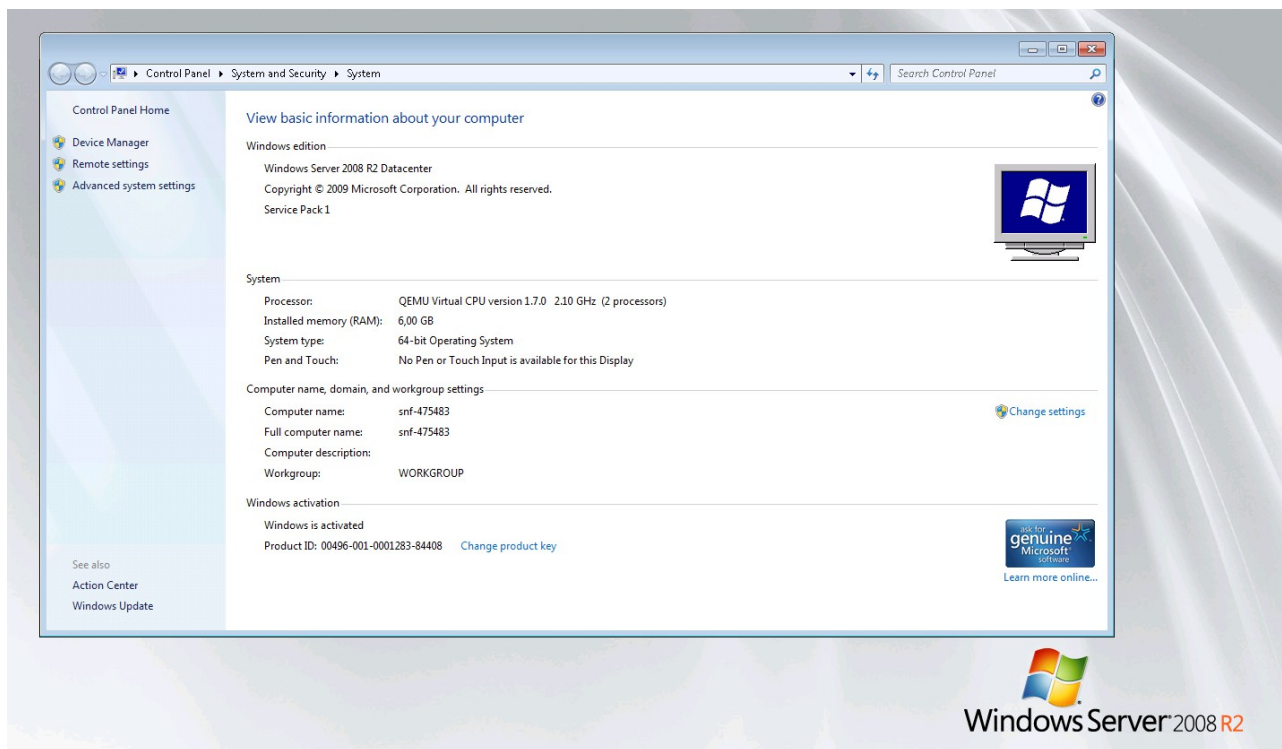


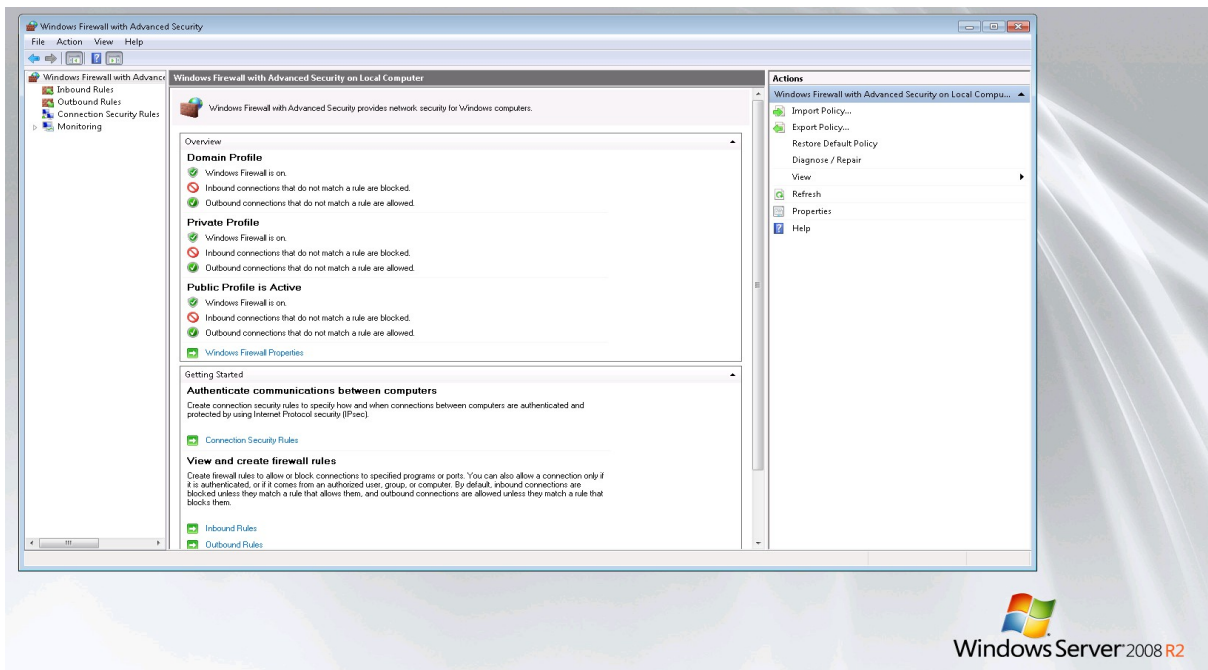
Windows Server

Σημείωση: Επειδή δεν ξέραμε αν ο Okeanos χρησιμοποιεί static ή dynamic IP, είχαμε πρόβλημα στο configuration του DNS και γενικά του server μας, οπότε δεν καταφέραμε να κάνουμε τα Penetration Tests.

-OS που χρησιμοποιήσαμε: Windows Server 2008R2



Αφού κάναμε τα απαραίτητα updates(αλλά δεν βάλαμε το Service Pack 1,2 ή 3), ενεργοποιήσαμε το Windows Firewall με Εξελεγμένη Ασφάλεια.



Οι υπηρεσίες που θεωρήσαμε ότι δεν χρειάζονται για τον server μας(τις οποίες βρήκαμε τρέχοντας το services.msc), είναι οι εξής:

- Mozilla Maintenance Service
- Telephony
- Tablet Input Service
- Print Spooler
- Smart Card
- Themes

,γιαυτό και τις διαγράψαμε.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Windows\system32
C:\Windows\System32>sc delete "MozillaMaintenance
[SC] DeleteService SUCCESS
C:\Windows\System32>sc delete Telephony
[SC] OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\Windows\System32>sc delete TabletInputService
[SC] DeleteService SUCCESS
C:\Windows\System32>sc delete TapiSrv
[SC] DeleteService SUCCESS
C:\Windows\System32>sc delete PrintSpooler
[SC] OpenService FAILED 1060:
The specified service does not exist as an installed service.

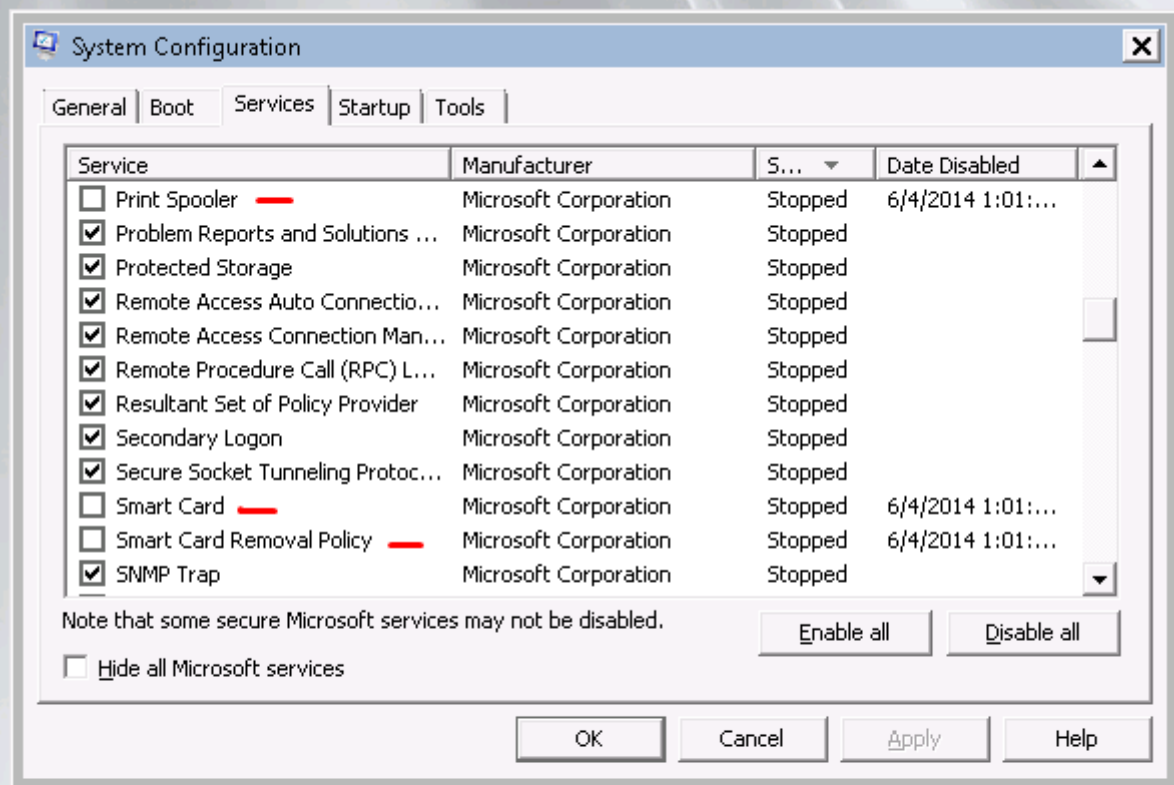
C:\Windows\System32>sc delete SmartCard
[SC] OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\Windows\System32>sc delete Smart Card
[SC] OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\Windows\System32>sc delete "Smart Card"
[SC] OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\Windows\System32>sc delete Themes
[SC] DeleteService SUCCESS
C:\Windows\System32>_
```

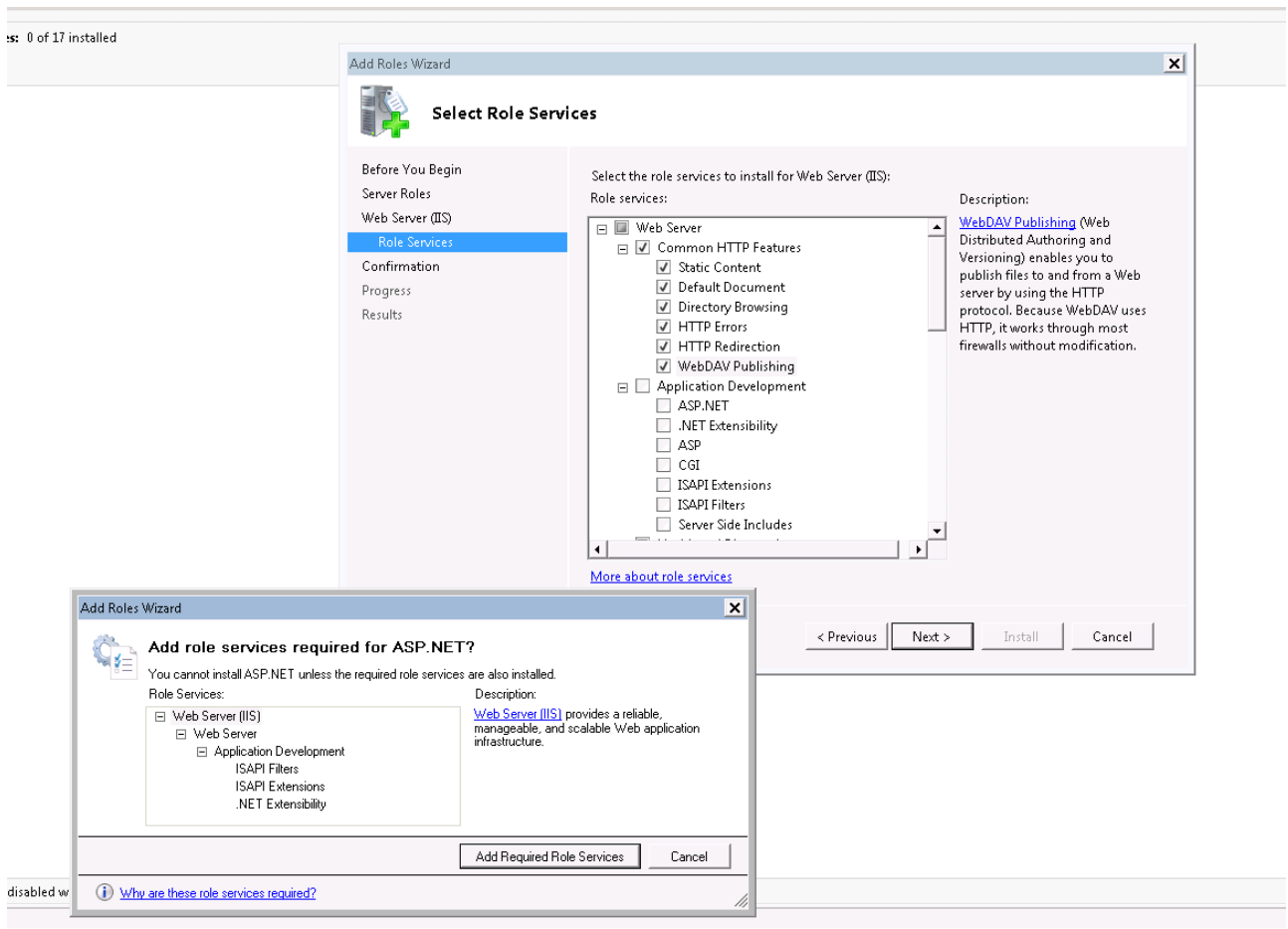
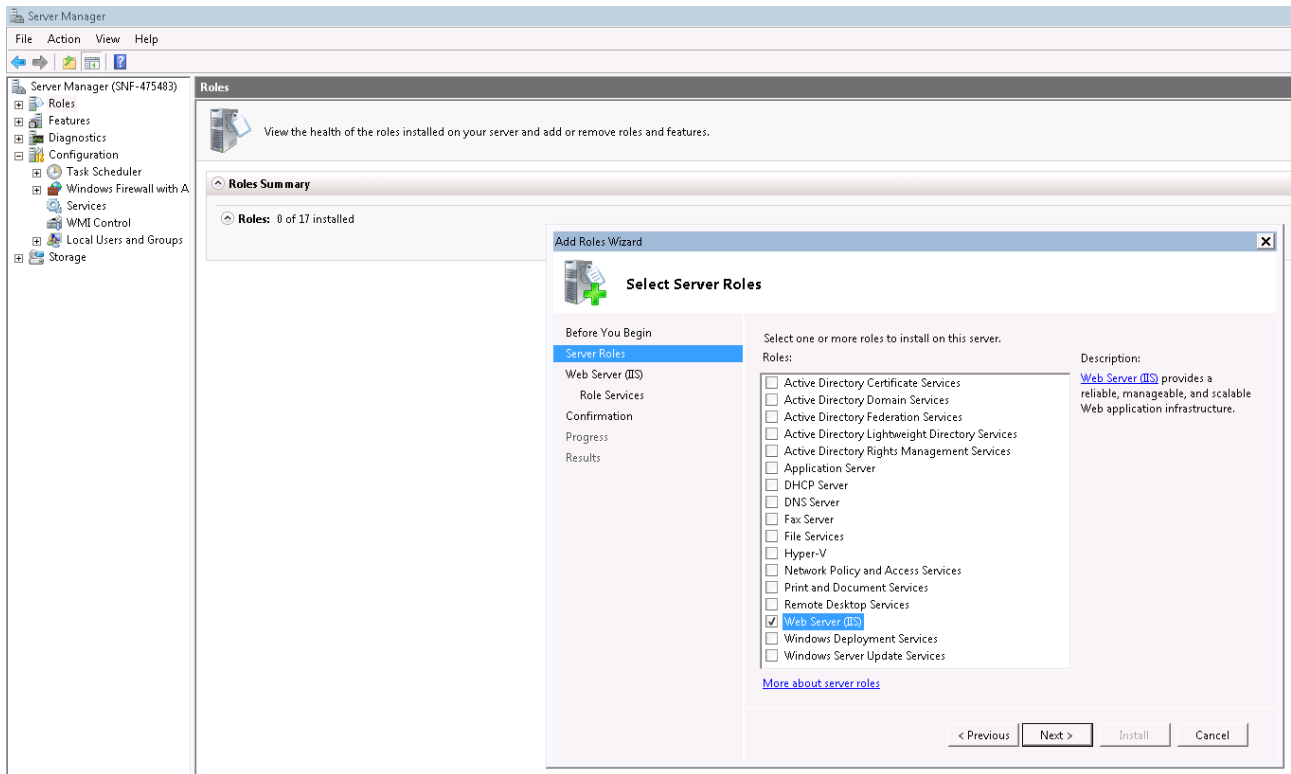
Όποιες υπηρεσίες δεν καταφέραμε να τις διαγράψουμε(όπως πχ η Print Spooler) μέσω του command line, τρέξαμε το msconfig και την απενεργοποιήσαμε εκεί:



Επίσης, μιας και ο server μας βρίσκεται στον Οκεανο, δεν διαγράψαμε τις υπηρεσίες για Remote Connectivity(Remote Desktop, κλπ κλπ).

