windows Color System πρόσθετα των windows που δε μας ενδιαφέρουν
- Windows Error Reporting Service <<
- Windows Font Cache Service <<
- Windows Remote Management, καθώς δε θέλουμε να γίνεται remote management στον υπολογιστή
- Secondary Logon, για λογούς ασφάλειας
- Windows Image Acquisition (WIA), καθώς δεν κάνουμε χρήση κάμερας ή scanner
- WMI Performance Adapters, καθώς δε το χρειαζόμαστε

B2. Ελέγξαμε για έξτρα προγράμματα και features στον υπολογιστή που δεν χρειαζόμασταν άλλα δεν είχαμε.

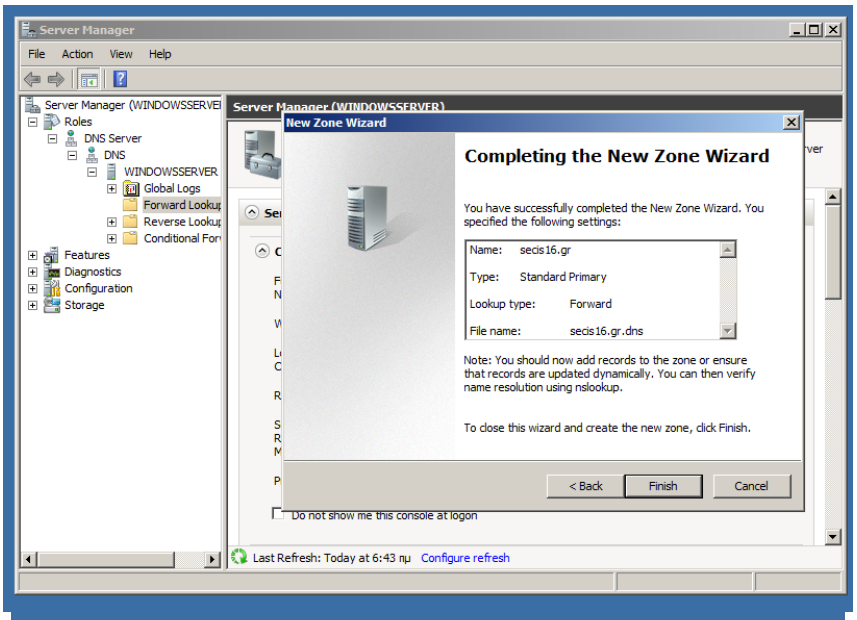


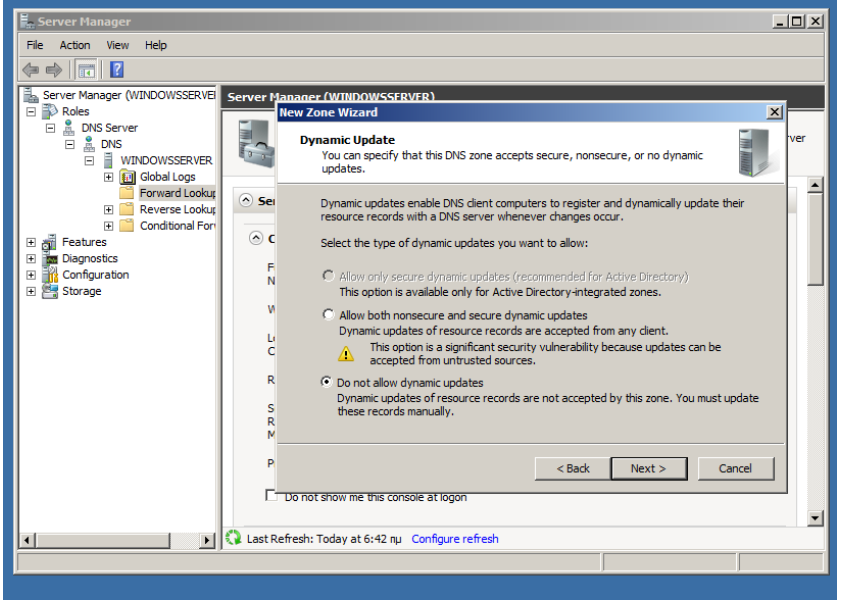
B3.

Υπηρεσία DNS:

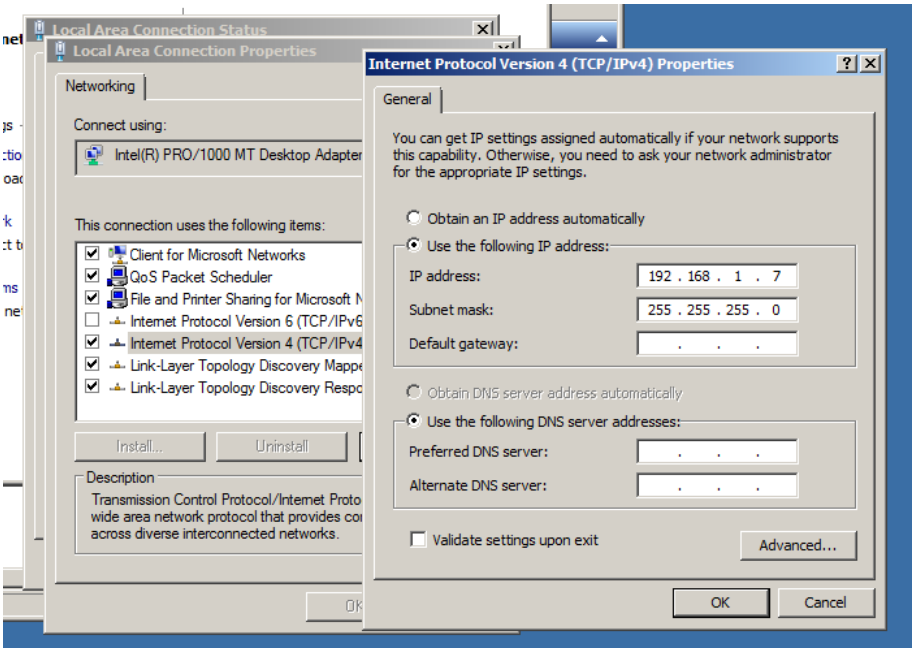


Δημιουργία τοποθεσίας secis16.gr:

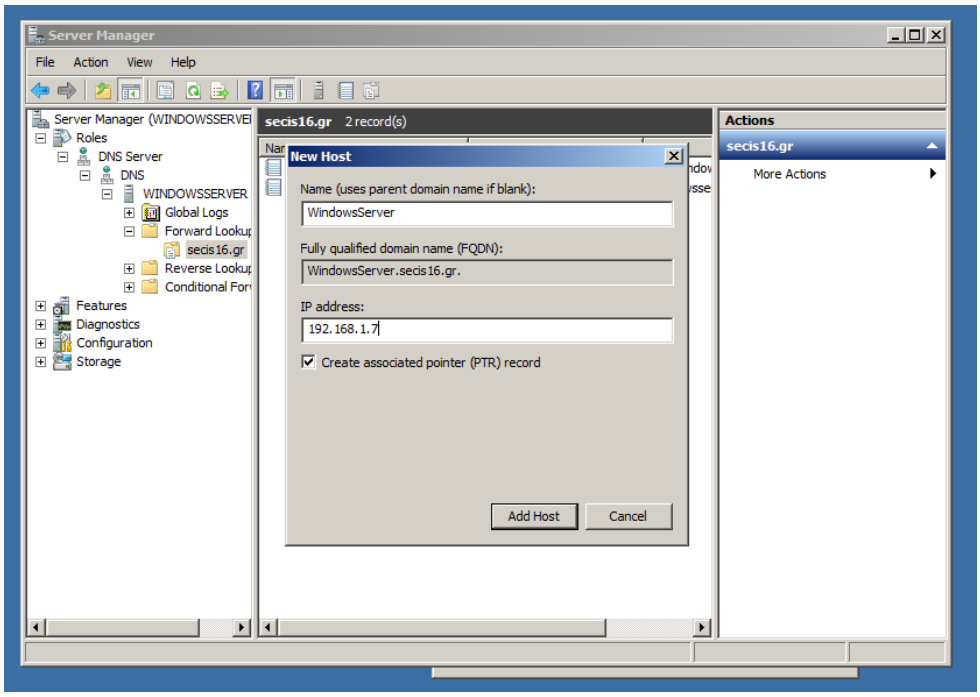




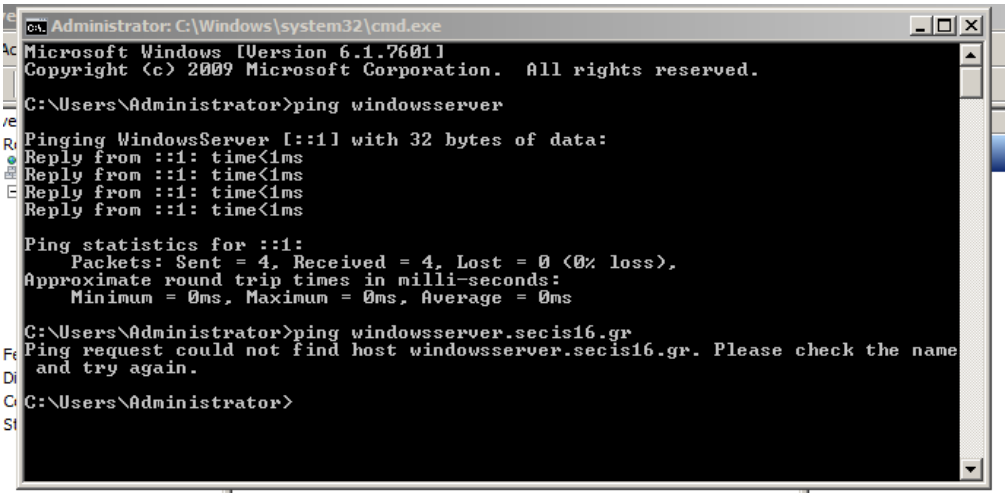
ορισμός στατικής διεύθυνσης:



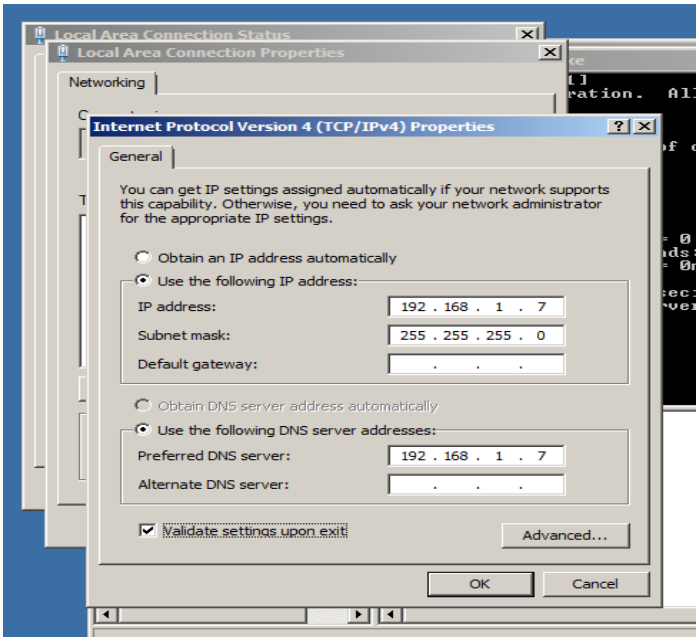
Δημιουργία Host:



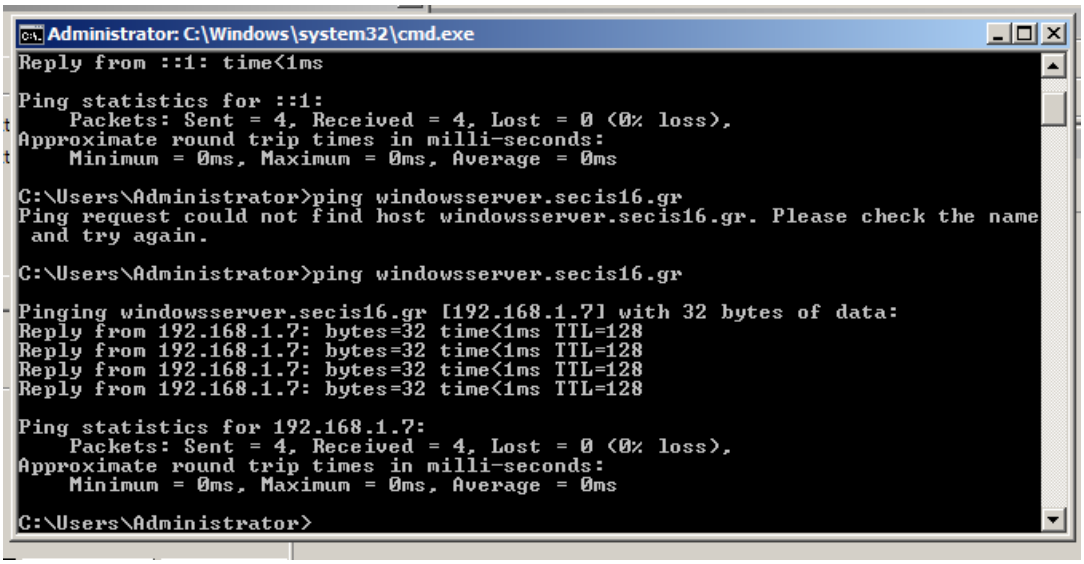
Έλεγχος με ping:



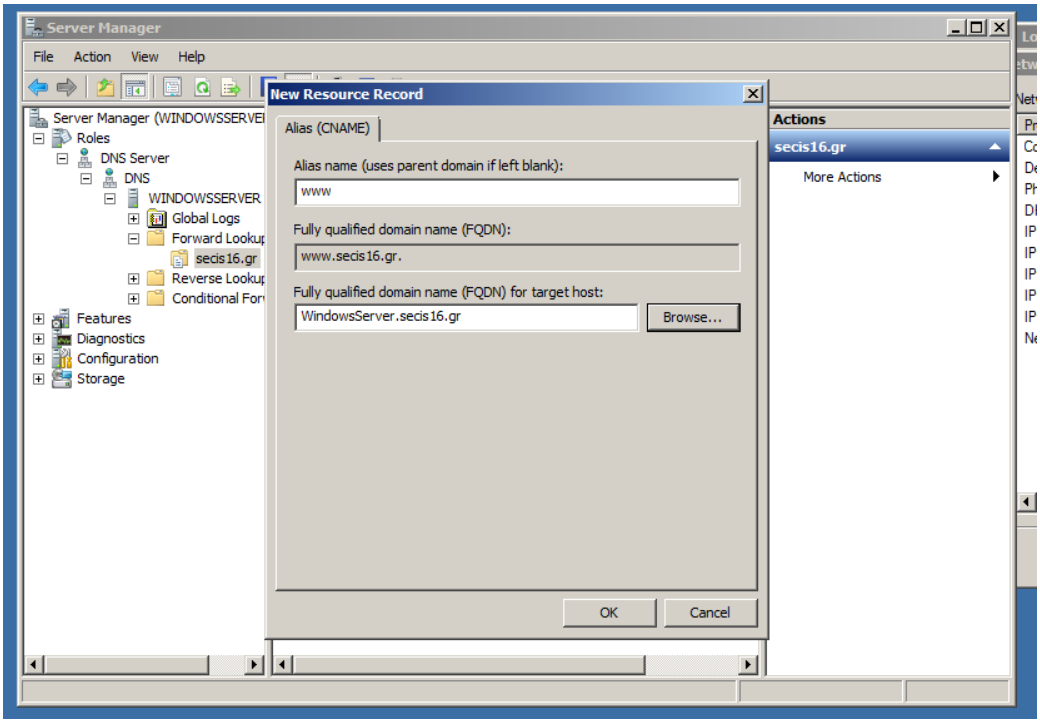
Ορισμός DNS:



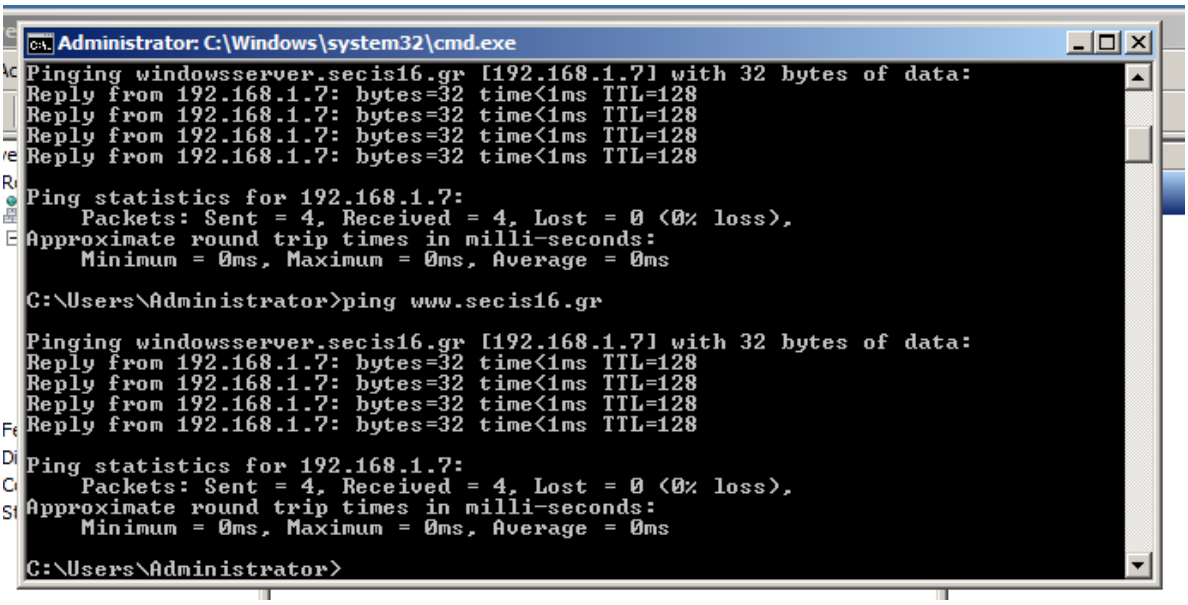
Έλεγχος με ping:



Ορισμός CNAME (www αντί για WindowsServer)

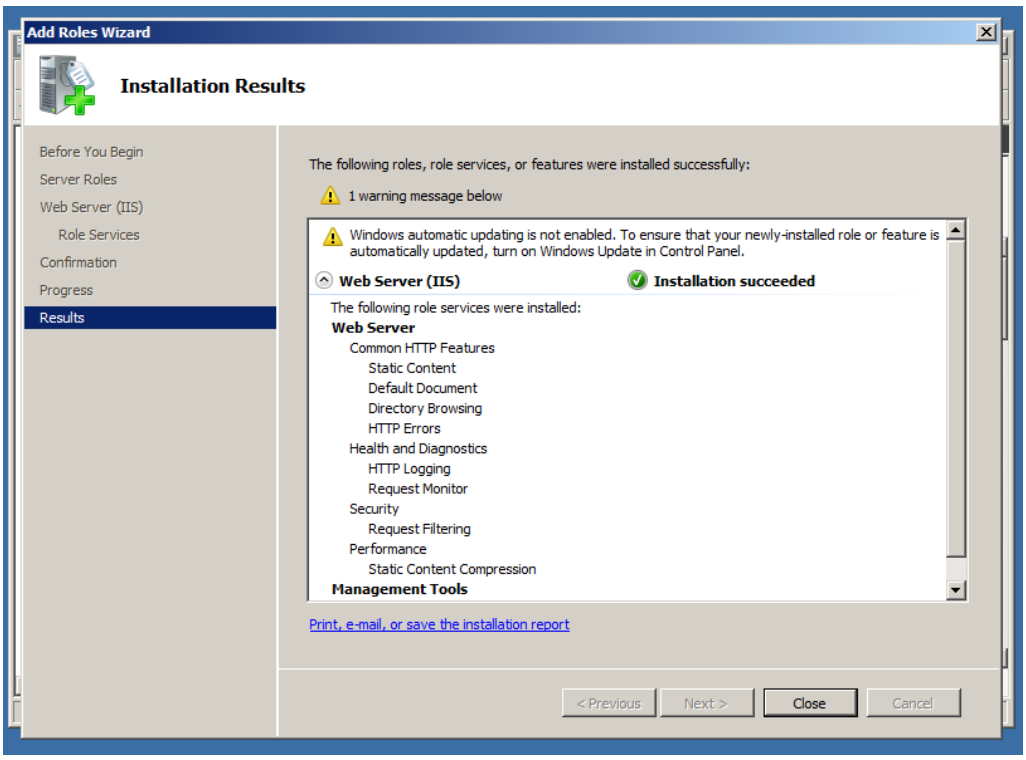


Έλεγχος διεύθυνσης www.secis16.gr:

