

Windows Server Core: Može i bez PowerShella!

pet, 2018-06-15 07:32 - Ratko Žižek



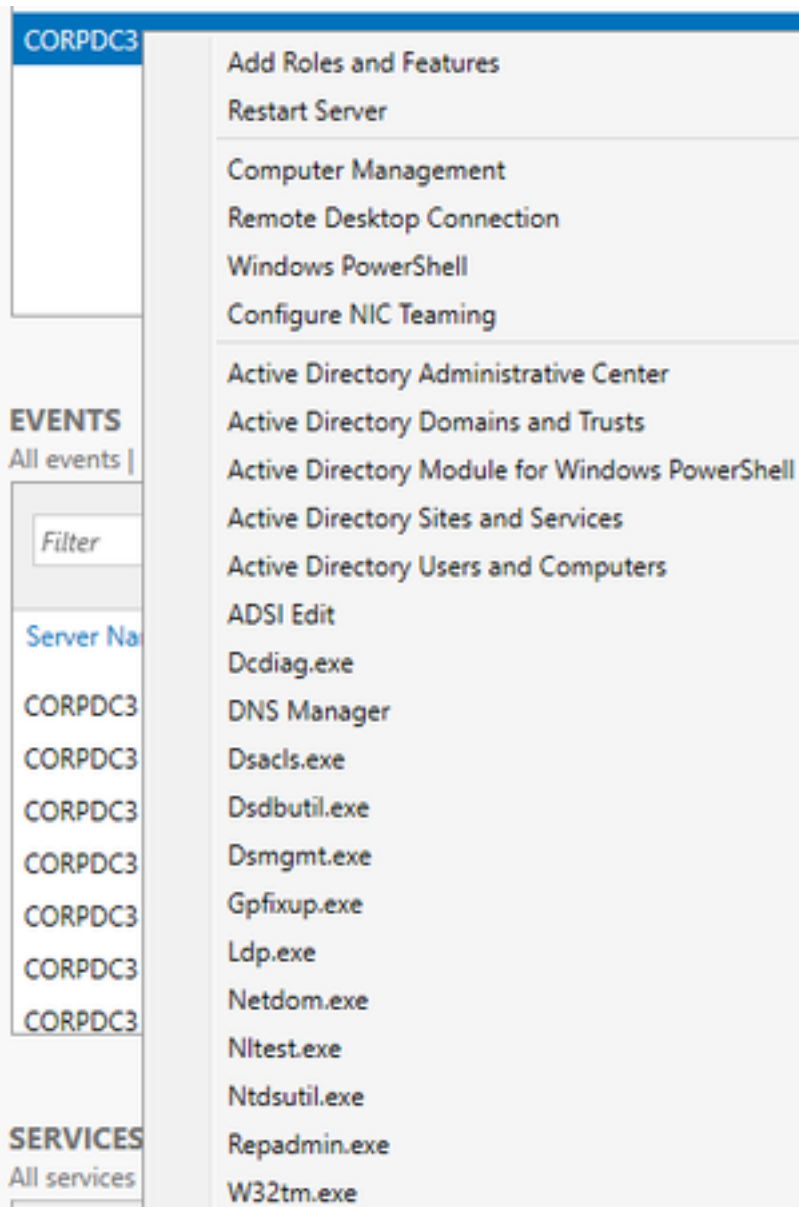
Nekolicina poznanika, nadam se i prijatelja, prati moje objave na ovom portalu. Pa se, nastavno na članak o skrivanju objekata u AD-u, pred neki dan razvilo živahno *on-line* čavrljanje na temu AD-a i njegove antiintruder zaštite, sve "uzduž i poprijeko", kako to biva u neslužbenoj komunikaciji. U jednom trenutku sam, iz konteksta poruka, shvatio da moji kolege, doduše, svašta znaju o toj temi ali jednostavno ignoriraju Core serversku ediciju kao osnovicu za Domain Controller (dalje: DC) ulogu i kao jedan od najvažnijih zaloga sigurnosti AD instalacija. Na moj stav da bi trebalo preferirati Core odmah su počele stizati poruke s bljakastim smajlicima uz riječ PowerShell... pa odaslah prijetnju s bijesnim smajlicem: "Ahaaa, vi (cenzurirano), o ovome će se čitati na portalu!" Eto, ne možete reći da nisam od riječi. :o)