Όπως μας ζητήθηκε, εγκαταστήσαμε και τροποποιήσαμε με γνώμονα την ασφάλεια του ΛΣ, τις υπηρεσίες «Φιλοξενίας Ιστοσελίδων» (Web - IIS), «Διευθυνσιοδότησης» (DNS Server) και «Βάσεων Δεδομένων» (Database Server – Microsoft Sql Server).

-Φιλοξενία Ιστοσελιδών(Web – IIS)



Roles

View the health of the roles installed on your server and add or remove roles and features.

Role Services: 22 installed

Role Service	Status
Web Server	Installed
Common HTTP Features	Installed
Static Content	Installed
Default Document	Installed
Directory Browsing	Installed
HTTP Errors	Installed
HTTP Redirection	Installed
WebDAV Publishing	Installed
Application Development	Installed
ASP.NET	Installed
.NET Extensibility	Installed
ASP	Not installed
CGI	Not installed
ISAPI Extensions	Installed
ISAPI Filters	Installed
Server Side Includes	Not installed
Health and Diagnostics	Installed
HTTP Logging	Installed
Logging Tools	Not installed
Request Monitor	Installed
Tracing	Not installed
Custom Logging	Not installed
ODBC Logging	Not installed
Security	Installed
Basic Authentication	Not installed
Windows Authentication	Not installed
Digest Authentication	Not installed
Client Certificate Mapping Authentication	Not installed
IS Client Certificate Mapping Authentication	Not installed
URL Authorization	Not installed
Request Filtering	Installed
IP and Domain Restrictions	Not installed
Performance	Installed
Static Content Compression	Installed
Dynamic Content Compression	Not installed
Management Tools	Installed
IS Management Console	Installed
IS Management Scripts and Tools	Not installed
Management Service	Not installed
IS 6 Management Compatibility	Not installed
IS 6 Metabase Compatibility	Not installed

Last Refresh: Today at 1:28 pm. [Configure refresh](#)

[Add Role Services](#)
[Remove Role Services](#)

-Λειτουργισιοδότηση(DNS Server)

Add Roles Wizard

Select Server Roles

Before You Begin

Server Roles

DNS Server

Confirmation

Progress

Results

Select one or more roles to install on this server.

