

AD health check

Tämän harjoituksen ja ohjeen tarkoitus on käydä läpi AD-ympäristön toiminnan kannalta keskeiset asiat ja varmistaa siten ympäristön mahdollisimman luotettava toiminta.

AD-tarkistuslista asentamisen jälkeen

Buutattuasi DC-palvelimen asennuksen jälkeen, suorita seuraavat toimenpiteet – voit ajaa ne tarkistuksen omaisesti myös milloin tahansa muulloinkin.

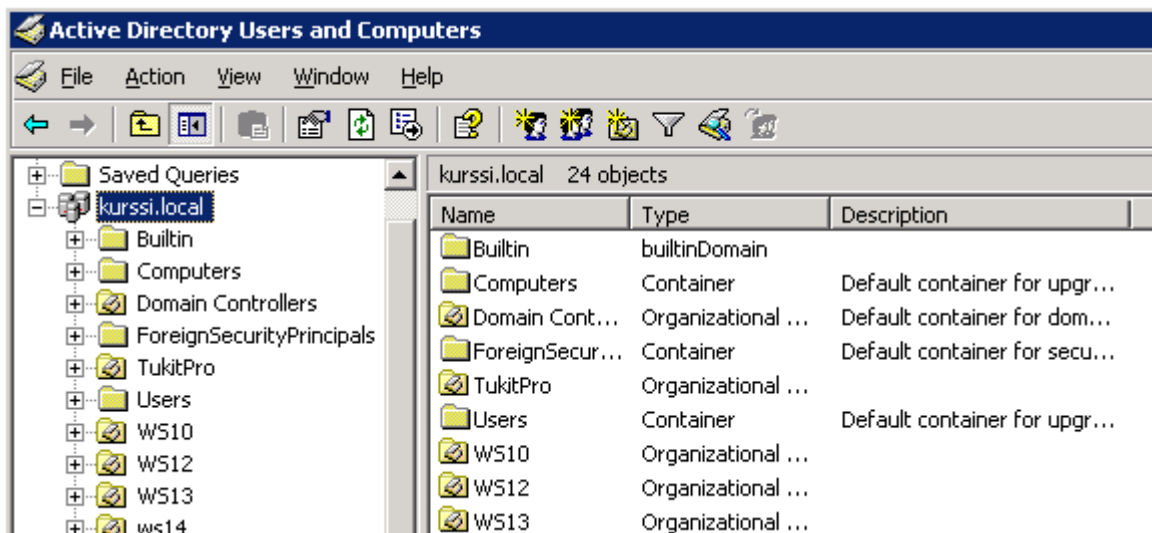
Ota etätyöpöytäyhteys admin-tunnuksella palvelimella

1. Tarkista että valvontatyökaluihin (Administrative tools) ovat tulleet uudet AD:n hallintavälineet



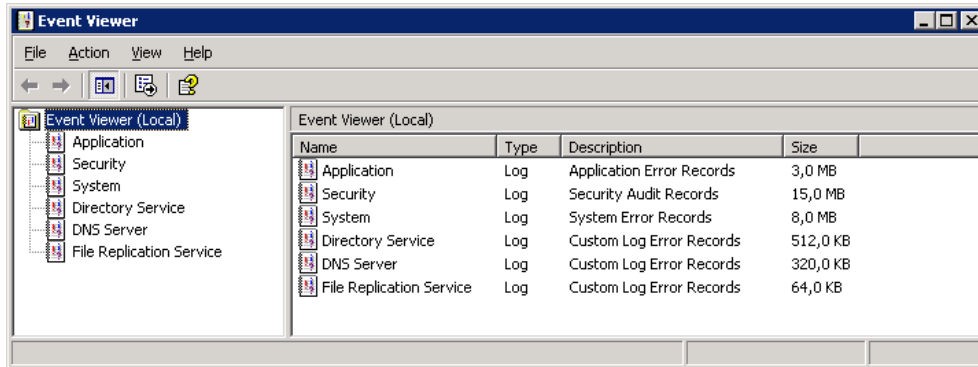
2. Käynnistä toimialueen Active Directory Users and Computers – helpoin tapa on Windows + R: dsa.msc ja tarkista että se aukeaa ja kansiot aukeavat

Muista – XP-työasemaan saat samat ohjelmat ajamalla 2003-asennusrompulta
 \i386\adminpack.msi – tai muihin palvelimiin,
 joissa ei ole esmes DC/DNS/DHCP toiminnassa

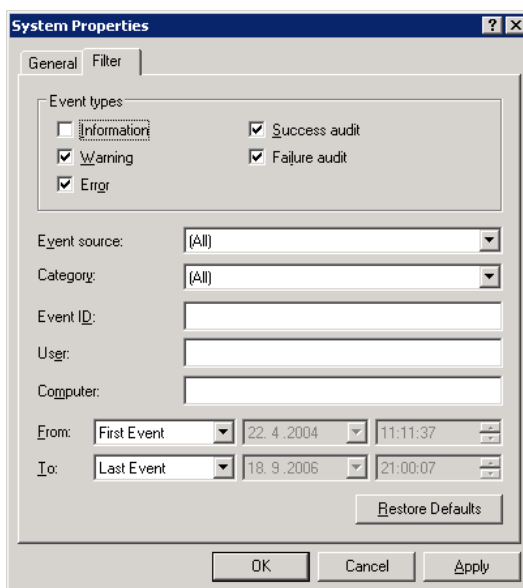


3. Tapahtumienvälvonta

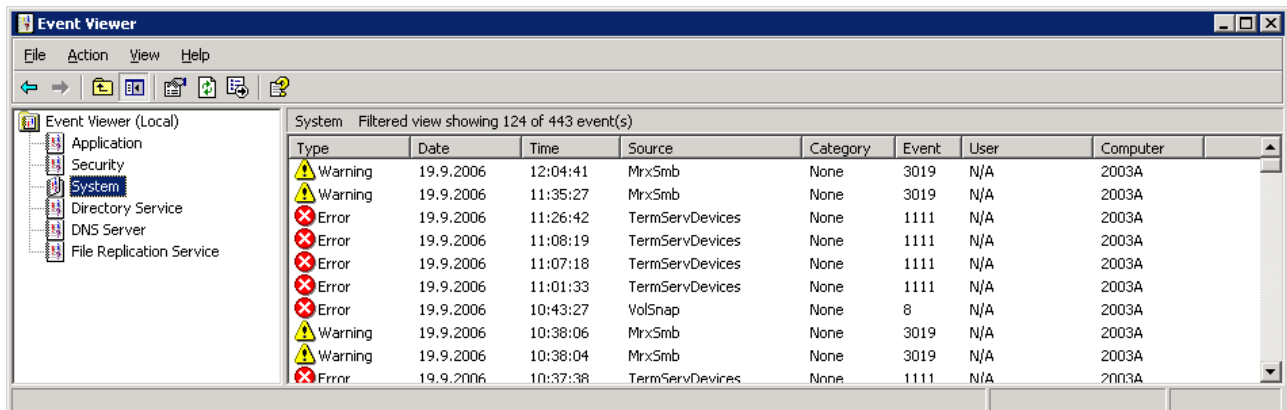
Katso tapahtumienvälvonnasta (eventvwr) kaikki kuusi lokia vaarallisimpien punaisten virheiden ja vaarattomampien keltaisten varoitusten varalta.



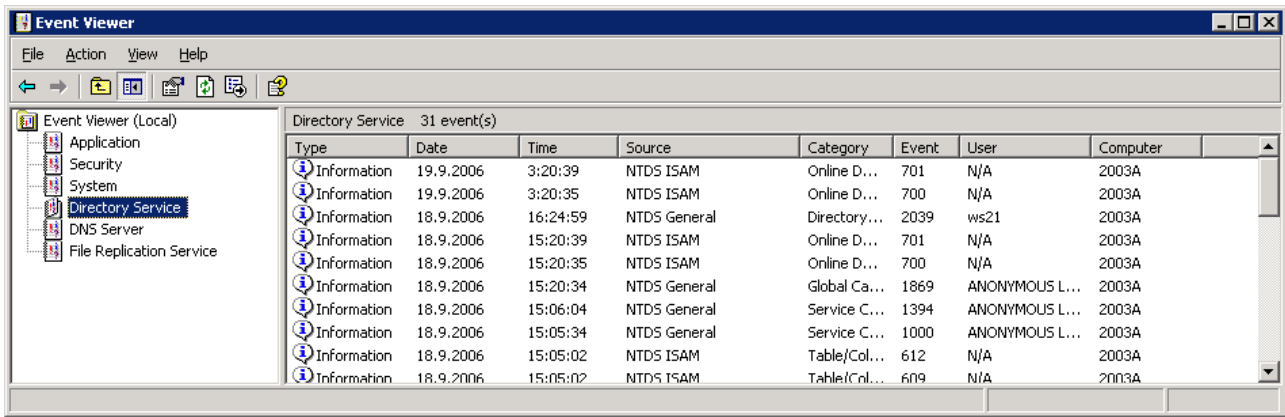
Helpoiten teet tämän ottamalla lokin ominaisuuksista (oikea painike | properties) rastin pois kohdasta information:



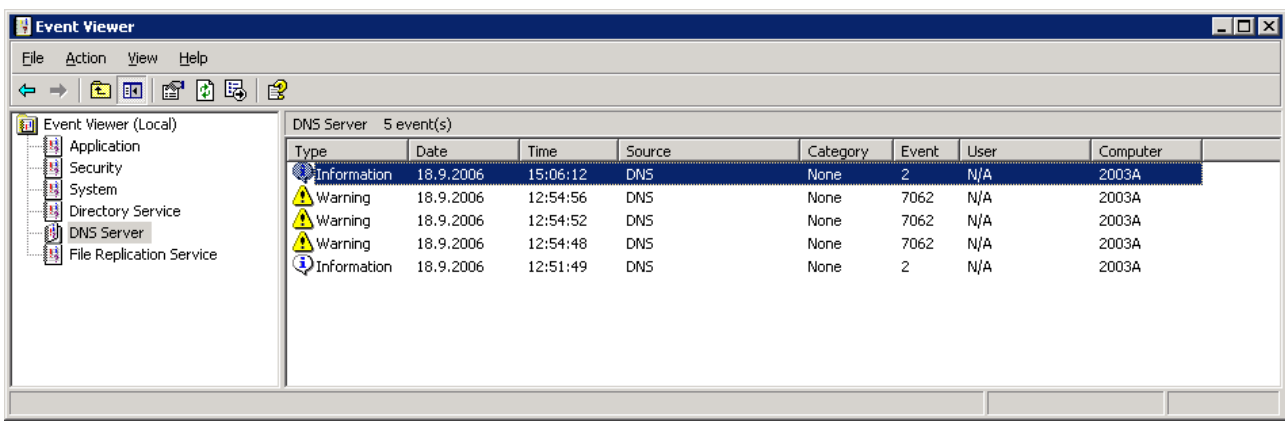
Tee tämä sama kaikille lokeille.