S PowerShellom se snalazim iako, ako ćemo iskreno, naklonjeniji sam Bash i Cmd interpreterima. Nećemo sada o razlozima, sporedno je u odnosu na ovo što slijedi: Windows Core kao Domain Controller možemo instalirati i nadalje ga administrirati rabeći GUI alate, uz sasvim sporadična i kratkotrajna druženja s PowerShell ili Cmd promptom! A što se tiče Corea kao edicije Windows OS-a, prednosti su toliko očite i poznate da na to ne treba trošiti riječi. Svima koji još uvijek zaziru od Domain Controllera na Core serveru, preporučam ovaj model: uvedite ga u produkciju - dakako, nakon razdoblja testiranja i privikavanja - uz postojeće GUI DC-eve. Kad ovladate njime - što će se brzo odvijati, vidjet ćete iz nižega zašto - zamijenite GUI DC-eve Core inačicama. Imat ćete manje briga a još ćete se moći hvaliti da ste prepolovili zauzeće poslužiteljskih resursa!

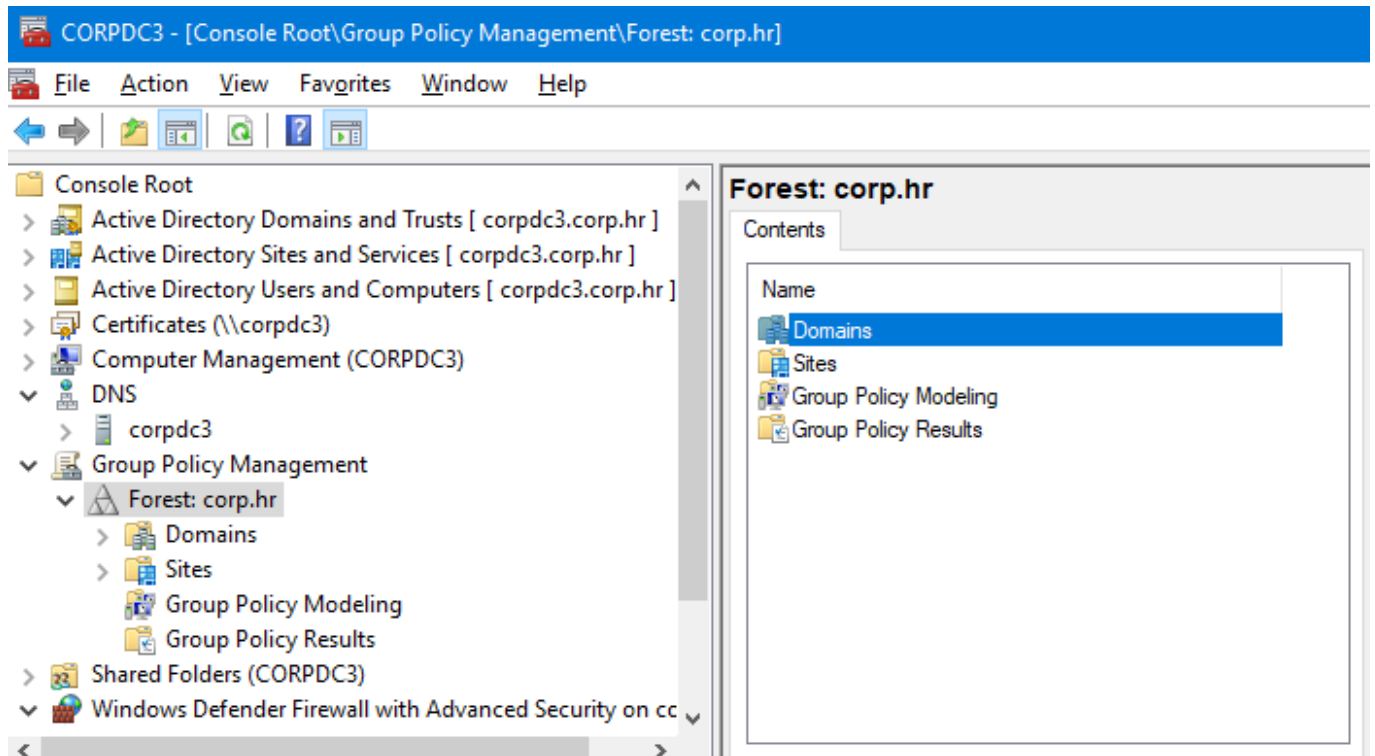
U "pokaznoj vježbi" što slijedi, polazimo od ovih pretpostavki:

- Izričajem se obraćamo kolegama kojima Active Directory nije nepoznanica;
- dva GUI Windows Server 2016 DC-a (ujedno drže interni DNS ogranak), su u poslužiteljskom segmentu korporativne mreže, želimo im dodati jedan Core 2016 DC;
- admin stanica je Windows 10, nalazi se u klijentskoj mreži, za njom sjedi lik učlanjen u Enterprise Admins domensku grupu, rabit će GUI alate.

A koji su to GUI alati? Ma ima ih i previše! Kad na stanicu instaliramo Remote Server Administration Tools (RSAT), dobit ćemo, pored namjenskih PowerShell/Cmd naredbi, i tucet MMC konzola za "šefovanje" na Domain Controllerima, i šire, na objektima AD sustava. Jedna od tih konzola je tipa "upravljačka ploča" (dashboard), imenovana kao Server Manager. Dakle, SrvManom se spojimo na Core server - na nižoj slici to je corpd3 - potom, nakon desnog klika na tom serveru, biramo potrebnu naredbu. Neke naredbe pokreću GUI alate a neke su komandnolinijske. Uočite da SrvMan prikazuje razne podatke o stanju servera, nudeći ujedno dodatnih par naredbi s grafičkim sučeljem.



Kad smo već instalirali RSAT, na admin stanici možemo si sami složiti "server manager" po svom ukusu. Naredba Run > mmc /a, potom kroz Add/Remove snap-in odaberemo sve namjenske konzole koje želimo imati objedinjene u općoj konzoli. Niža slika prikazuje moju kolekciju konzola za administriranje Core DC-a corpdc3.



Važan detalj! Da bi nas SrvMan i MMC konzole vjerno služile, moramo na vatrozidu Core DC-a otvoriti određene portove. Najjednostavnije ćemo to odraditi tako da se spojimo Remote Desktopom na Core i zadamo par nižih naredbi. Prva je ova:

netsh advfirewall firewall set rule group="Windows Firewall Remote Management" new enable=yes

Nakon te naredbe možemo se s admin stanice spojiti na Core konzolom Windows Defender Firewall pa konfigurirati Coreov vatrozid, ali jednostavnije nam je prizvati izvršenu naredbu u naredbeni redak, sukcesivno ju preoblikovati u niže izložene naredbe i tako taj dio brzopotezno riješiti. Iz opisa grupa na koje djelujemo jasno je o čemu se radi.

a) **netsh advfirewall firewall set rule group="Remote Service Management" new enable=yes**