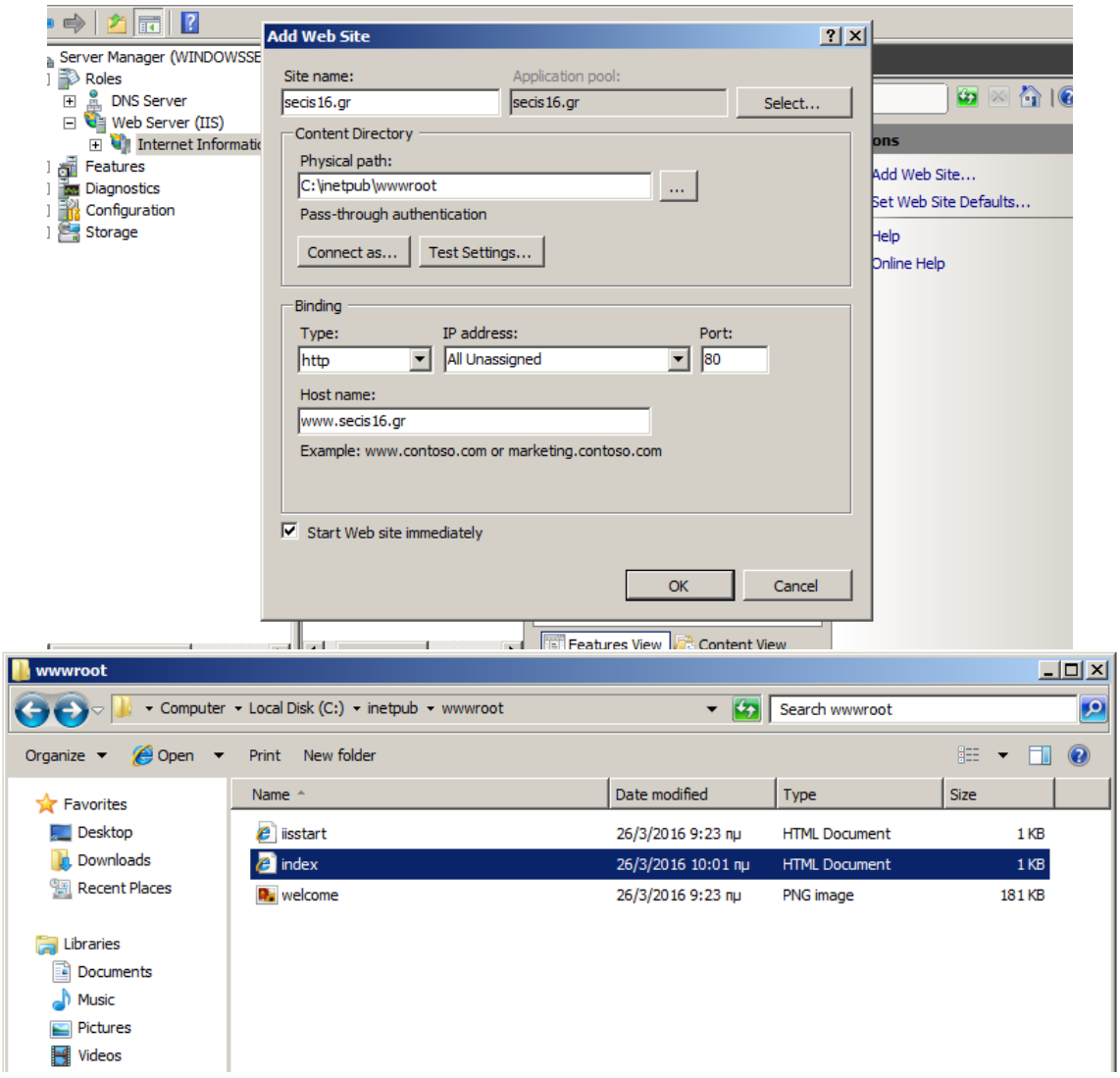


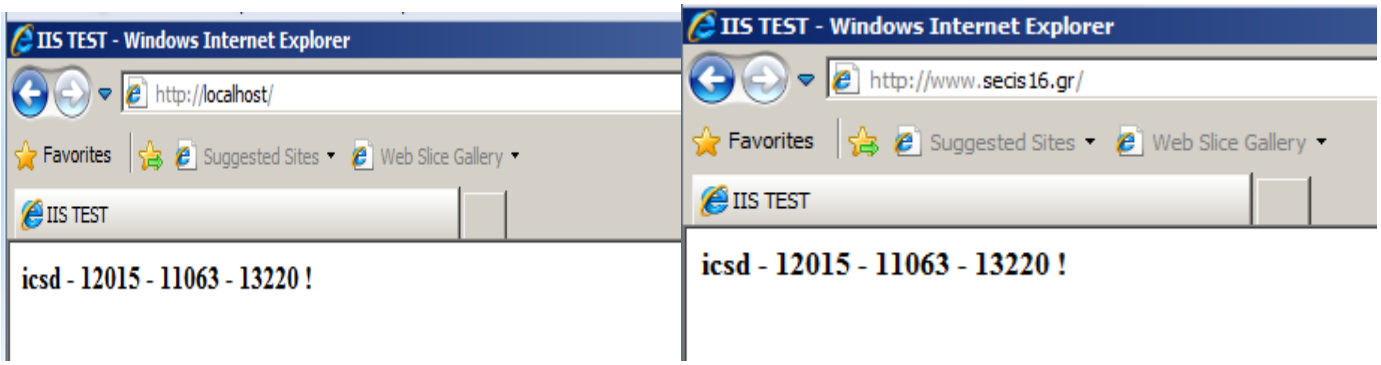
Υπηρεσία IIS:

Εγκατάσταση IIS:



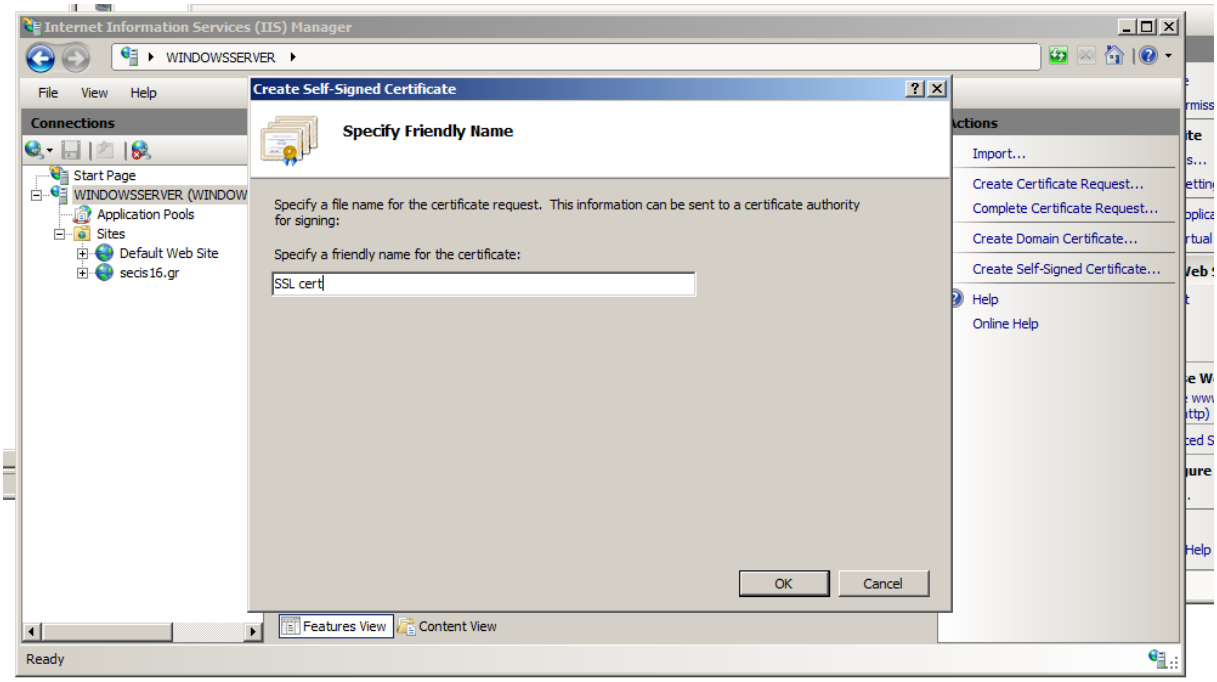
Δημιουργία ιστοσελίδας:



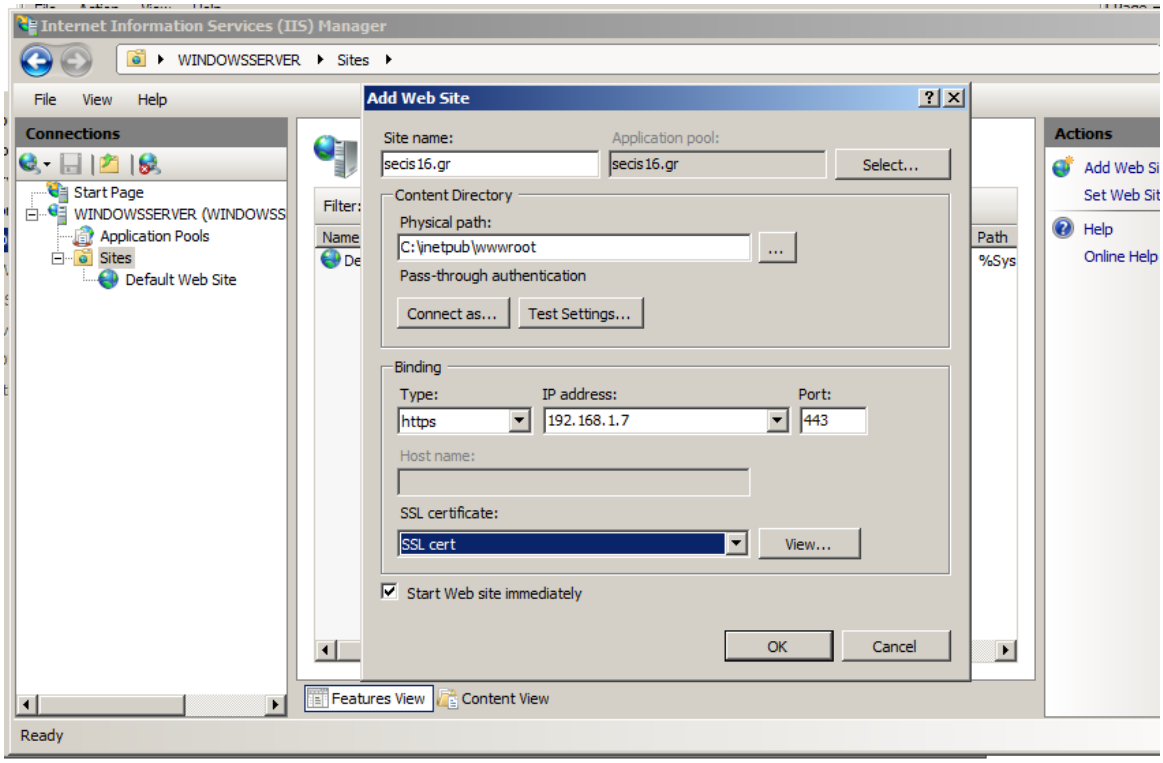


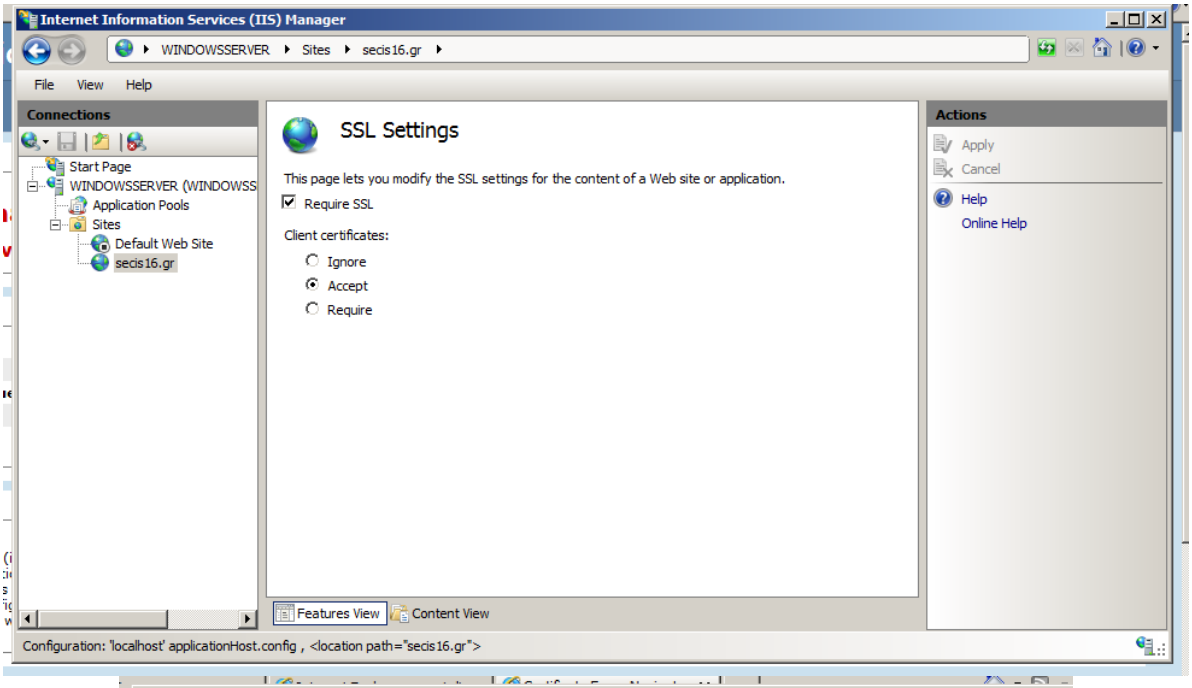
Επίσης δοκιμάσαμε να βάλουμε σελίδα με πρωτόκολλο HTTPS:

Δημιουργία SSL πιστοποιητικου:

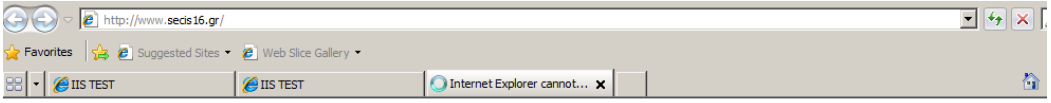


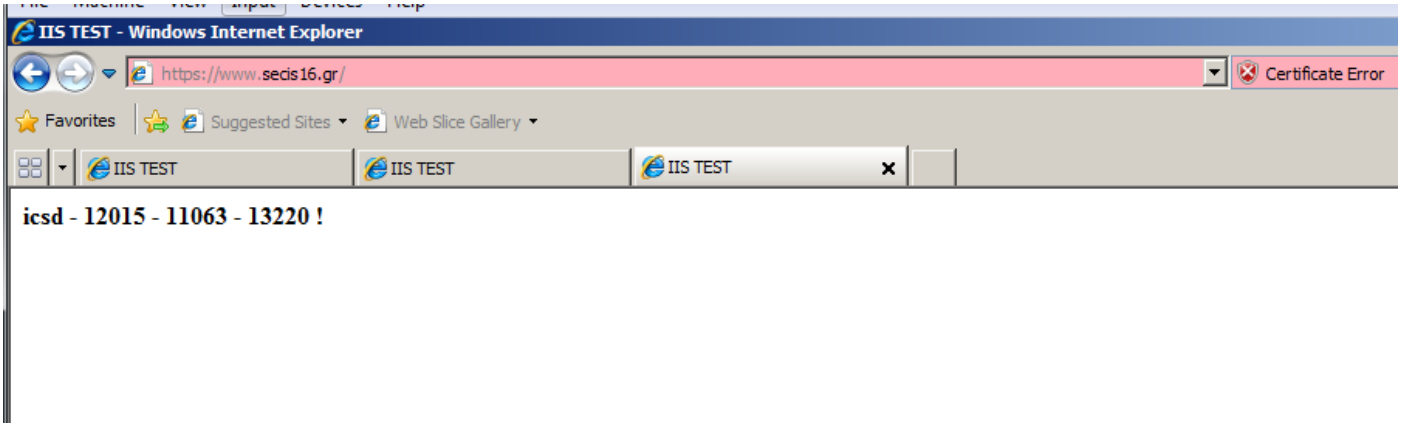
Δημιουργία ιστοσελίδας:



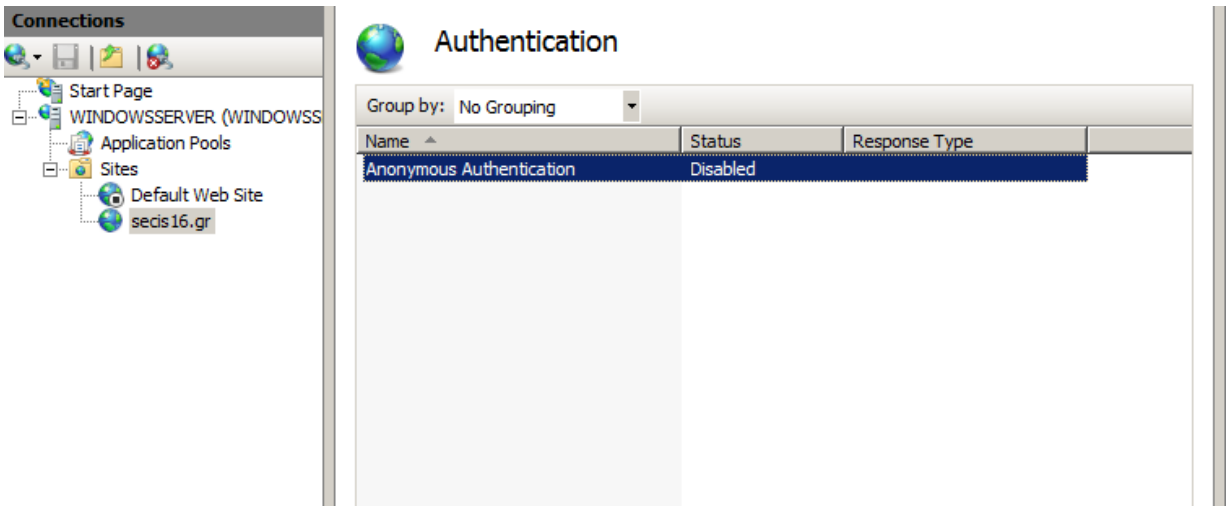


Τώρα γινεται συνδεση στον ιστοτοπο μονο με πρωτοκολλο https:

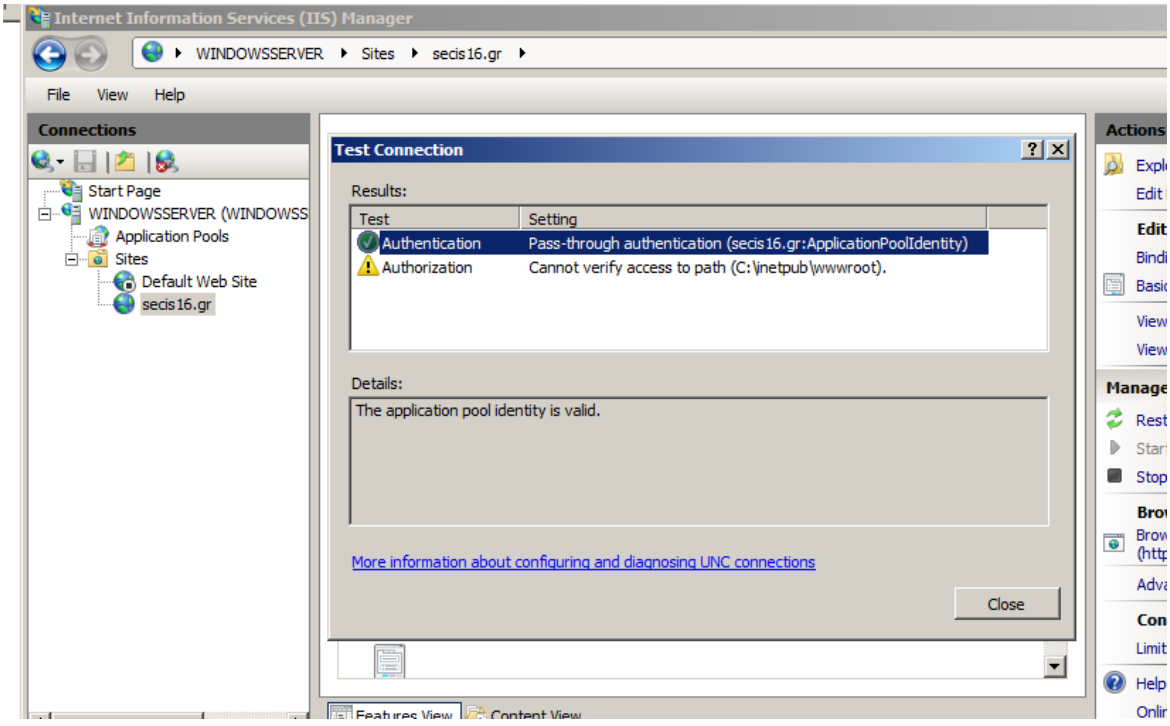


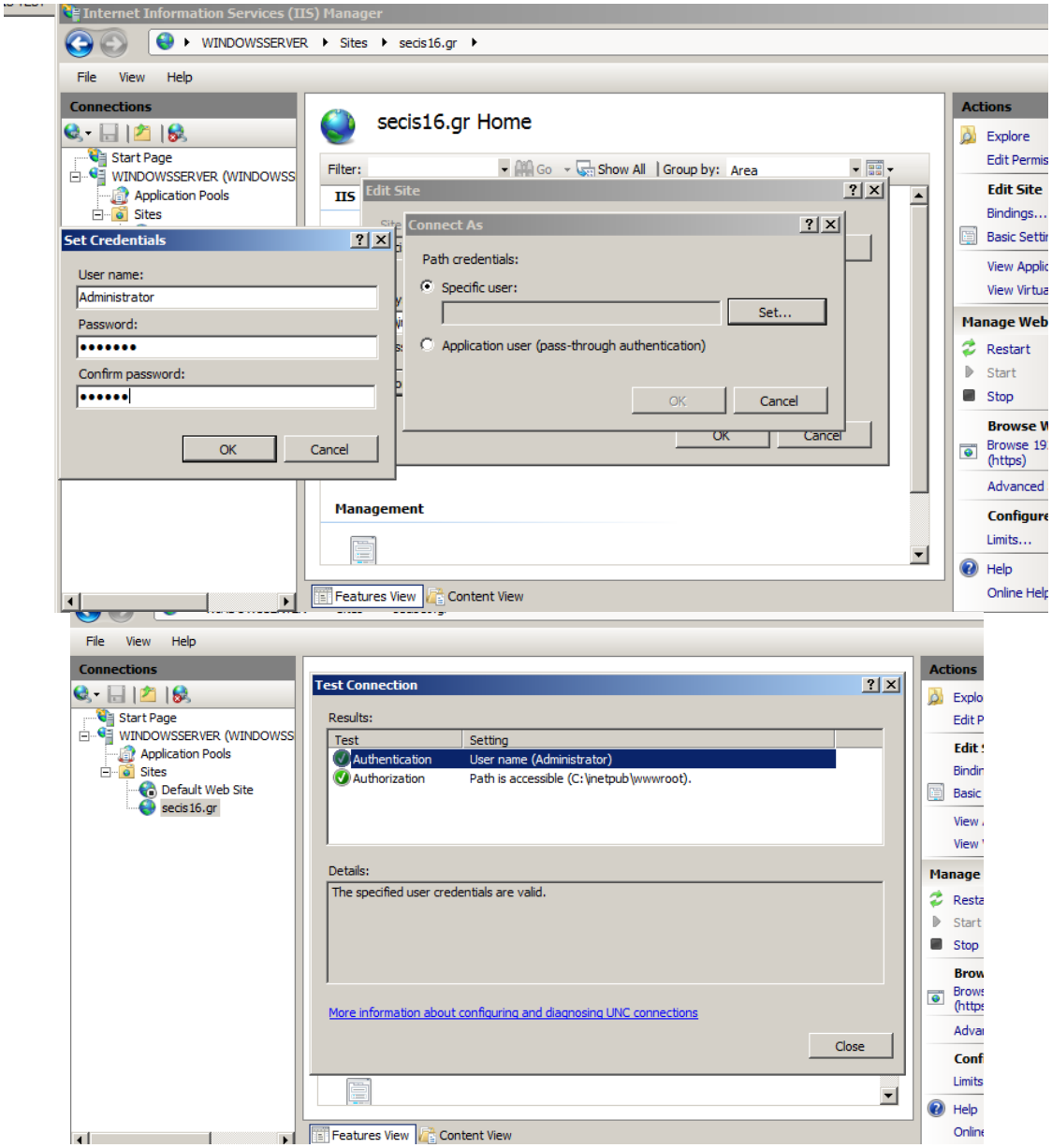


Επίσης δοκιμάσαμε να επιτρέπουμε την σύνδεση μόνο σε domain χρηστές με αυθεντικοποίηση:

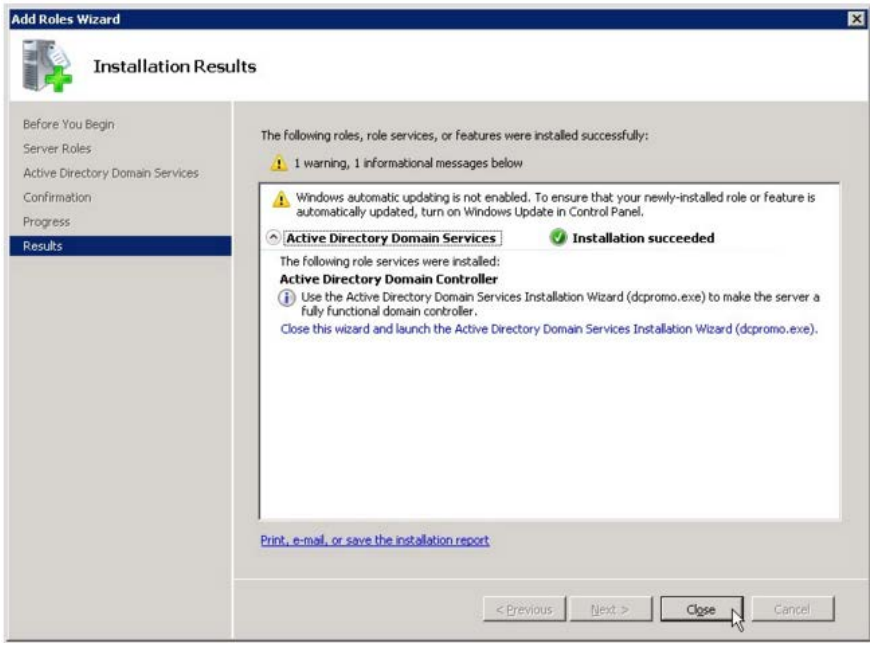


Edit Site -> Test Connection:

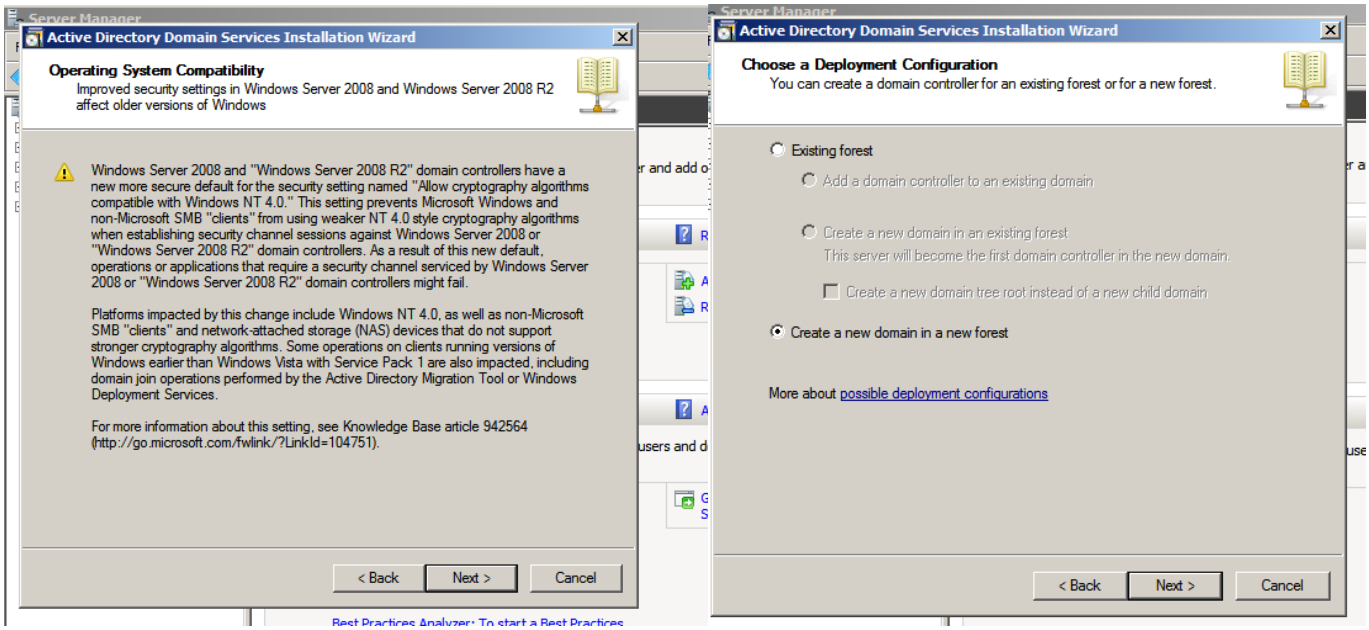


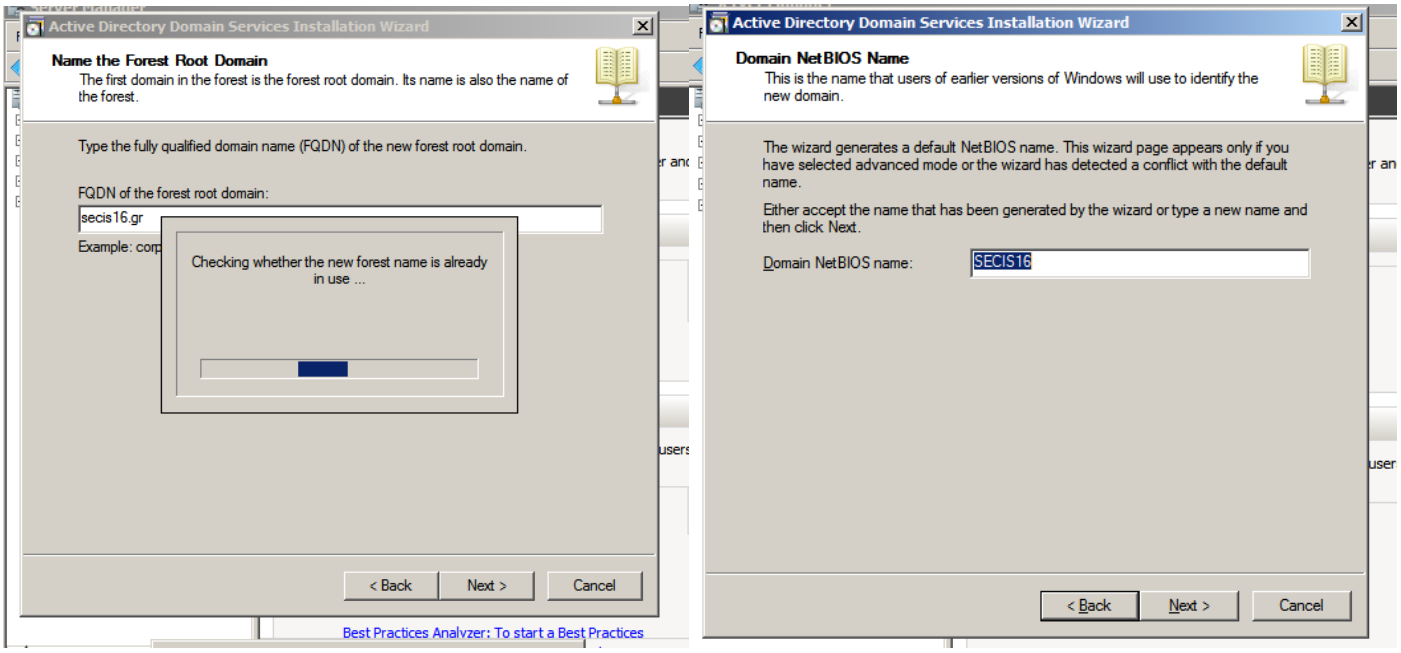


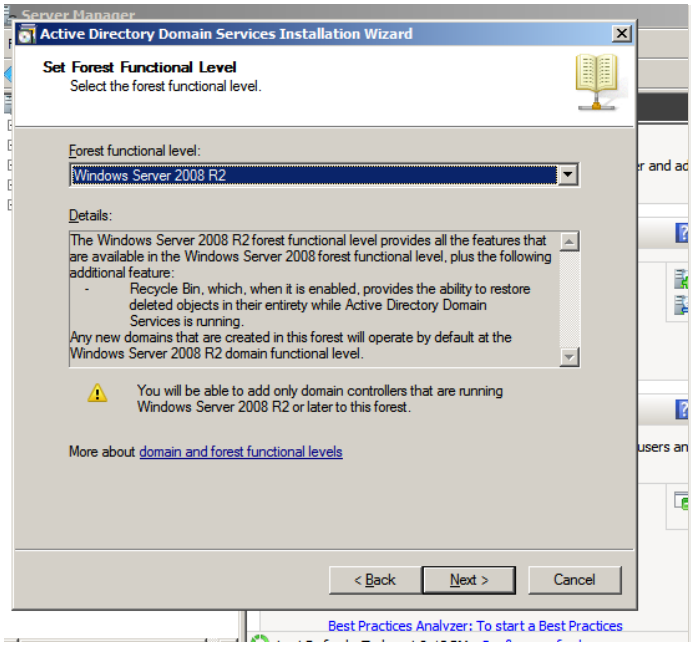
Υπηρεσία Active Directory:

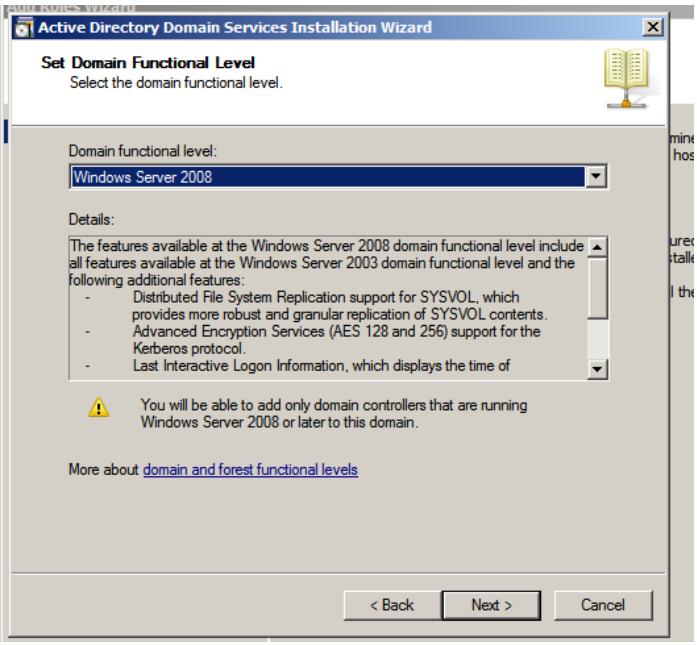


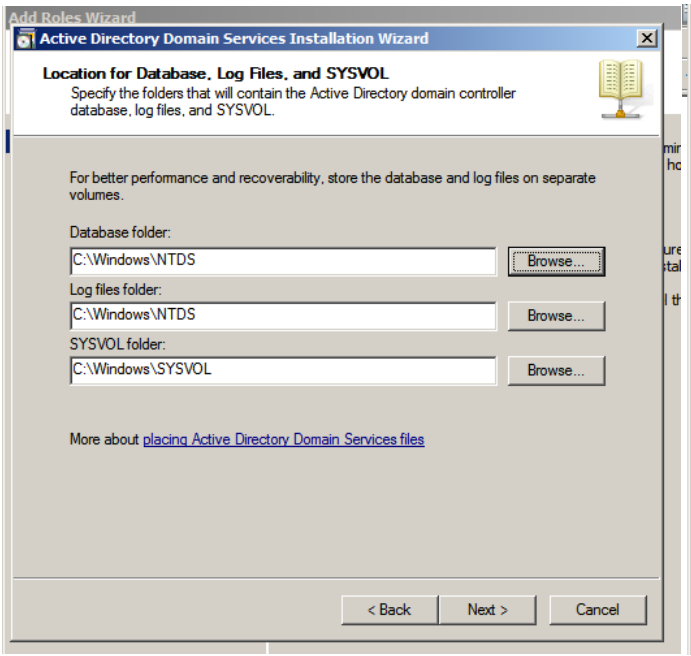

Server Manager
File Action View Help
Server Manager (8R2-64)
Roles
Active Directory Domain Services
Web Server (IIS)
Features
Diagnostics
Configuration
Storage
Active Directory Domain Services
Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.
Summary
This server is not yet running as a domain controller. Run the Active Directory Domain Services Installation Wizard (dcpromo.exe).
Events: None in the last 24 hours
Go to Event Viewer

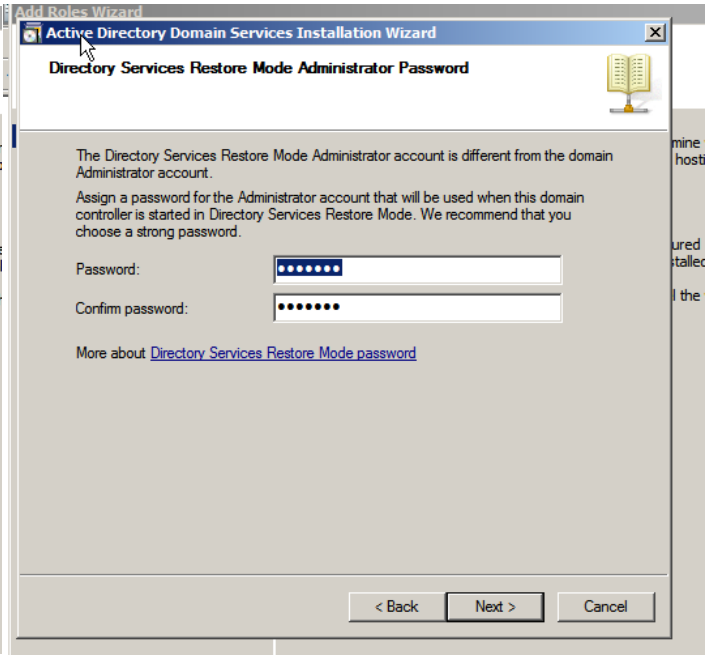

Active Directory Domain Services Installation Wizard
Operating System Compatibility
Improved security settings in Windows Server 2008 and Windows Server 2008 R2 affect older versions of Windows
Windows Server 2008 and "Windows Server 2008 R2" domain controllers have a new more secure default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0." This setting prevents Microsoft Windows and non-Microsoft SMB "clients" from using weaker NT 4.0 style cryptography algorithms when establishing security channel sessions against Windows Server 2008 or "Windows Server 2008 R2" domain controllers. As a result of this new default, operations or applications that require a security channel serviced by Windows Server 2008 or "Windows Server 2008 R2" domain controllers might fail.
Platforms impacted by this change include Windows NT 4.0, as well as non-Microsoft SMB "clients" and network-attached storage (NAS) devices that do not support stronger cryptography algorithms. Some operations on clients running versions of Windows earlier than Windows Vista with Service Pack 1 are also impacted, including domain join operations performed by the Active Directory Migration Tool or Windows Deployment Services.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
< Back
Next >
Cancel
Active Directory Domain Services Installation Wizard
Choose a Deployment Configuration
You can create a domain controller for an existing forest or for a new forest.
Existing forest
Add a domain controller to an existing domain
Create a new domain in an existing forest
This server will become the first domain controller in the new domain.
Create a new domain tree root instead of a new child domain
Create a new domain in a new forest
More about possible deployment configurations
< Back
Next >
Cancel


Active Directory Domain Services Installation Wizard
Name the Forest Root Domain
The first domain in the forest is the forest root domain. Its name is also the name of the forest.
Type the fully qualified domain name (FQDN) of the new forest root domain.
FQDN of the forest root domain:
secis16.gr
Example: corp
Checking whether the new forest name is already in use ...
< Back
Next >
Cancel
Best Practices Analyzer: To start a Best Practices
Active Directory Domain Services Installation Wizard
Domain NetBIOS Name
This is the name that users of earlier versions of Windows will use to identify the new domain.
The wizard generates a default NetBIOS name. This wizard page appears only if you have selected advanced mode or the wizard has detected a conflict with the default name.
Either accept the name that has been generated by the wizard or type a new name and then click Next.
Domain NetBIOS name:
SECIS16
< Back
Next >
Cancel