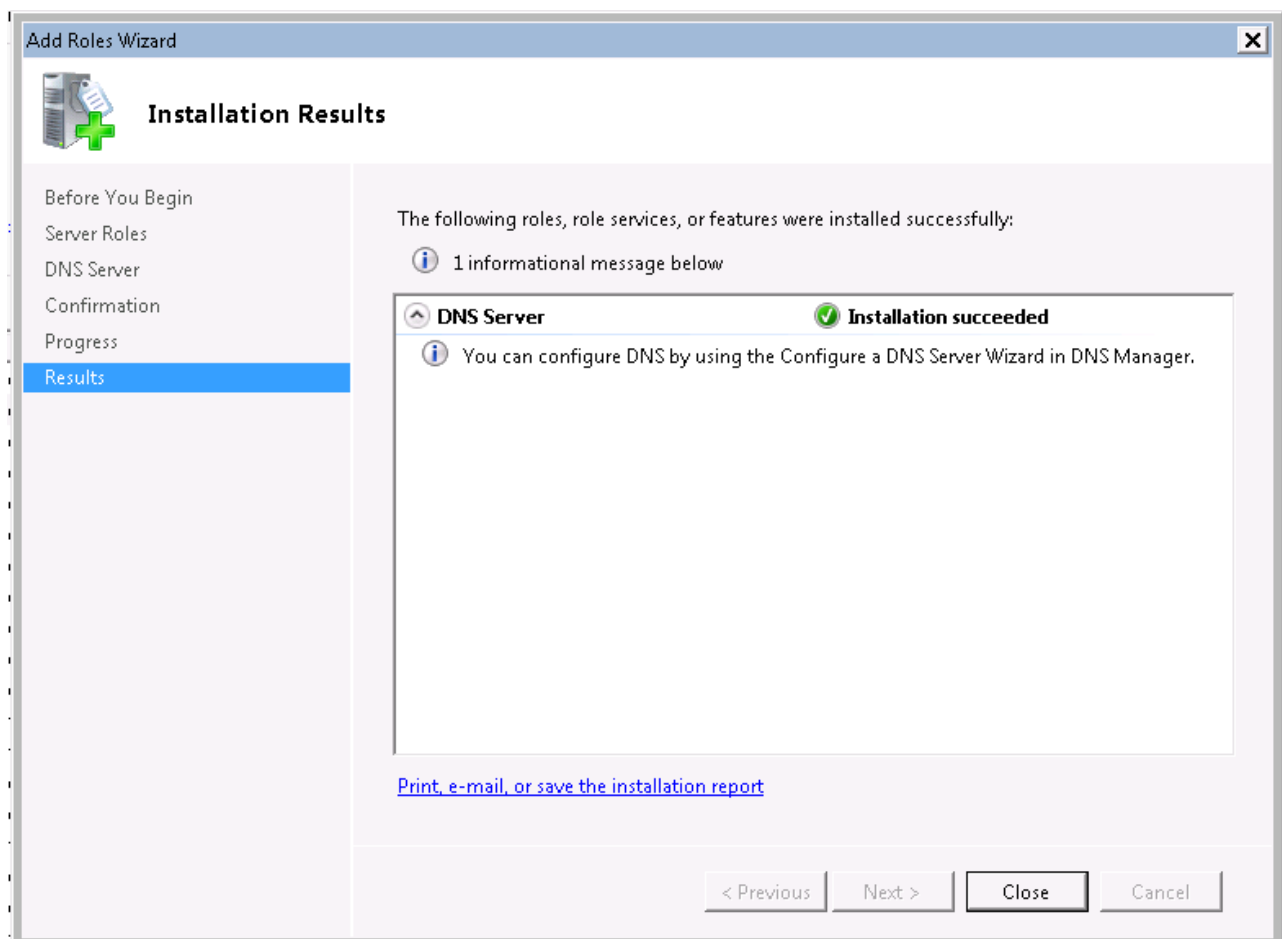
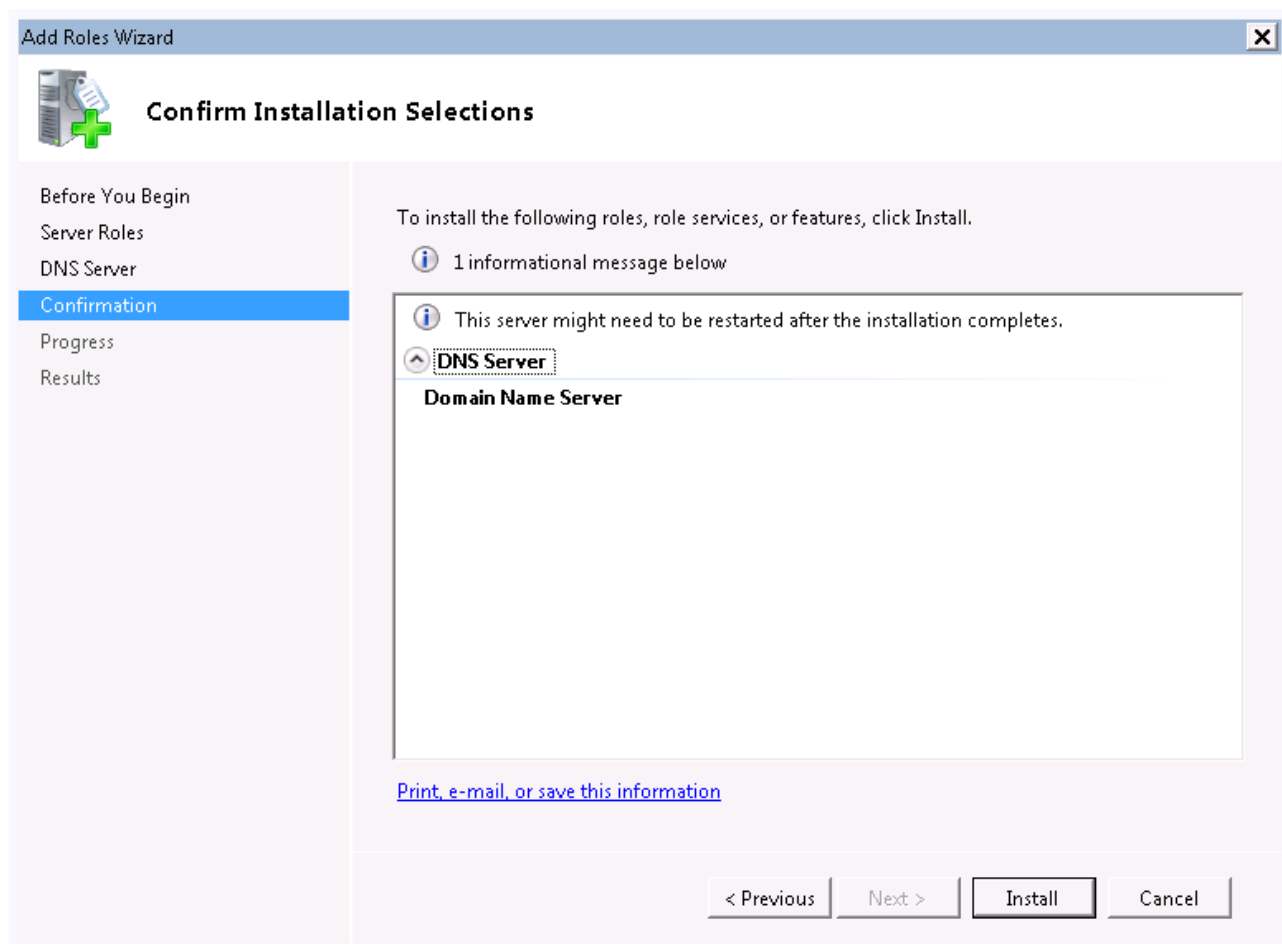
Roles:

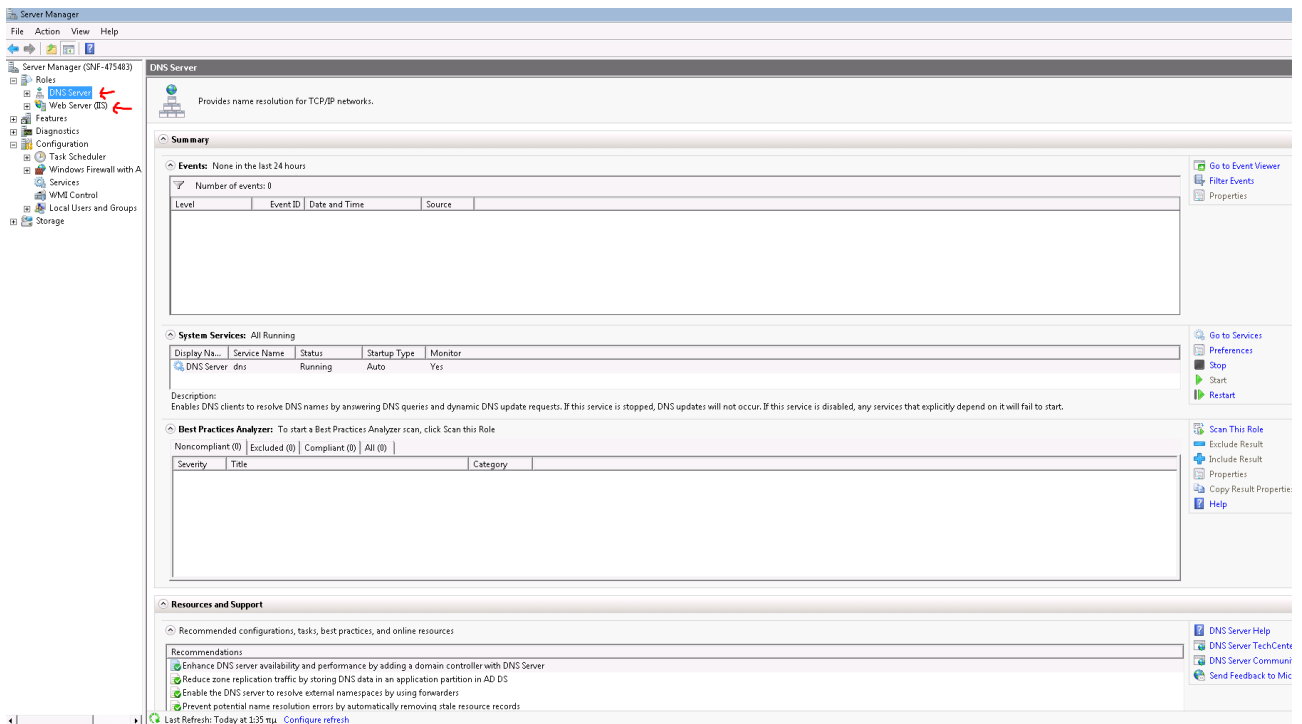
- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☒ **DNS Server**
- ☐ Fax Server
- ☐ File Services
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Desktop Services
- ☒ Web Server (IIS) (Installed)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

[More about server roles](#)

Description:
[Domain Name System \(DNS\) Server](#) provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

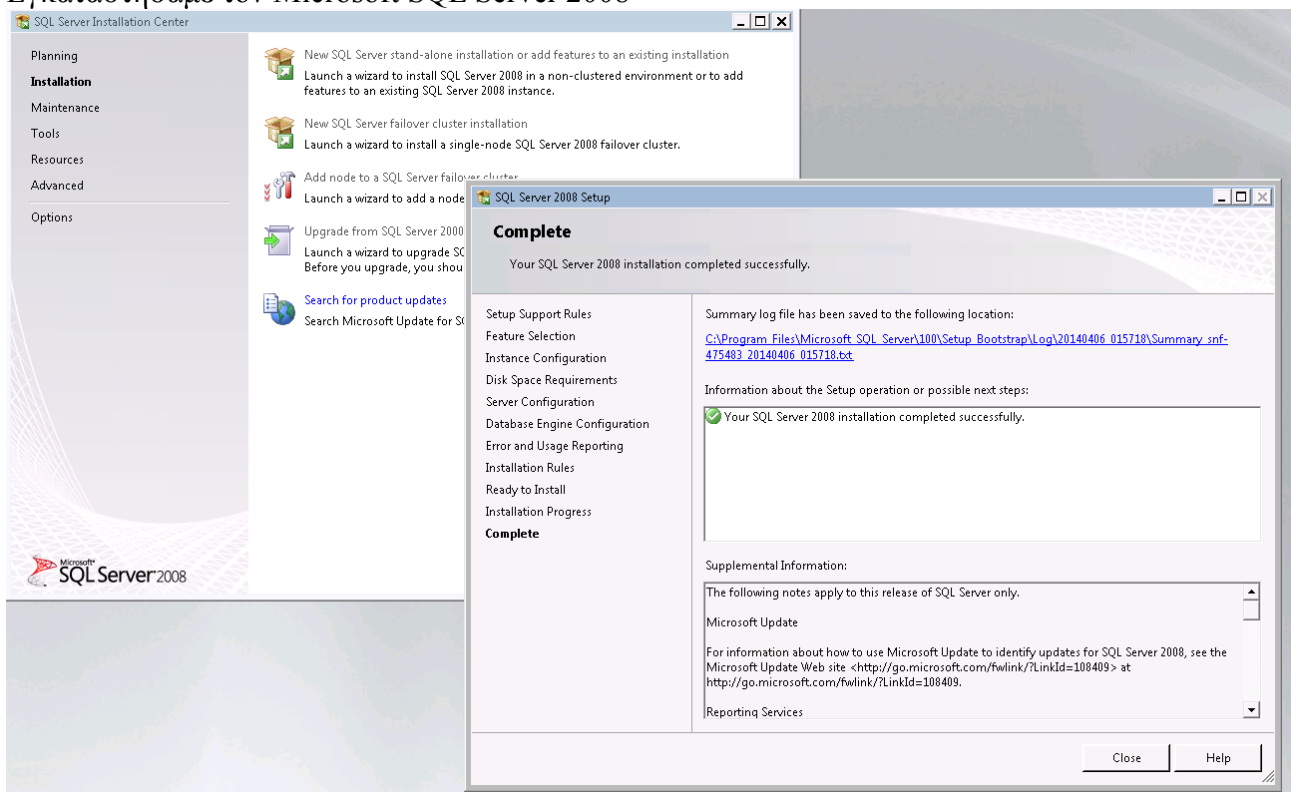
< Previous Next > Install Cancel





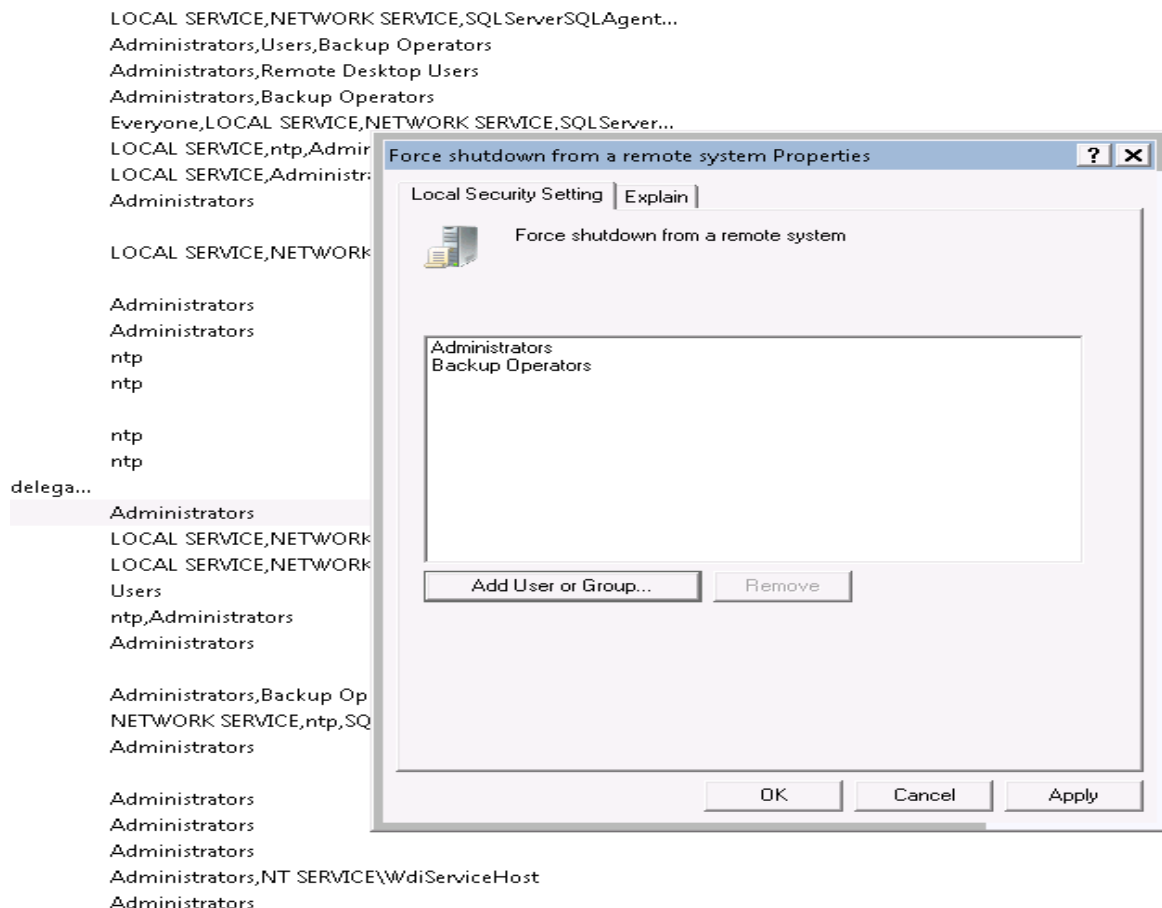
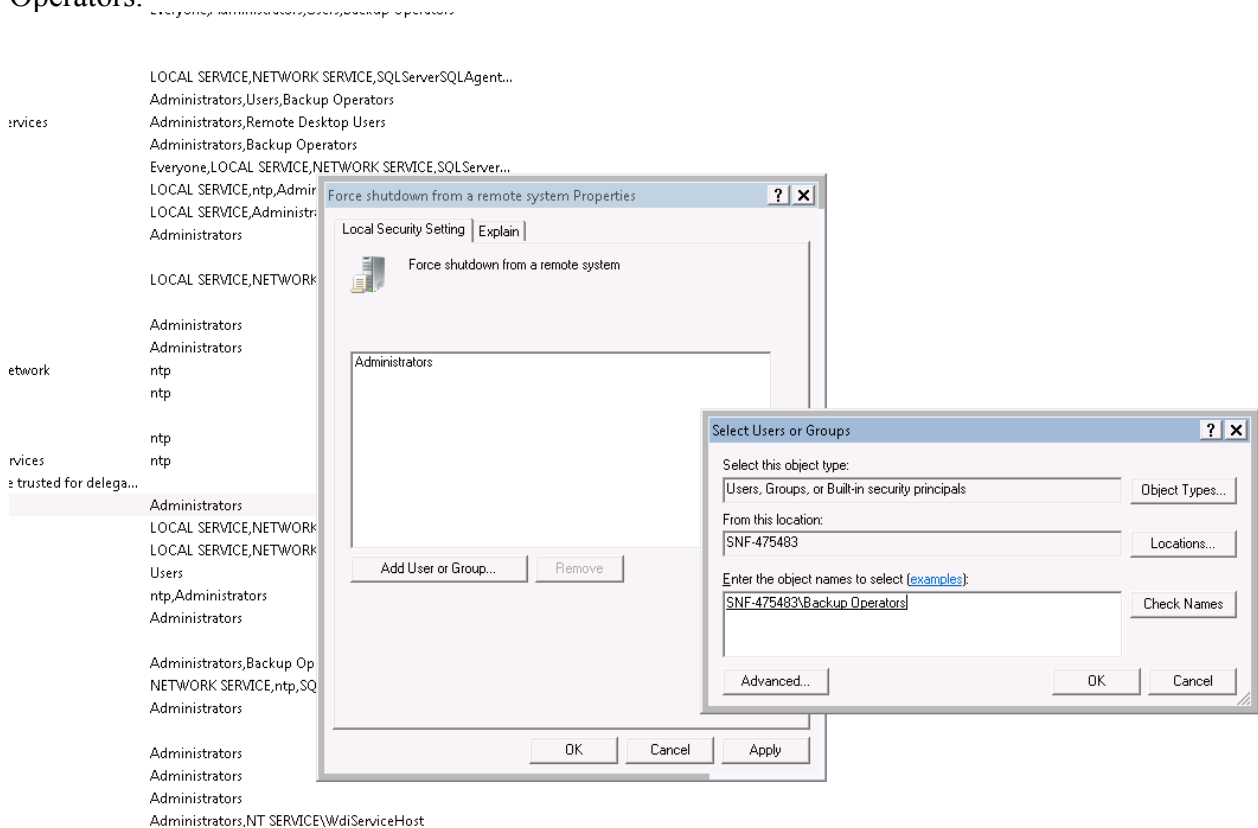
-Βάση Δεδομένων(Database Server – Microsoft SQL Server)

Εγκαταστήσαμε τον Microsoft SQL Server 2008

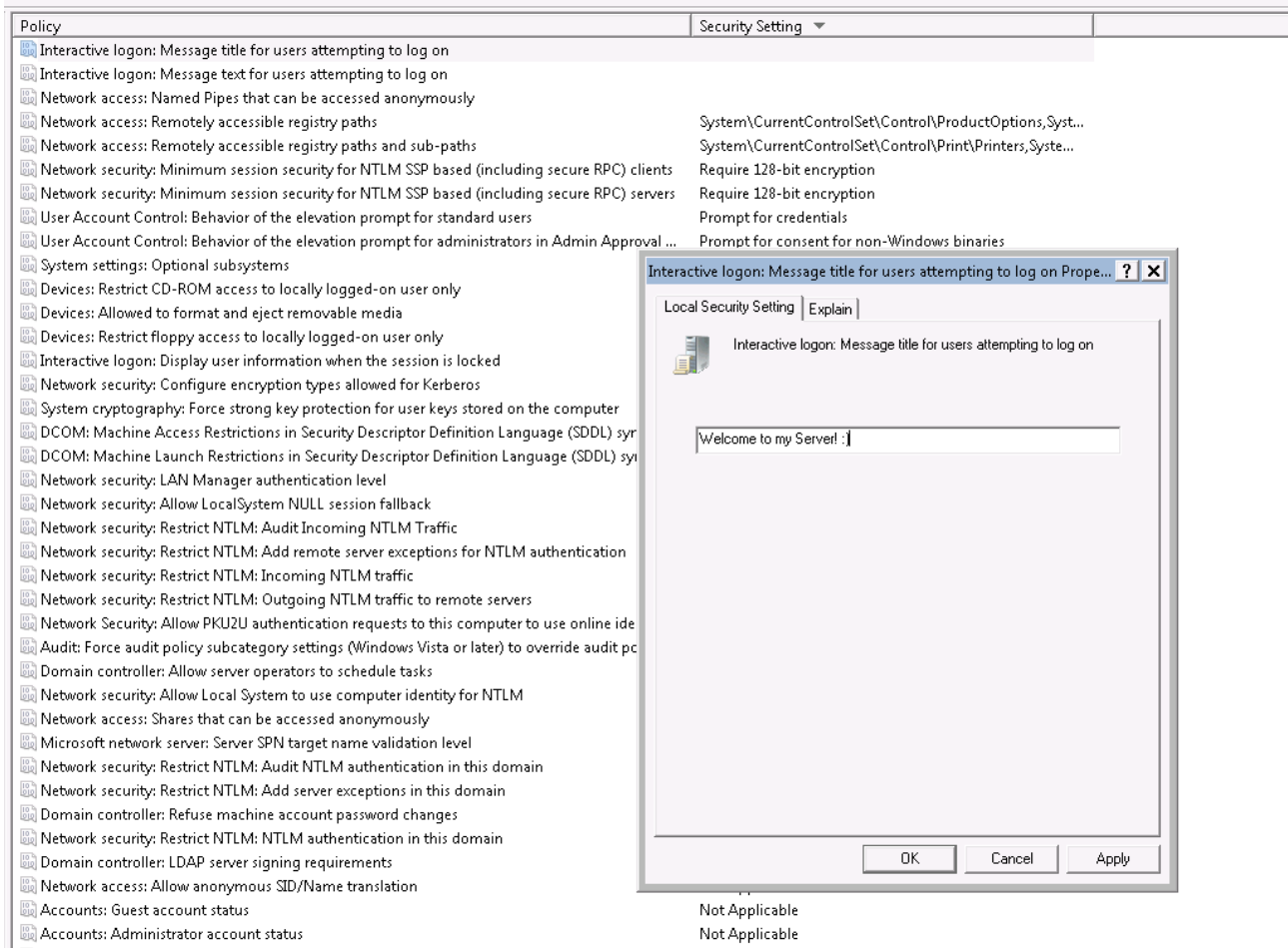


Αλλάξαμε κάποια security settings και κάποιες πολιτικές ασφαλείας στον server μας.