Tilanne ei pitäisi näyttää tällaiselta vaan ainoastaan sinisiä ilmoituksia!

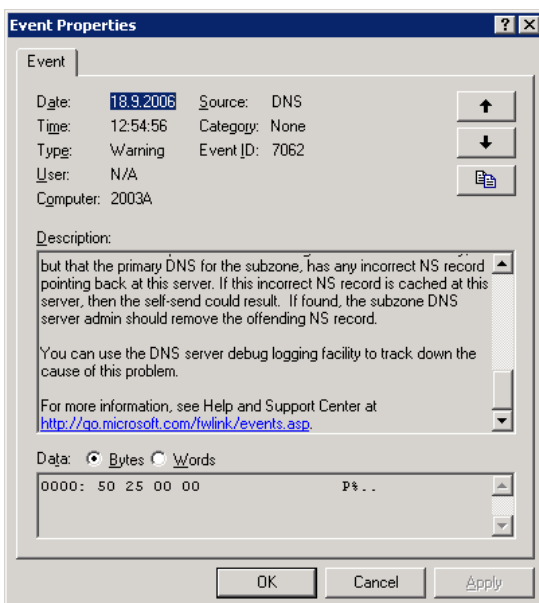


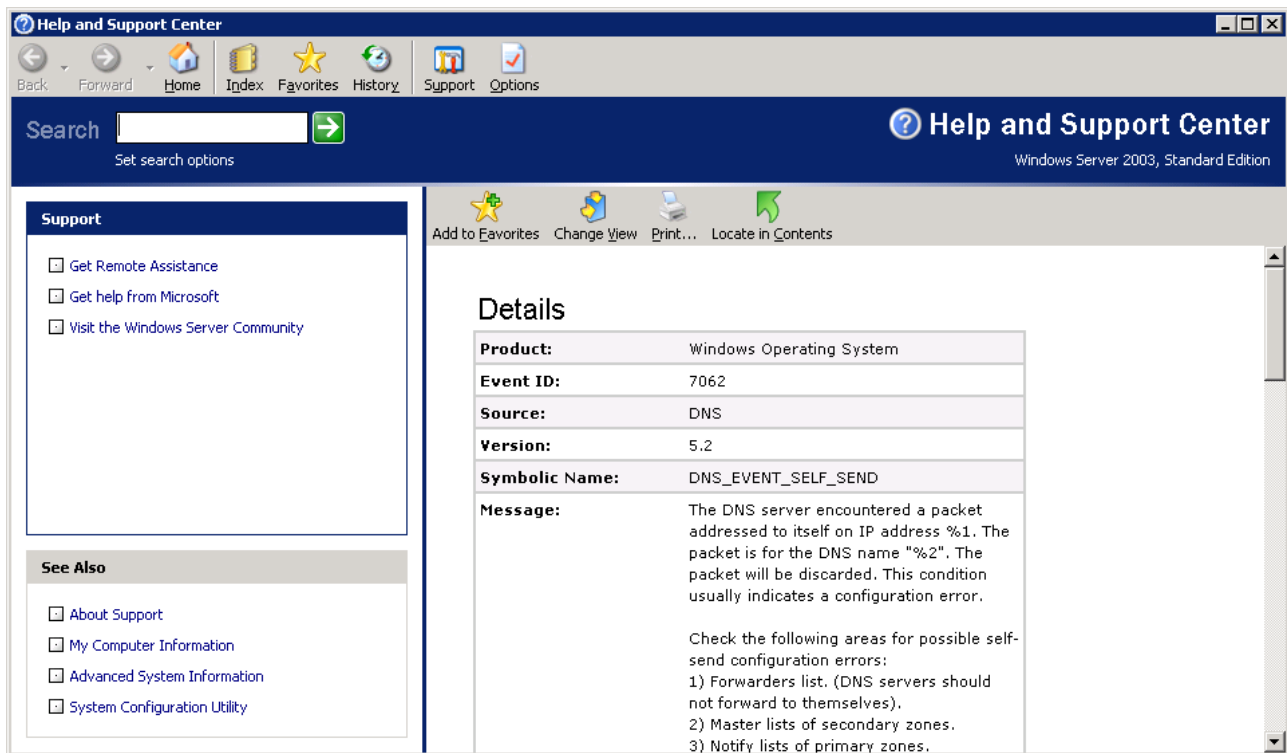
Kaikista tärkeintä AD:n kannalta on se, että Directory Service ja DNS Server ovat ok:



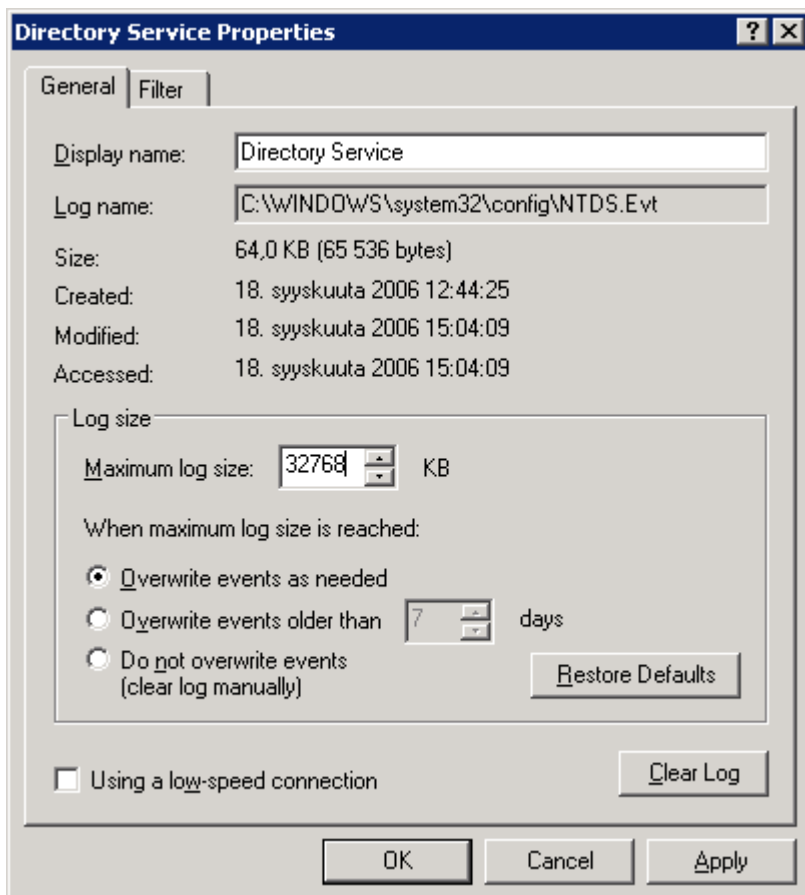
Vaikka tuossa on kaksi keltaista, ylin sininen ”kuittaa” edelliset ongelmat eli no hätä.

Jos löydät huolestuttavia uusia ilmoituksia, saat niistä lisätietoja joko googlolla tai www.eventid.net. Kokeile myös ilmoituksesta aukeavaa Microsoftin omaa ohjetta, johon on linkki aivan Description kohdan lopussa.





Täältä löytyy kanssa usein apua.



Kasvata myös kaikkien lokien koko vähintään 32 megatavuun, jos tapahtumia tulee enemmän, tarvittaessa vaikkapa 40-50 megatavuun.

