UPGRADE ACTIVE DIRECTORY SUSTAVA 2003 SP2 x86 NA 2012 x64

Ratko Žižek, MCSE-MCITP

1. UVOD

Nećemo sada o razlozima, ali nema dvojbe da je Active Directory izrazito popularan imenični servis odn. alat za centralizirano administriranje digitalnih identiteta – korisnika, računala i servisa. Budući da se u osnovi radi o jednom od servisa Windows serverskih edicija, svaka nova Windows Server distribucija donosi i unaprijeđenu inačicu Active Directory servisa. Pa je u redu da mi, sistemci, tada zasučemo rukave i osuvremenimo naš postojeći Active Directory sustav, jel'te. Ako uspijemo u naumu, bit ćemo na dobitku i mi informatičari i korisnici. Ako, pak, taj naš upgrade završi krahom sustava, jadna nam majka jer prestat će raditi sve što o njemu ovisi...

Zbog svega gore spomenutog nije neobično što su se na Internetu počeli pojavljivati naputci i „naputci" za upgrade prethodnih verzija Active Directorya (dalje: **AD**) na verziju Windows Server 2012 čak i prije nego što je Microsoft službeno plasirao taj OS na tržište. Sada, kad je Windows Server 2012 u prodaji, tih savjeta & uputa ima napretek. Ali svima je zajedničko jedno: bave se upgradeom 64-bitne verzije AD-a (2003, 2008) na 64-bitnu verziju Windows 2012 AD-a. A vaš autor je, „srećković", angažiran da odradi upgrade Windows 2003 **32**-bitne verzije AD-a na Windows 2012 64-bitnu. Dosta sam testirao, puno grickao nokte tijekom upgradea produkcijskog foresta... i sve je dobro završilo.

Njuškanjem po svakojakim forumima uočio sam da su 32-bitne instalacije AD-a još uvijek brojne pa odlučih izraditi podsjetnik za sve vas koji ćete možda doći u situaciju poput moje. Ističem, riječ je o podsjetniku, smjernicama, a ne o formuli koja garantira uspjeh, znači, **u konačnici ipak sve ovisi o vašoj upućenosti u AD problematiku i poznavanju najnovijeg Microsoftovog serverskog OS-a**.

2. UPGRADE 32-BITNOG AD-a

AD sustav kojega sam upgraedirao opsluživala su tri Windows 2003 SP2 32-bitna Domain Controllera, dva na centralnoj lokaciji a jedan isturen u drugi grad. Forest je bio (i ostao) jednodomenski, izvorno je radio u Windows 2003 native modu. Svi su DC-evi bili domenski DNS serveri sa Active Directory integrated zonama pa je ta časna uloga dodijeljena i novim DC-ima.

1. Rabiti account koji je u domenskim Enterprise i Schema Admins grupama; provjeriti da je Enterprise Admins zaista član lokalne grupe Builtin/Administrators za sve DC-e.

2. Windows 2003 SP2 Domain Controllere (dalje: DC-e) opremiti sa Support Tools i Admin Tools alatima za SP2; primijeniti sve relevantne zakrpe.

3. Ako već nisu, svim DC-ima dodijeliti ulogu Global Catalog.

4. Ukoliko su FSMO uloge razdijeljene po DC-ima, sve ih izmjestiti na onaj DC koji već obnaša ulogu PDC emulatora (kasnije će nam baš taj DC biti direktan replikacijski partner prvom Windows 2012 DC-u).

5. Dijagnostičkim alatima poput dcdiag, replmon, netdiag... uvjeriti se da ispravno funkcionira svaki DC pojedinačno i AD sustav kao cjelina; možemo uključiti i samodijagnostiku AD-a kroz Registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics

6. Instalirati Windows 2012 server, obaviti osnovnu konfiguraciju; možemo instalirati i DNS servis (ja nisam jer sam se uvjerio da AD DS setup to odlično odradi).