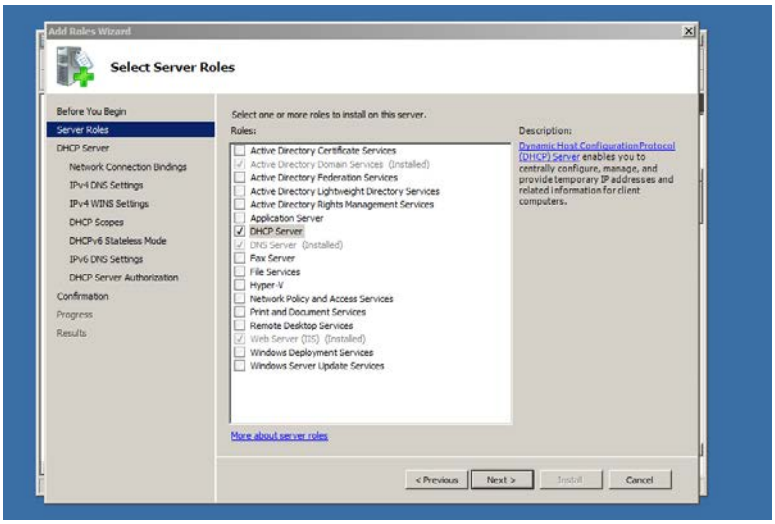


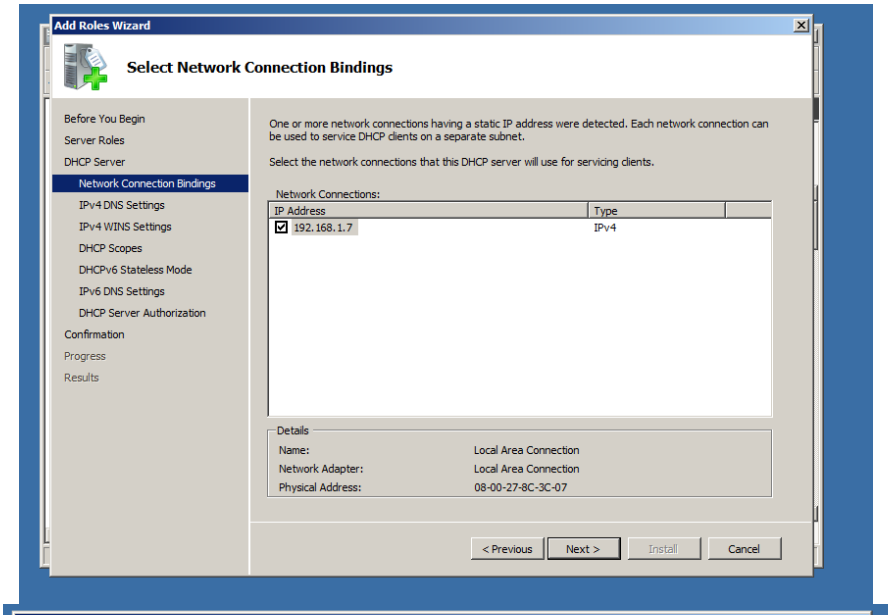


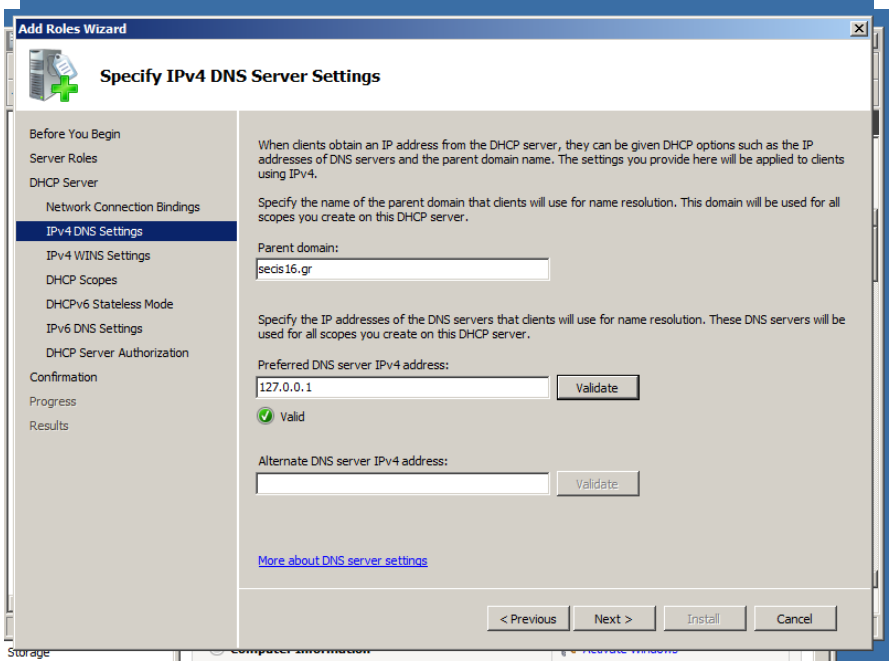


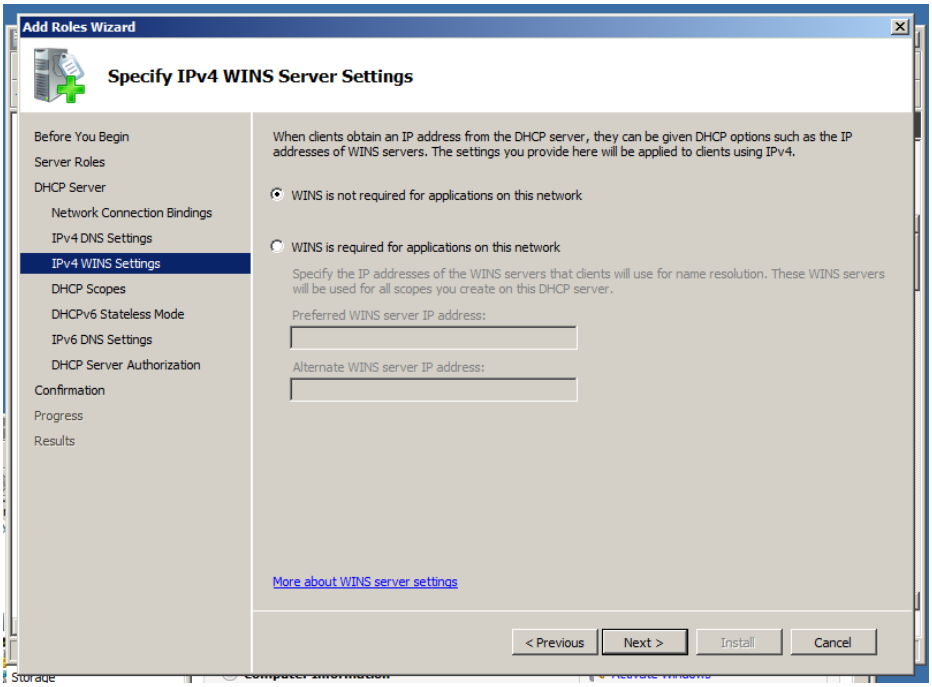


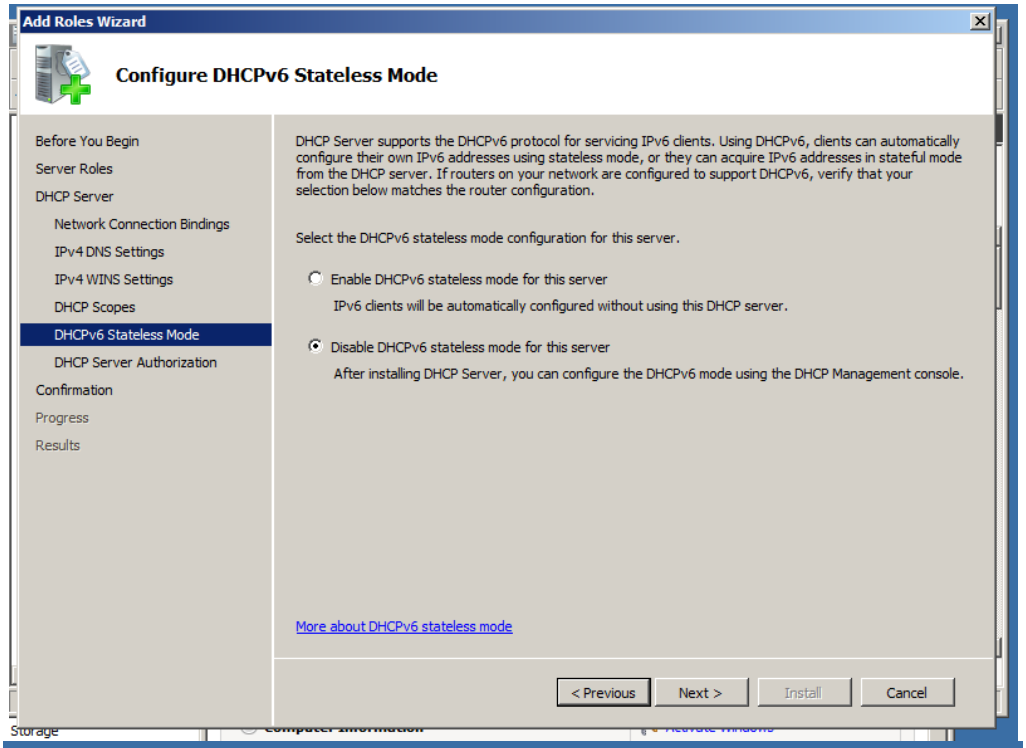
Υπηρεσία DHCP:

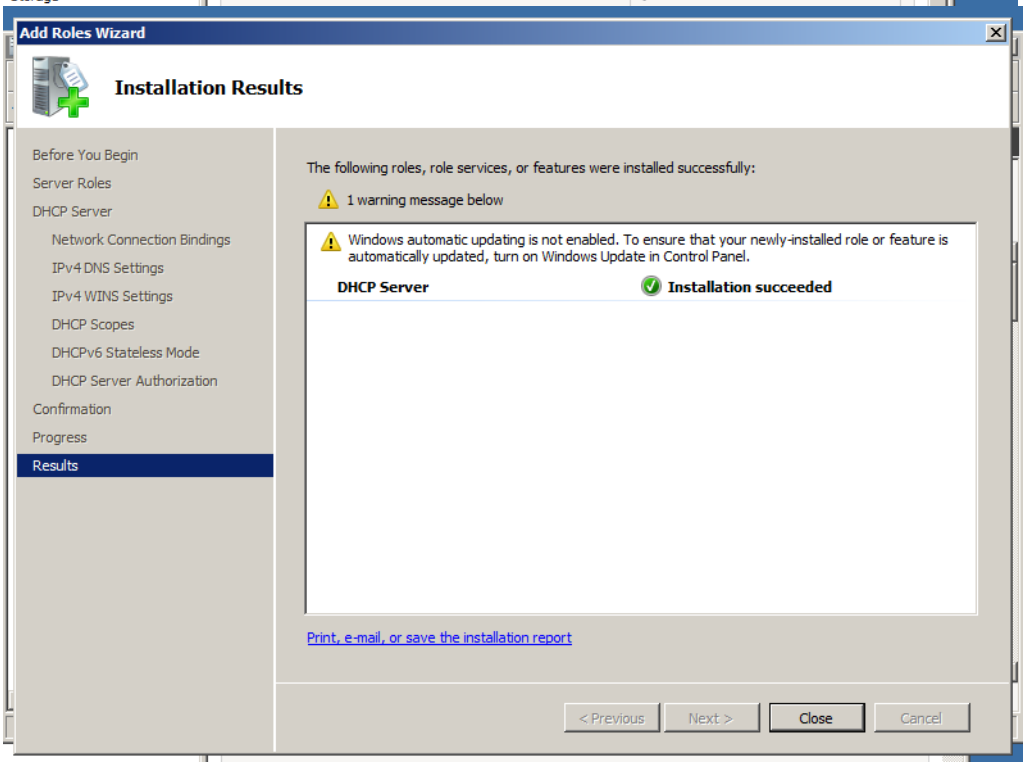



Add Roles Wizard
Select Network Connection Bindings
Before You Begin
Server Roles
DHCP Server
Network Connection Bindings
IPv4 DNS Settings
IPv4 WINS Settings
DHCP Scopes
DHCPv6 Stateless Mode
IPv6 DNS Settings
DHCP Server Authorization
Confirmation
Progress
Results
One or more network connections having a static IP address were detected. Each network connection can be used to service DHCP clients on a separate subnet.
Select the network connections that this DHCP server will use for servicing clients.
Network Connections:
IP Address
Type
192.168.1.7
IPv4
Details
Name:
Local Area Connection
Network Adapter:
Local Area Connection
Physical Address:
08-00-27-8C-3C-07
< Previous
Next >
Install
Cancel

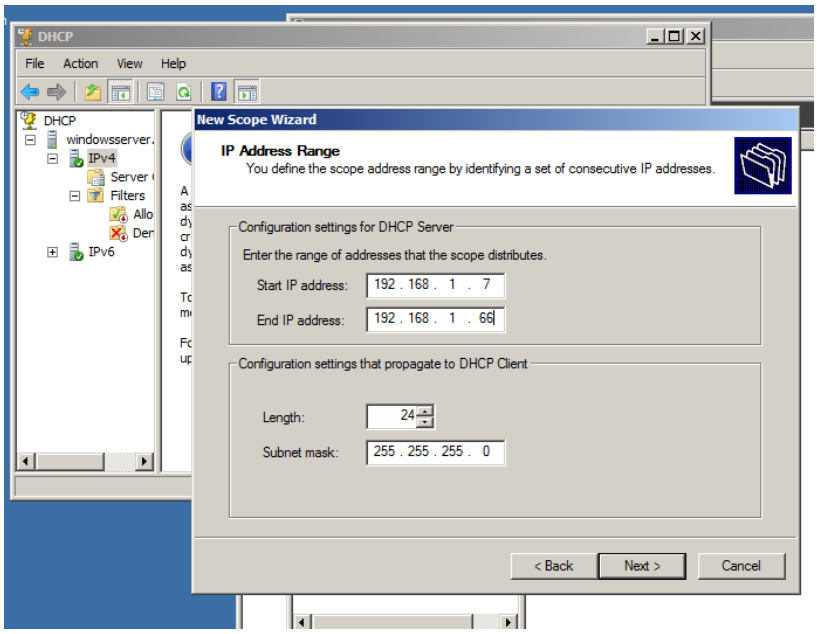

Add Roles Wizard
Specify IPv4 DNS Server Settings
Before You Begin
Server Roles
DHCP Server
Network Connection Bindings
IPv4 DNS Settings
IPv4 WINS Settings
DHCP Scopes
DHCPv6 Stateless Mode
IPv6 DNS Settings
DHCP Server Authorization
Confirmation
Progress
Results
When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of DNS servers and the parent domain name. The settings you provide here will be applied to clients using IPv4.
Specify the name of the parent domain that clients will use for name resolution. This domain will be used for all scopes you create on this DHCP server.
Parent domain:
secis16.gr
Specify the IP addresses of the DNS servers that clients will use for name resolution. These DNS servers will be used for all scopes you create on this DHCP server.
Preferred DNS server IPv4 address:
127.0.0.1
Validate
Valid
Alternate DNS server IPv4 address:
Validate
More about DNS server settings
< Previous
Next >
Install
Cancel
Storage


Add Roles Wizard
Specify IPv4 WINS Server Settings
Before You Begin
Server Roles
DHCP Server
Network Connection Bindings
IPv4 DNS Settings
IPv4 WINS Settings
DHCP Scopes
DHCPv6 Stateless Mode
IPv6 DNS Settings
DHCP Server Authorization
Confirmation
Progress
Results
When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of WINS servers. The settings you provide here will be applied to clients using IPv4.
WINS is not required for applications on this network
WINS is required for applications on this network
Specify the IP addresses of the WINS servers that clients will use for name resolution. These WINS servers will be used for all scopes you create on this DHCP server.
Preferred WINS server IP address:
Alternate WINS server IP address:
More about WINS server settings
< Previous
Next >
Install
Cancel
Storage

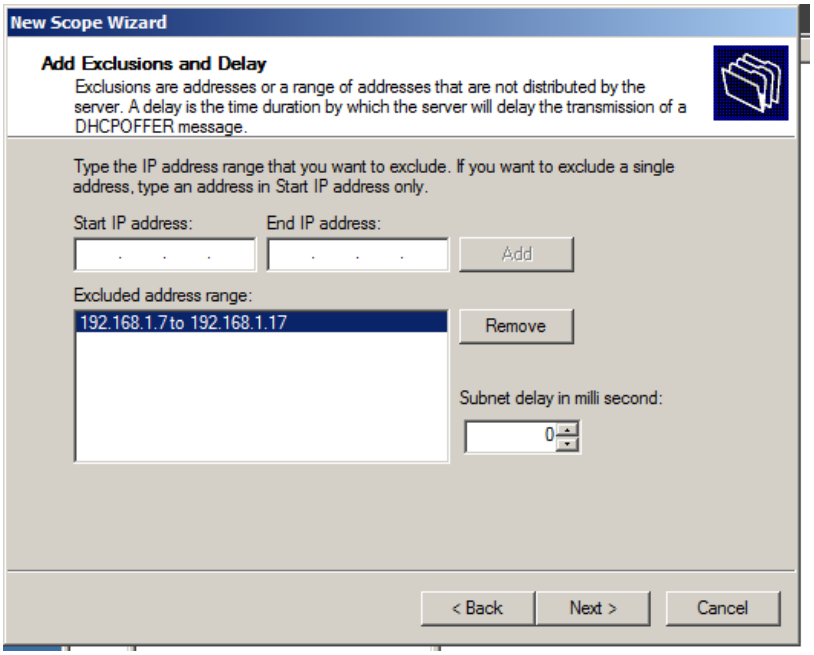

Add Roles Wizard
Configure DHCPv6 Stateless Mode
Before You Begin
Server Roles
DHCP Server
Network Connection Bindings
IPv4 DNS Settings
IPv4 WINS Settings
DHCP Scopes
DHCPv6 Stateless Mode
DHCP Server Authorization
Confirmation
Progress
Results
DHCP Server supports the DHCPv6 protocol for servicing IPv6 clients. Using DHCPv6, clients can automatically configure their own IPv6 addresses using stateless mode, or they can acquire IPv6 addresses in stateful mode from the DHCP server. If routers on your network are configured to support DHCPv6, verify that your selection below matches the router configuration.
Select the DHCPv6 stateless mode configuration for this server.
Enable DHCPv6 stateless mode for this server
IPv6 clients will be automatically configured without using this DHCP server.
Disable DHCPv6 stateless mode for this server
After installing DHCP Server, you can configure the DHCPv6 mode using the DHCP Management console.
More about DHCPv6 stateless mode
< Previous
Next >
Install
Cancel

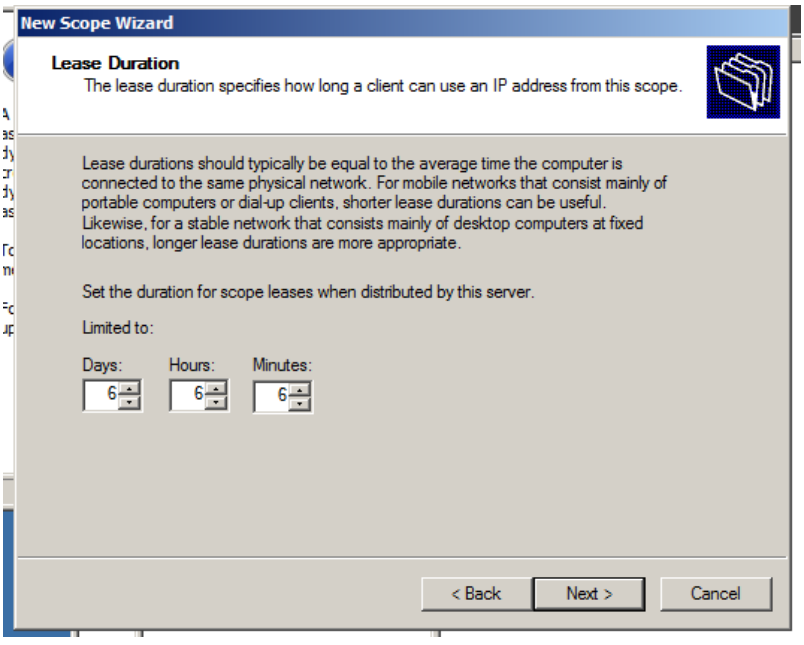

Add Roles Wizard
Installation Results
Before You Begin
Server Roles
DHCP Server
Network Connection Bindings
IPv4 DNS Settings
IPv4 WINS Settings
DHCP Scopes
DHCPv6 Stateless Mode
DHCP Server Authorization
Confirmation
Progress
Results
The following roles, role services, or features were installed successfully:
1 warning message below
Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update in Control Panel.
DHCP Server
Installation succeeded
Print, e-mail, or save the installation report
< Previous
Next >
Close
Cancel

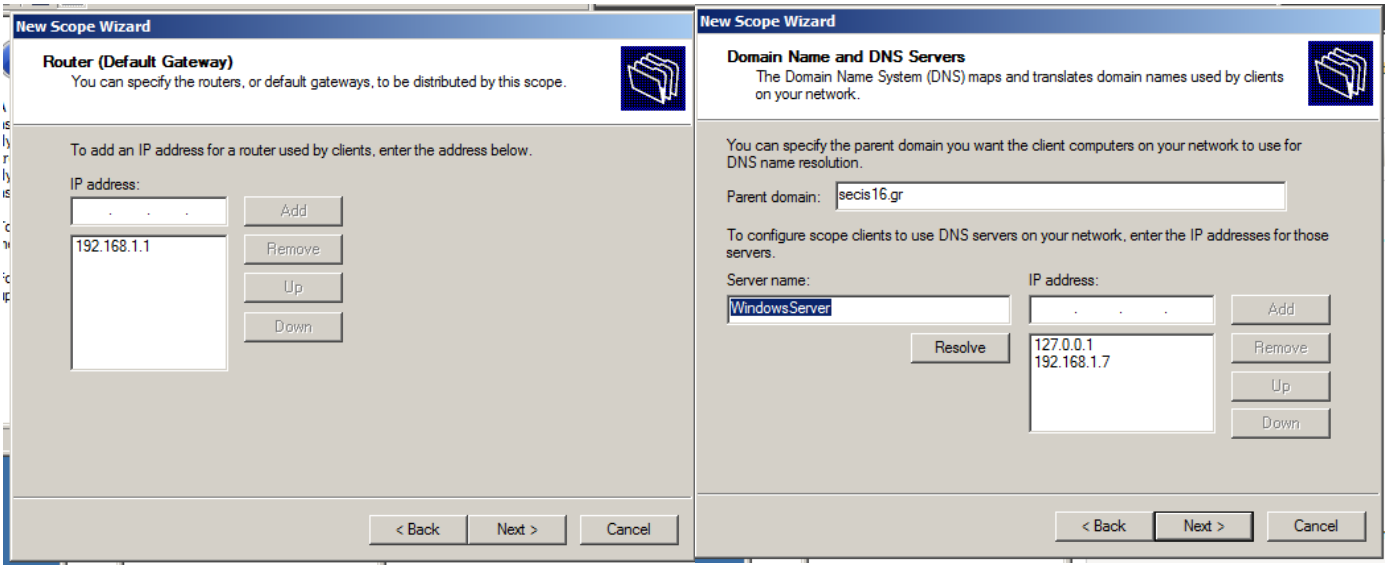
Δέσμευση Διευθύνσεων 7 – 66:



Αποκλεισμός διευθυνσιοδότησης διευθύνσεων 7 -17:

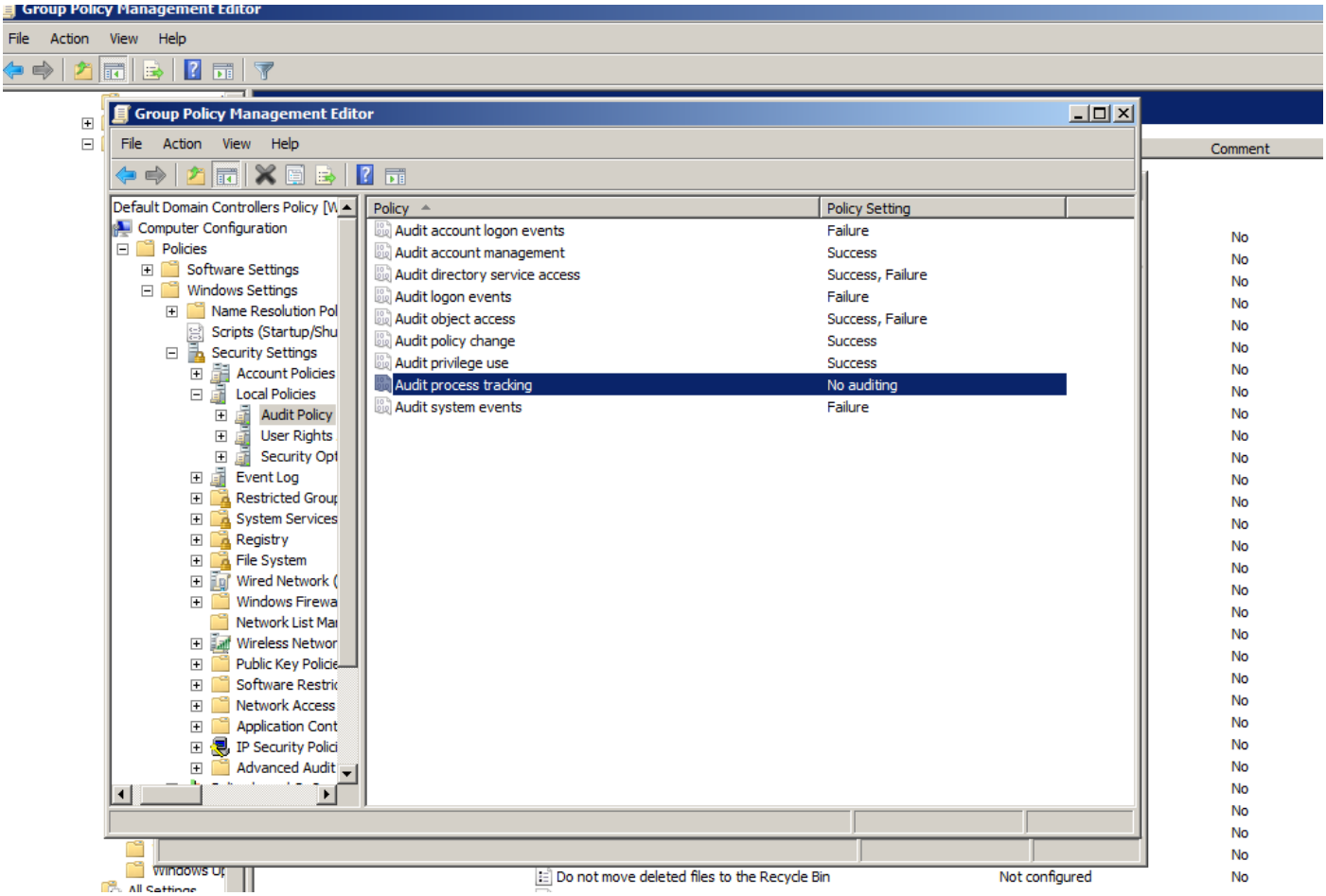




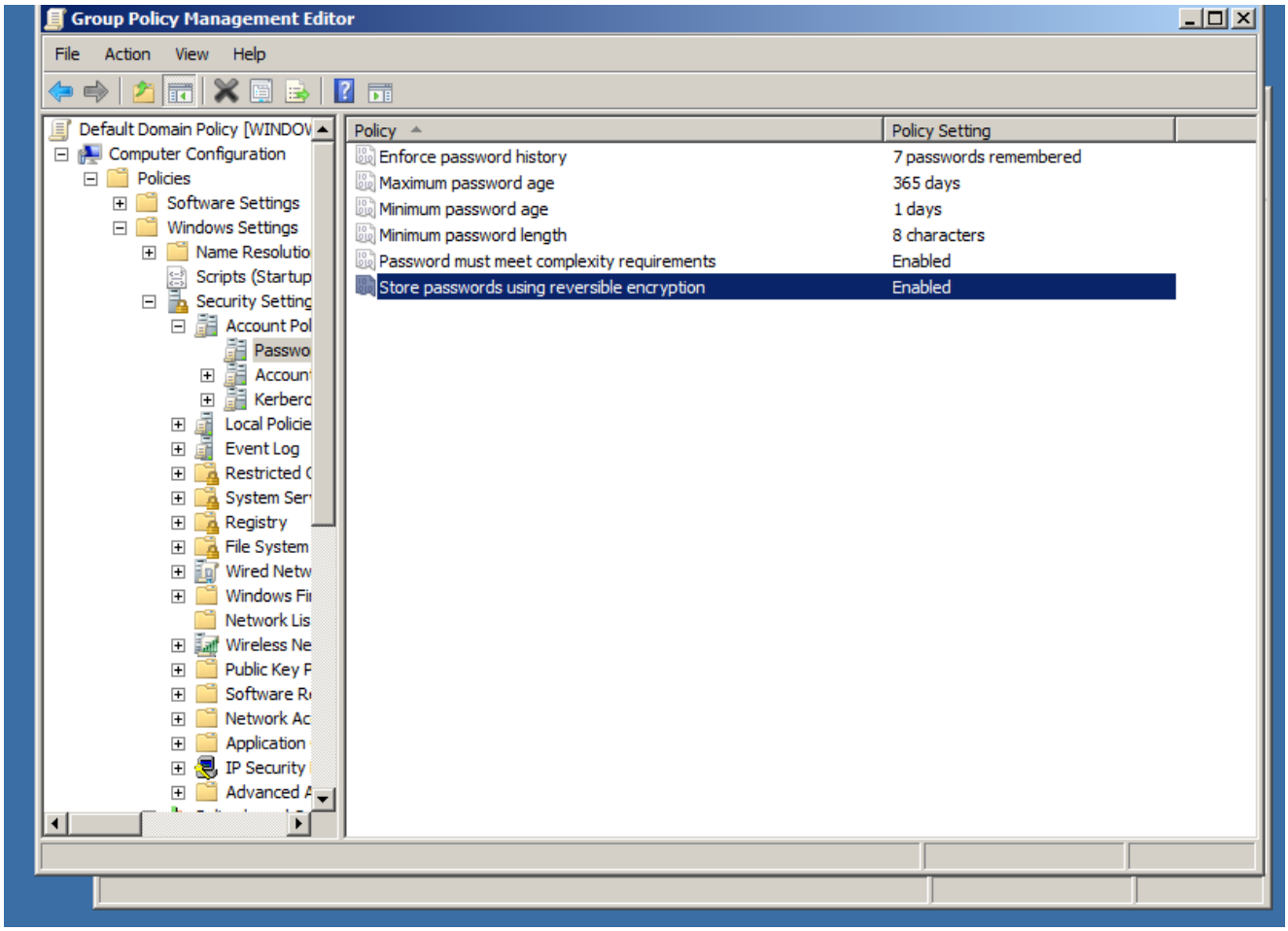


B4., password policies, lockout policies:

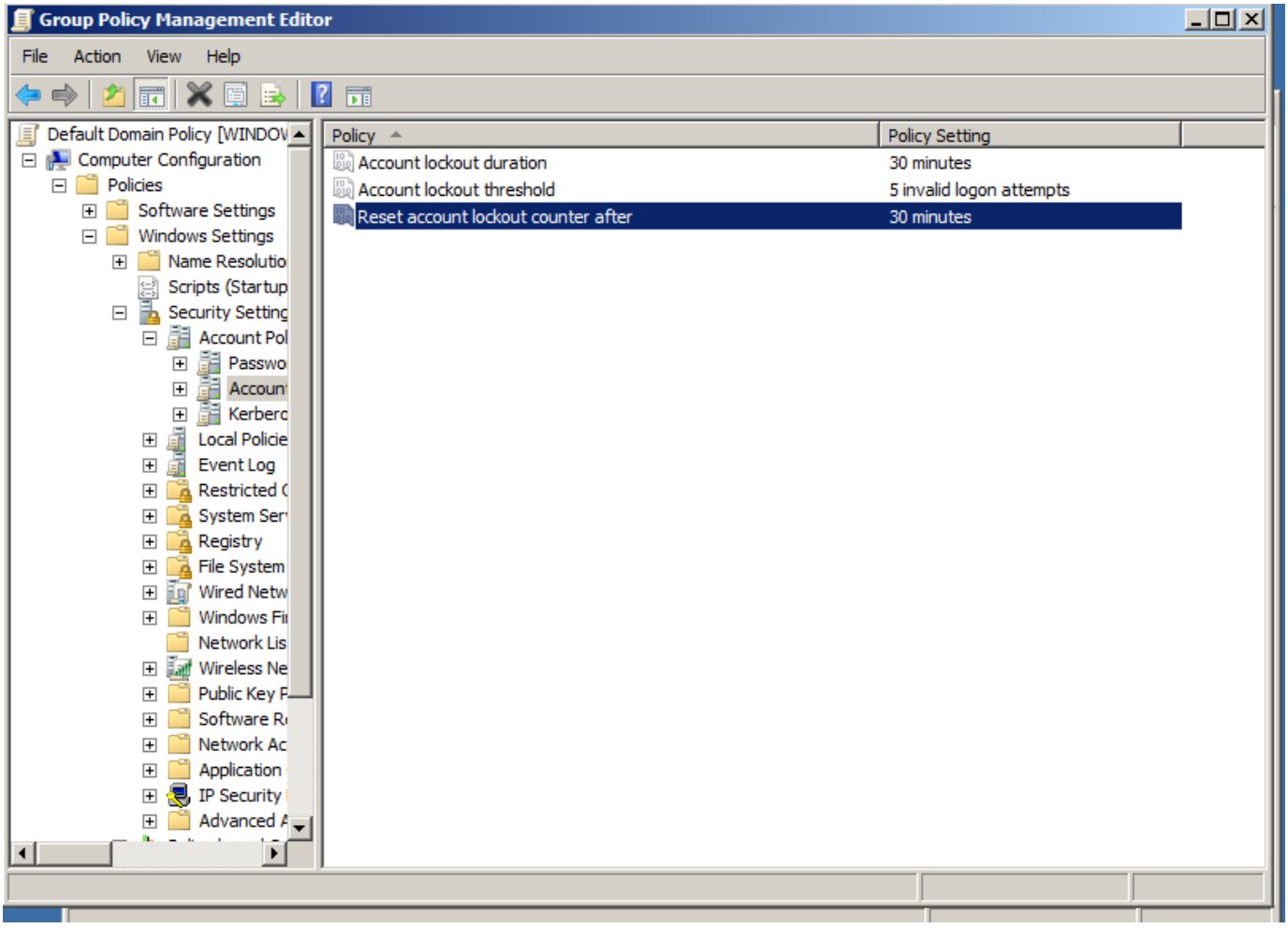
Ρύθμιση Audit Policies (για προβολή στο event viewer):



Ρυθμιση Password Policies:

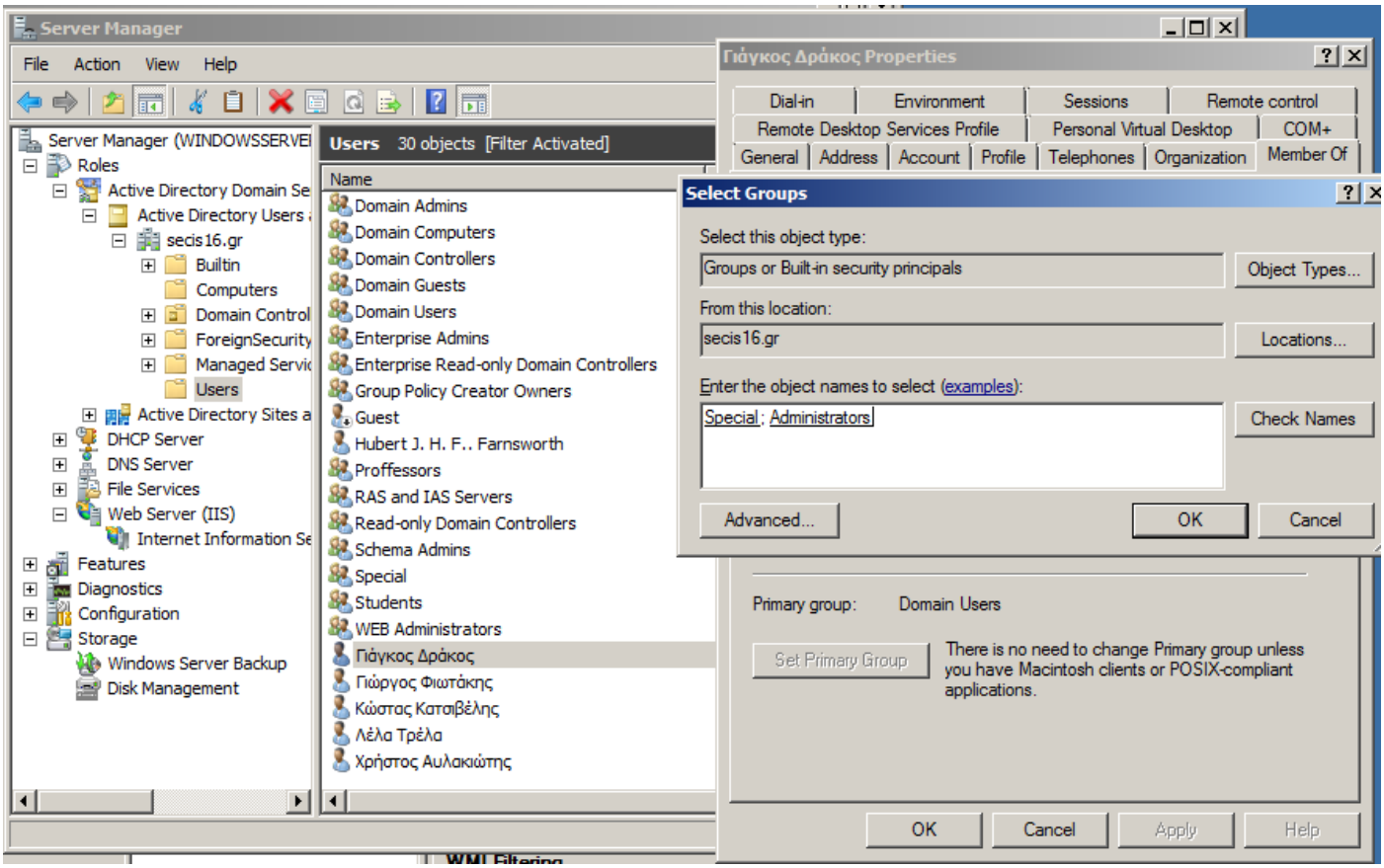


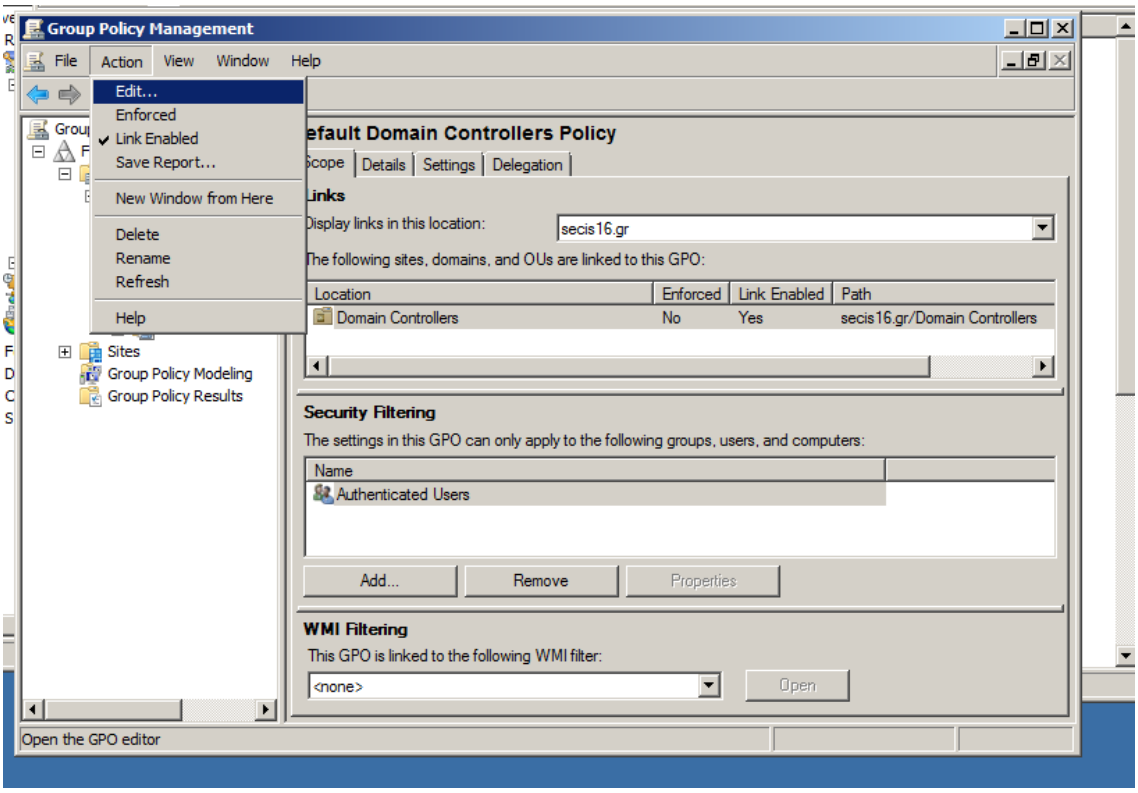
Ρύθμιση Lockout Policies:



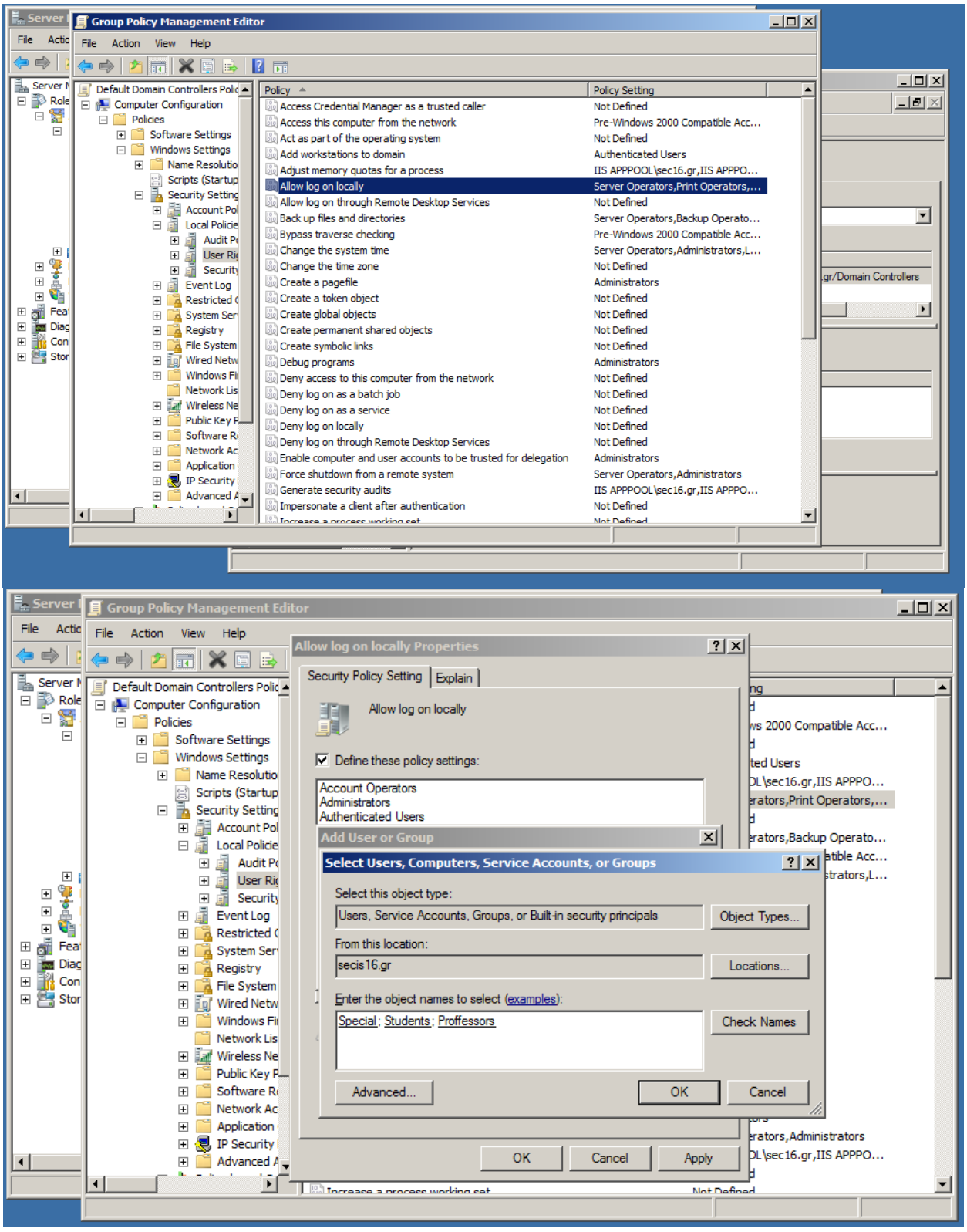
B5.

Δημιουργία ομάδων και χρηστών: (Ομάδες: Special, WEB Administrators):



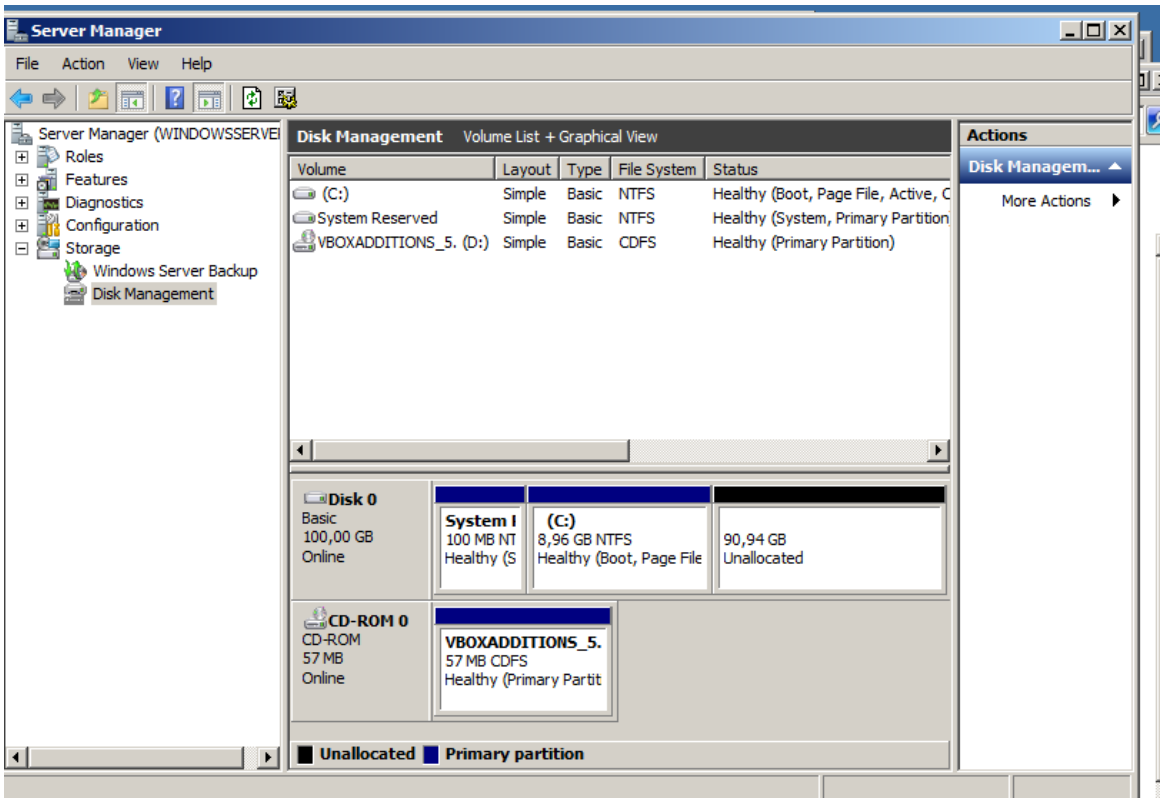


Για να επιτρέψουμε να συνδέονται οι χρηστές τοπικά:

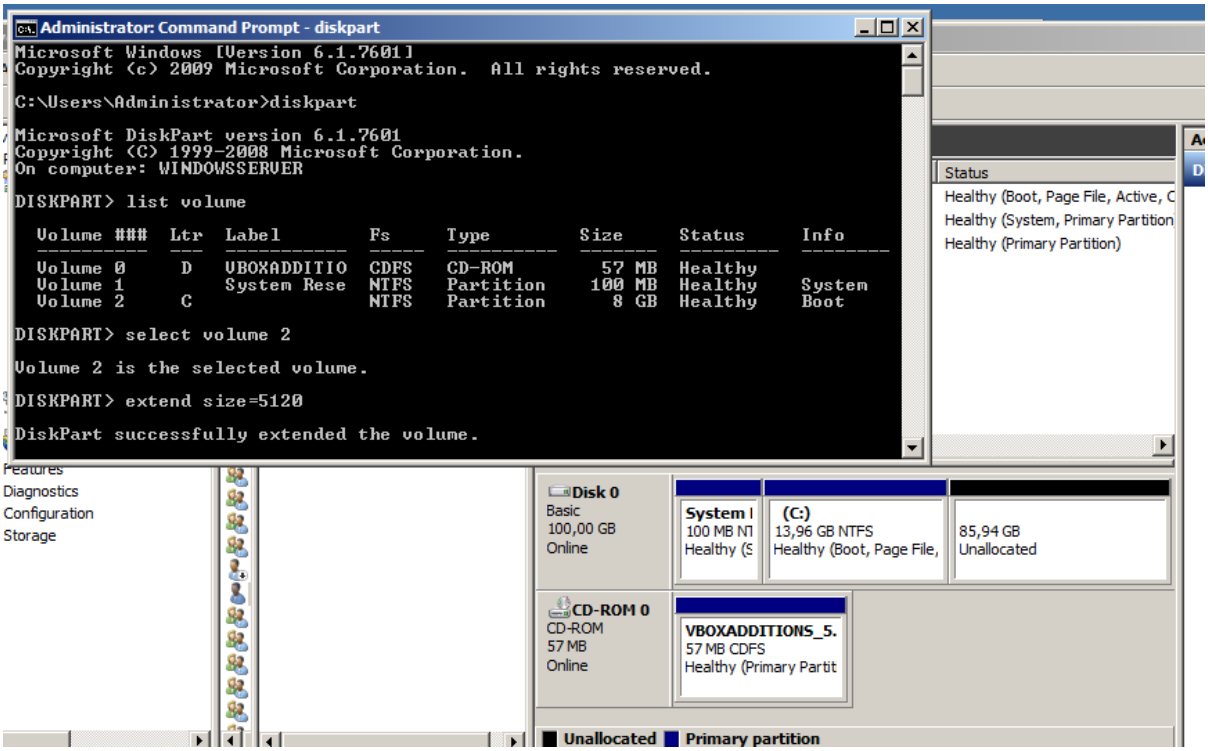


Δημιουργία Partition στον δίσκο για τα HOME_FOLDERS: (possible error)