4. Palvelimien sijainti oikeissa toimipaikoissa

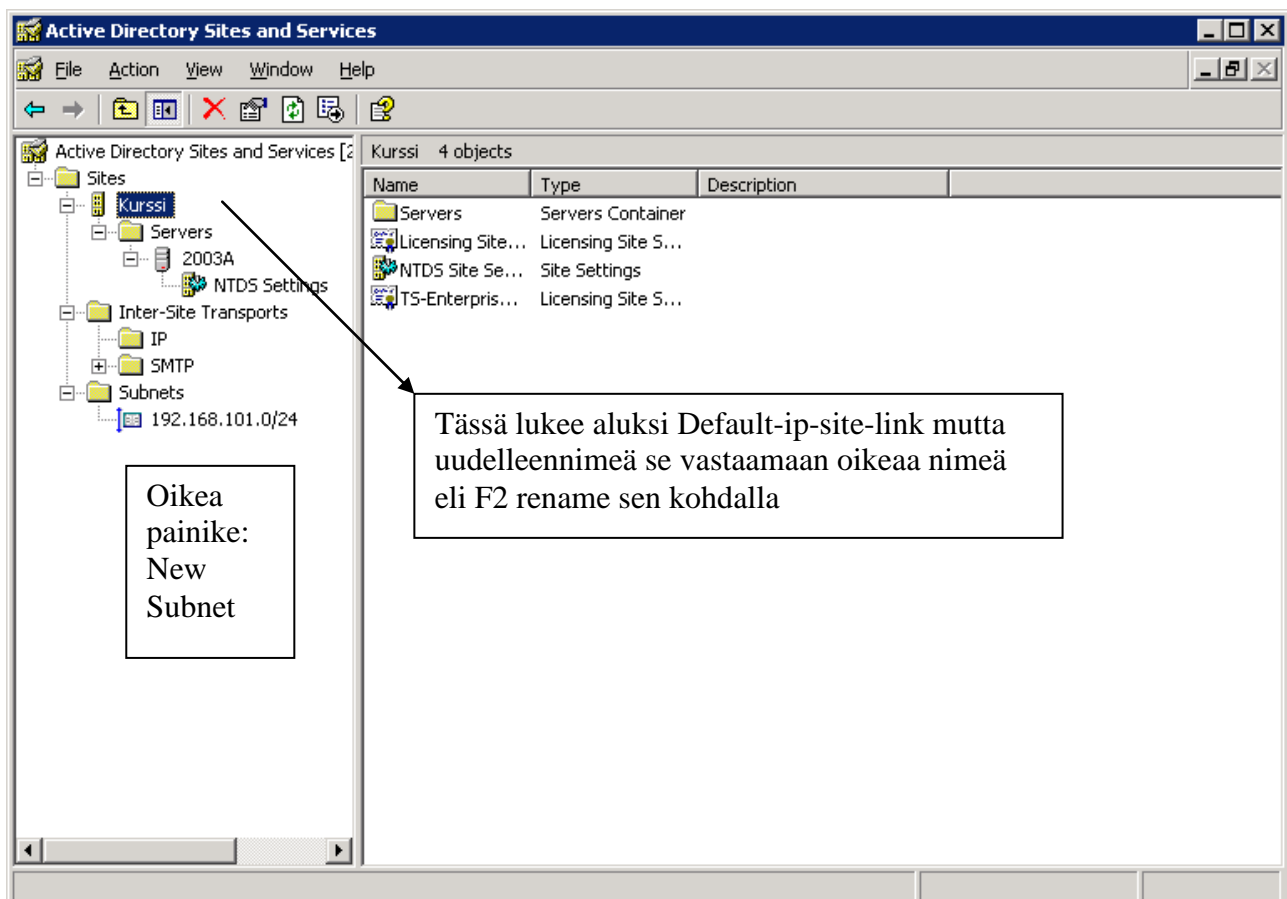
AD:n oikeaoppisen toiminnan kannalta jokaisessa toimipaikassa kannattaisi useimmissa tapauksissa sijaita oma DC-palvelin. Mikäli toimipaikan koko on pieni tai tietoliikenneyhteys toiseen DC-palvelimen sisältävään paikkaan on nopea, ei DC-palvelinta välttämättä tarvita.

Joka tapauksessa olemassa olevat palvelimet pitää sijoittaa olemassa oleviin ip-aliverkkoihin ja mahdollisiin toimipaikkoihin.

AD Sites and services-ohjelma:

Katso Active Directory Sites and Services ja sieltä Default-First-Site-Name ja varmista että asennettu palvelin löytyy sieltä. Kurssin tapauksessa siellä lukee jo Kurssi.

Luo Subnets-kohtaan tarvittaessa puuttuvat aliverkot ja lisää / uusi palvelin & tarkista että muut palvelimet sijaitsevat oikeissa toimipaikoissa (site).



New Subnet-valinnalla liitetään aliverkko – site – ja palvelin toisiinsa:

New Object - Subnet

Create in: kurssi.local/Configuration/Sites/Subnets

Address: 0 . 0 . 0 . 0

Mask: 0 . 0 . 0 . 0

Name:

Enter the subnet address and mask. This will be automatically translated into a subnet name in the form network/bits-masked.
Example: address 10.14.209.14 mask 255.255.240.0 becomes subnet 10.14.208.0/20.

Select a site object for this subnet.

Site Name
Kurssi

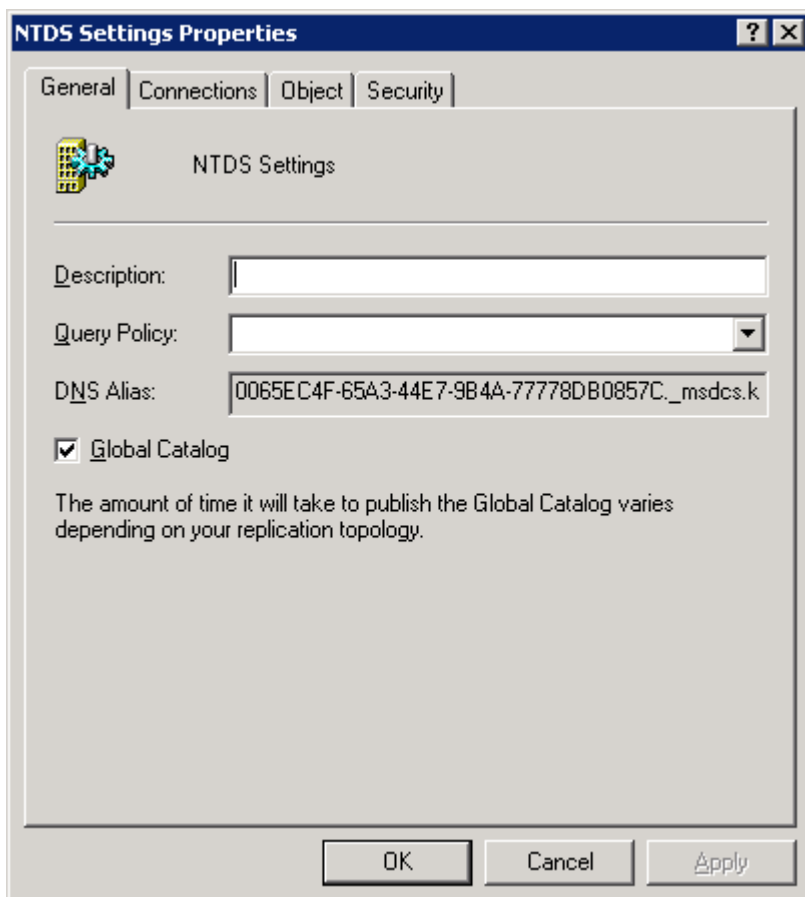
OK Cancel

Global Catalog Server ominaisuus

Edelleen edellisessä AD Sites and Services-ohjelmassa:

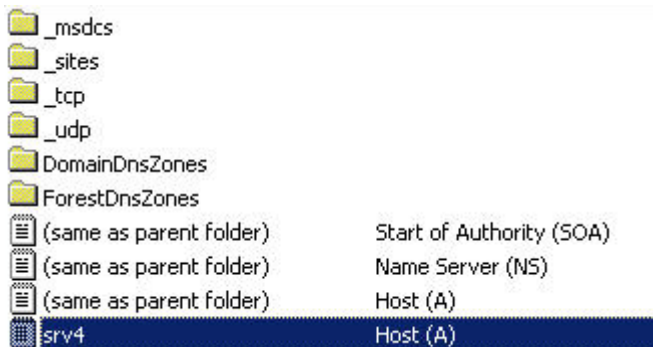
Kaksoisnapauta Sites, avaa Servers ja valitse asentamasi palvelin ja hae sieltä NTDS Settings.

Napauta sen kohdalla oikea painike ja Properties eli ominaisuudet. General-välilehdellä tulisi olla rasti kohdassa Global Catalog.



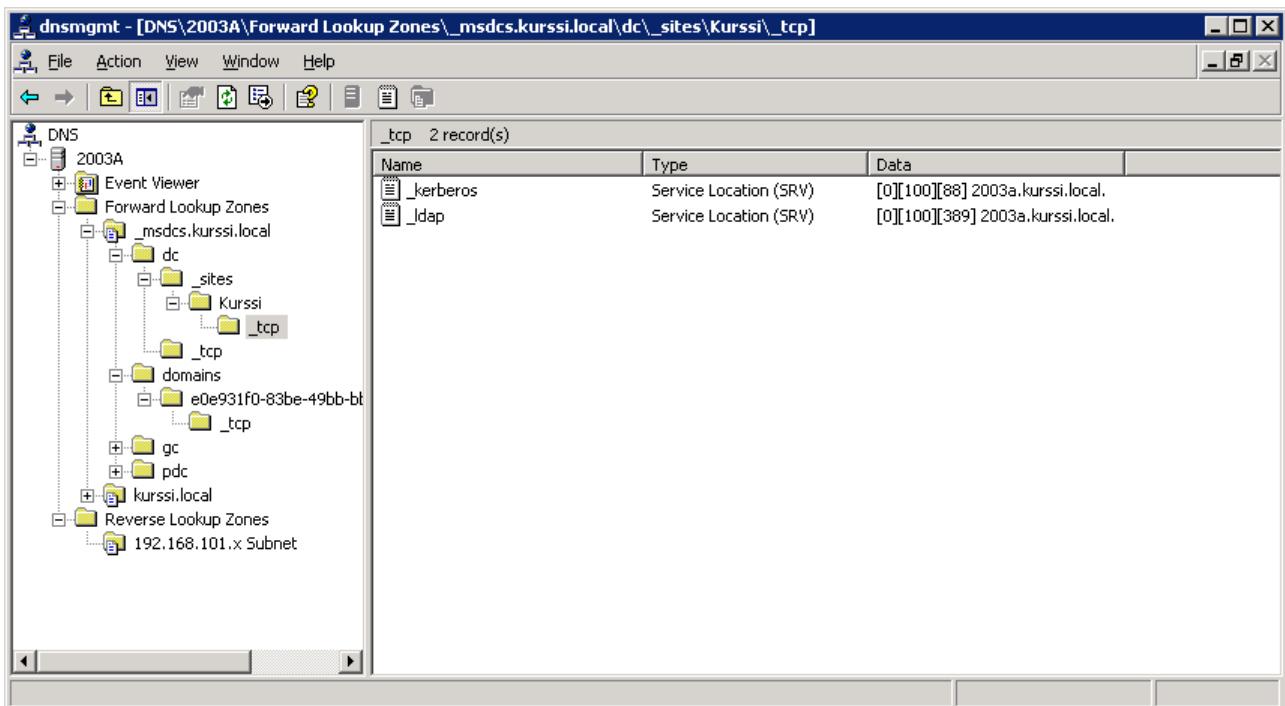
5. DNS:n toiminta ja määrittelyt

Avaa DNS-hallinta ja avaa sieltä laatimasi toimialueen-mukainen dns-vyöhyke. Tarkista, että se sisältää alla olevat neljä tietuetta:



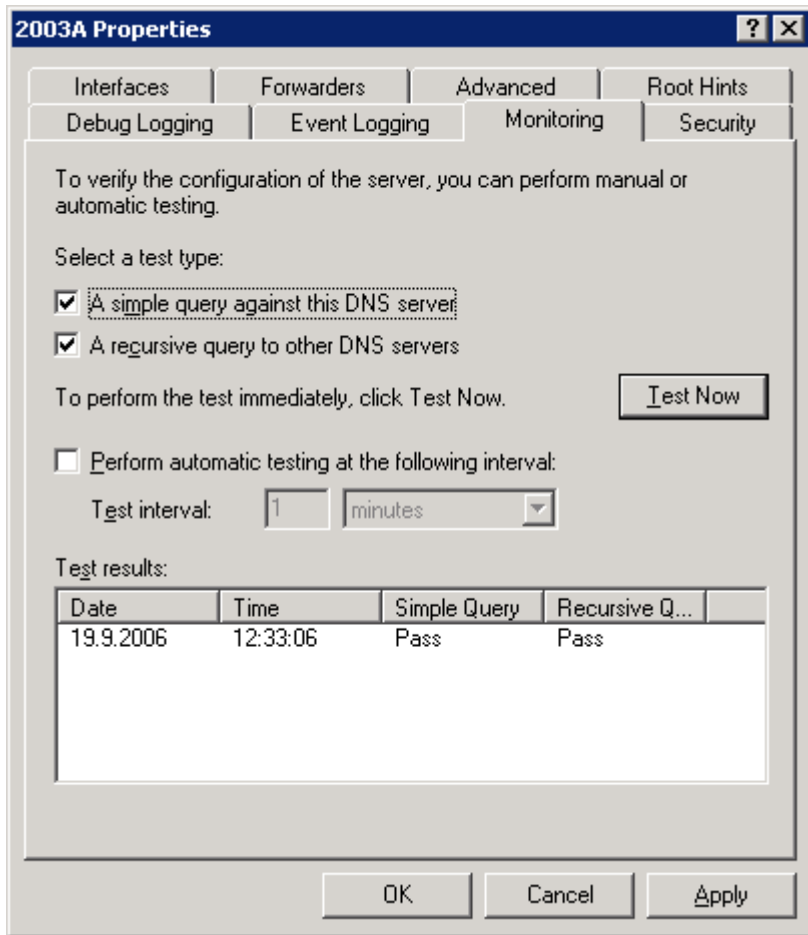
Jos näitä ei löydy, AD / palvelin ei tule toimimaan oikein.

Tarkemmin auki purettuna:

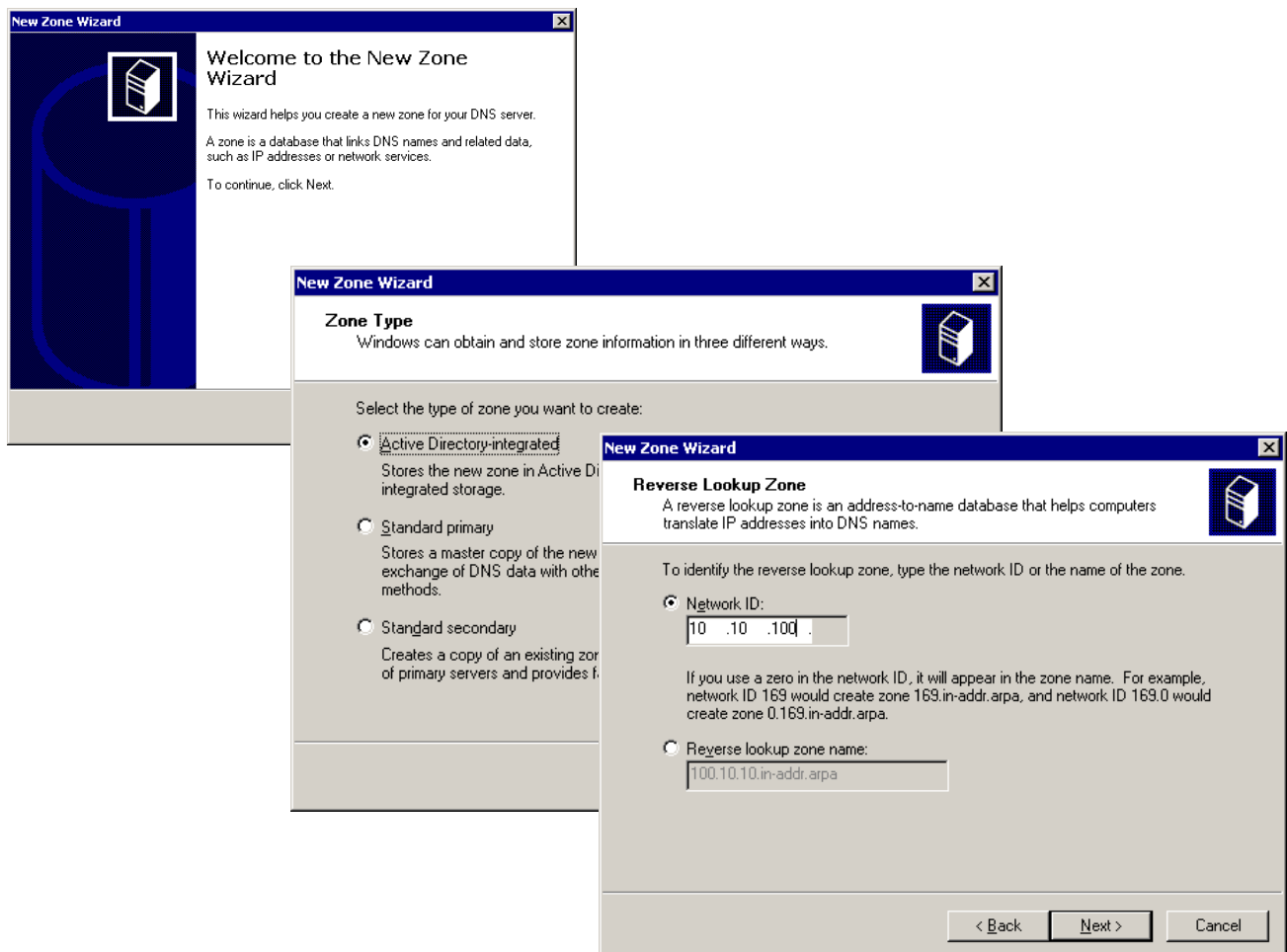


Kun avaat kansioita, huomaat miksi DNS on niin tärkeä – kaikki oleellinen on tallennettu tänne!

Testaa DNS-kyseylyiden toiminta eli valitse 2003a-palvelimen päältä oikea painike | Properties | Monitoring-välilehti | rastit | Test now:

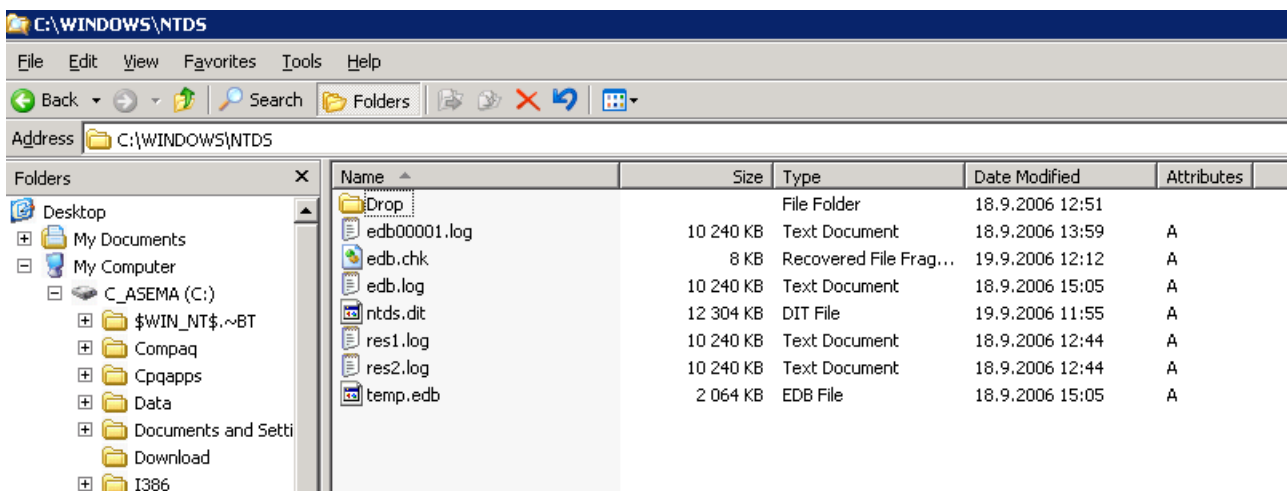
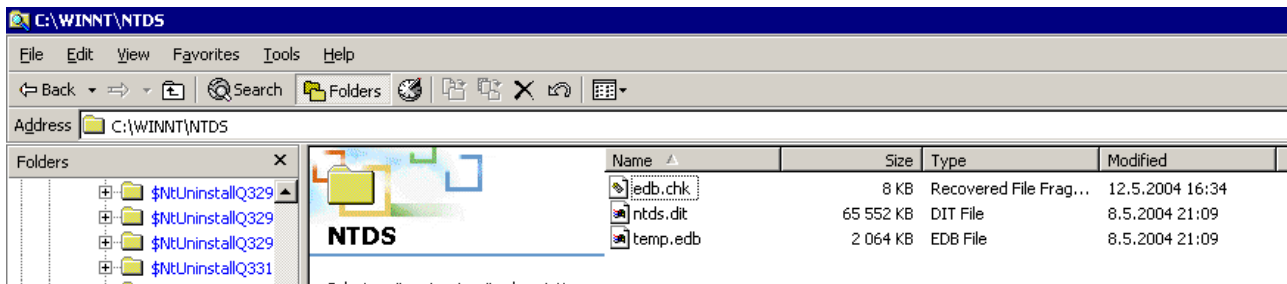


Tee käänteinen nimiselvitysvyöhyke kaikille käytössä oleville IP-avaruuksille:



7. NTDS.DIT-tietokantatiedosto

Tarkista että AD-tietokanta löytyy eli c:\windows\ntds ja siellä ennen kaikkea ntds.dit-tiedosto.



Kaikki tietokannan käsittely tehdään NTDSUTIL-apuohjelmalla – joko kun AD eli kanta on päällä (esimerkiksi FSMO-roolien siirto | roles tai kun buutataan Directory Services Restore Mode (vaatii asennuksen yhteydessä määritetyn admin-tunnuksen) ja sieltä voidaan defragmentoida tietokanta tai tehdä tietokannan palautus.

```

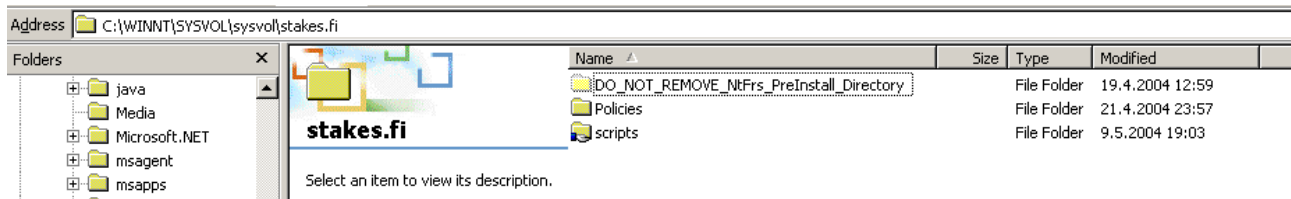
C:\WINNT\system32\cmd.exe - ntdsutil
C:\Documents and Settings\admin>ntdsutil
ntdsutil: roles
fsmo maintenance: ?
?
Connections          - Print this help information
Help                 - Connect to a specific domain controller
Help                 - Print this help information
Quit                 - Return to the prior menu
Seize domain naming master - Overwrite domain role on connected server
Seize infrastructure master - Overwrite infrastructure role on connected server
Seize PDC             - Overwrite PDC role on connected server
Seize RID master     - Overwrite RID role on connected server
Seize schema master  - Overwrite schema role on connected server
Select operation target - Select sites, servers, domains, roles and Naming Contexts
Transfer domain naming master - Make connected server the domain naming master
Transfer infrastructure master - Make connected server the infrastructure master
Transfer PDC         - Make connected server the PDC
Transfer RID master  - Make connected server the RID master
Transfer schema master - Make connected server the schema master
fsmo maintenance: _

```

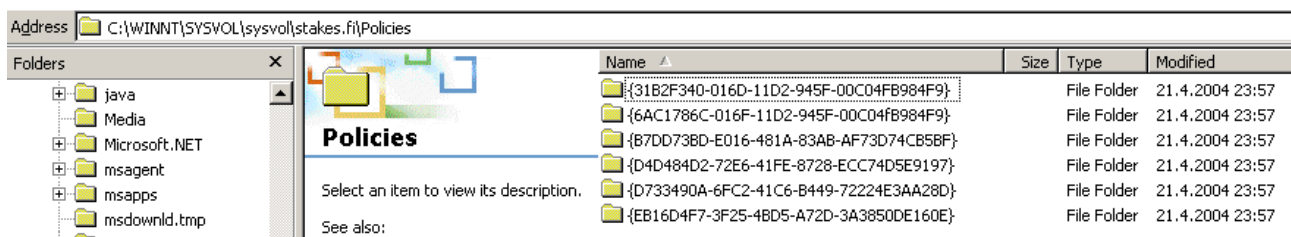
Seize = alkuperäinen palvelin ei ole pystyssä eikä IKINÄ enää nouse
 Transfer = alkuperäinen on ihan ok ja online eli roolit halutaan vain siirtää esimerkiksi uuteen, luotettavampaan ja suorituskykyisempään palvelimeen

6. SYSVOL-resurssi ja ryhmäkäytännöt

Tarkista että sysvol-kansio / resurssi löytyy eli c:\windows\sysvol\sysvol\domain nimesi.



Sen alla pitäisi olla mm. policies ja scripts-kansiot. Policies alta löytyy ryhmäkäytännöt, oletuksena siellä pitäisi olla:



eli kaksi ensimmäistä ovat ns. sisäänrakennettuja, muut ovat uusia, itse tehtyjä ryhmäkäytäntöjä:

{31B2F340-016D-11D2-945F-00C04FB984F9} - Default Domain policy

{6AC1786C-016F-11D2-945F-00C04FB984F9} - Default Domain Controllers policy

ja tarkemmalla tasolla:

\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}

Name	Size	Type	Modified
Adm		File Folder	21.4.2004 23:57
MACHINE		File Folder	21.4.2004 23:56
USER		File Folder	21.4.2004 23:57
GPT.INI	1 KB	Configuration Settings	10.5.2004 12:20

\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE

Name	Size	Type	Modified
Applications		File Folder	18.1.2001 14:54
Microsoft		File Folder	21.4.2004 23:56
Scripts		File Folder	21.4.2004 23:57
Registry.pol	3 KB	POL File	16.1.2001 16:54

Muista komennot:

gpupdate W2k: secedit /refreshpolicy machinepolicy tai computerpolicy
 gresult
 gresult /v
 rsop.msc

Katso komentokehotteessa net share:

- pitäisi löytyä sekä netlogon että sysvol

```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\admin>net share

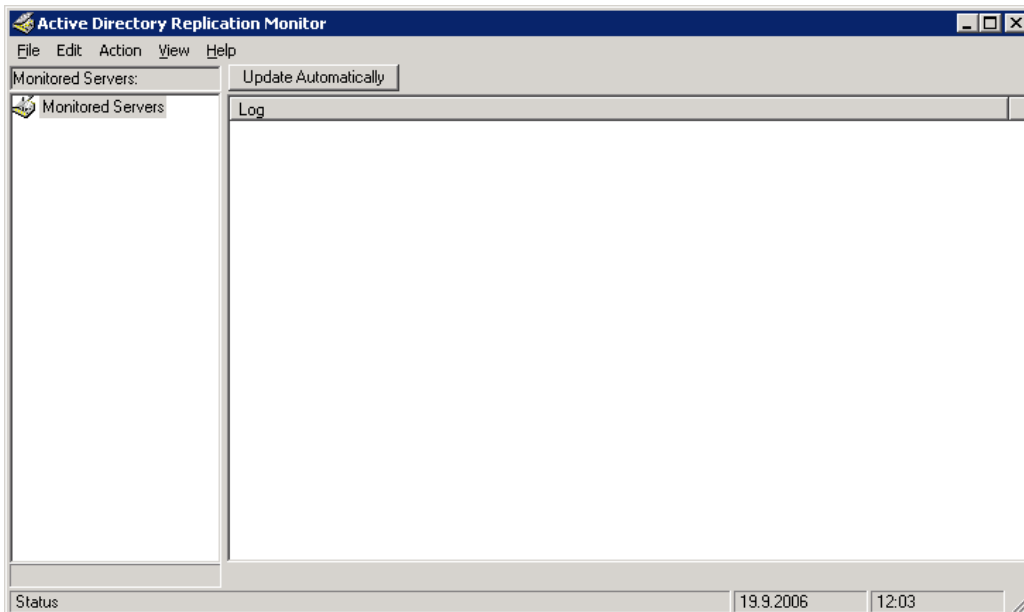
Share name      Resource                                Remark
-----
IPC$            Remote IPC
D$              D:\                                     Default share
C$              C:\                                     Default share
F$              F:\                                     Default share
ADMIN$          C:\WINNT                               Remote Admin
E$              E:\                                     Default share
NETLOGON        C:\WINNT\SYSTEM32\sysvol\stages.f i\SCRIPTS
Logon server share
SYSVOL          C:\WINNT\SYSTEM32\sysvol               Logon server share
The command completed successfully.

C:\Documents and Settings\admin>_
```

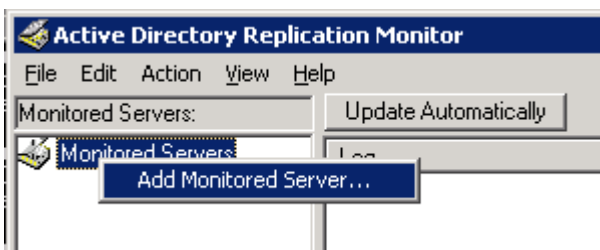
Netlogon on siis "NT" netlogon eli netlogon-skriptit yms sinne!