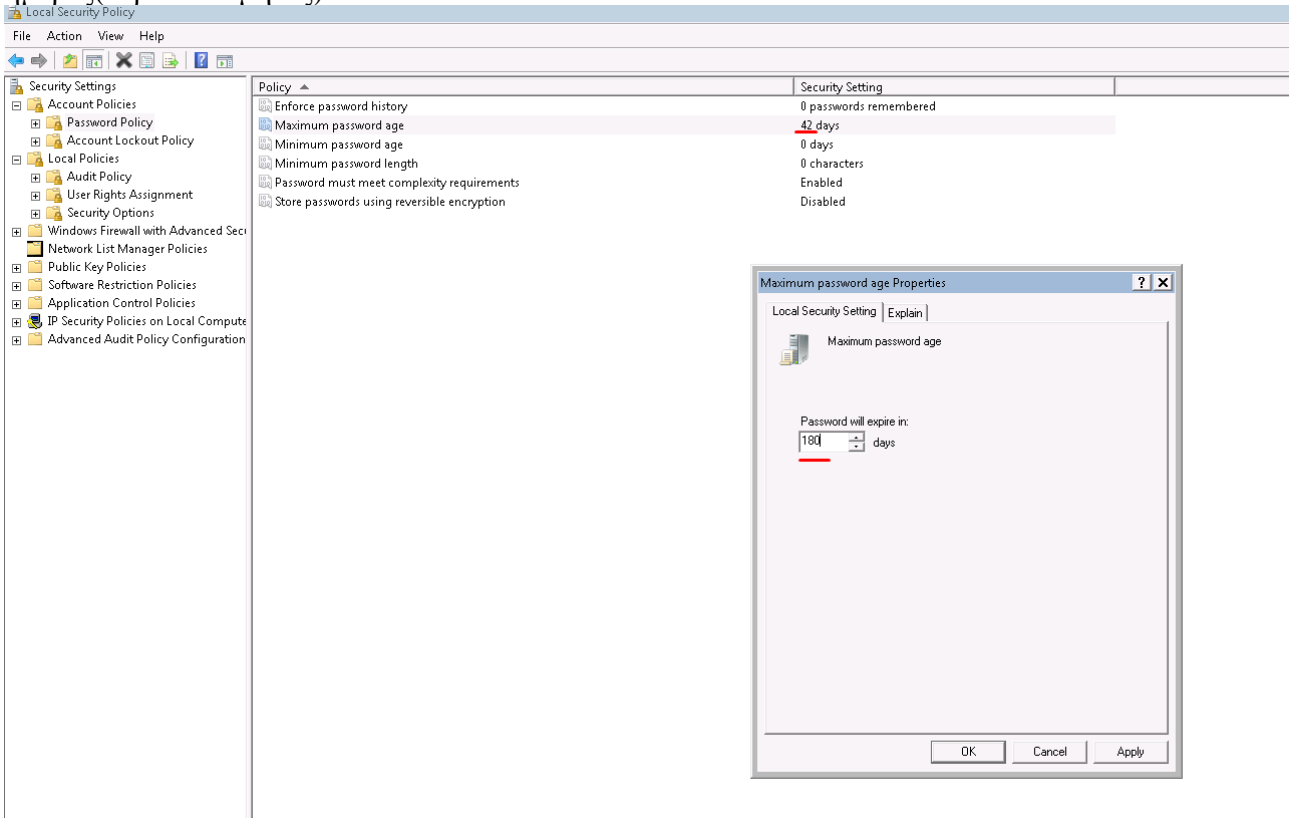
Π.χ. Shutdown from a Remote System: μπορούν να κάνουν μόνο οι Administrators και οι Backup Operators.



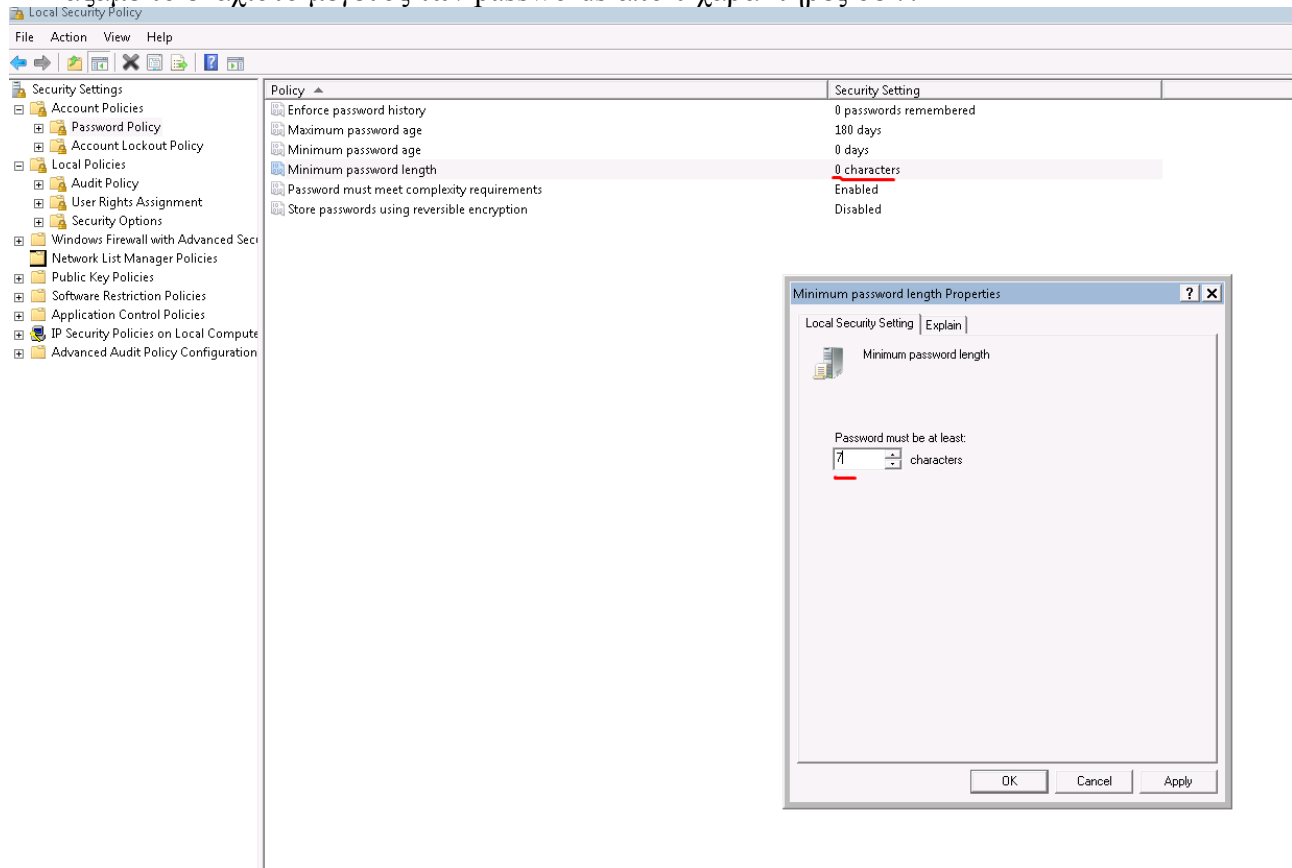
Βάλαμε να εμφανίζεται ένα welcome message κάθε φορά που κάνει κάποιος login στον server μας.