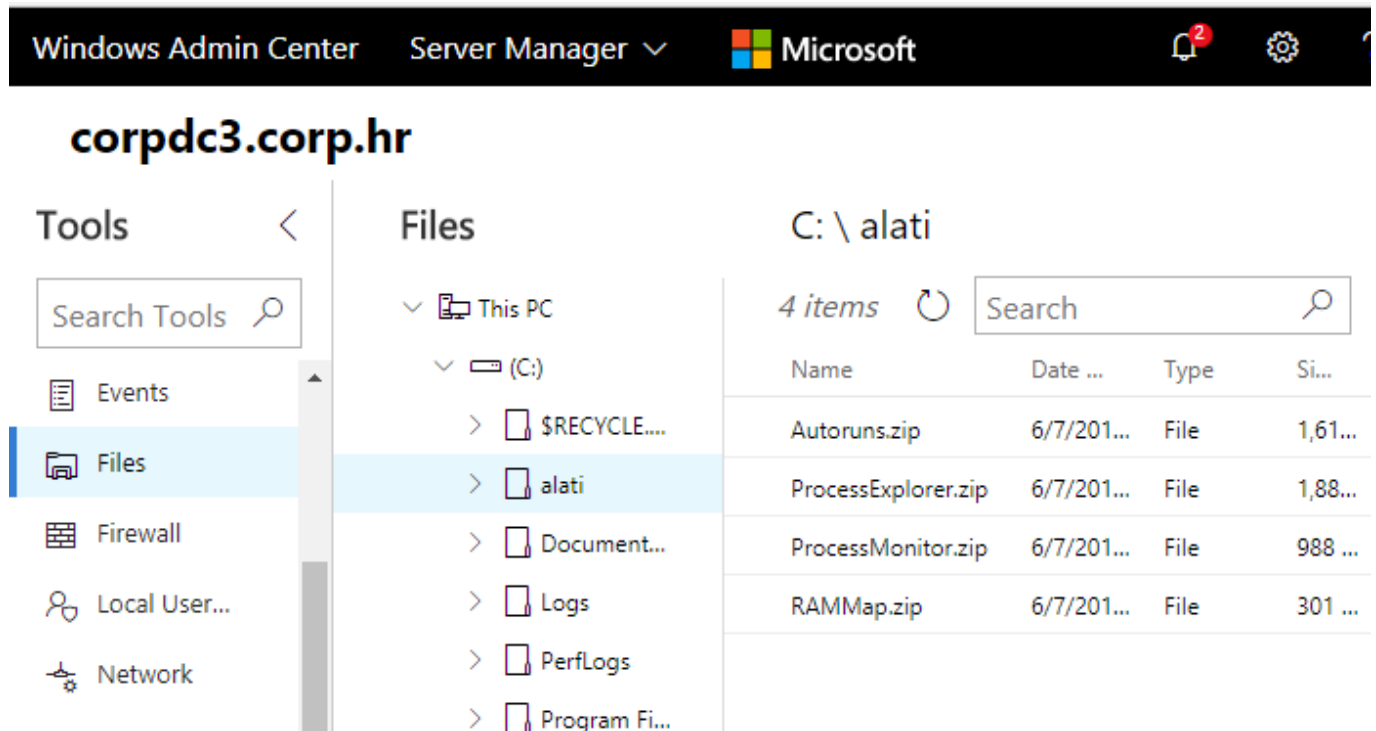
b) **netsh advfirewall firewall set rule group="Remote Event Log Management" new enable=yes**

c) **netsh advfirewall firewall set rule group="Remote Scheduled Tasks Management" new enable=yes**

d) **netsh advfirewall firewall set rule group="Remote Volume Management" new enable=yes**

Još jedan važan-i-sve-važniji GUI alat je Windows Admin Centar (WAC). Do nedavno je bio poznat kao Honolulu, obradili smo ga na adresi <https://sysportal.carnet.hr/node/1771> [1]. Microsoft ga ubrzano razvija, nije finaliziran no zreo je za produkcijski rad. Ako već raspoložemo sa SrvManom i MMC konzolama, za poslove koje ćemo odraditi u ovom članku WAC nam nije stvarno potreban ali isplati se upogoniti ga jer Microsoft njime želi zamijeniti postojeće administrativne alate. Za WAC ne moramo na Coreu ništa podešavati, *listener* servisa WinRM željno očekuje konekcije na TCP 5985. To je, kako smo u spomenutom članku objasnili, jedna od velikih prednosti WAC-a. Glede niže slike: s admin stanice kopiramo neke GUI alate na corpdc3 Core server, 7-zip je već na njemu. Kopiranje smo, doduše, mogli brže odraditi tako da se Windows Explorerom spojimo na Coreov administrativni