7. Replication Monitor eli replmon-ohjelma

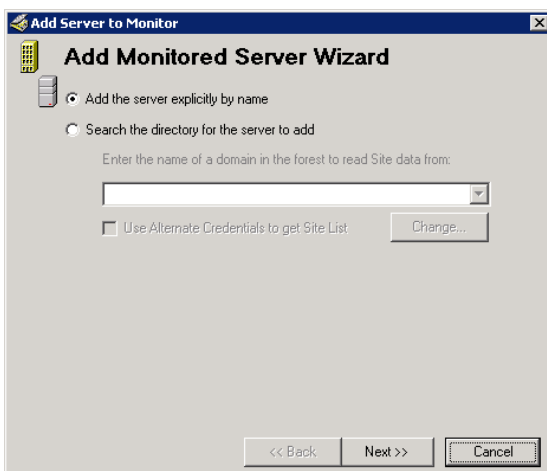
Asenna Support Tools (on kurssilla yleensä valmiiksi asennettu) ja aja sieltä Active Directory Replication Monitor. Saat sen käyntiin myös komennolla Win + R ja syötä: replmon

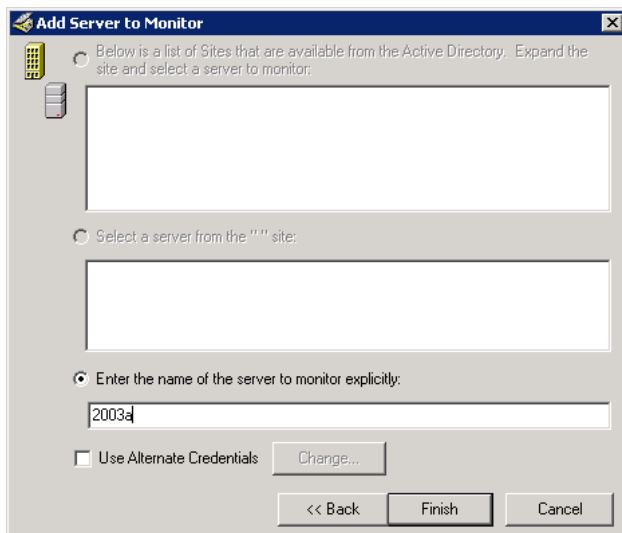


Napauta hiiren oikea painike Monitored Servers-kohdalla:

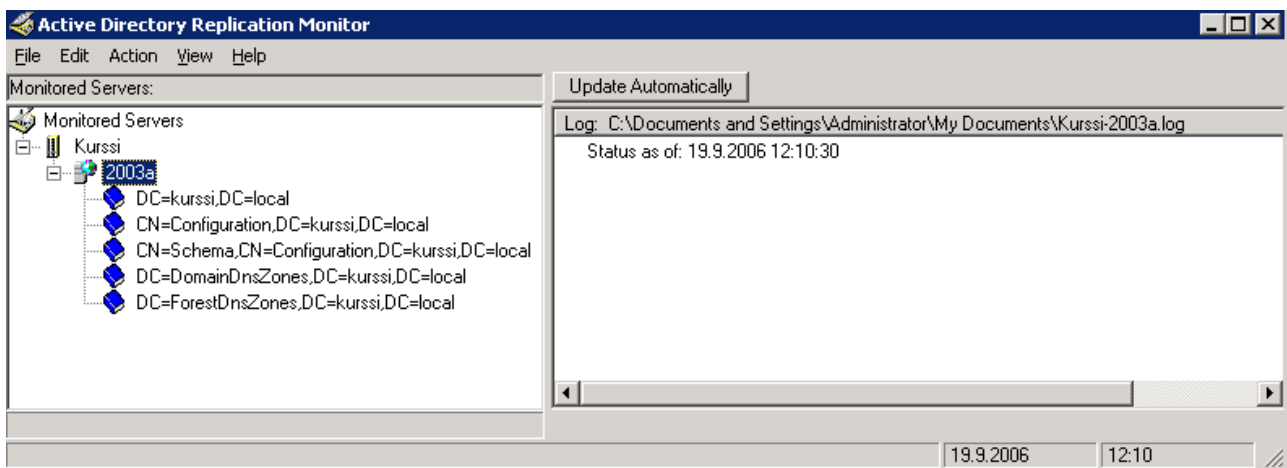


Napauta Next:





Syötä palvelimen osoite eli tässä tapauksessa: **2003a**
ja napauta Finish.

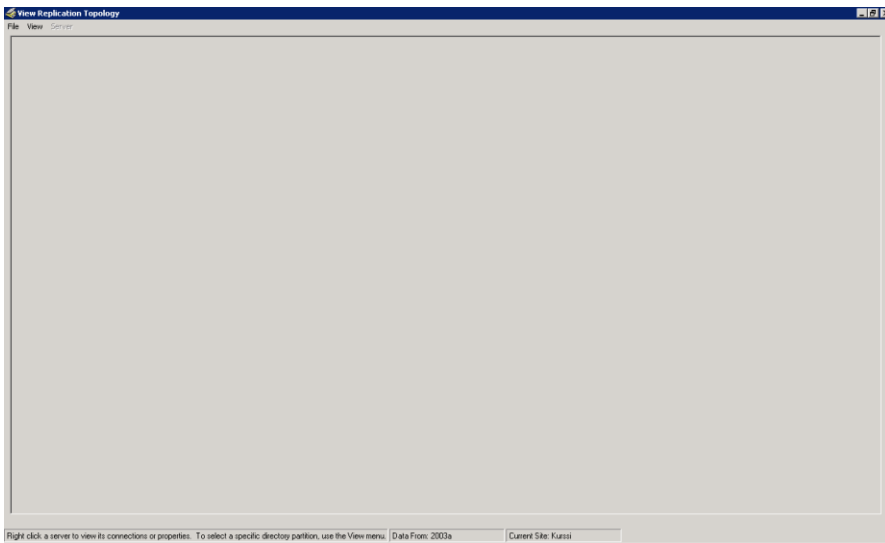


Lisää samalla tavalla muut DC-palvelimet.

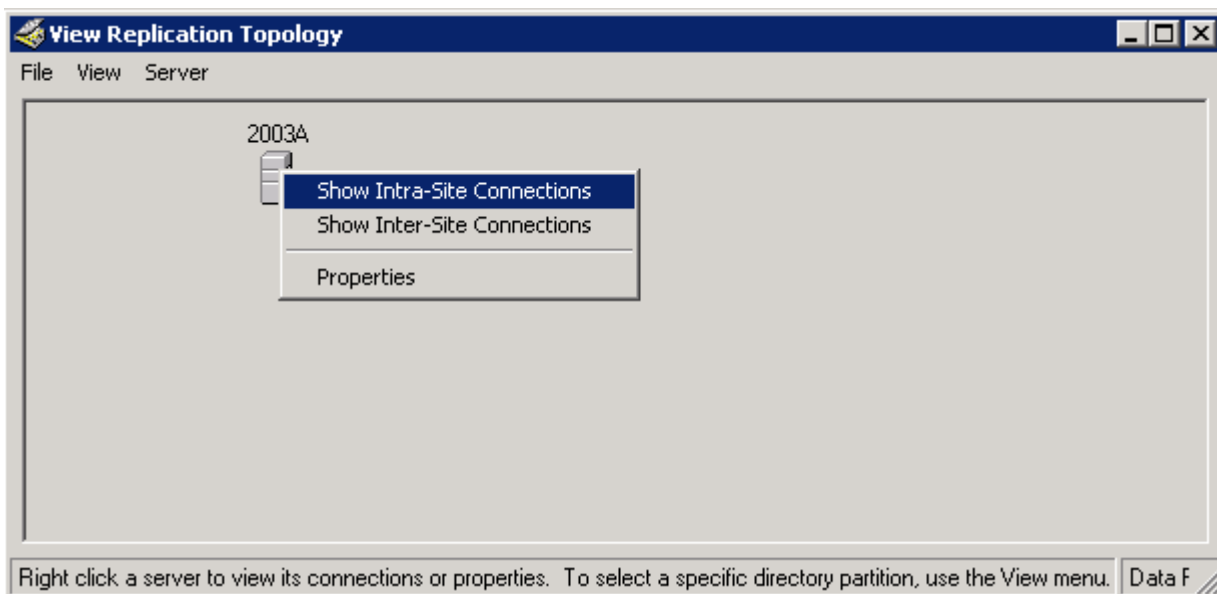
Kaikista oleellisin on hiiren oikea painike palvelimen kohdalla:



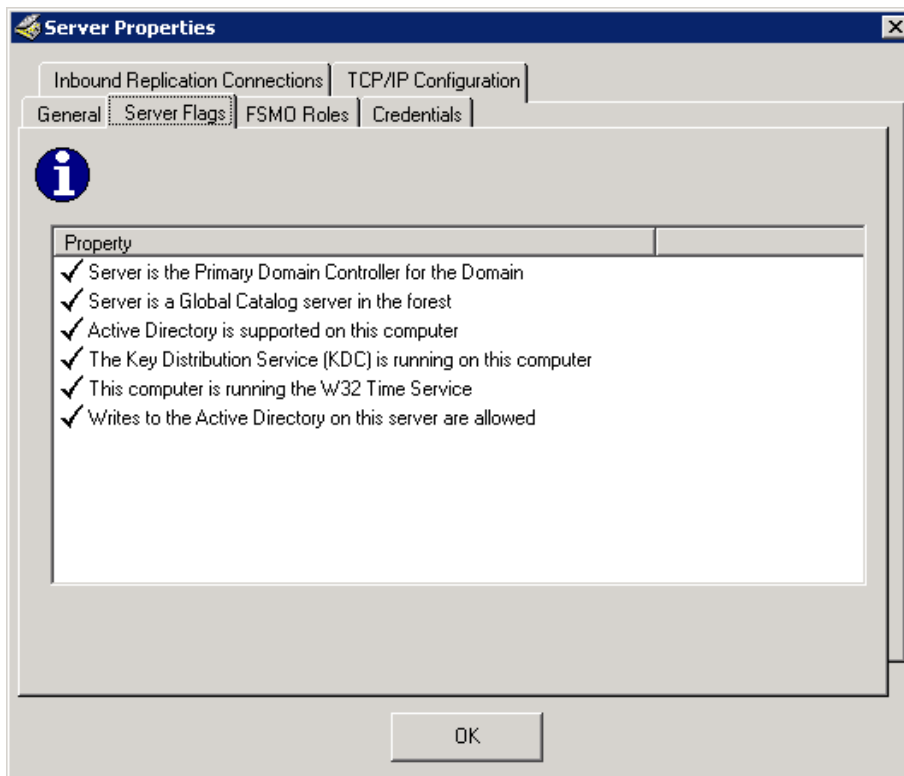
Kokeile kaikki eri vaihtoehdot paitsi Clear Log ja Delete! Osa valinnoista ei kenties kerro alkuvaiheessa mitään tai kysyy tarkempia tietoja, jolloin voit sen kohdan keskeyttää. Huomaa vielä, että valinnassa Show Replication Topologies saat esille:



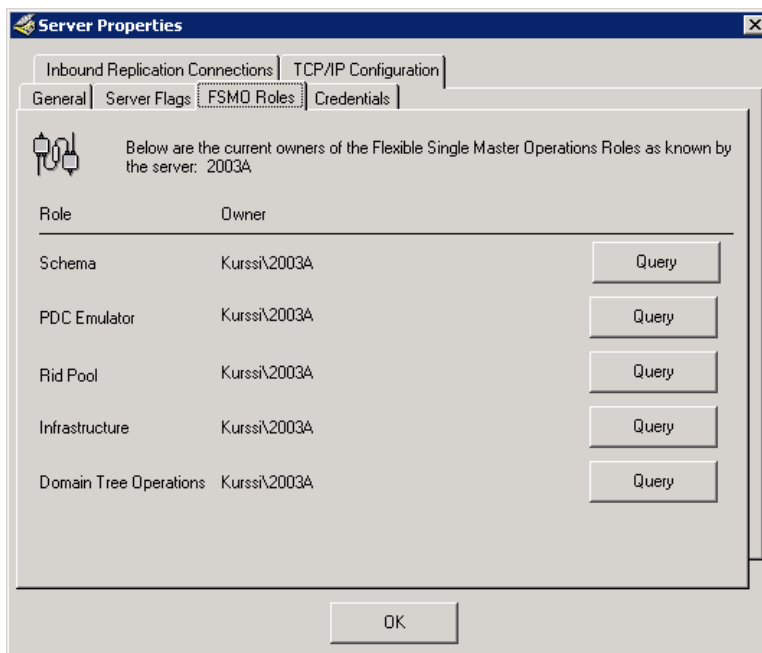
Valitse View-valikon kohta Connection Objects Only.



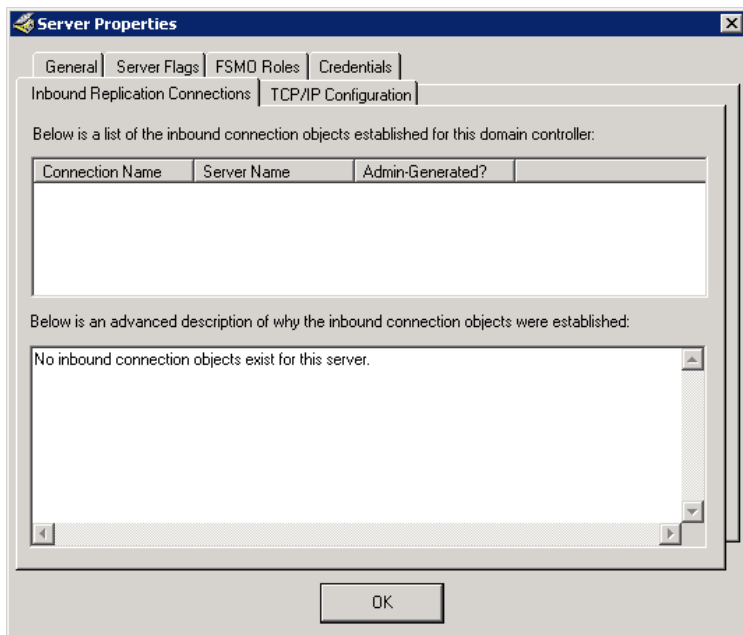
Napauttamalla palvelimen kohdalla voit pyytää ohjelmaa esittämään replikoinnin toimipaikan sisällä (Show intra-site connections) ja toimipaikkojen välillä (Show Inter-Site Connections). Katso myös properties-kohta. Sen takaa löytyy mm:



- keskeiset palvelimen toimintatilat eli mm. PDC-ominaisuus ja GC
- aikapalvelut



FSMO-roolit – query-valinnalla voit varmistaa, että ne ovat ok.

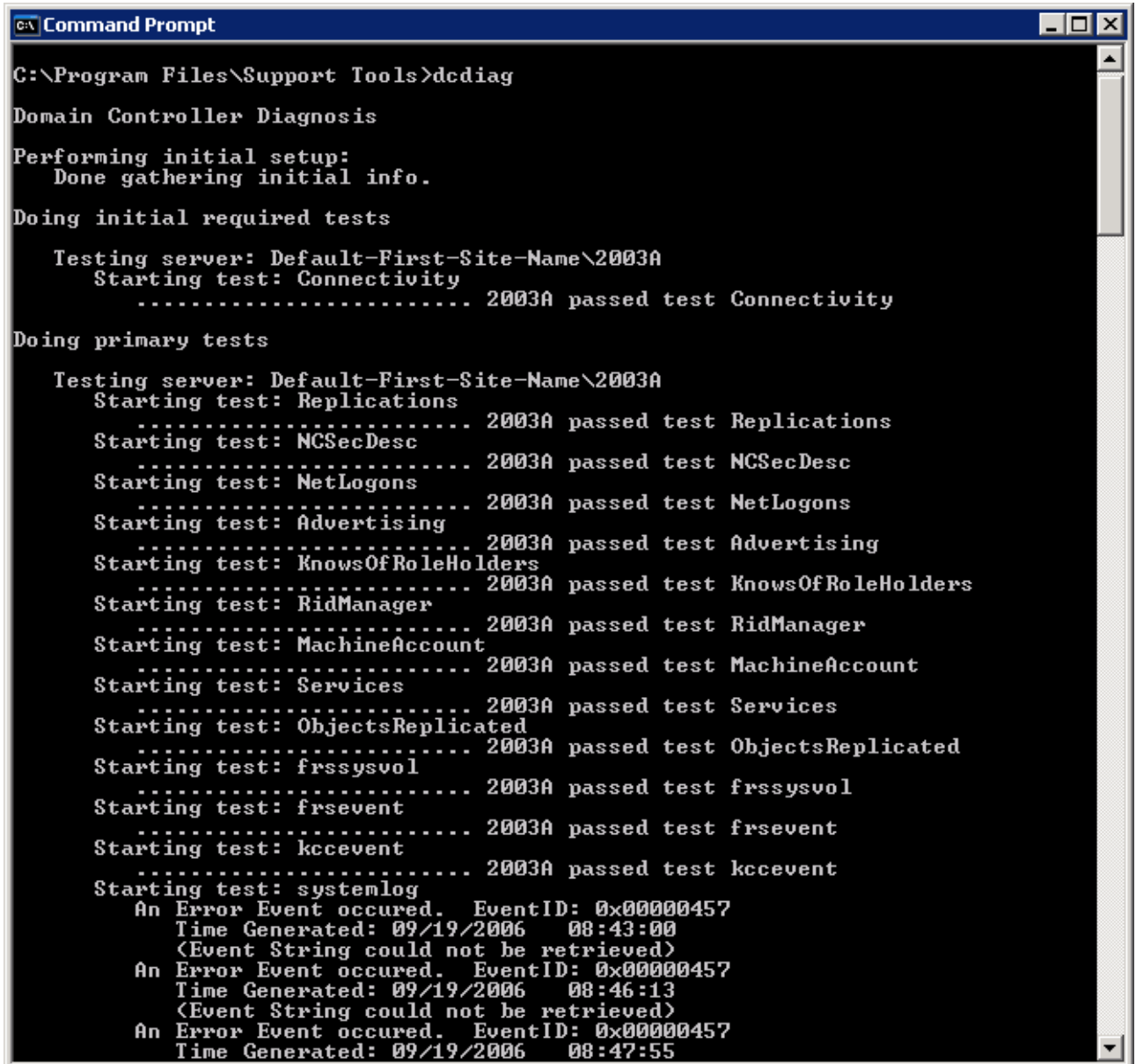


Replikointi on tyhjä, koska muita palvelimia ei ole.