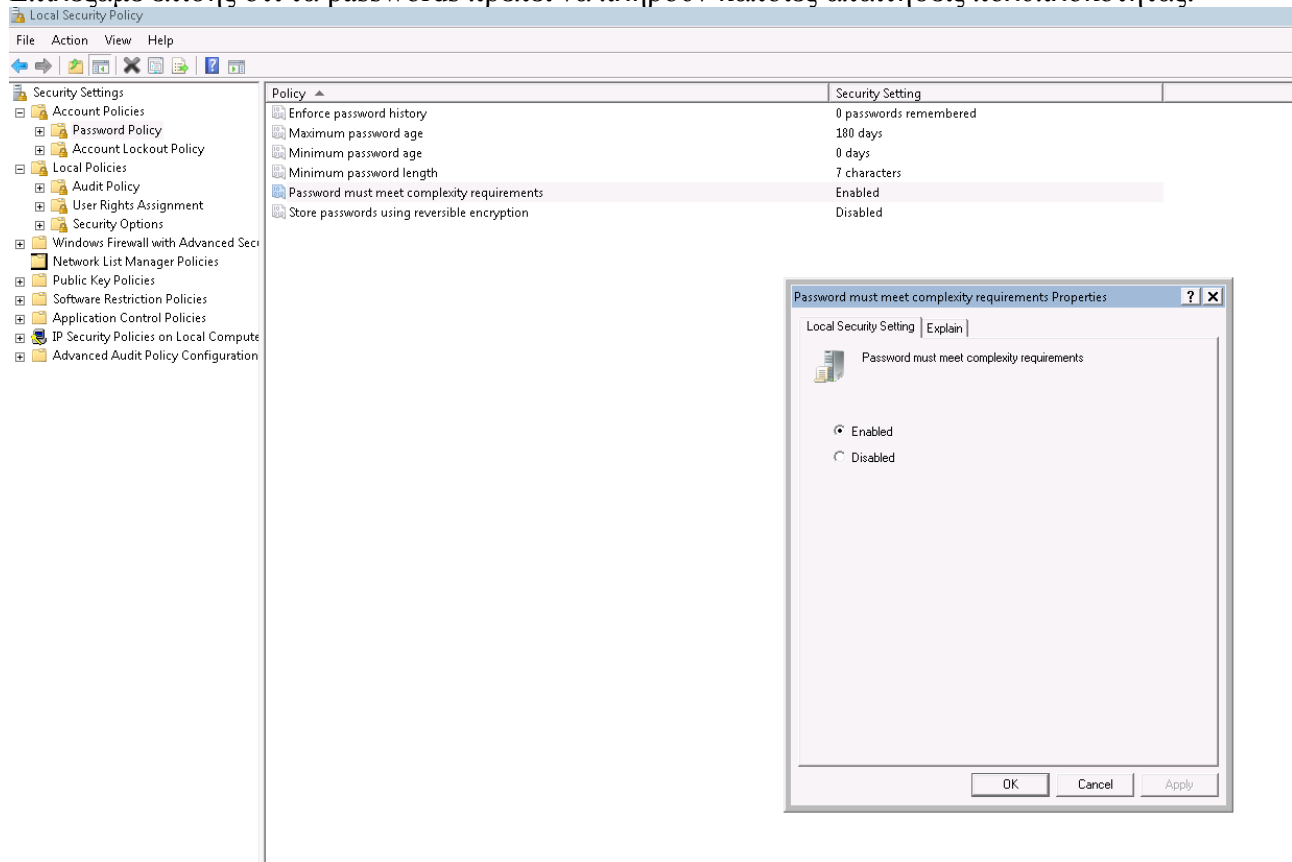
Αλλάξαμε την μέγιστη διάρκεια ζωής των passwords από 42 ημέρες(που ήταν η default τιμή) σε 180 ημέρες(περίπου 6 μήνες).



Αλλάξαμε το ελάχιστο μέγεθος των passwords από 0 χαρακτήρες σε 7.



Επιλέξαμε επίσης ότι τα passwords πρέπει να πληρούν κάποιες απαιτήσεις πολυπλοκότητας.



Εδώ βλέπουμε τις αλλαγές στις πολιτικές που αποφασίσαμε να επιλέξουμε.

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Audit account logon events Properties


Local Security Setting | Explain

Audit account logon events

Audit these attempts:

☒ Success

☒ Failure

 This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see [Audit account logon events](#). (Q921468)

OK Cancel Apply

Αποφασίσαμε να κάνουμε audit όλες τις πολιτικές, είτε σε Success, είτε σε Failure.

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Δημιουργία Χρηστών

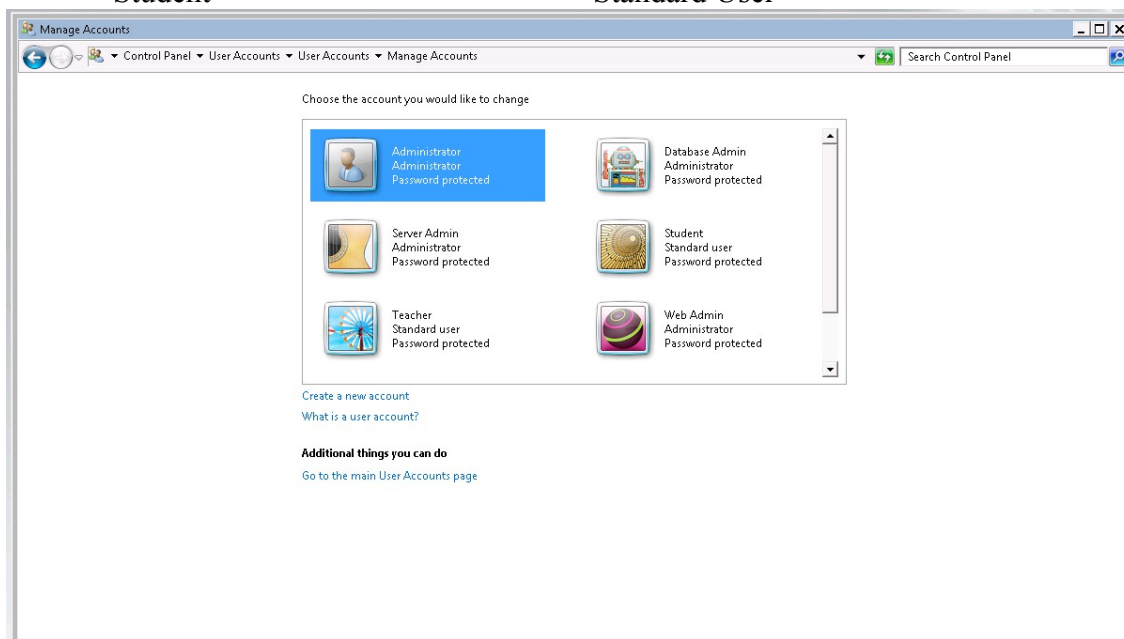
Όπως μας ζητήθηκε από την εργασία, φτιάξαμε τους εξής χρήστες(εκτός από τον ήδη υπάρχον Administrator):

Όνομα Λογαριασμού

- Server Admin
- Web Admin
- Database Admin
- Teacher
- Student

Τύπος Λογαριασμού

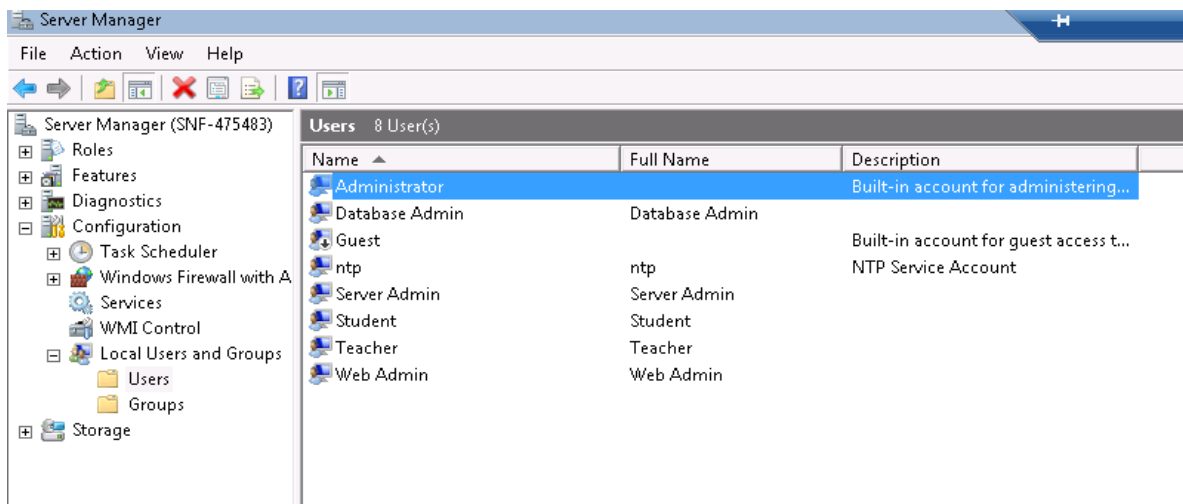
- Administrator
- Administrator
- Administrator
- Standard User
- Standard User



Windows Server 2008 R2

Όπως είναι φυσικό, ο καθένας έχει διαφορετικό password αρκετής δυσκολίας!

Server Admin pass:	Azd38@_
Web Admin pass:	B_aSg@7
Database Admin pass:	DB_B0ss
Teacher pass:	Haha_y0u_F41L3d
Student pass:	G0d_pl34s3_h3lp_m3!



Δώσαμε στον καθένα από αυτούς τους Users τα αντίστοιχα δικαιώματα που τους αναλογούν, και τοποθετήσαμε τον καθένα στο αντίστοιχο Group που ανοίκει.

-Web Admin

Groups 20 Group(s)

Name	Description
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Certificate Service DC...	Members of this group are allowe...
Cryptographic Operat...	Members are authorized to perfor...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Print Operators	Members can administer domain ...
Remote Desktop Users	Members in this group are grante...
Replicator	Supports file replication in a dom...
Users	Users are prevented from making ...
SQLServer2005SQLBro...	Members in the group have the re...
SQLServerMSSQLServ...	Members in the group have the re...
SQLServerMSSQLUser...	Members in the group have the re...
SQLServerSQLAgentU...	Members in the group have the re...

IIS_IUSRS Properties

General

IIS_IUSRS

Description: Built-in group used by Internet Information Services.

Members:

Web Admin

Add...

Remove

Changes to a user's group membership are not effective until the next time the user logs on.

OK

Cancel

Apply

Help

-Database Admin(στα 4 τελευταία Groups)

Groups 20 Group(s)

Name	Description
Administrators	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Certificate Service DCOM Access	Members of this group are allowed to connect to Certification Authorities in the enterprise
Cryptographic Operators	Members are authorized to perform cryptographic operations.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects on this machine.
Event Log Readers	Members of this group can read event logs from local machine
Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
IIS_IUSRS	Built-in group used by Internet Information Services.