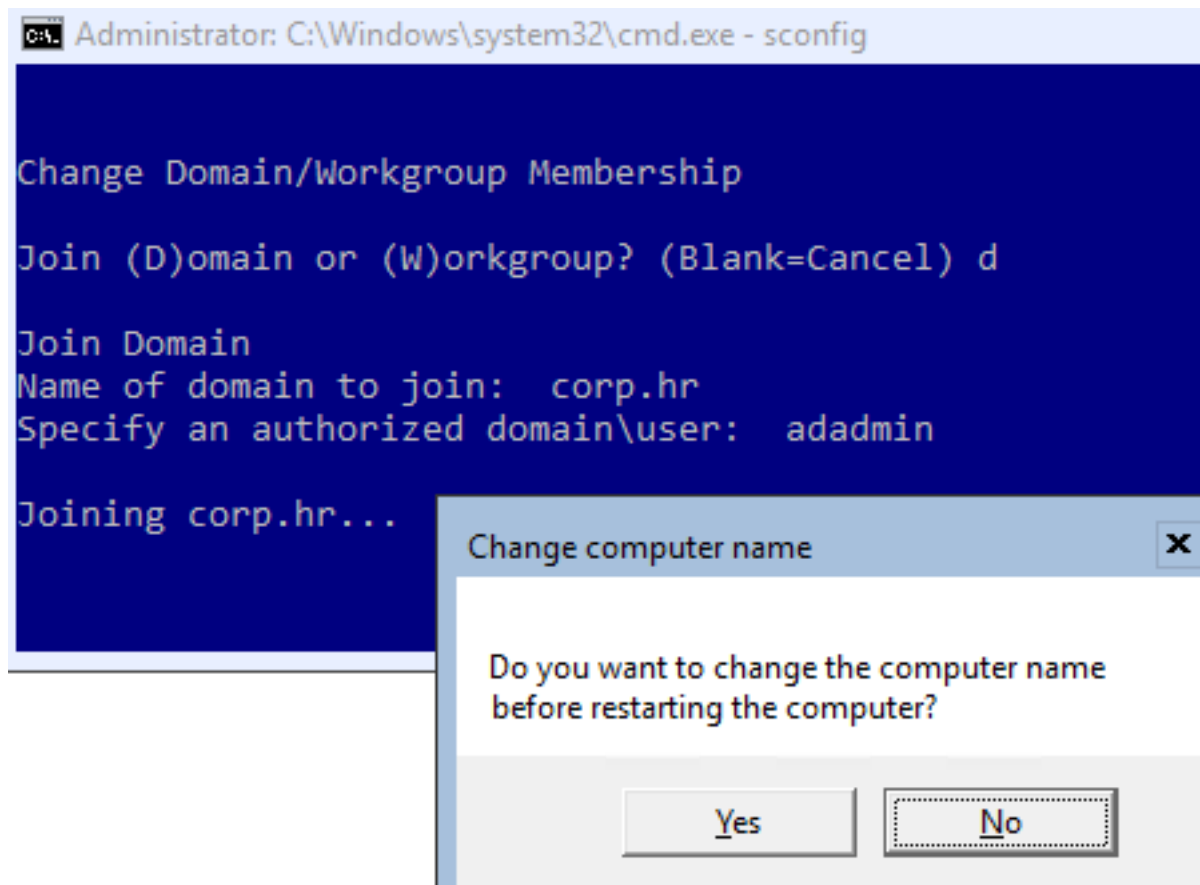
share, tipično c\$, ali ovo je novotarija pa je "fora"... :o).



Na kraju ovog pregleda raspoloživih alata, valja spomenuti da nam i sam GUI DC može glumiti admin stanicu, u njegov SrvMan možemo učlaniti Core server, ili si na njemu složimo kolekciju MMC konzola usmjerenih ka Core serveru.

Sad kad smo se oboržali GUI alatima, učlanit ćemo Core server u corp.hr Active Directory i pretvoriti ga u Domain Controller s DNS-om.

1. Nakon instalacije, inicijalno podešavanje Core servera - od postavljanja IP parametara i primjene zakrpi preko uključivanja Remote Desktop pristupa do učlanjenja u domenu - odradit ćemo njegovim semigrafičkim alatom **sconfig**. Na nižoj slici vidimo kako tijekom učlanjenja u domenu sconfig skripta omogućuje preimenovanje servera. Preimenovali ga mi ili ne, nakon restarta Core se sam prijavljuje u domenski DNS (jasno, ako je u ovom omogućen Dynamic Update), znači, postaje dostupan po imenu i DC-evima i admin stanicu.