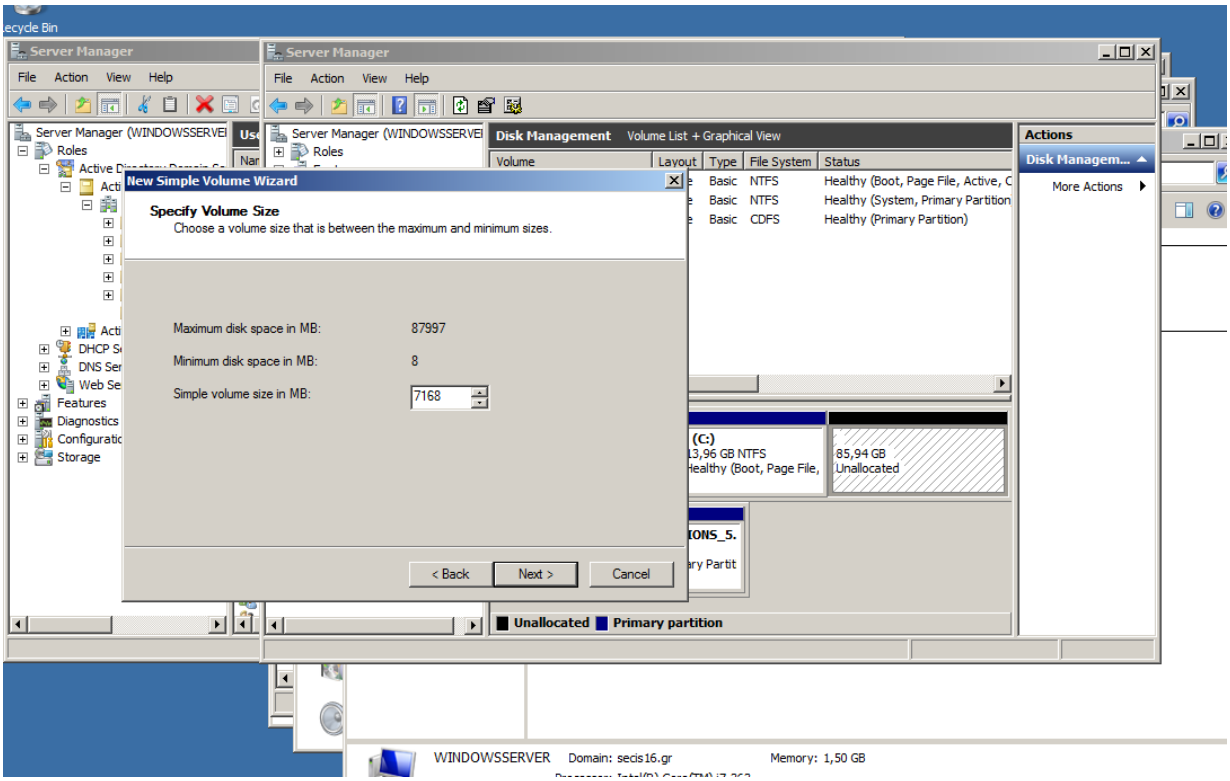
Στην αρχή ο δίσκος C είναι ενιαία μονάδα, πατήσαμε δεξί κλικ -> Shrink volume

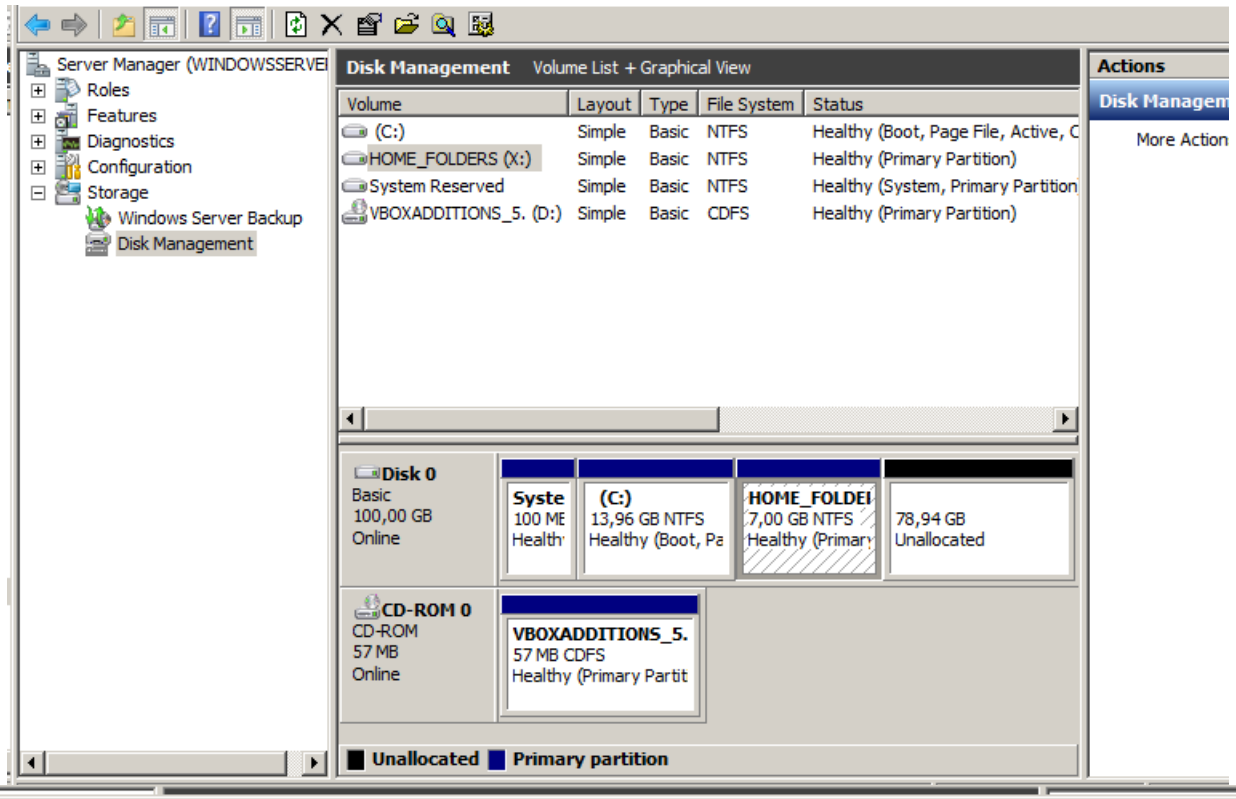


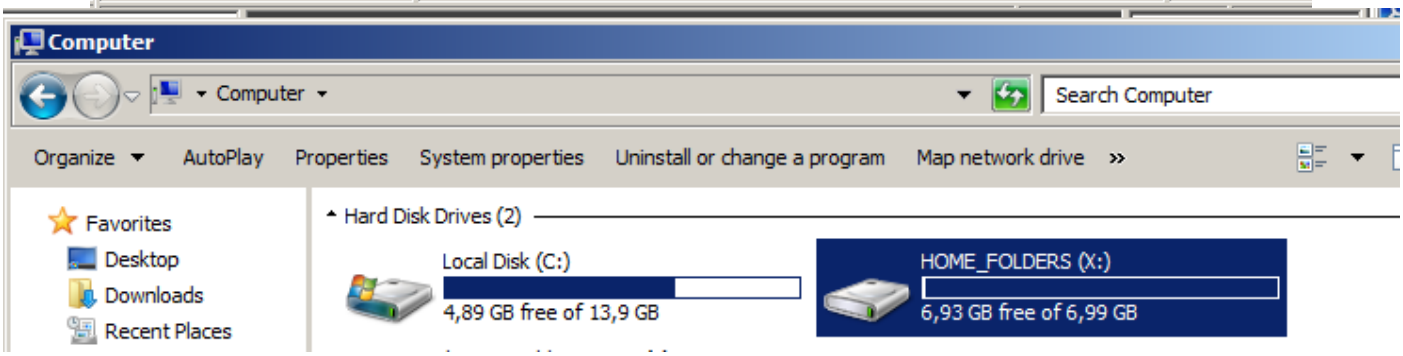
Έπειτα όμως έπρεπε να βάλουμε παραπάνω χώρο στον C γιατί δεν είχε άλλο ελεύθερο αφού συγκεντρώσαμε μόνο τον χρησιμοποιημένο. Έτσι του δώσαμε άλλα 5Gb με το diskpart των Windows



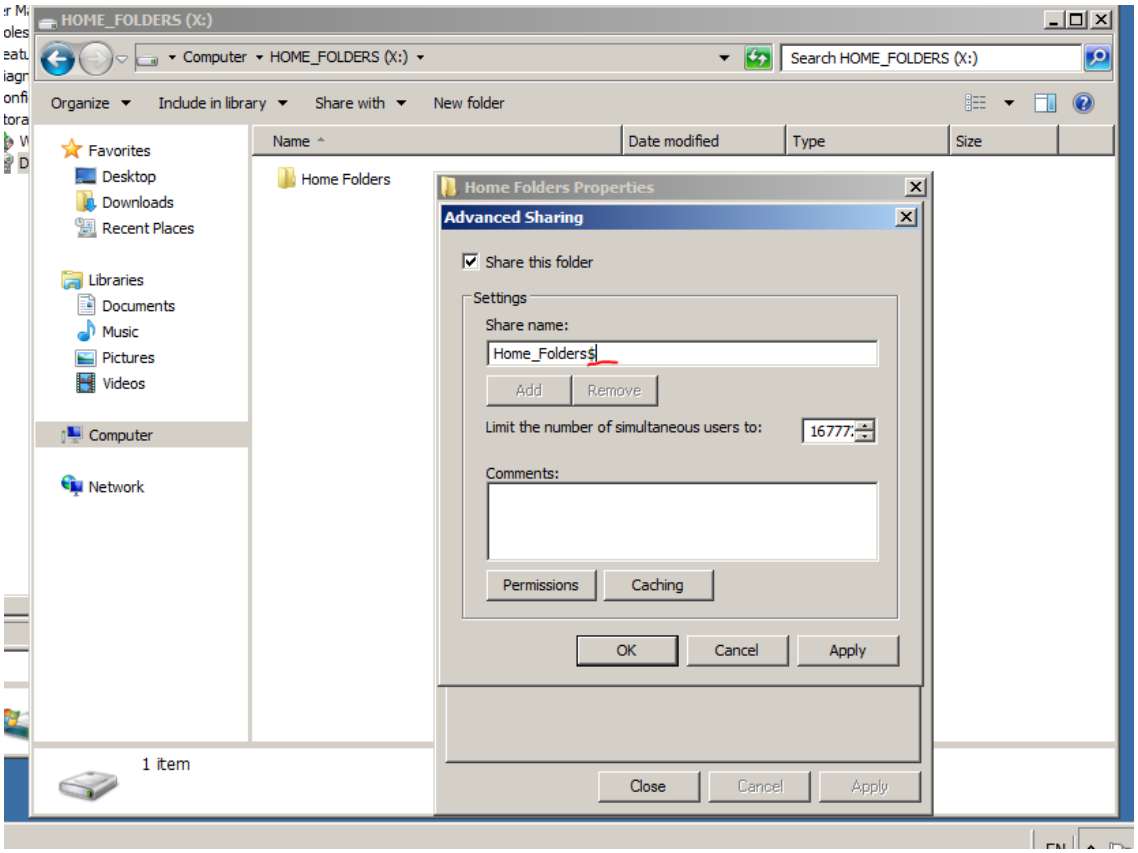
Στη συνεχεία δεσμεύσαμε από τον Αχρησιμοποίητο χώρο το Partition για τα Home Folders



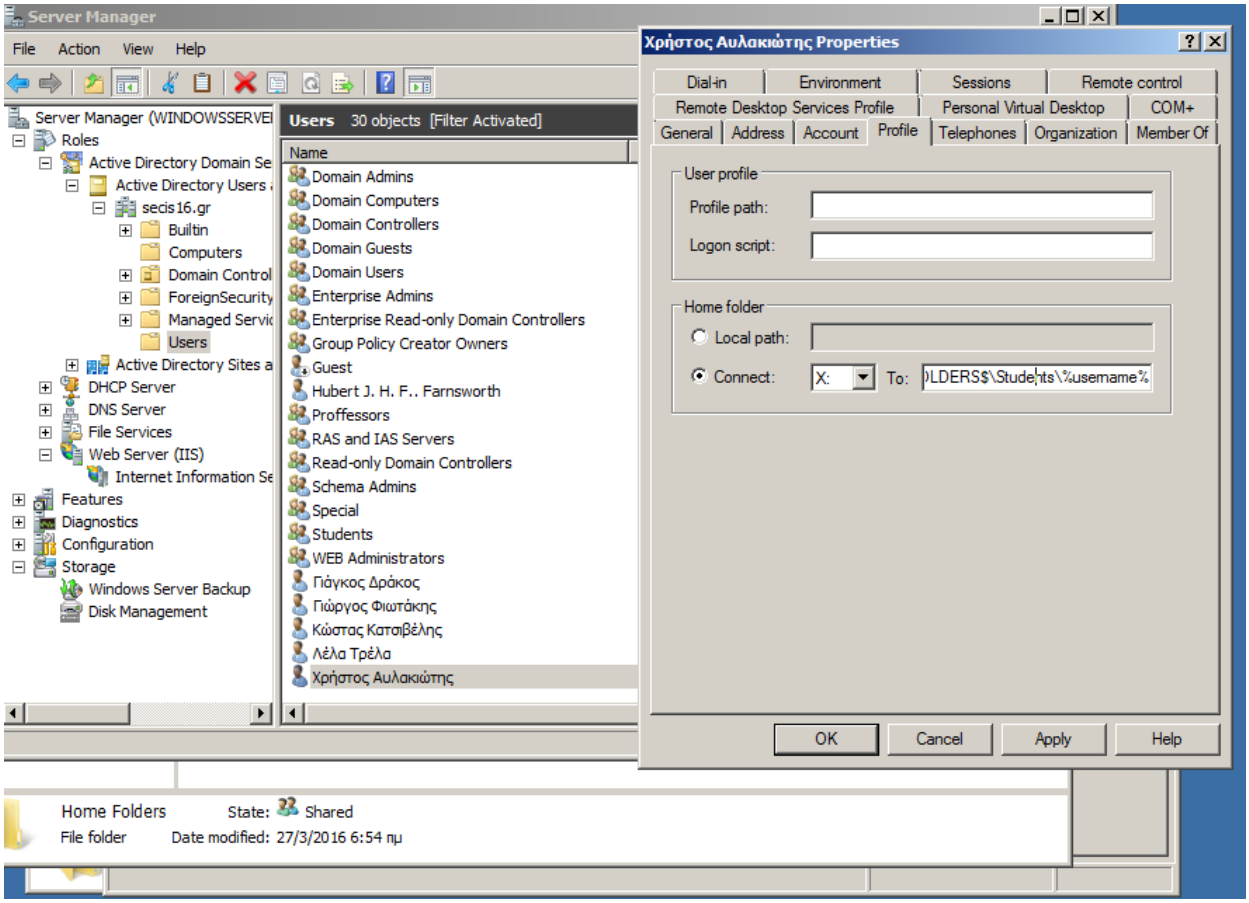




Έπειτα δημιουργήσαμε ένα αρχείο μέσα και το κάναμε sharing (το $ για να μη φαίνεται το path)

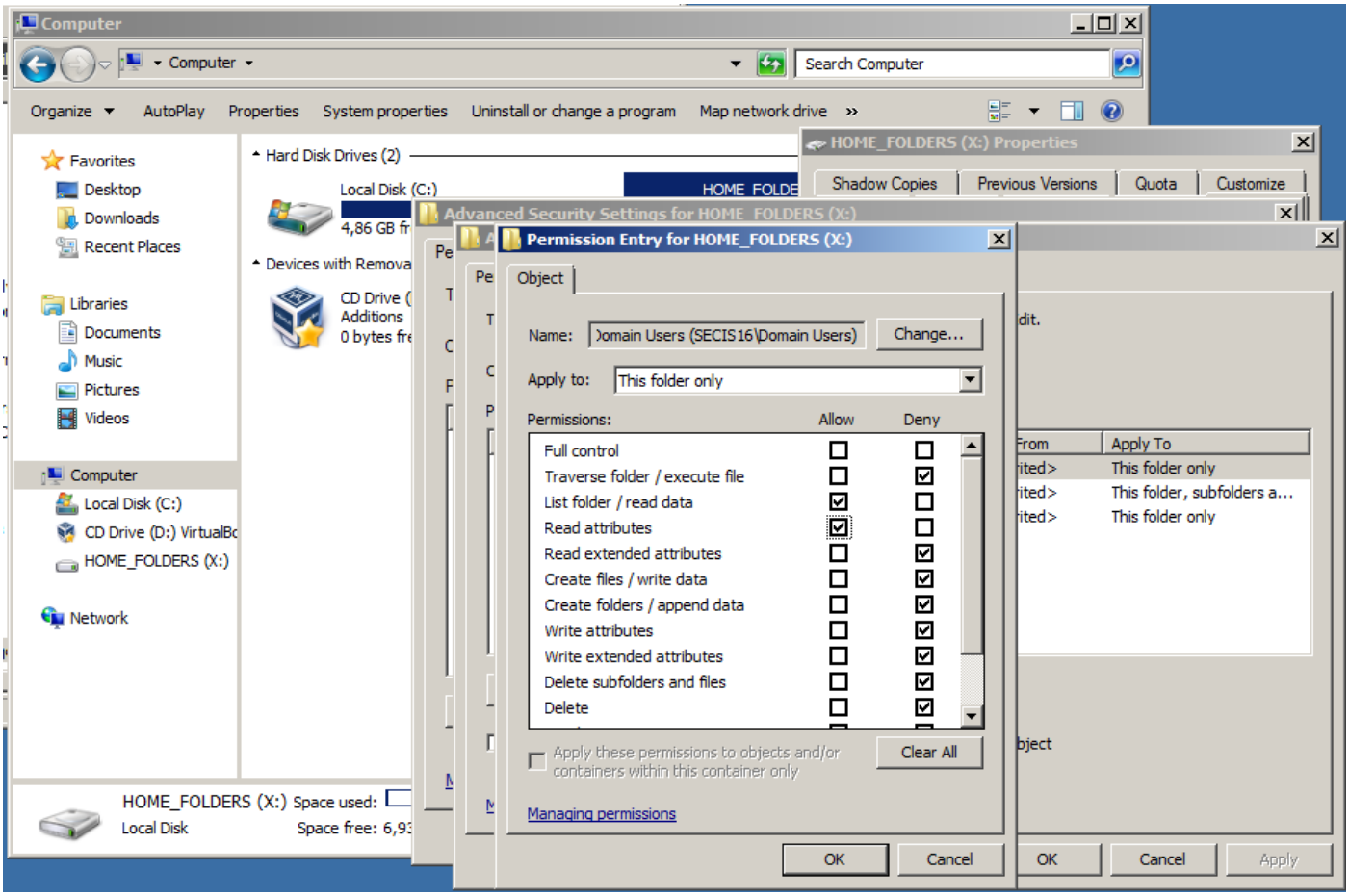


Έπειτα ορίσαμε στην υπηρεσία Active Directory το home folder κάθε χρηστή:

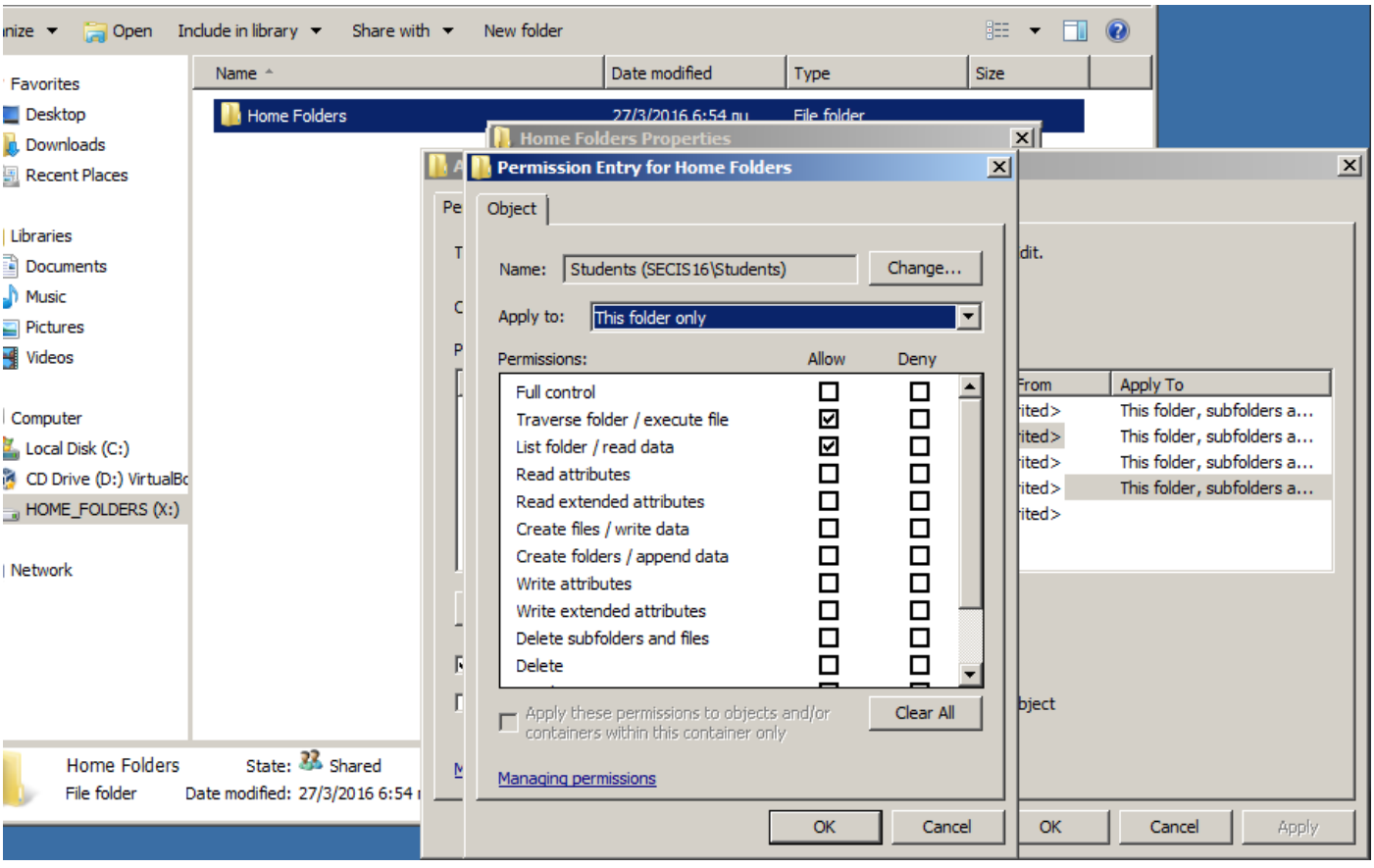


Τέλος ρυθμίσαμε τα permissions για κάθε φάκελο ώστε ο κάθε user να χει πρόσβαση μόνο στο δικό του directory