Network Configuration Operators	Members in this group can have some administrative privileges to manage configuration of networking features
Performance Log Users	Members of this group may schedule logs
Performance Monitor Users	Members of this group can access performance data
Power Users	Power Users are included for backwards compatibility
Print Operators	Members can administer domain printers
Remote Desktop Users	Members in this group are granted the right to use Remote Desktop
Replicator	Supports file replication in a domain
Users	Users are prevented from making accidental changes to the system
SQLServer2005SQLBrowserUser\$SNF-475483	Members in the group have the required access and privileges to be assigned as the log on account for the SQL Server Browser service
SQLServerMSSQLServerADHelperUser\$SNF-475483	Members in the group have the required access and privileges to be assigned as the log on account for the SQL Server Active Directory Helper service
SQLServerMSSQLUser\$SNF-475483\$SQLEXPRESS	Members in the group have the required access and privileges to be assigned as the log on account for the SQL Server Express instance
SQLServerSQLAgentUser\$SNF-475483\$SQLEXPRESS	Members in the group have the required access and privileges to be assigned as the log on account for the SQL Server Agent service

SQLServer2005SQLBrowserUser\$SNF-475483 Properties

General

SQLServer2005SQLBrowserUser\$SNF-475483

Description: Members in the group have the required access and privileges to be assigned as the log on account for the SQL Server Browser service.

Members:

Database Admin

Add...

Remove

Changes to a user's group membership are not effective until the next time the user logs on.

OK

Cancel

Apply

Help

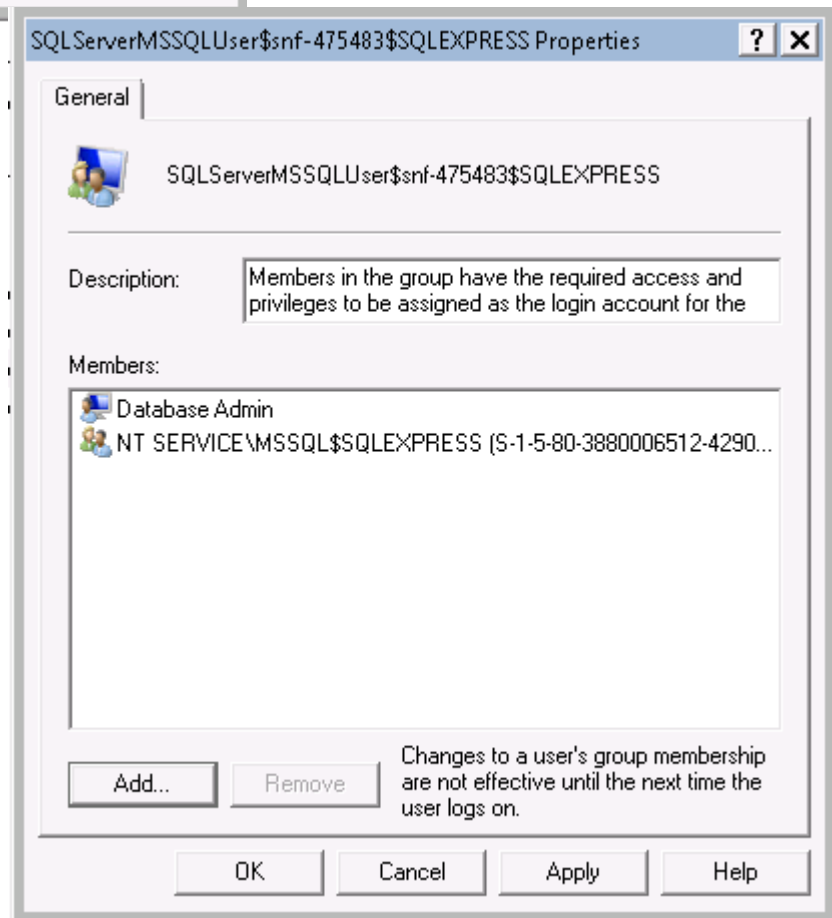
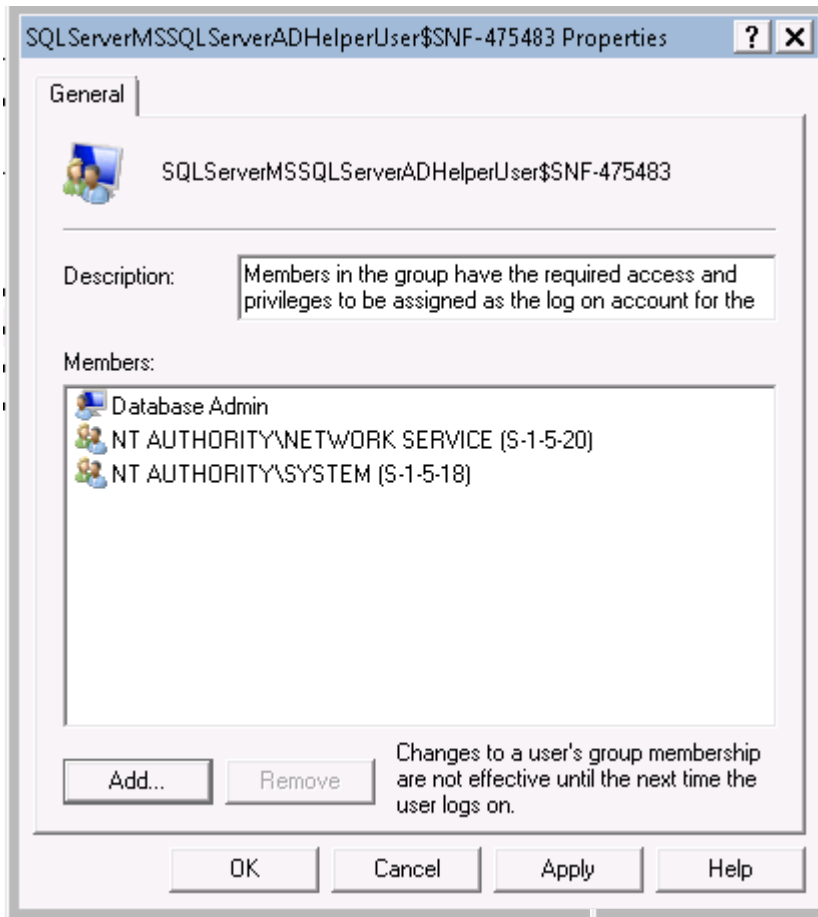
both locally and via remote access to this computer

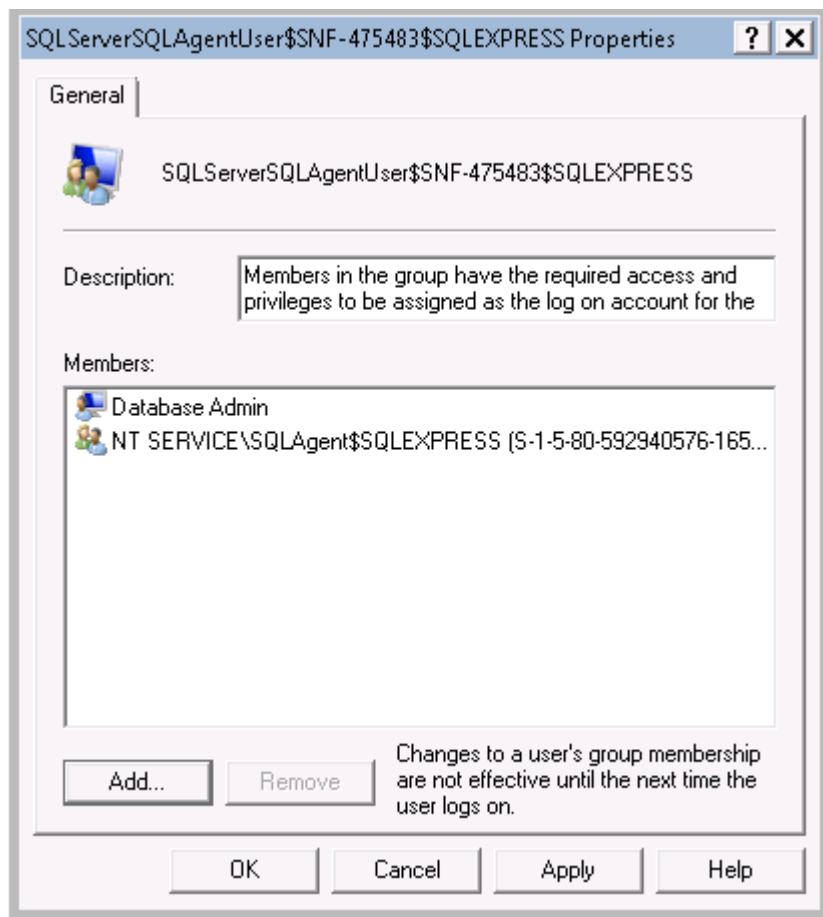
ance of SQL Server Browser in SQL Server 2008.

ance of SQL Server Active Directory Helper in SQL Server 2008.

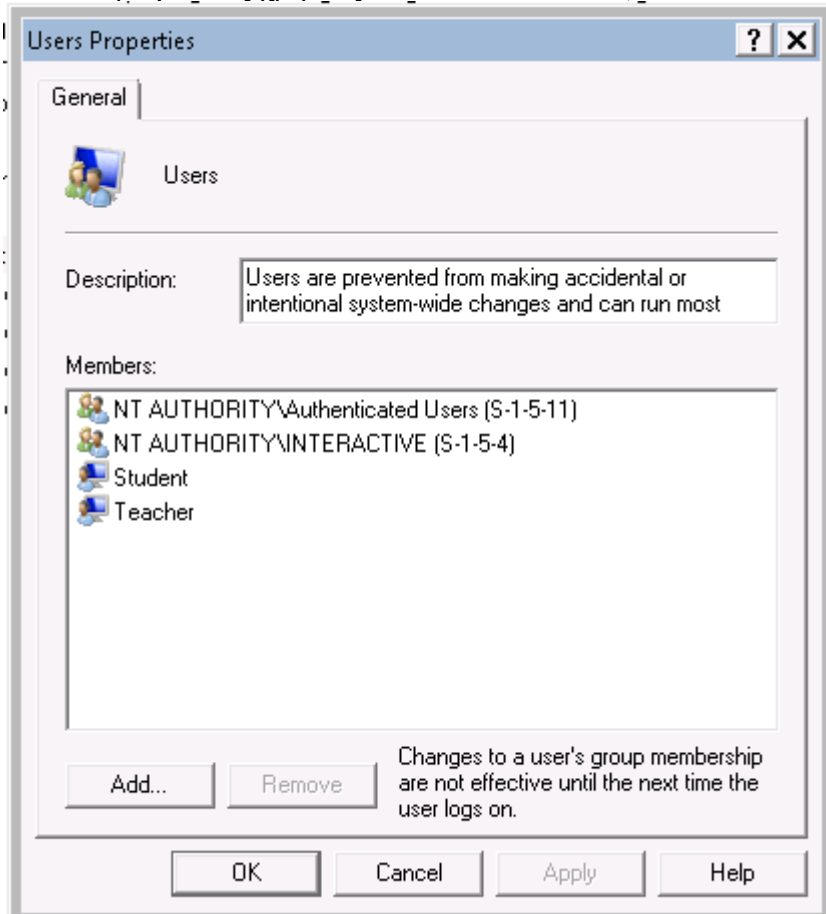
ce of SQL Server.