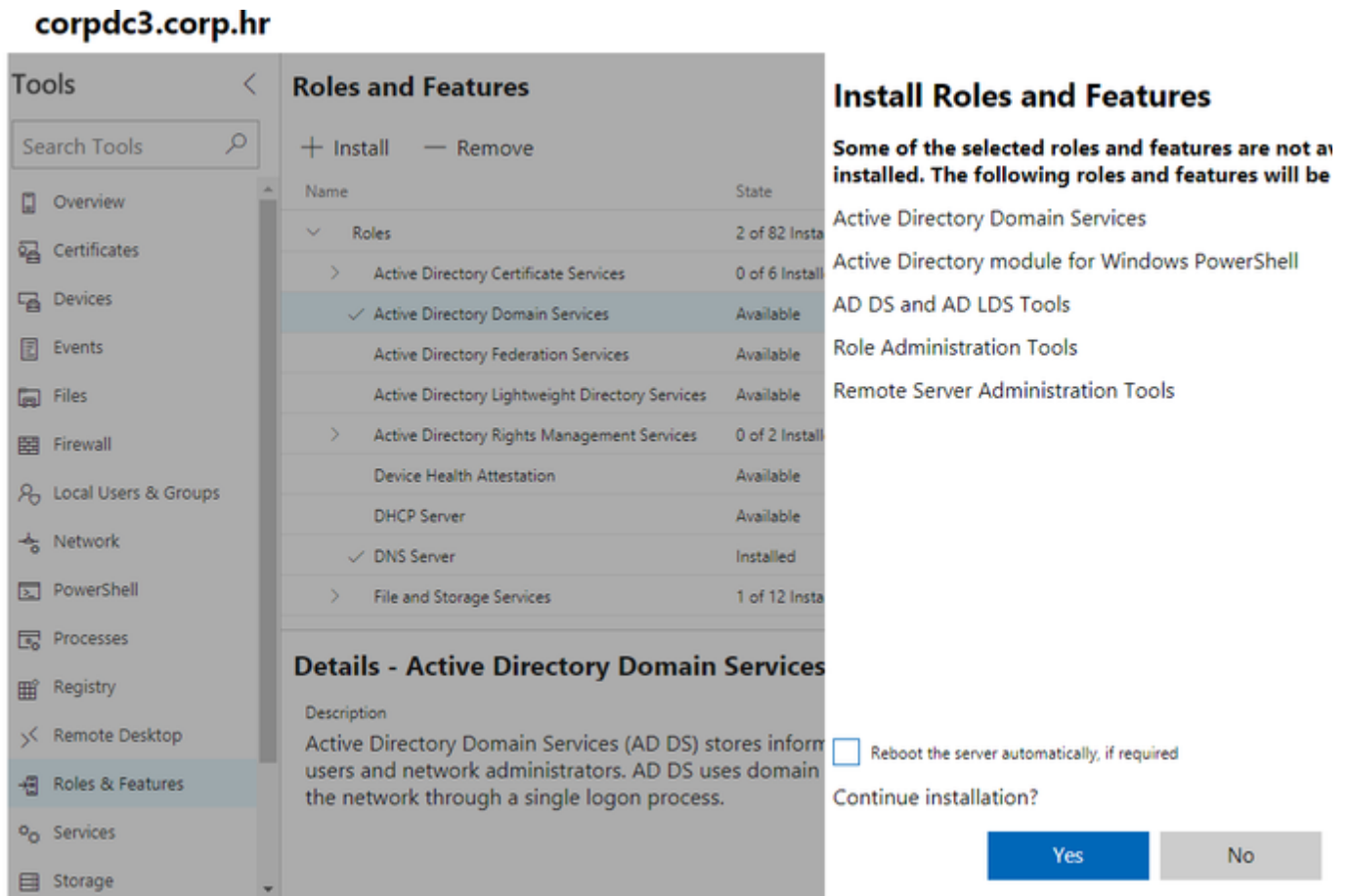
2. Na Coreu otvaramo portove za uporabu RSAT konzola, kako je maloprije opisano.

3. Iz Server Managera (izbornik Manage, naredba Add Roles and Features) ili WAC-a (u lijevom stupcu klik na Roles & Features, označimo stavku DNS pa klik na gumbu Install) instaliramo rolu DNS. Mudro je odmah pod Features odabrati Telnet klijenta, znamo zašto.