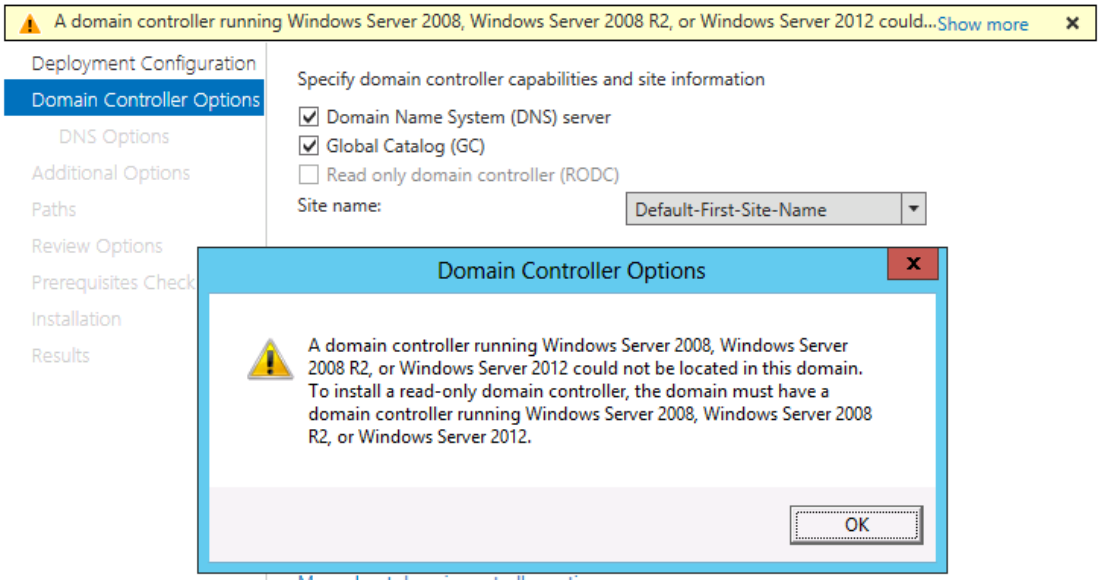
7. Kao primarni DNS 2012-ici postaviti IP adresu FSMO mastera; uključiti opciju za dinamičko prijavljivanje u domenski DNS i učlaniti taj server u domenu.

   Nastojte da ovaj novi server, budući DC, ima **maksimalno pouzdanu konekciju** sa FSMO masterom jer, tijekom promocije u DC, Windows 2012 u većoj ili manjoj mjeri modificira sve particije AD-a a treba nam i za degradiranje FSMO mastera.

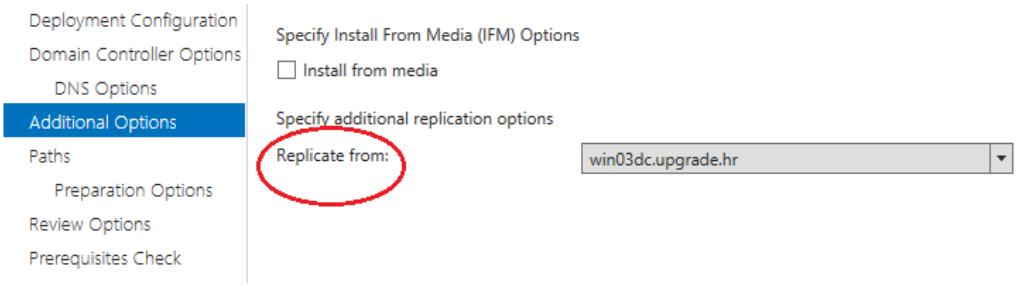
8. Krećemo sa instalacijom AD DS role na Windows Server 2012. Skrećem pozornost samo na ključne, potencijalno zbunjujuće situacije!

   a) Add Roles and Features – odabrati AD DS servis te prihvatiti prijedlog da se instaliraju prateće komponente poput Group Policy i admin alata. Nakon ovoga pokrećemo proceduru promocije servera u DC/DNS.