Voit lopettaa ja sulkea tämän ikkunan.

9. DCDIAG-ohjelma

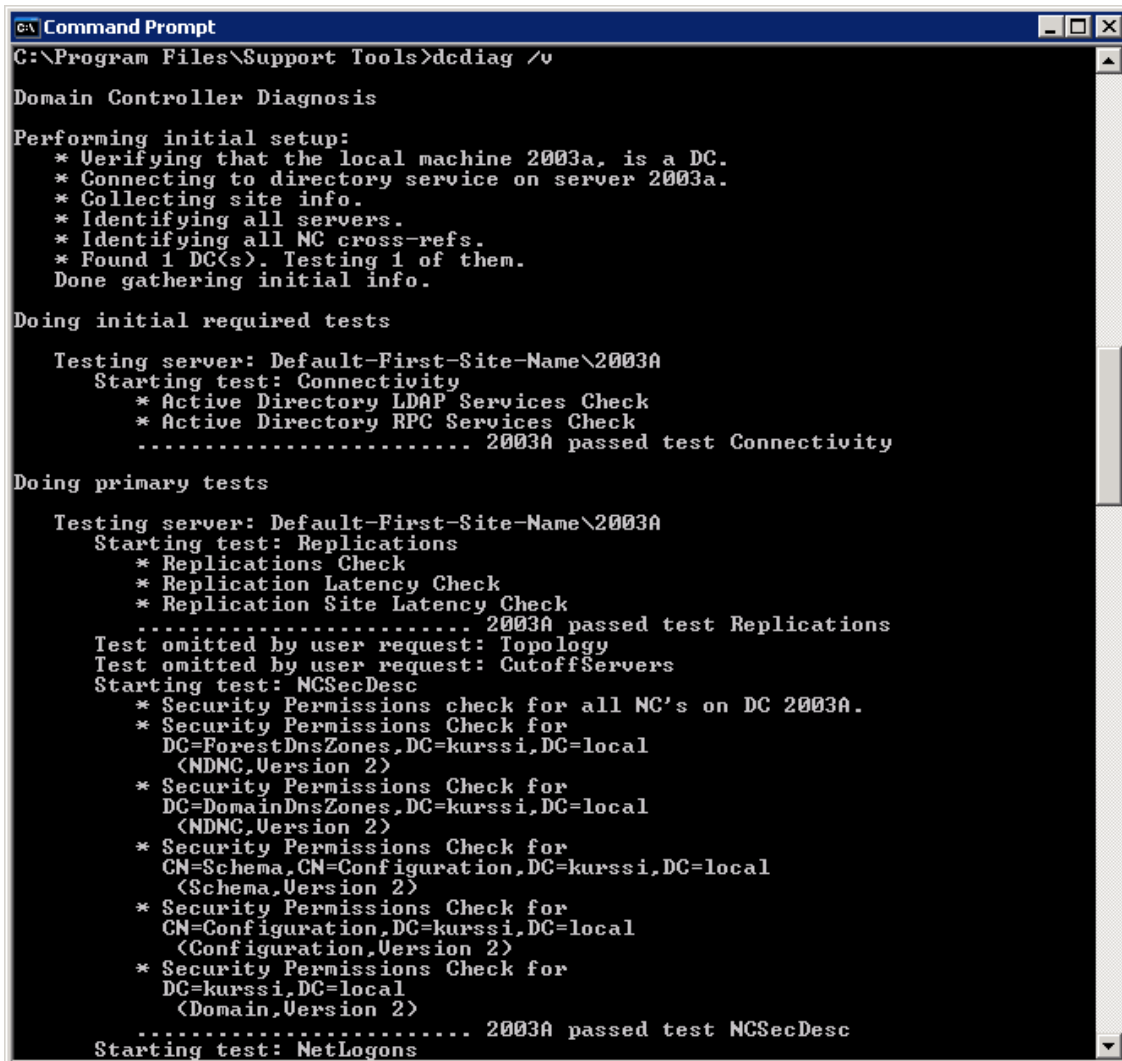
Replication monitor-ohjelman ohella toinen ”must”-ohjelma näihin terveystarkastuksiin on dcdiag-ohjelma, joka tulee support tools-ohjelmapaketin mukana. Komento on todella monipuolinen eli sisältää kymmeniä eri valitsimia.



```
C:\Program Files\Support Tools>dcdiag
Domain Controller Diagnosis
Performing initial setup:
  Done gathering initial info.
Doing initial required tests
  Testing server: Default-First-Site-Name\2003A
  Starting test: Connectivity
  ..... 2003A passed test Connectivity
Doing primary tests
  Testing server: Default-First-Site-Name\2003A
  Starting test: Replications
  ..... 2003A passed test Replications
  Starting test: NCSecDesc
  ..... 2003A passed test NCSecDesc
  Starting test: NetLogons
  ..... 2003A passed test NetLogons
  Starting test: Advertising
  ..... 2003A passed test Advertising
  Starting test: KnowsOfRoleHolders
  ..... 2003A passed test KnowsOfRoleHolders
  Starting test: RidManager
  ..... 2003A passed test RidManager
  Starting test: MachineAccount
  ..... 2003A passed test MachineAccount
  Starting test: Services
  ..... 2003A passed test Services
  Starting test: ObjectsReplicated
  ..... 2003A passed test ObjectsReplicated
  Starting test: frssysvol
  ..... 2003A passed test frssysvol
  Starting test: frsevent
  ..... 2003A passed test frsevent
  Starting test: kccevent
  ..... 2003A passed test kccevent
  Starting test: systemlog
  An Error Event occurred.  EventID: 0x00000457
  Time Generated: 09/19/2006 08:43:00
  (Event String could not be retrieved)
  An Error Event occurred.  EventID: 0x00000457
  Time Generated: 09/19/2006 08:46:13
  (Event String could not be retrieved)
  An Error Event occurred.  EventID: 0x00000457
  Time Generated: 09/19/2006 08:47:55
```

Huomaa, että komento pitää ajaa support tools-ohjelmistot sisältävässä kansiossa.

Aja komento /v – valitsimella (verbose):



```
C:\Program Files\Support Tools>dcdiag /v

Domain Controller Diagnosis

Performing initial setup:
 * Verifying that the local machine 2003a, is a DC.
 * Connecting to directory service on server 2003a.
 * Collecting site info.
 * Identifying all servers.
 * Identifying all NC cross-refs.
 * Found 1 DC(s). Testing 1 of them.
 Done gathering initial info.

Doing initial required tests

Testing server: Default-First-Site-Name\2003A
Starting test: Connectivity
 * Active Directory LDAP Services Check
 * Active Directory RPC Services Check
 ..... 2003A passed test Connectivity

Doing primary tests

Testing server: Default-First-Site-Name\2003A
Starting test: Replications
 * Replications Check
 * Replication Latency Check
 * Replication Site Latency Check
 ..... 2003A passed test Replications
Test omitted by user request: Topology
Test omitted by user request: CutoffServers
Starting test: NCSecDesc
 * Security Permissions check for all NC's on DC 2003A.
 * Security Permissions Check for
  DC=ForestDnsZones,DC=kurssi,DC=local
  (NDNC,Version 2)
 * Security Permissions Check for
  DC=DomainDnsZones,DC=kurssi,DC=local
  (NDNC,Version 2)
 * Security Permissions Check for
  CN=Schema,CN=Configuration,DC=kurssi,DC=local
  (Schema,Version 2)
 * Security Permissions Check for
  CN=Configuration,DC=kurssi,DC=local
  (Configuration,Version 2)
 * Security Permissions Check for
  DC=kurssi,DC=local
  (Domain,Version 2)
 ..... 2003A passed test NCSecDesc
Starting test: NetLogons
```

tätä ei ole niin helppo tutkia, kokeile:

```
dcdiag >dc.txt
dc.txt
```

eli tutki lokia tätä kautta!

Näet valitsimet (todella runsaasti) komennolla dcdiag /?

Kokeile vielä yksittäisenä testinä:

```
dcdiag /test:fsmocheck
sekä
dcdiag /test:fsmocheck /v
```

Kysymys:

Miten testaat pelkän dns-toiminnan mahdollisimman kattavasti dcdiag-komennolla?
Miten testaat topologian eli palvelinten väliset yhteydet?

10. Toimialueen 1. palvelimen kellonaika

Määritä ensimmäisen FSMO-roolit (mm. PDC-emulator) sisältävälle palvelimelle kellonaika. Helpoin tapa on komentokehoteessa:

```
net time /setsntp:xx.yy.xx.ww
```

- siis palvelimen oma IP-osoite – jatkossa EventVieweriin ei tule w32time-herjoja

Suosittelava tapa:

```
net time /setsntp:ulkoinen aikapalvelin
```

-sekä palomuriin sallitaan liikenne porttiin UDP/123 ulospäin meneväksi portiksi

11. Tarkista tietoturvapäivitykset palvelimelta

Katso IE – Tools | WindowsUpdate ettei ole tullut mitään uutta päivitettävää – muista myös Win + R: wupdmgr

12. Salli kahden hallinnoitsijan samanaikainen etätyöpöytäyhteys

Aseta päälle eli salli Remote Desktop: Windows + Pause – Remote ja rasti alempaan kohtaan.

Asenna lisäohjelmia:

Kaikkea mielenkiintoista:

<http://www.microsoft.com/windowsserver2003/downloads/featurepacks/default.mspx>

http://www.window networking.com/articles_tutorials/Using-Remote-Assistance-Windows-Firewall-Enabled.html

- hyvä ohje etätuen käyttämisestä AD-ympäristössä