4. Slijedi kratko sređivanje DNS-a:

- Na glavnom DC-u postavimo Core kao još jedan domenski DNS (kartica Name Servers) i pobrinemo se da je na kartici Zone Transfers uključena odgovarajuća opcija za prijenos zone;
- iskoristimo DNS konzolu iz zbirke konzola koju smo si priredili za Core server kako bismo u konfiguraciji njegovog DNS-a, kroz karticu Root Hints, izbrisali sve *root* servere globalne DNS hijerarhije.

5. Kao u trećem koraku, odaberemo ili SrvMan ili WAC da bismo na Core instalirali Domain Controller rolu. U ovom slučaju, što se vidi na nižoj slici, rabimo WAC, znači, u prikazanoj situaciji samo klik na gumbu Yes.



6. Ovaj korak, samo zato što je kritičan, odradit ćemo direktno na Coreu. RDP-om se spojimo na server i zadamo jednu-jedinu superjednostavnu Powershell naredbu: **install-addsdomaincontroller**. Iskočit će par upozorenja, ali ako se radi o porukama poput niže prikazanih, to su obavijesti, nisu greške.... uglavnom, nakon inicijalne sinkronizacije s kolegama DC-ima, Core se sam restarta.

```

C:\> Administrator: C:\Windows\system32\cmd.exe - powershell
Confirm SafeModeAdministratorPassword: *****

Install-ADDSDomainController
    Determining replication source DC
    Validating environment and user input
    All tests completed successfully
    [ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
    Installing new domain controller
    Replicating CN=Configuration,DC=corp,DC=hr: received 1000

WARNING: A delegation for this DNS server cannot be created because
the parent zone does not run Windows DNS server. If you are integrating with an existing
DNS server, you must create a delegation to this DNS server in the parent zone to ensure
"corp.hr". Otherwise, no action is required.

WARNING: Windows Server 2016 domain controllers have a default
setting for "Prevent weaker channel sessions" that is incompatible with
"Prevent weaker channel sessions" algorithms compatible with Windows NT 4.0" that prevents weaker
channel sessions.

For more information about this setting, see Knowledge Base article
KB2993586 (http://go.microsoft.com/fwlink/?LinkId=104751).

WARNING: A delegation for this DNS server cannot be created because
the parent zone does not run Windows DNS server. If you are integrating with an existing
DNS server, you must create a delegation to this DNS server in the parent zone to ensure
"corp.hr". Otherwise, no action is required.
    
```

7. Iz sučelja Sconfig naredbe, ili WAC-a, redefiniramo DNS postavke na mrežnoj kartici Core servera tako da mu kao primarni DNS postavimo 127.0.0.1 a sekundarni su mu drugi DC-evi. Ovima, pak, dodamo Core DC kao sekundarni.

8. Kako se Core DC uklopio u domenu lako provjerimo na razne načine, u ovoj situaciji najbolje je na Coreu zadati naredbu:

dcdiag /c /v /f:dcdiagini.txt & notepad dcdiagini.txt

Primjećujete da ćemo izvještaj dcdiag naredbe čitati u GUI alatu Notepad. Core je opremljen s kojih desetak GUI programčića, spomenimo uistinu korisne **taskmgr** i **msinfo32**.

Znadete li da ove godine Windows Server Core edicija navršava jubilarnih 10 godina postojanja? Da, da, pravi je to momak postao, utoliko, ako već radimo s Windows serverima, vrijeme je da ga prihvatimo kao pouzdanog i susretljivog suradnika.

Vijesti: [Windows](#) [2]
Kuharice: [Windows](#) [3]

Kategorije: [Operacijski sustavi](#) [4]**Vote:** 0

No votes yet

story_tag: [windows_core](#) [5][powershell](#) [6][active_directory](#) [7][domain_controller](#) [8]**Source URL:** <https://sysportal.carnet.hr./node/1813>**Links**[1] <https://sysportal.carnet.hr/node/1771>[2] <https://sysportal.carnet.hr./taxonomy/term/12>[3] <https://sysportal.carnet.hr./taxonomy/term/18>[4] <https://sysportal.carnet.hr./taxonomy/term/26>[5] <https://sysportal.carnet.hr./taxonomy/term/249>[6] <https://sysportal.carnet.hr./taxonomy/term/250>[7] <https://sysportal.carnet.hr./taxonomy/term/154>[8] <https://sysportal.carnet.hr./taxonomy/term/251>