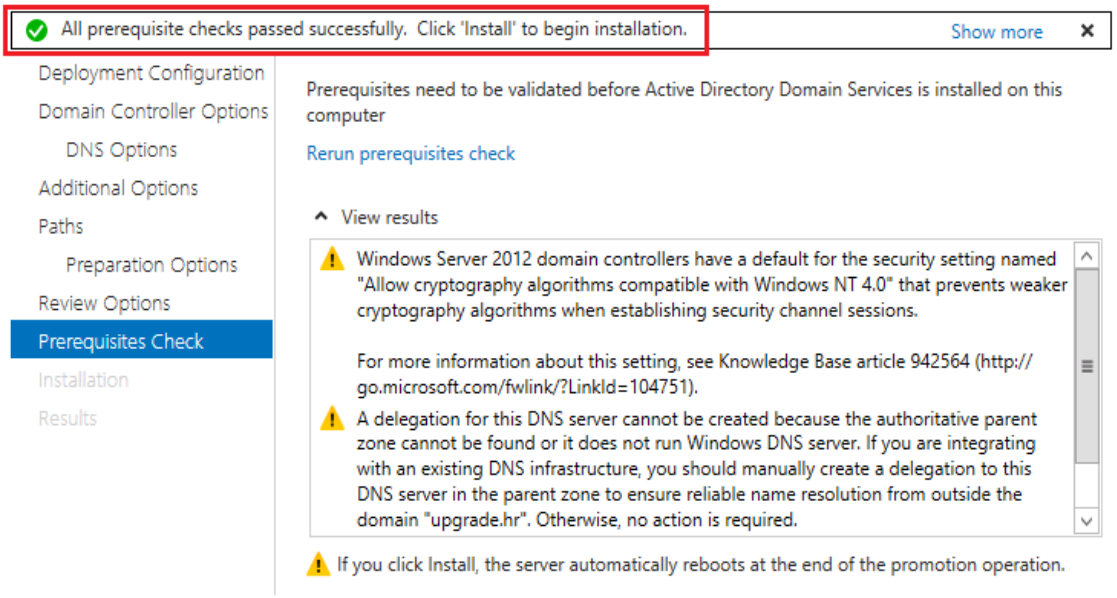
   b) Niže upozorenje odnosi se isključivo na Read-only Domain Controller, dakle, za nas je to nebitno. Uočite da smo uključili DNS i GC opcije.



c) Kad dođemo do koraka Additional options > Specify additional replicate options **odabrat ćemo FSMO mastera kao replikacijskog partnera**.

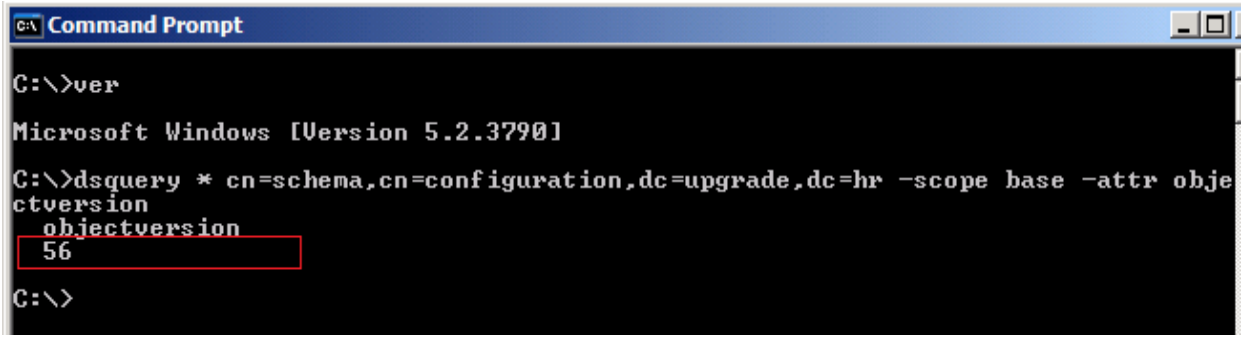


d) Nastavljamo s procedurom... i u koraku Prerequisities Check dočekat će nas svakojaka uznemirujuća upozorenja. Ipak, ako u zaglavlju tog izvještaja piše ovo što je označeno na nižoj slici, u stvari je sve OK i možemo dalje.