ance of SQL Server Agent.

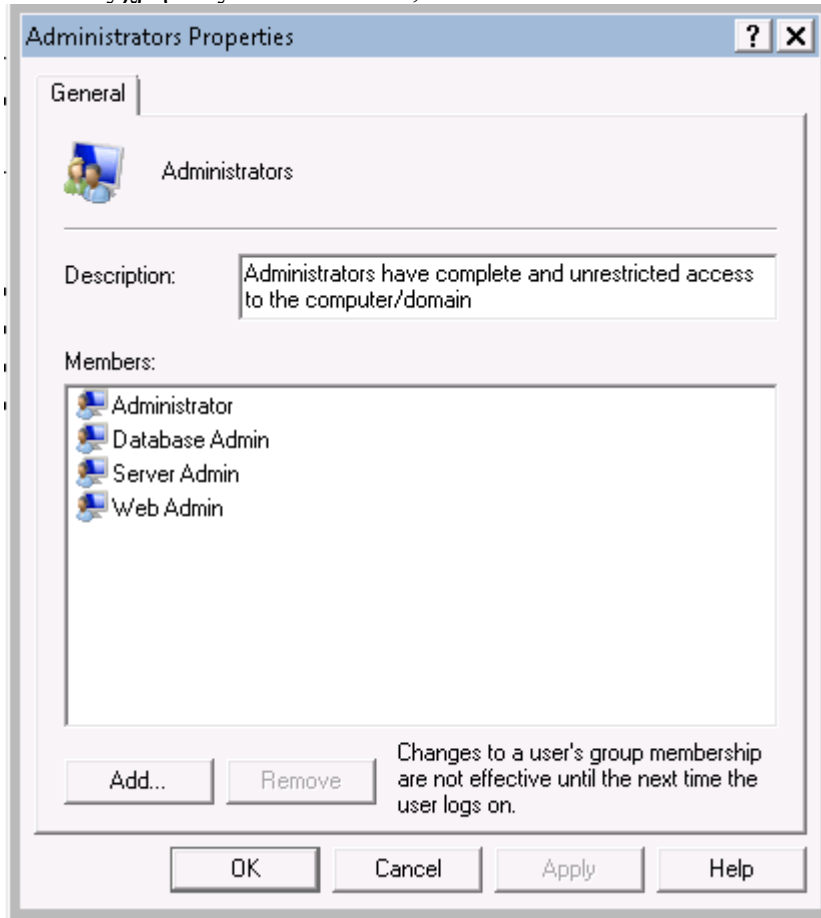




Τοποθετήσαμε τους χρήστες Teacher και Student, οι οποίοι είναι Standard Users στο group Users.



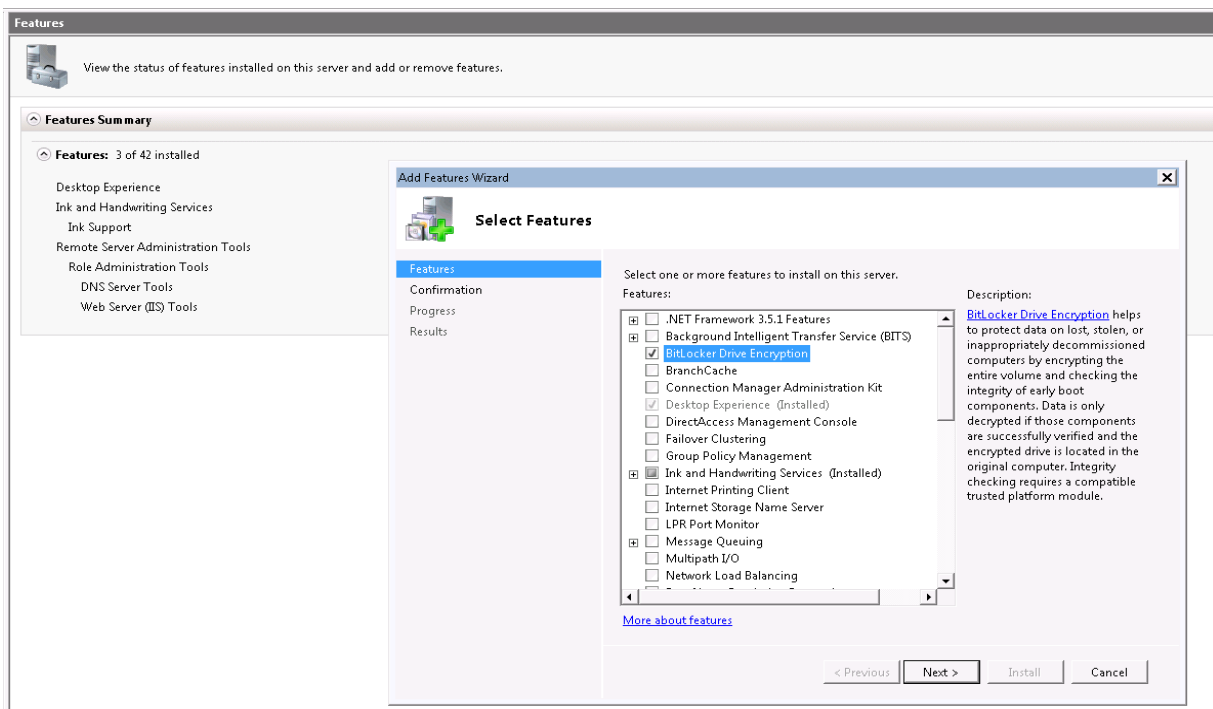
Και τους χρήστες Server Admin, Web Admin και Database Admin στο group Administrators.

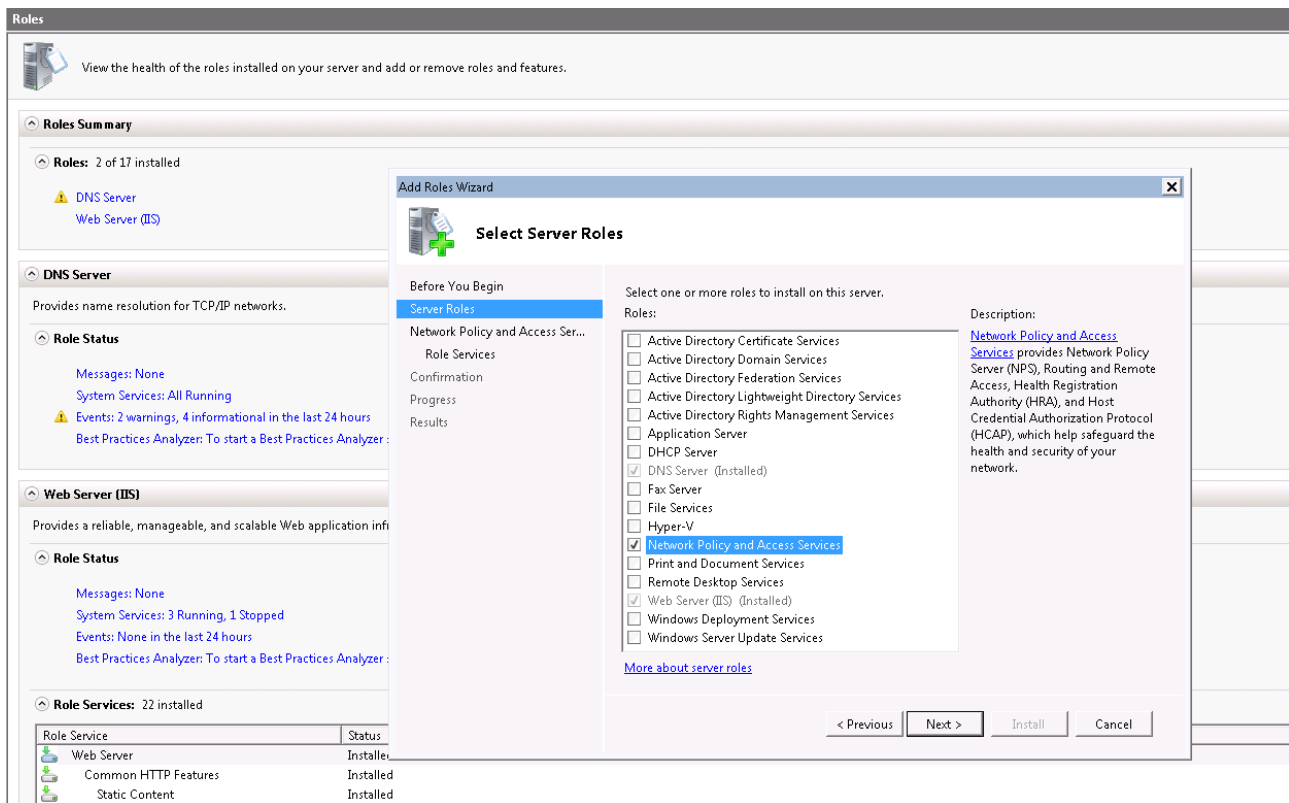


Συνεχίζοντας, εγκαταστήσαμε τα εξής:

-προστασία Δικτυακής Πρόσβασης (*Network Access Protection – NAP*)

-κρυπτογράφηση των σκληρών δίσκων (τεχνολογία *BitLocker Drive Encryption*)





Τελειώνοντας, κάναμε μία τελική αξιολόγηση του συστήματός μας, χρησιμοποιώντας το Microsoft Baseline Security Analyzer.

Σημείωση: Λόγω του μεγέθους του αρχείου txt, επισυνάπτεται μέσα στο rar αρχείο που θα σας στείλουμε.

-Βιβλιογραφία-Βοηθητικοί Συνδέσμοι

-<http://infosecawareness.in/sysadmin/Windows-2008-Hardening.pdf>
“*Hardening Windows Server 2008*”

-<https://www.youtube.com/watch?v=qjW4NSadIM8>
“*How to Configure Windows Server 2008 R2*”

-<https://www.youtube.com/watch?v=Buj9oEgbRt8>
“*Installing a Domain Controller - Best Practices for Windows Server 2008 R2*”