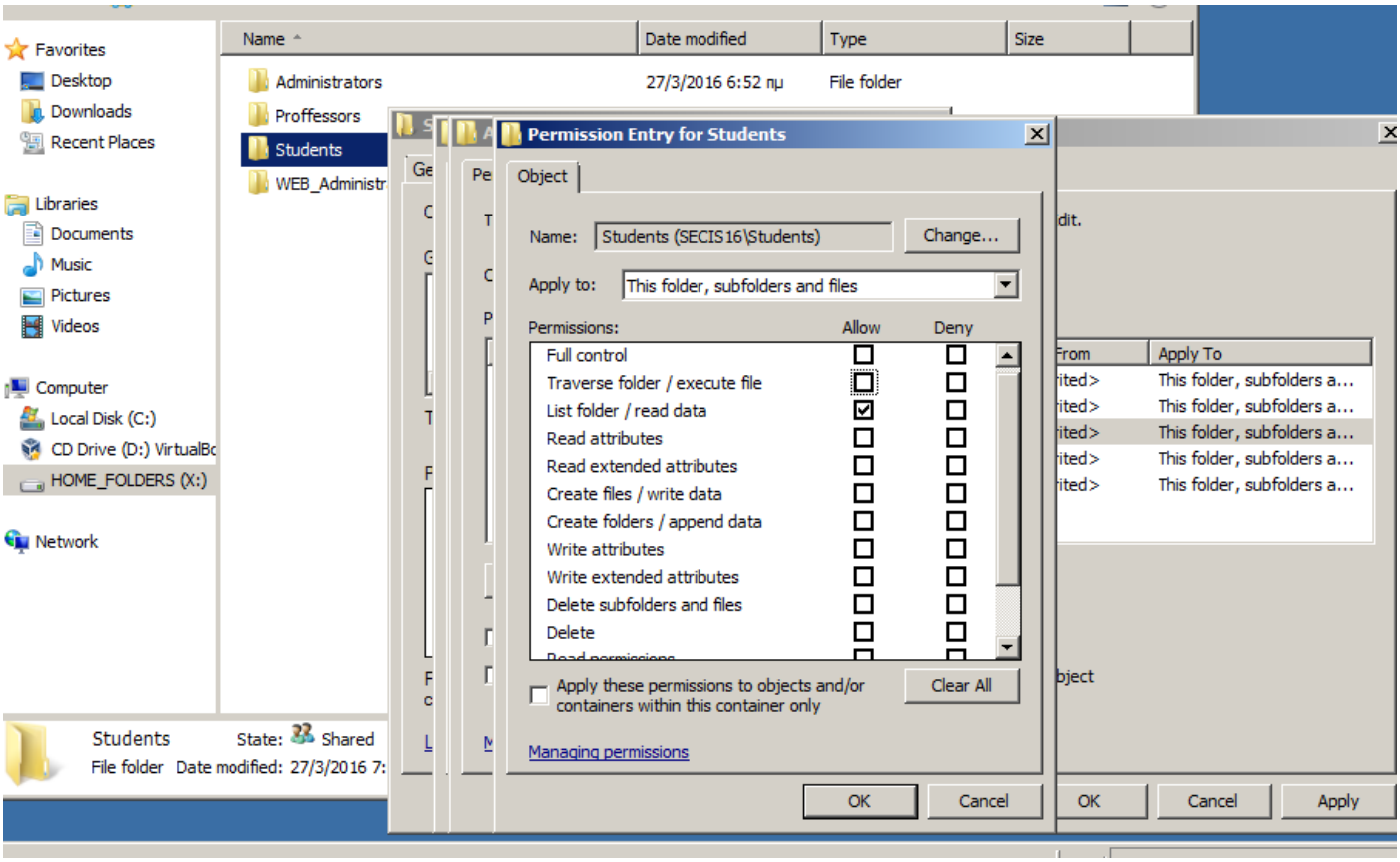
Volume X:



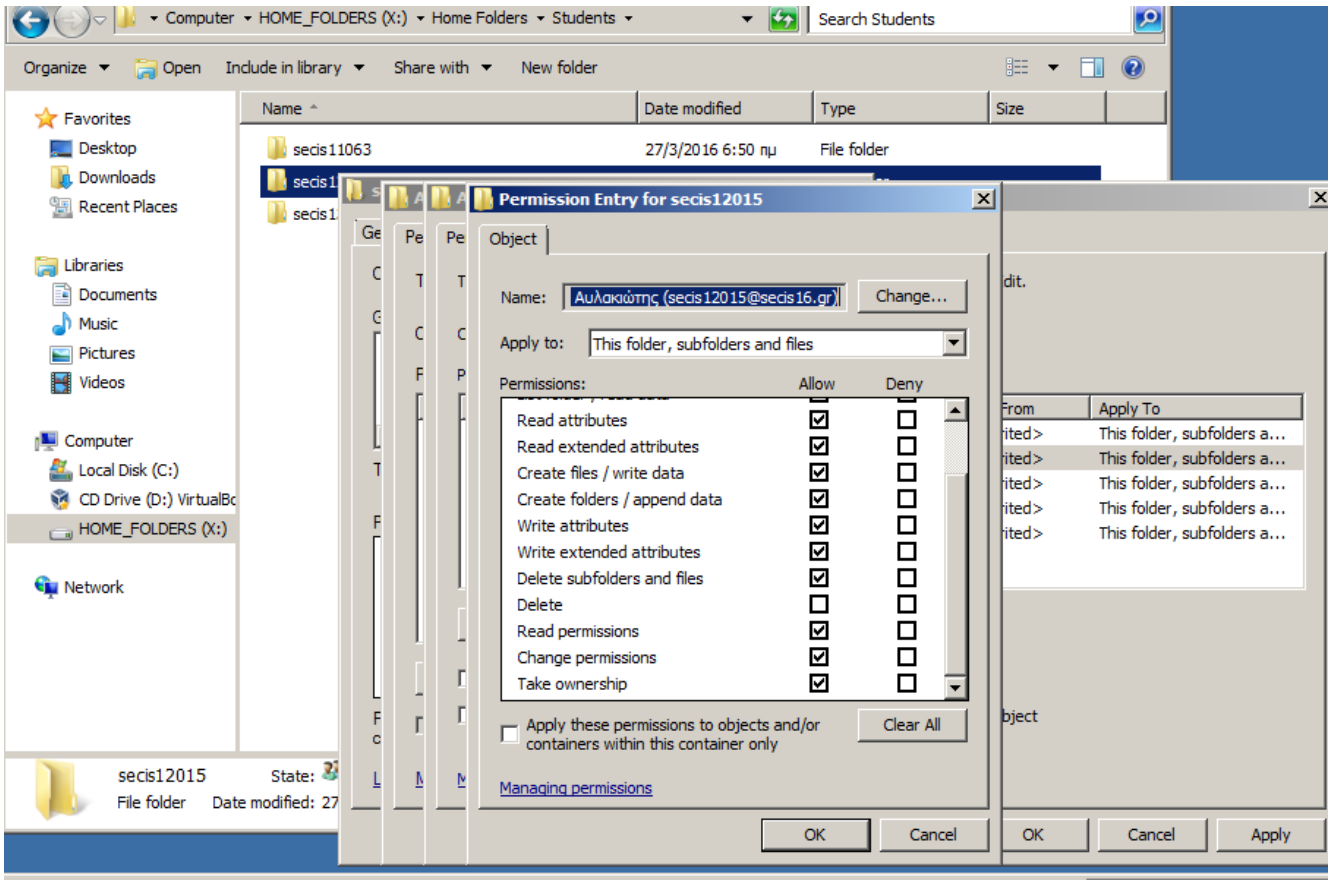
Home Folders



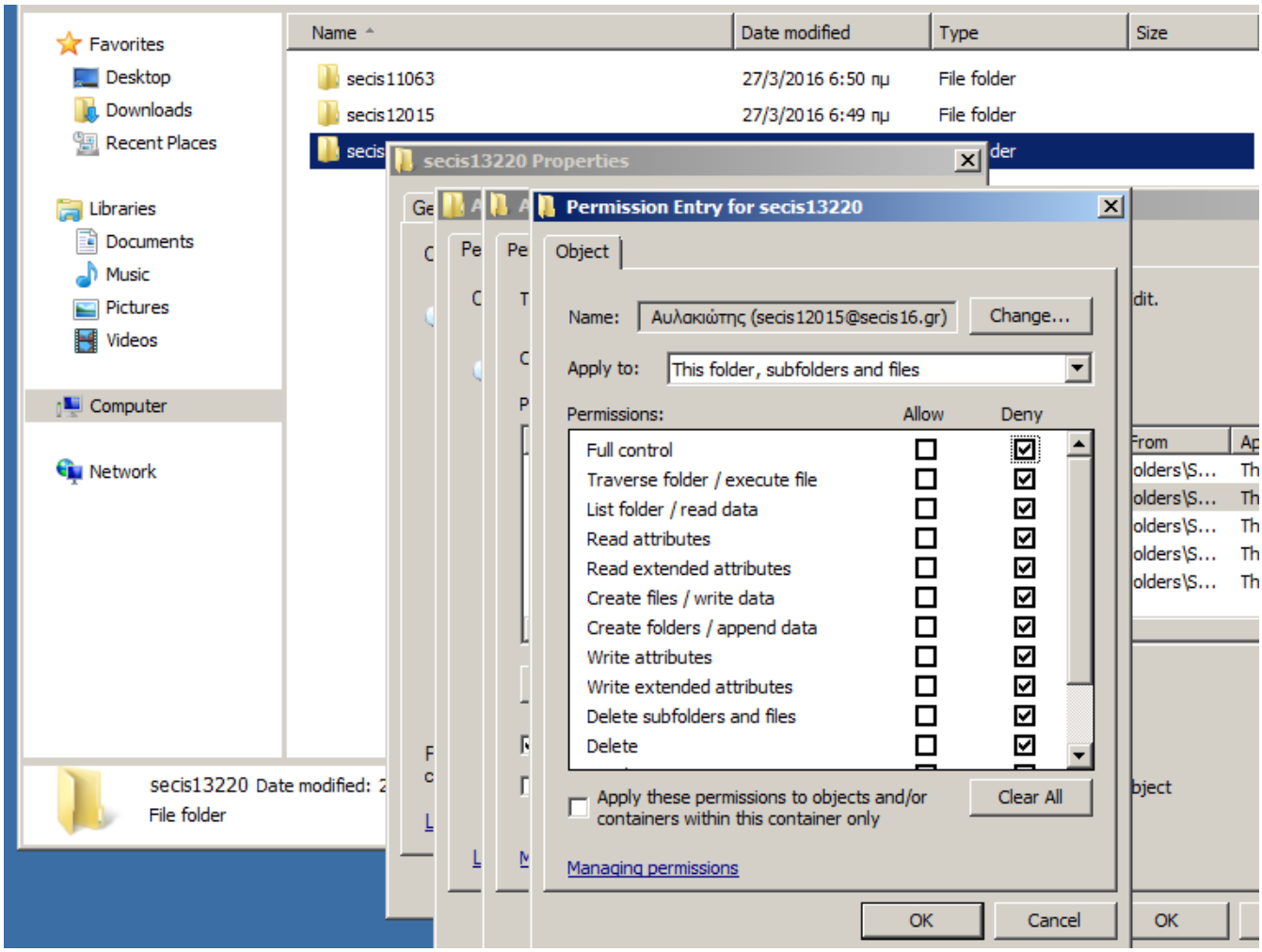
Home Folders – Subfolders (για τον καθένα)



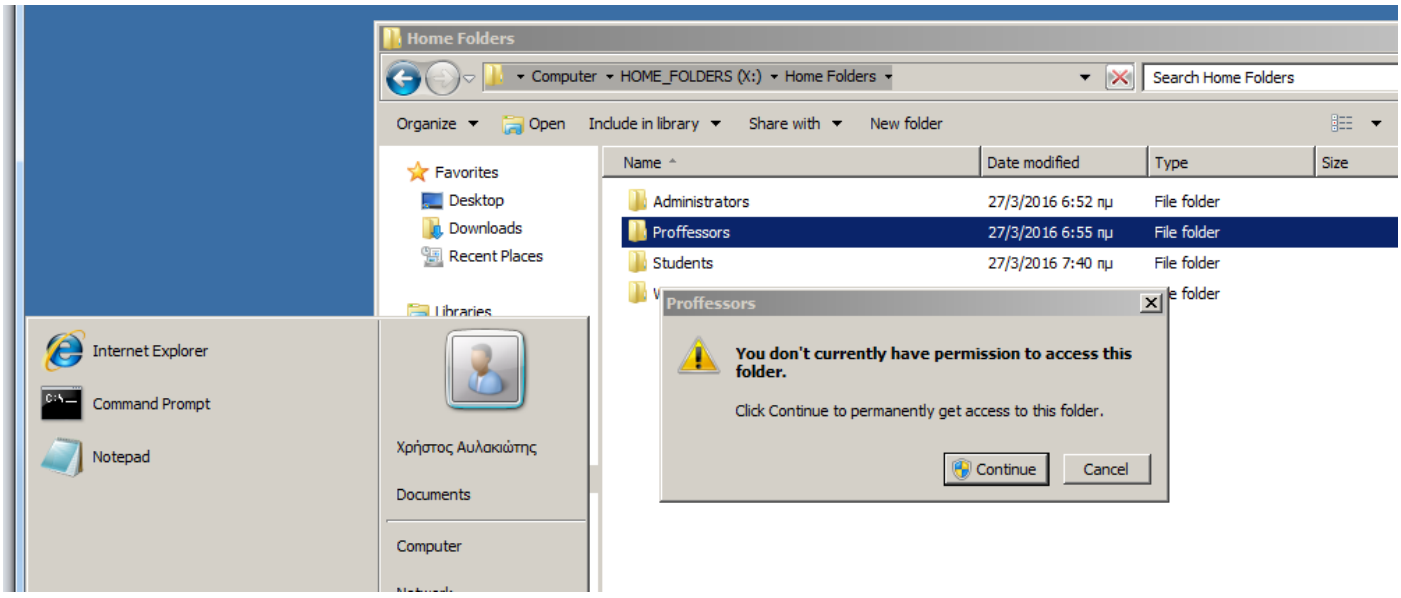
Home Folders – Subfolders – Subfolders (για τον καθένα)

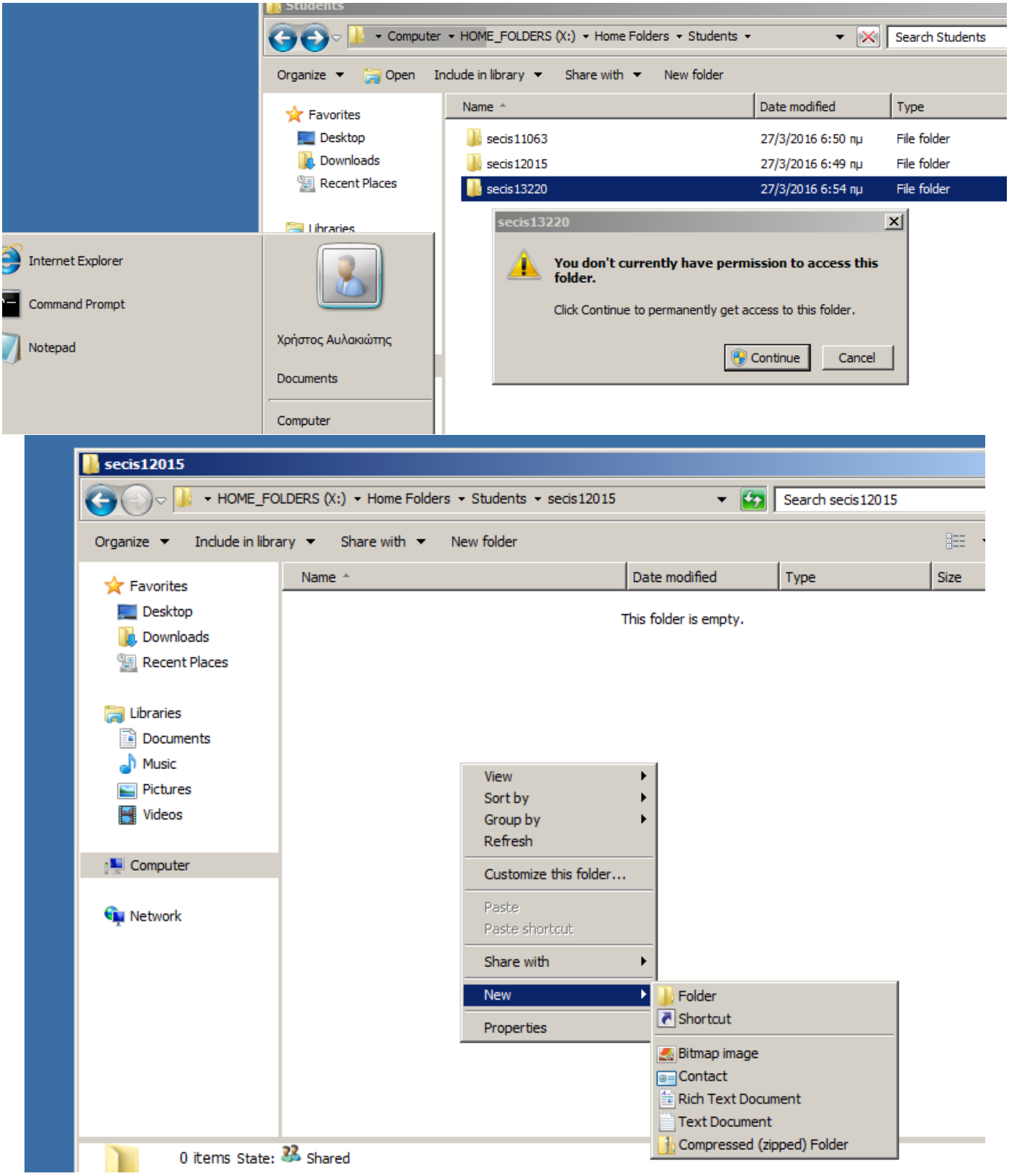


Εδώ επίσης κάναμε deny όλα τα permissions στους άλλους χρηστές για μεγαλύτερη ασφάλεια



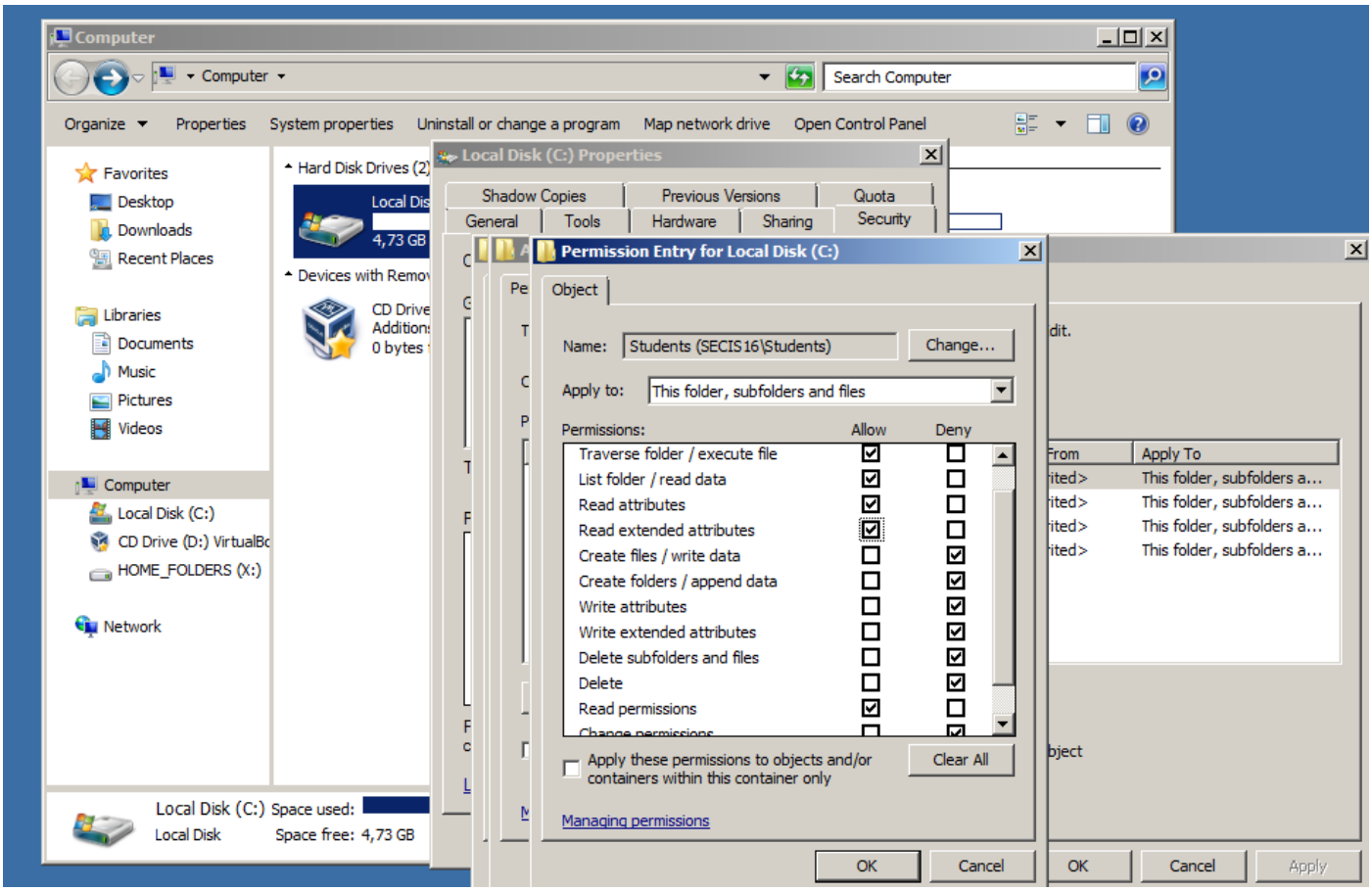
Έλεγχος:



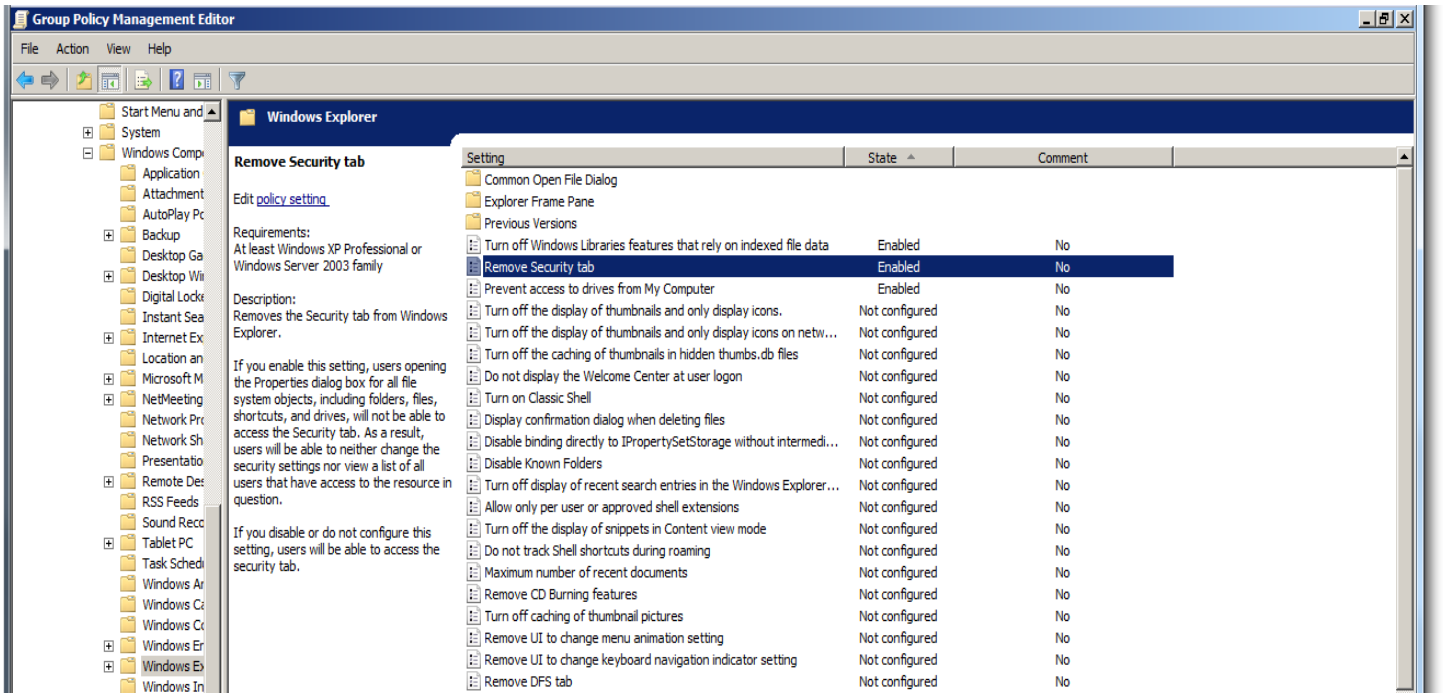


Ο κάθε χρήστης έχει δικαιώματα μόνο στο δικό του φάκελο

Επίσης αποτρέψαμε τη πρόσβαση των χρηστών στον τοπικό δίσκο και περιορίσαμε τα permissions

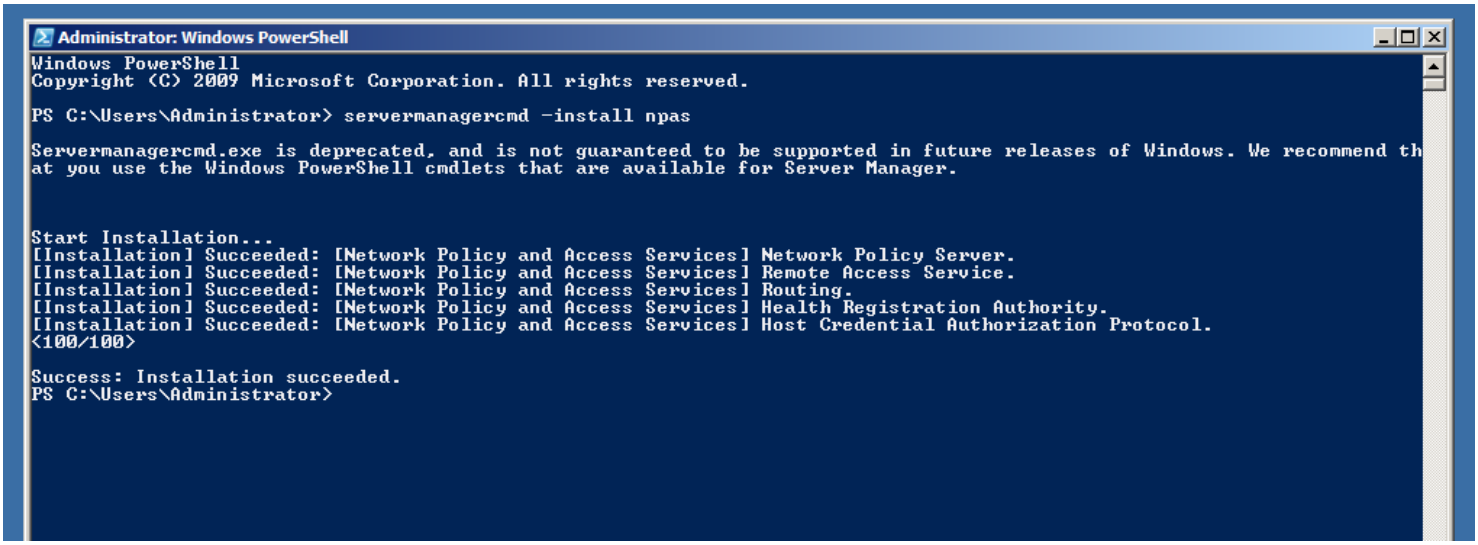


Έξτρα: όχι καρτέλα Ασφάλειας και όχι Libraries

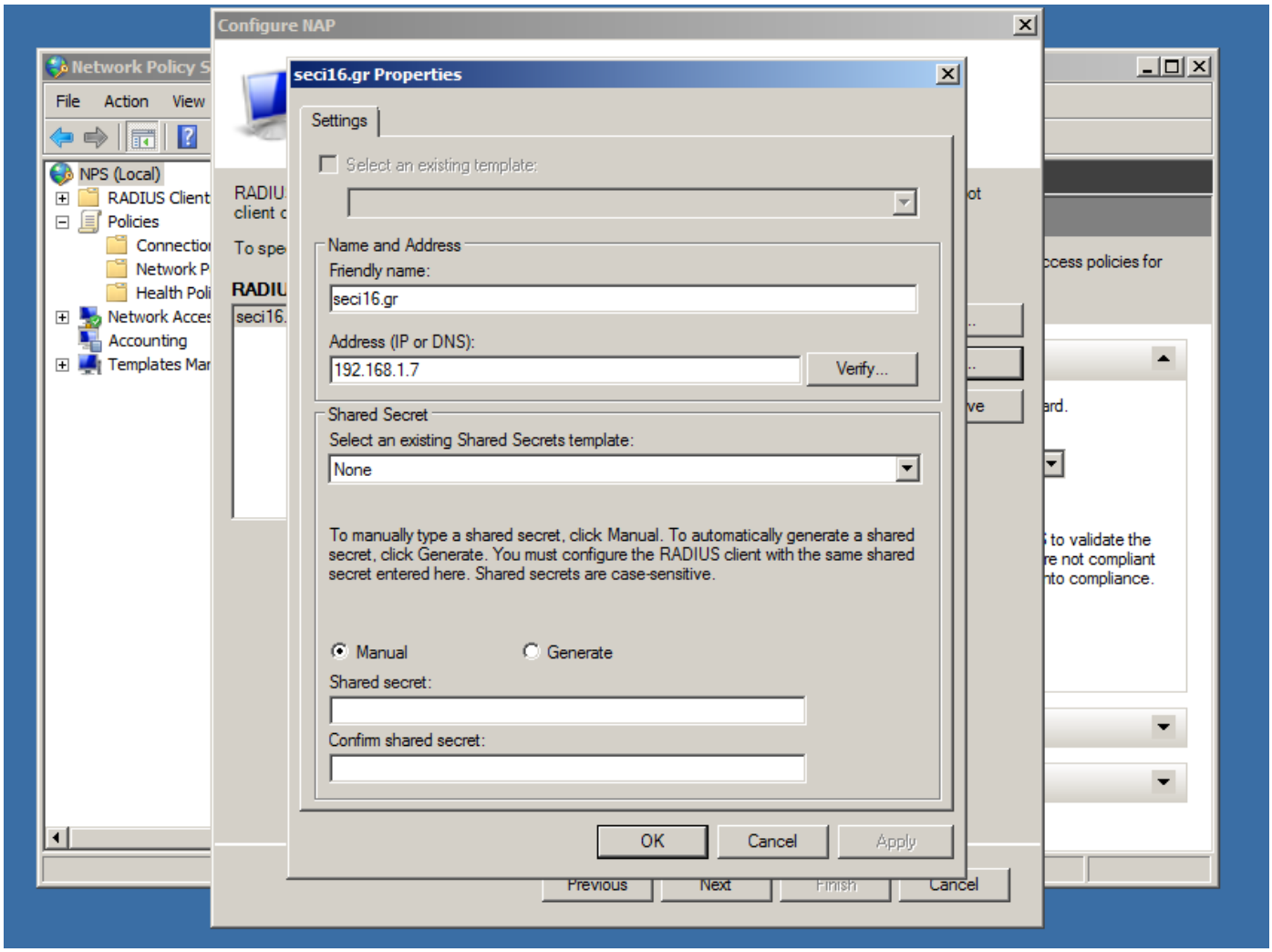


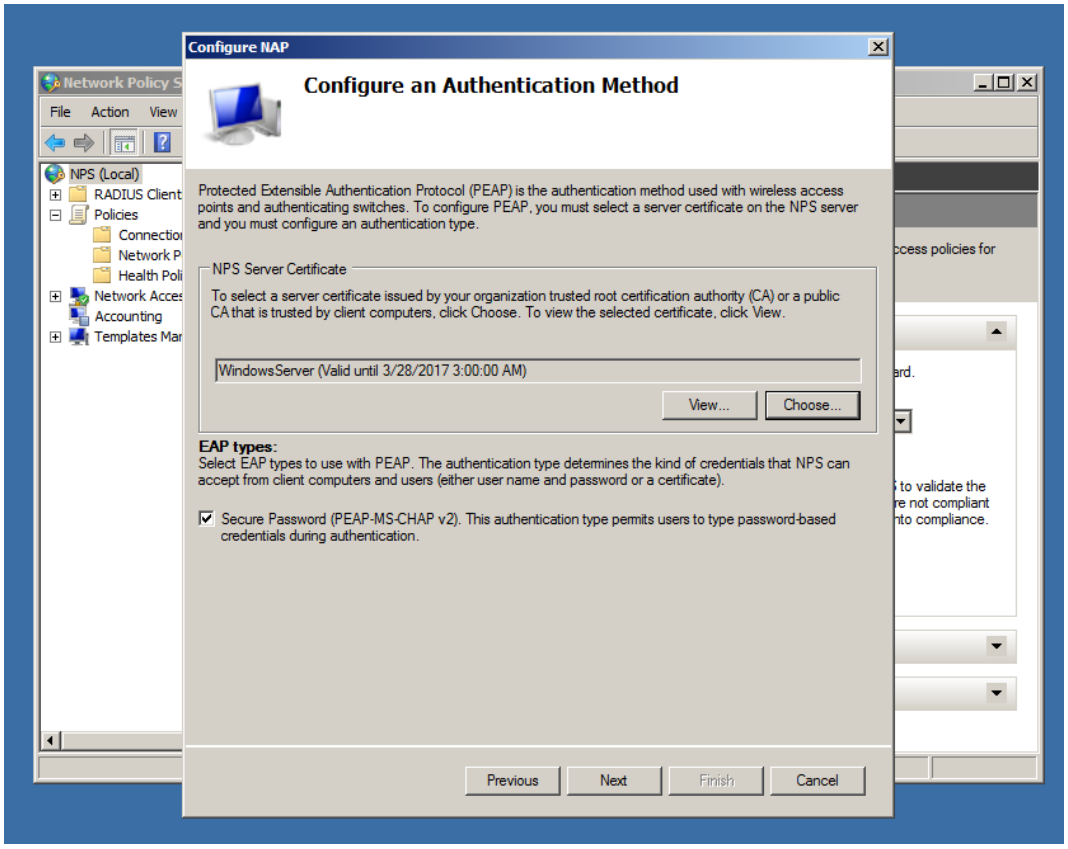
B6.

Εγκατασταση NAP:

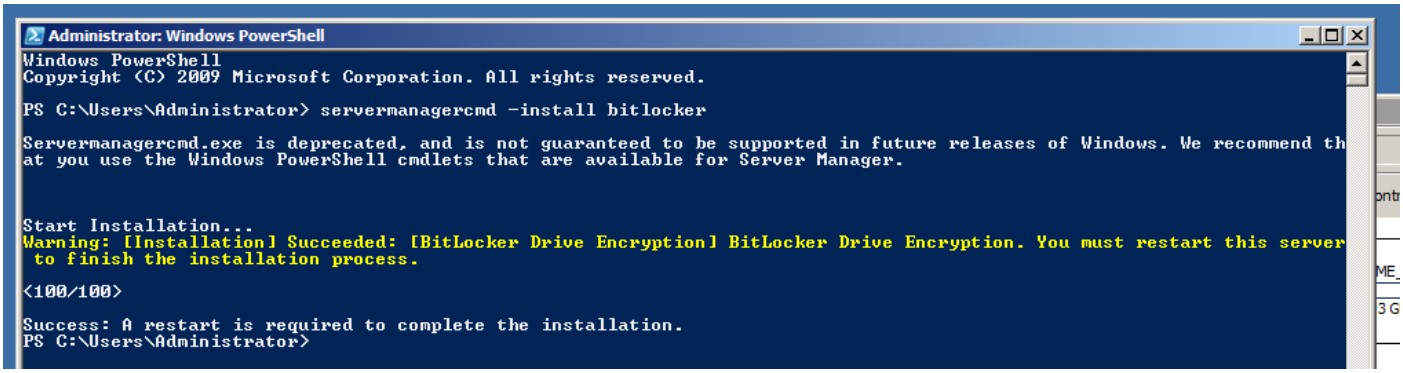


Παραμετροποίηση NAP

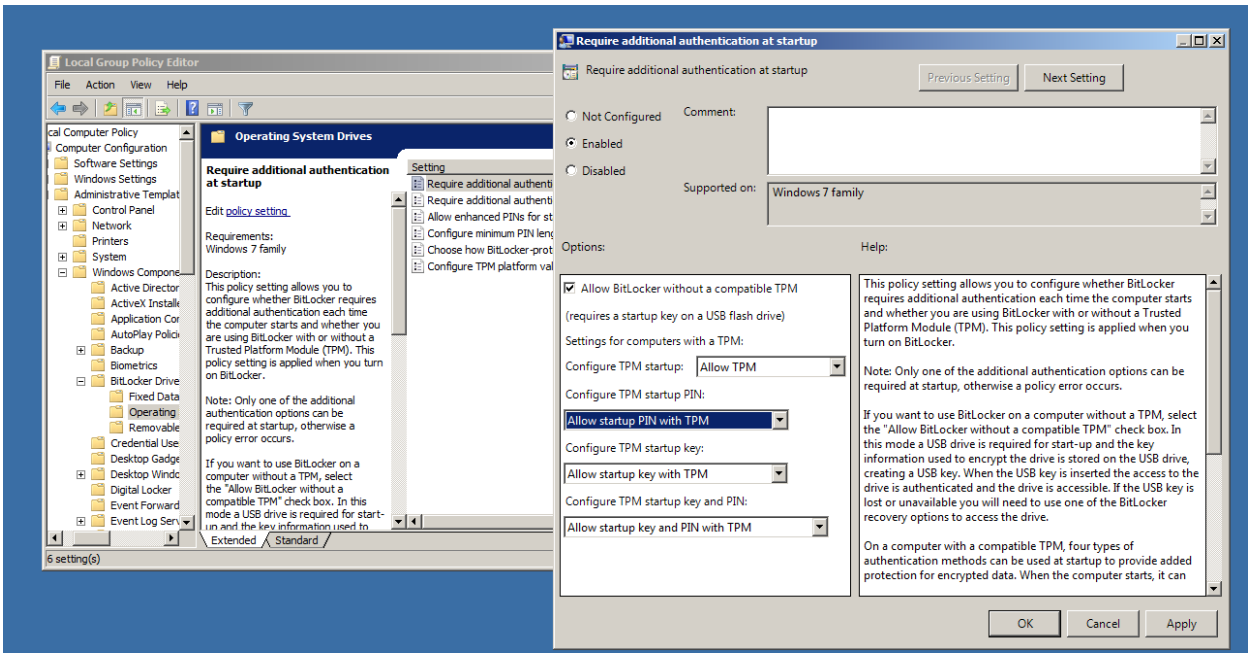




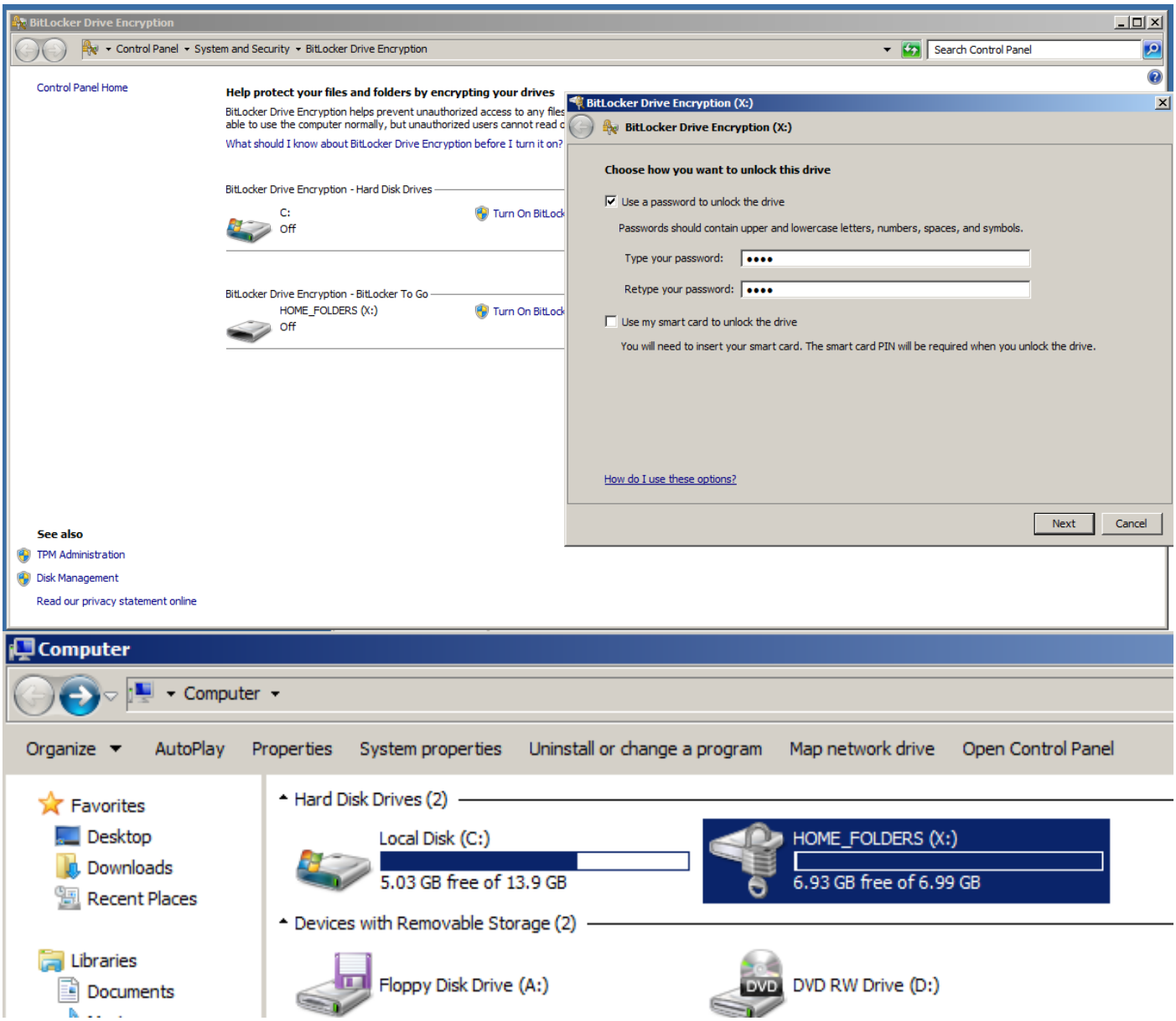
Εγκατάσταση Bitlocker



Ενεργοποίηση Bitlocker στα policies



Κρυπτογράφηση μονάδας X:



Σύγκριση δυο λειτουργικών.

Και τα δυο λειτουργικά χρειάζονται πολύ καλή γνώση του χρήστη για την παραμετροποίηση και λειτουργία τους. Και τα δυο διαθέτουν τις ίδιες βασικές ρυθμίσεις ασφαλείας και όσο και μειονεκτήματα και αδυναμίες.

Πηγές.

Security Strategies in Windows Platforms and Applications, Michael G. Solomon

http://www.techrepublic.com/blog/the-enterprise-cloud/how-do-i-install-and-configure-a-dns-server-in-windows-server-2008/

http://www.itzgeek.com/how-tos/windows/how-to-setup-configure-dns-server-on-windows-2008-r2-server.html

https://technet.microsoft.com/

http://www.webhostingtalk.com/showthread.php?t=1238491

Τέλος θα θέλαμε να πούμε πως δεν είχαμε προσέξει την οδηγία να φαίνονται οι ημερομηνίες και όταν το είδαμε είπαμε στο τέλος να βγάλουμε ένα screenshot που θα έδειχνε features στον Manager, www.secis16.gr, users και Windows Calendar άλλα λέγω αυτού του προβλήματος δε το κάναμε. Ωστόσο η εργασία και τα screenshots είναι καθαρά δική μας εκπόνηση και παραδόθηκε πριν τη λήξη της προθεσμίας.