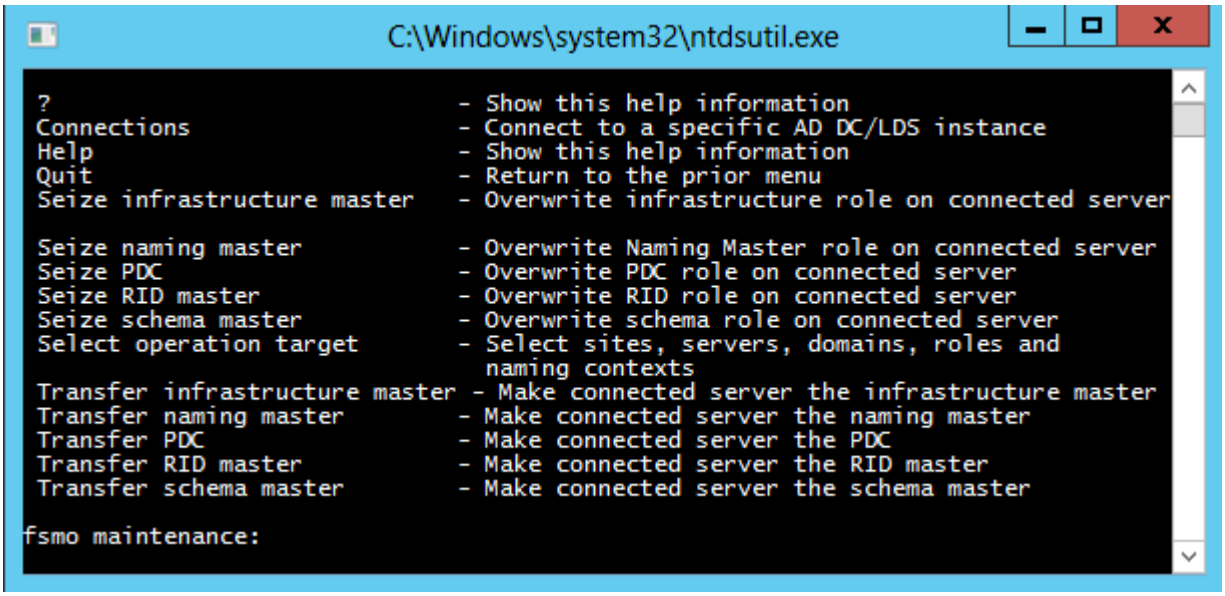


9. Nakon podizanja DC funkcionalnosti na 2012-ici, koji se odmah oglašava kao GC, postaviti joj sebe za primarni DNS a FSMO mastera kao sekundarni; isto tako postupiti na FSMO masteru – samom sebi je primarni DNS a novi DC mu je sekundarni.

10. Sada ćemo svojim omiljenim CMD i GUI alatima provjeriti stanje u AD sustavu, i to sa svakog od dva ključna DC-a (novi i FSMO master): imaju li isti pogled na topologiju AD-a, repliciraju li se, resolviraju li ispravno SRV i prateće DNS zapise... i sl. Na nižoj slici Windows 2003 DC poručuje da radi s Windows 2012 AD schemom. Cool! :-)



11. Prebacujemo FSMO role sa starog na novi DC, najbolje je rabiti **ntdsutil** alat. Pokrećemo ga **na 2012-ici**, radimo **transfer** i to baš redom prikazanim na slici.



* **Ne zaboravite** novog FSMO mastera usmjeriti na autoritativni time source, također, ako je domenski DNS ulančan u korporativnu DNS hijerarhiju, što je uobičajeno rješenje, trebamo na novom DC-u podesiti forwarding a na gornjem DNS-u ažurirati delegaciju za DNS domenu koja je pod kontrolom DC-eva.

12. Sada nam predstoji skidanje DC role sa Win 2003 DC-a: obavezno starom DC-u postaviti novi 2012 DC kao primarni DNS, potom zadajemo samo **dcpromo**, dakle, **ne** rabimo opciju /forceremoval jer demoting sa tom opcijom ostavlja u AD-u puno referenci na taj stari DC koje onda moramo ručno uklanjati.

*

Gornjim koracima učinili smo najvažnije: podigli smo Windows 2003 32-bitni forest na Windows 2012 64-bitni i omogućili njegovo daljnje nesmetano funkcioniranje. Mudro ćemo postupiti ako što prije dignemo još jedan Windows 2012 DC, potom situaciji primjerenom dinamikom ukidamo Windows 2003 DC-e.

<kraj>